GUIA DO USUÁRIO

Bitdefender CONSUMER SOLUTIONS

Security for Creators

Bitdefender Total Security

Guia do usuário

Data de publicação 27/07/2023

Notícia legal

Bitdefender

Índice

SOBRE ESTE GUIA

Objetivo e Público-Alvo

Este guia fornece assistência para a configuração e o uso dos produtos incluídos em sua assinatura, personalizados especificamente para criadores de conteúdo como você: Bitdefender Security for Creators.

Você pode descobrir como configurar o Bitdefender em diferentes dispositivos para mantê-los protegidos de todos os tipos de ameaças e, o mais importante, descobrir como manter sua conta do YouTube protegida contra ataques cibernéticos diretos e tentativas de hacking.

Como usar este guia

Este guia está organizado em torno dos quatro produtos incluídos no pacote **Bitdefender Security for Creators**:

- Segurança para criadores (página 4)
  Descubra como usar o Security for Creators para melhor proteger e monitorar seu canal do YouTube, evitando qualquer possibilidade de sua conta ser invadida e seu conteúdo sabotado.
- Email Protection
  Saiba como proteger melhor sua caixa de entrada de e-mail contra spam, e-mails maliciosos e tentativas de phishing usando a Proteção de E-mail.
- Segurança Total para PC (página 16)
  Saiba como usar o produto em seus PCs e laptops com Windows.
- Antivírus para Mac (página 156)
  Saiba como usar o produto em seus Macs.
- Segurança móvel para Android (página 189)
  Saiba como usar o produto em seus smartphones e tablets com Android.
- Segurança móvel para iOS (página 222)
  Saiba como usar o produto em seus smartphones e tablets com iOS.
- VPN (página 237)

Saiba como ocultar sua identidade on-line usando o Bitdefender VPN em qualquer um dos seus dispositivos.

❍ Conseguindo ajuda (página 261)
Descubra onde procurar ajuda se algo inesperado surgir.

Convenções utilizadas neste guia

Convenções Tipográficas

São utilizados diversos estilos de texto neste manual para uma maior facilidade de leitura. O seu aspecto e significado são apresentados na tabela abaixo.

Aparência	Descrição
sample syntax	As amostras de sintaxe são impressas com monospaced personagens.
https://www.bitdefender.com	A hiperligação URL aponta para uma localização externa em servidores http ou ftp.
documentation@bitdefender.com	Endereços de email são inseridos no texto para contactar a solicitar mais informação.
Sobre este Guia (página 1)	Esta é uma hiperligação interna que o leva para uma localização dentro do documento.
filename	Arquivos e diretórios são impressos usando monospaced Fonte.
opção	Todas as opções de produtos são impressas usando **audacioso** personagens.
palavra-chave	Palavras-chave ou frases importantes são destacadas usando **audacioso** personagens.

Avisos

Os avisos estão em notas internas do texto, com marcação gráfica, que chamam a sua atenção para informações adicionais relacionadas ao parágrafo atual.

Observação

A nota é apenas uma observação curta. Apesar de a poder omitir, a nota providencia-lhe informação valiosa, tal como uma característica específica ou um link para um determinado tópico.

Importante

Este ponto requer a sua atenção e não é recomendável ignorá-lo. Normalmente, providencia-lhe informação bastante importante.

Aviso

Trata-se de informação critica que deve de tratar com cuidados redobrados. Nada de negativo acontecerá se você seguir as indicações. Deve de lê-lo e compreendê-lo, porque descreve algo extremamente arriscado.

Pedido de Comentários

Convidamo-lo a ajudar-nos a melhorar este manual. Nós verificamos e testamos toda a informação com o máximo dos cuidados. Por favor escreva-nos acerca de quaisquer falhas que descubra neste manual ou a forma como acha que o mesmo poderia ser melhorado, de forma a ajudar-nos a dar-lhe a si a melhor documentação possível.

Informe-nos enviando um e-mail para documentation@bitdefender.com. Escreva todos os seus e-mails relacionados à documentação em inglês para que possamos processá-los com eficiência.

1. SEGURANÇA PARA CRIADORES

1.1. O que é o Bitdefender Security for Creators

O Bitdefender Security for Creators é a solução de cibersegurança da Bitdefender projetada especificamente para proteger todos os criadores de conteúdo, independentemente do conteúdo do canal e do número de assinantes. Ele inclui:

- **Proteção do canal do YouTube:** monitora seu canal do YouTube 24 horas por dia, 7 dias por semana, em busca de tentativas de invasão de conta e fornece um guia fácil de recuperação passo a passo caso sua conta seja invadida.
- **Proteção do dispositivo:** o aplicativo de segurança Bitdefender protege todos os seus dispositivos, protege suas credenciais de login e o uso público de Wi-Fi, sinaliza e-mails de patrocinadores falsos e muito mais.

> **Atenção**
> Atualmente, o Security for Creators monitora e protege apenas as contas do YouTube, mas estamos trabalhando ativamente para expandir nossa cobertura para todas as principais plataformas usadas pelos criadores de conteúdo atualmente.

Todos os dias, os canais do YouTube são invadidos para hospedar transmissões ao vivo falsas, promover golpes, como sorteios falsos de criptomoedas ou exigir resgate. O Bitdefender Security for Creators é tudo o que os criadores de conteúdo precisam para manter sua conta do YouTube segura. Ele ajuda na recuperação rápida de contas roubadas caso elas sejam invadidas e notifica o usuário sobre todas as alterações suspeitas feitas no canal, como a exclusão de vários vídeos em um curto espaço de tempo e modificações rápidas nas fotos do perfil e do banner, descrições e outros componentes de um canal do YouTube, comportamentos típicos de uma situação de “conta roubada”.

1.2. Configurar o Security for Creators

Para começar a configurar sua assinatura do Bitdefender Security for Creators, primeiro você precisará ativar o produto para iniciar o processo:

- **Ative a solução:** imediatamente após fazer a compra, você deve receber um e-mail em sua caixa de entrada. Siga as instruções no e-mail de confirmação para ativar sua assinatura do Bitdefender Security for Creators.

Feito isso, é hora de configurar seu plano Bitdefender:

1. Na tela confirmando que sua assinatura foi ativada, clique no botão **Começar** para iniciar a configuração.
   Como alternativa, se você saiu dessa janela, clique em **Security for Creators** no menu à esquerda da sua conta Bitdefender.
2. Clique no botão **Vamos começar** para passar por um rápido processo de configuração.
3. Conecte seu canal do YouTube:
   a. Clicando no botão **Fazer login com o Google**.
   b. Use a conta do Google vinculada ao seu canal do YouTube. Digite sua senha e verifique seu número de telefone, se solicitado, depois clique em **Próximo**.
   c. Clique em **Continuar** para aprovar as permissões necessárias e permitir que o Bitdefender proteja seu canal do YouTube.
4. Proteja seus dispositivos. Baixe e instale o aplicativo Bitdefender para impedir quaisquer ameaças às quais seu dispositivo possa estar exposto.
   a. Clique no botão **Download**.
   b. Siga as instruções na tela para instalar o aplicativo Bitdefender em seu dispositivo.
   c. Depois de instalado, clique em **Próximo** para continuar.
5. **Conclua a configuração:** clique no botão **Pular** para o painel abrir o painel geral do Bitdefender Central.

O processo de integração está concluído!

1.3. Recursos e Funcionalidades

Você pode encontrar o painel Security for Creators no menu à esquerda da sua conta Bitdefender.

A partir daqui, você pode proteger e recuperar facilmente seu canal do YouTube, gerenciar o acesso da equipe e monitorar as atividades, garantindo um ambiente mais seguro e produtivo para seu trabalho criativo. Abaixo, detalhamos os recursos e funcionalidades do Bitdefender Security for Creators.

1.3.1. Atividade

Detalhes do canal:

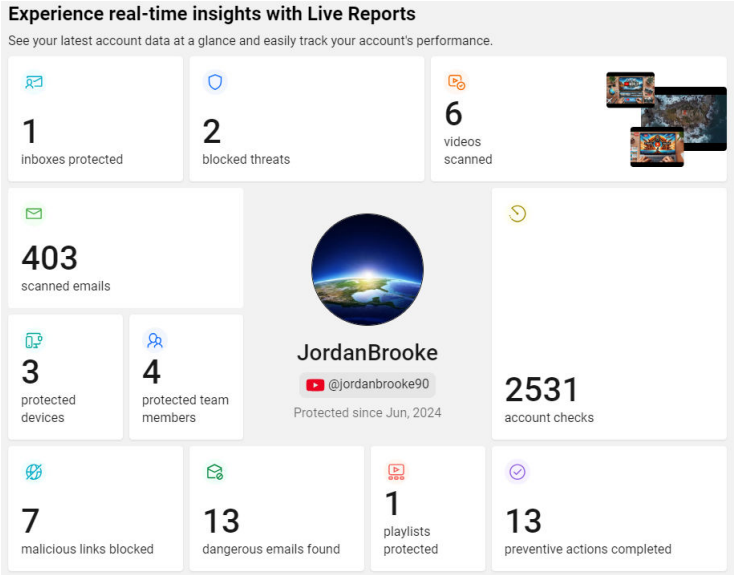
Na parte superior da guia Atividade, você encontrará todas as informações básicas sobre seu canal do YouTube.

- Foto do perfil e nome do canal
- Número de inscritos e o número de vídeos atualmente enviados.

Relatórios ao vivo:

O botão Relatórios ao vivo fornece análises e insights em tempo real sobre o status de segurança do seu canal, incluindo:

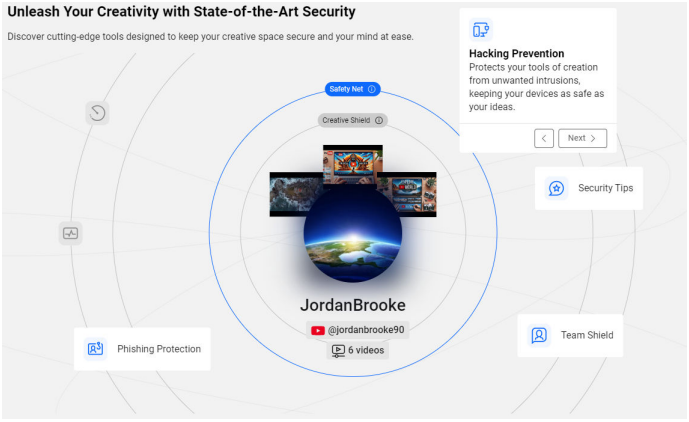
- Número de dispositivos e membros da equipe monitorados e protegidos, caixas de entrada monitoradas.
- Número de e-mails perigosos e URLs maliciosos bloqueados.
- Número de e-mails e vídeos analisados, bem como o número de verificações de conta feitas pelo Bitdefender.



Tecnologias:

As tecnologias facilitam a exploração de todos os recursos do Bitdefender Security for Creators.

Pressione o botão **Próximo** ou clique em qualquer recurso específico para ler mais:



Informações de segurança em tempo real:

Se rolar para baixo na página de atividades você verá:

- **Atividade do canal do YouTube:** informações atualizadas sobre as atividades recentes do seu canal.
- **Recomendações de segurança:** dicas de segurança para manter sua conta protegida contra hackers. Para cada recomendação de segurança (por exemplo. “Revisar aplicativos de terceiros” ou “Revisar opções de recuperação”), clique no botão **Revisar**. Em seguida, você será direcionado para uma página na qual poderá revisar ou remover itens conforme necessário.
  Depois de aplicar as ações recomendadas, clique no botão **Marcar como concluído**.
- **Alertas críticos e orientações de recuperação:** no caso de atividades suspeitas (por exemplo, vários vídeos excluídos ou transmissões e alterações incomuns de conteúdo), a guia **Atividade** emitirá alertas críticos. Esses alertas orientam você por meio de ações passo a passo para recuperar e proteger rapidamente seu canal do YouTube contra novos ataques de hackers.

1.3.2. Segurança

Na guia **Segurança**, você pode verificar rapidamente seu status de segurança e visualizar seus dispositivos protegidos, e-mails e ameaças bloqueados no passado. A guia **Segurança** é dividida em duas seções: **Meus dispositivos** e **Proteção de e-mail**.

- **Meu dispositivo**
  - Proteja novos dispositivos Windows, macOS, Android e iOS.
  - Veja um resumo das ameaças à segurança cibernética detectadas recentemente.
  - Visualize os dispositivos atualmente protegidos pelo Bitdefender.
- **Proteção de e-mail**
  - Veja o total de e-mails analisados pelo Bitdefender Email Protection nos últimos 30 dias, divididos em e-mails seguros e perigosos.
  - Veja todas as caixas de correio protegidas e seu status atual.

1.3.3. Membros da equipe

A guia **Membros da equipe** permite que você gerencie os membros da equipe do seu canal do YouTube:

- Envie convites por e-mail para proteger os novos membros da equipe.
- Remova os membros existentes da equipe.

1.4. Remover e adicionar um canal diferente do YouTube

Para remover um canal monitorado do YouTube e configurar o Bitdefender Security for Creators para uma conta diferente, remover um canal monitorado do YouTube e configurar o Bitdefender Security for Creators para uma conta diferente, vamos seguir a lista de instruções abaixo:

1.4.1. Remover um canal monitorado do YouTube

1. Faça login em sua conta da Bitdefender Central.
2. Depois de fazer login, clique no ícone do seu nome de usuário ou perfil localizado no canto superior direito da página.
3. Selecione **Configurações** no menu. A página de configurações da conta Bitdefender será aberta.
4. Na seção **Gerenciar contas**, clique em **Remover conta**.
5. Um pop-up aparecerá perguntando se você tem certeza se deseja ou não remover o canal.
   Clique em **Remover conta** para confirmar a ação.

   ! Importante
   Quando o Bitdefender Security for Creators parar de monitorar um canal do YouTube, você não receberá mais alertas se essa conta for invadida por hackers.

1.4.2. Adicionar um canal diferente do YouTube

1. Acesse as configurações da sua conta:
   - Se você acabou de remover uma conta do YouTube, verá um botão **Conectar sua conta** na seção **Gerenciar contas**.

- Se você está começando do zero, entre na sua conta do Bitdefender Central, clique no ícone do seu nome de usuário ou perfil e selecione **Configurações** no menu.

2. Clique no botão **Conectar sua conta** na seção **Gerenciar contas**.
3. Você será direcionado para o painel do Bitdefender Security for Creators.
   Role para baixo e clique no botão **Reconectar** no painel **do canal do YouTube desconectado**.
4. Um pop-up solicitará que você conecte sua conta do YouTube. Clicando no botão **Fazer login com o Google**.
5. Escolha a conta do Google vinculada ao canal do YouTube que você deseja monitorar.
   Digite sua senha, se solicitado, e clique em **Próximo**.
6. Clique em **Continuar** para permitir que o Bitdefender Security for Creators proteja sua conta do YouTube.

Quando a conexão for bem-sucedida, o nome e a foto do perfil do canal do YouTube conectado aparecerão na parte superior do painel do Bitdefender Security for Creators.

1.5. Recuperar uma conta invadida do YouTube

A ação imediata é crucial para recuperar o controle e proteger sua conta contra outros ataques semelhantes. Se você estiver usando o Bitdefender Security for Creators, recuperar um canal do YouTube invadido é um processo fácil e guiado passo a passo.

Veja o que fazer se seu canal do YouTube for invadido:

Etapa 1: Abra o e-mail do Bitdefender recebido recentemente

Você receberá por e-mail um alerta do Bitdefender intitulado **Atividade suspeita detectada**, assim que seu canal do YouTube for invadido. Este e-mail é enviado para o endereço de e-mail que você usou para criar sua conta do Bitdefender Central. Ele contém informações sobre todas as atividades suspeitas e ações notáveis encontradas no canal, como:

- Porcentagem de vídeos excluídos (por exemplo. 55% dos vídeos removidos).

- Alterações no banner, nas miniaturas do vídeo, na foto do perfil e na descrição do canal.

Clique no botão **Proteja sua conta agora** no e-mail.

Etapa 2: O que aconteceu?

Isso leva você à sua conta do Bitdefender Central, onde um pop-up informa que seu canal do YouTube está comprometido.

Na seção **Veja o que aconteceu**, você encontrará - e, portanto, poderá revisitar - uma lista detalhada de todas as alterações feitas em sua conta do YouTube.

Etapa 3: Recupere o canal hackeado do YouTube em quatro etapas

1. **Acesse sua conta:** siga os links no menu **Acesse sua conta** para recuperar sua conta rapidamente. Se você não conseguir fazer login, entre rapidamente em contato com o suporte do YouTube usando os links fornecidos.
2. **Redefina sua senha:** clique no link no menu **Redefina sua senha** para definir uma senha forte e exclusiva com pelo menos oito caracteres, incluindo letras maiúsculas e minúsculas, números e caracteres especiais.
3. **Revise suas configurações:** siga os links para remover membros desconhecidos da equipe, dispositivos não autorizados e aplicativos suspeitos de terceiros.
4. **Verifique suas informações de recuperação:** certifique-se de que suas informações de recuperação estejam corretas para evitar futuros acessos não autorizados.

Se sua conta foi usada para publicar conteúdo impróprio ou se os vídeos foram excluídos, lembre-se de se comunicar com seu público. Publique um vídeo ou uma atualização da comunidade explicando a situação e as medidas que você tomou para resolvê-la. A transparência pode ajudar a manter a confiança e o apoio de seus assinantes.

1.6. Perguntas Mais Freqüentes

Como o Bitdefender ajuda se meu canal do YouTube for invadido?

Caso seu canal do YouTube seja invadido, o Bitdefender enviará um alerta por e-mail com um guia passo a passo e links diretos para o Google/YouTube para ajudá-lo a recuperar rapidamente o controle de sua conta.

O Bitdefender pode ajudar a impedir que meu canal do YouTube seja invadido?

Sim. Para evitar que sua conta do YouTube seja invadida, o Bitdefender fornece dicas e estratégias de segurança personalizadas, além do que o Google já oferece.

O Bitdefender Security for Creators pode proteger contra e-mails falsos de patrocinadores?

Sim, o recurso Scam Guard sinaliza e-mails suspeitos com anexos ou links maliciosos, protegendo você de golpes disfarçados de ofertas de patrocínio.

O 2FA é suficiente para proteger meu canal do YouTube contra hackers?

O 2FA (autenticação de dois fatores) adiciona uma camada extra de segurança, mas não é infalível. Os hackers ainda podem contornar o 2FA por meio de métodos como phishing ou troca de SIM.

Posso alterar a conta do YouTube conectada ao Bitdefender Security for Creators?

Sim, você pode mudar o canal monitorado do YouTube a qualquer momento:

1. Faça login em sua conta da Bitdefender Central.
2. Clique no ícone do seu nome de usuário ou perfil no canto superior direito e selecione **Configurações**.
3. Clique em **Remover conta**.
4. Clique em **Conectar sua conta** para adicionar um canal diferente do YouTube.

Como posso restaurar vídeos excluídos do YouTube se eu não tiver backups?

A exclusão de um vídeo do YouTube é permanente e não pode ser desfeita. Depois que os vídeos do YouTube são excluídos da sua conta, restaurá-los pode ser um desafio se você não tiver backups em armazenamento externo ou serviços em nuvem. Você pode tentar entrar em contato com o suporte do YouTube para solicitar assistência. No entanto, a recuperação não é garantida.

O que devo fazer se tiver problemas para conectar minha conta do YouTube?

Se você encontrar problemas ao conectar o YouTube ao Bitdefender Security for Creators, é melhor:

- Certificar-se de que sua conexão com a internet esteja estável.
- Verificar se você está selecionando a conta do Google correta associada ao seu canal do YouTube.
- Digitar a senha correta.
- Verificar se você aprovou todas as permissões necessárias.

2. PROTEÇÃO DO CORREIO ELETRÓNICO

Seu e-mail é uma parte importante da sua vida digital e, dadas as suas múltiplas aplicações na vida real, tornou-se um vetor de ataque preferido para malfeitores e uma das principais preocupações de segurança cibernética do usuário diário.

Proteção do correio eletrónico é um recurso de segurança que permite verificar e identificar conteúdo potencialmente perigoso em e-mails recebidos em sua caixa de entrada. Esse recurso é um pacote de diversas tecnologias reunidas no mesmo módulo de proteção, como software antiphishing, antimalware, antispam, antifraude e anti-scam.

Ao criar uma conexão direta entre o Bitdefender e seu provedor de serviços de e-mail, você permite que o antivírus verifique seus e-mails diretamente e elimine as limitações incorridas pelo uso de diferentes dispositivos ou clientes de e-mail.

> **Observação**
> Você pode proteger até 5 contas de e-mail diferentes.

2.1. Configurando sua conta

Este recurso está perfeitamente integrado à interface do usuário. Para começar a usar o Proteção do correio eletrónico:

1. Sob **Proteção**, clique **Abrir** no **Proteção do correio eletrónico** cartão.
2. Escolha o seu provedor de e-mail para a conta de e-mail que você deseja proteger.

   > **Observação**
   > O Proteção do correio eletrónico está atualmente disponível para contas do Google, contas do Outlook e em breve também estará disponível para o Yahoo Mail.

3. Clique no **Entrar** botão.
   A operação continuará então no seu navegador.
4. Digite seu endereço de e-mail e clique no botão **Próximo** botão
5. Para continuar, digite sua senha e clique no botão **Próximo** botão.

6. Verifique as permissões solicitadas na tela e permita que o Bitdefender proteja sua conta de e-mail.

Sua conta de e-mail agora está protegida e todos os e-mails recebidos recentemente serão verificados contra ameaças.

> **Observação**
> Cada e-mail digitalizado será marcado com uma etiqueta para indicar seus níveis de segurança.

2.2. Painel

O painel exibirá seus e-mails protegidos, nos quais você encontrará:

- data de configuração (a data em que a conta foi configurada para Proteção do correio eletrónico)
- status (ativo ou inativo)
- número de e-mails filtrados nos últimos 30 dias.
  Aqui você verá um gráfico mostrando o número de e-mails seguros e e-mails perigosos recebidos.

Para adicionar várias contas de e-mail Clique no **Adicionar outra conta** e siga o processo de configuração acima para cada um deles.

Para pausar a verificação ou remover uma conta neste recurso, clique nos três pontos ao lado da conta em questão e clique em **Gerenciar conta**.

3. SEGURANÇA TOTAL PARA PC

3.1. Instalação

3.1.1. A preparar a instalação

Antes de instalar o Bitdefender Total Security, complete estes procedimentos para assegurar uma boa instalação:

- Assegure-se que o dispositivo onde deseja instalar o Bitdefender tem os requisitos de sistema mínimos. Caso o dispositivo não cumpra os requisitos de sistema, o Bitdefender não será instalado ou caso seja instalado, não irá trabalhar de forma apropriada e irá causar lentidão e instabilidade do sistema. Para ver a lista completa dos requisitos mínimos do sistema, consulte o Requisitos do sistema (página 16).
- Ligue-se ao dispositivo utilizando uma conta de Administrador.
- Remova quaisquer outros softwares semelhantes do seu dispositivo. Se for detetada qualquer coisa durante o processo de instalação da Bitdefender, será notificado para desinstalar. Executar dois programas de segurança simultaneamente poderá afetar o seu funcionamento e causar grandes problemas no sistema. O Windows Defender será desativado durante a instalação.
- Desativar ou remover qualquer programa de firewall que possa estar em execução no dispositivo. Executar dois programas de firewall simultaneamente poderá afetar o seu funcionamento e causar grandes problemas no sistema. A Firewall do Windows será desativada durante a instalação.
- Recomenda-se que o seu dispositivo esteja ligado à Internet durante a instalação, mesmo quando realizar a instalação a partir de um CD/DVD. Se estiverem disponíveis versões mais recentes dos ficheiros da aplicação incluidos no pacote de instalação, o Bitdefender irá descarregá-las e instalá-las.

3.1.2. Requisitos do sistema

Só pode instalar o Bitdefender Total Security nos dispositivos que tenham os seguintes sistemas operativos:

- Windows 7 com o Service Pack 1
- Windows 8.1
- Windows 10
- 2,5 GB de espaço disponível em disco rígido (pelo menos 800 MB na unidade do sistema)
- 2 GB de memória (RAM)

Importante
O desempenho do sistema pode ser afetado em dispositivos com CPUs de geração antiga.

Observação
Para saber qual é o sistema operativo Windows executado no seu dispositivo e informações do hardware:

- No **Windows 7**, clique com o botão direito em **Meu Computador** na área de trabalho, depois selecione **Propriedades** no menu.
- No **Windows 8**, a partir do ecrã Iniciar, localize **Computador** (por exemplo, pode começar a escrever "Computador" diretamente no ecrã Iniciar) e, em seguida, clique com o botão direito do rato no seu ícone. No **Windows 8.1**, localize **Este PC**.
  Selecione **Propriedades** no menu inferior. Verifique a área do **Sistema** para encontrar mais informações sobre o sistema.
- No **Windows 10**, escreva **Sistema** na caixa de pesquisa da barra de tarefas e clique no ícone correspondente. Procure na área de **Sistema** para encontrar informações sobre o seu tipo de sistema.

3.1.3. Requisitos de Software

Para conseguir utilizar o Bitdefender e todas as suas funcionalidades, o seu dispositivo deve cumprir os seguintes requisitos de software:

- Microsoft Edge 40 e superior
- Internet Explorer 10 ou superior
- Mozilla Firefox 51 e superior
- Google Chrome 34 e superior
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 e superior

3.1.4. Instalação do seu produto Bitdefender

Pode instalar o Bitdefender utilizando o disco de instalação ou através do instalador Web transferido para o seu dispositivo na **Bitdefender Central**.

Se a sua aquisição cobrir mais do que um dispositivo, repita o processo de instalação e ative o seu produto com a mesma conta em cada dispositivo. A conta a ser utilizada deve ser igual à que contém a sua subscrição ativa do Bitdefender.

A instalar a partir da Central Bitdefender

Na Bitdefender Central pode transferir o kit de instalação que corresponde à assinatura adquirida. Uma vez que o processo de instalação estiver concluído, o Bitdefender Total Security é ativado.

Para transferir Bitdefender Total Security a partir do Bitdefender Central:

1. Aceda à **Central da Bitdefender**.
2. Selecione o painel **Os meus dispositivos** e, em seguida, clique em **INSTALAR PROTEÇÃO**.
3. Escolha uma das duas opções disponíveis:
   - **Proteger este dispositivo**
     a. Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
     b. Guarde o ficheiro de instalação.
   - **Proteger outros dispositivos**
     a. Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, clique no botão correspondente.
     b. Clique em **ENVIAR LINK PARA A TRANSFERÊNCIA**.
     c. Escreva um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**.
     Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

d. No dispositivo em que deseja instalar o seu produto Bitdefender, verifique a conta de e-mail que escreveu e clique no botão de download correspondente.

4. Aguarde pela conclusão da transferência, em seguida, execute o instalador:

A validar a instalação

Em primeiro lugar, o Bitdefender verifica o seu sistema para validar a instalação.

Se o seu sistema não apresenta os requisitos do sistema para a instalação Bitdefender, será informado das áreas que precisam ser melhoradas antes de poder prosseguir.

Se for detetada uma solução de segurança incompatível ou uma versão anterior do Bitdefender, será solicitado a removê-lo do seu sistema. Por favor siga as instruções para remover o software do seu sistema, evitando assim que ocorram problemas mais tarde. Pode ser necessário reiniciar o dispositivo para concluir a remoção das soluções de segurança detetadas.

O pacote de instalação do Bitdefender Total Security é constantemente atualizado.

> **Observação**
> Fazer download dos ficheiros de instalação pode demorar muito tempo, especialmente se tiver uma ligação à internet que seja lenta.

Assim que a instalação estiver validada, o assistente de configuração irá aparecer. Siga os passos para instalar Bitdefender Total Security.

Passo 1 - Instalação do Bitdefender

Antes de concluir o processo de instalação, deve concordar com o Contrato de Subscrição. Leia o Acordo de Subscrição com calma, já que ele contém os termos e condições segundo os quais pode utilizar o Bitdefender Total Security.

Se não concorda com estes termos, feche a janela. O processo de instalação terminará e sairá do mesmo.

Podem ser realizadas duas tarefas adicionais neste passo:

- Mantenha a opção **Enviar relatórios de produto** ativada. Ao permitir esta opção, os relatórios que contêm informação sobre como usa o

produto são enviados para os servidores Bitdefender. Esta informação é essencial para melhorar o produto e pode ajudar-nos a oferecer-lhe uma experiência melhor no futuro. Tenha em atenção que estes relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e que não serão usados para fins comerciais.

- Selecione o idioma em que pretende instalar o produto.

Clique em **INSTALAR** para iniciar o processo de instalação do produto Bitdefender.

Passo 2 - Instalação em progresso

Espere até que a instalação termine. É apresentada informação detalhada sobre a evolução.

Passo 3 - Instalação concluída

O seu produto Bitdefender foi instalado com sucesso.

É apresentado um resumo da instalação. Se tiver sido detetada uma ameaça ativa e removida durante a instalação, pode ser necessário reiniciar o sistema.

Passo 4 - Análise do dispositivo

Agora ser-lhe-á perguntado se deseja realizar uma análise do seu dispositivo, para garantir que ele está seguro. Durante este passo, o Bitdefender irá verificar áreas críticas do sistema. Clique em **Iniciar análise de dispositivo** para a iniciar.

Pode ocultar a interface da análise ao clicar em **Executar análise em segundo plano**. Em seguida, escolha se deseja ser informado quando a análise terminar ou não.

Quando a análise estiver concluída, clique em **Abrir Interface do Bitdefender**.

> **Observação**
> Como alternativa, se não deseja realizar a análise, basta clicar em **Ignorar**.

Passo 5 - Introdução

Na janela **Introdução**, pode ver os detalhes sobre a sua subscrição ativa.

Clique em **TERMINAR** para aceder à Bitdefender Total Security interface.

Instalar a partir do disco de instalação

Para instalar o Bitdefender a partir do disco de instalação, insira o disco na unidade de leitura.

Deve aparecer um ecrã de instalação em alguns momentos. Siga as instruções para iniciar a instalação.

Se o ecrã de instalação não aparecer, utilize o Explorador do Windows para navegar até ao diretório de raiz do disco e clique duas vezes no ficheiro autorun.exe.

Se a velocidade da sua internet for lenta ou o seu sistema não estiver ligado à internet, clique no botão **Instalar de CD/DVD**. Neste caso, o produto Bitdefender disponível no disco será instalado e uma versão mais recente será transferida dos servidores Bitdefender através da atualização do produto.

A validar a instalação

Em primeiro lugar, o Bitdefender verifica o seu sistema para validar a instalação.

Se o seu sistema não apresenta os requisitos do sistema para a instalação Bitdefender, será informado das áreas que precisam ser melhoradas antes de poder prosseguir.

Se for detetada uma solução de segurança incompatível ou uma versão anterior do Bitdefender, será solicitado a removê-lo do seu sistema. Por favor siga as instruções para remover o software do seu sistema, evitando assim que ocorram problemas mais tarde. Pode ser necessário reiniciar o dispositivo para concluir a remoção das soluções de segurança detetadas.

O pacote de instalação do Bitdefender Total Security é constantemente atualizado.

> **Observação**
> Fazer download dos ficheiros de instalação pode demorar muito tempo, especialmente se tiver uma ligação à internet que seja lenta.

Assim que a instalação estiver validada, o assistente de configuração irá aparecer. Siga os passos para instalar Bitdefender Total Security.

Passo 1 - Instalação do Bitdefender

Antes de prosseguir com a instalação, você deve concordar com o Contrato de Assinatura. Reserve algum tempo para ler o Contrato de Assinatura, pois contém os termos e condições sob os quais você pode usar Bitdefender Total Security.

Se você não concorda com estes termos, feche a janela. O processo de instalação será abandonado e você sairá do setup.

Duas tarefas adicionais podem ser executadas nesta etapa:

- Mantenha o **Enviar relatórios de produtos** opção habilitada. Ao permitir esta opção, os relatórios contendo informações sobre como você usa o produto são enviados para os servidores da Bitdefender. Essas informações são essenciais para melhorar o produto e podem nos ajudar a proporcionar uma experiência melhor no futuro. Observe que esses relatórios não contêm dados confidenciais, como seu nome ou endereço IP, e que não serão usados para fins comerciais.
- Selecione o idioma no qual deseja instalar o produto.

Clique **INSTALAR** para iniciar o processo de instalação do seu produto Bitdefender.

Passo 2 - Instalação em processo

Aguarde a conclusão da instalação. Informações detalhadas sobre o progresso são exibidas.

Passo 3 - Instalação concluída

Um resumo da instalação é exibido. Se alguma ameaça ativa foi detectada e removida durante a instalação, uma reinicialização do sistema pode ser necessária.

Etapa 4 - Análise do dispositivo

Agora você será perguntado se deseja realizar uma análise do seu dispositivo, para garantir que ele seja seguro. Durante esta etapa, o Bitdefender verificará as áreas críticas do sistema. Clique **Iniciar análise do dispositivo** para iniciá-lo.

Você pode ocultar a interface de digitalização clicando em **Executar verificação em segundo plano**. Depois disso, escolha se deseja ser informado quando a verificação for concluída ou não.

Quando a análise estiver concluída, clique em **Continuar com a Criação da conta**.

> **Observação**
> Como alternativa, se você não deseja realizar a verificação, basta clicar em **Pular**.

Passo 5 - Conta Bitdefender

Após concluir a configuração inicial, a janela Bitdefender Account aparece. É necessária uma conta Bitdefender para ativar o produto e utilizar as suas ferramentas online. Para mais informação, dirija-se a Bitdefender Central.

Proceda consoante a sua situação.

- **Pretendo criar uma conta Bitdefender**

  1. Digite as informações solicitadas nos campos correspondentes. Os dados que nos fornecer serão mantidos confidenciais. A palavra-passe deve ter no mínimo 8 carateres, incluindo pelo menos um número ou símbolo, um carater minúsculo e um maiúsculo.
  2. Antes de continuar, deve concordar com os Termos de utilização. Aceda aos Termos de Utilização e leia-os com atenção, pois eles contêm os termos e condições segundo os quais pode utilizar o Bitdefender.
     Além disso, pode aceder e ler a Política de Privacidade.
  3. Clique em **CRIAR CONTA**.

     > **Observação**
     > Uma vez que a conta for criada, pode utilizar o endereço de e-mail e palavra-passe fornecidos para entrar na sua conta em https://central.bitdefender.com, ou na aplicação da Bitdefender Central, desde que esteja instalado num dos seus dispositivos Android ou iOS. Para instalar a app Bitdefender Central no Android, precisa de aceder ao Google Play, pesquisar por Bitdefender Central e, em seguida, tocar na opção de instalação correspondente. Para instalar a app Bitdefender Central no iOs, precisa de aceder à App Store, pesquisar por Bitdefender Central e, em seguida, tocar na opção de instalação correspondente.

- **Já tenho uma conta Bitdefender**

  1. Clique em **Iniciar sessão**.
  2. Introduza o endereço de e-mail no campo correspondente e clique em **PRÓXIMO**.
  3. Introduza a sua palavra-passe e depois clique em **ENTRAR**.
     Se tiver esquecido a palavra-passe da sua conta ou caso queira repô-la:
     a. Clique em **Esqueceu-se da palavra-passe?**
     b. Introduza o seu endereço de e-mail e depois clique em **PRÓXIMO**.
     c. Verifique a sua conta de e-mail, introduza o código de segurança que recebeu e depois clique em **PRÓXIMO**.
     Ou pode clicar em **Alterar palavra-passe** no e-mail que recebeu.
     d. Introduza a nova palavra-passe que deseja definir, depois introduza-a novamente. Clique em **GUARDAR**.

     Observação
     Caso já tenha uma conta MyBitdefender, pode utilizá-la para entrar na sua conta Bitdefender. Caso se tenha esquecido da palavra-passe, deve ir primeiro a https://my.bitdefender.com para repô-la. Em seguida, utilize as credenciais atualizadas para entrar na sua conta Bitdefender.

- **Quero iniciar sessão com a minha conta do Microsoft, Facebook ou Google.**
  Para iniciar sessão na sua conta Microsoft, Facebook ou Google:

  1. Selecione o serviço que deseja usar. Seá redireccionado para a página de início de sessão daquele serviço.
  2. Siga as instruções fornecidas pelo serviço selecionado para ligar a sua conta ao Bitdefender.

Observação
O Bitdefender não obtém acesso a qualquer informação confidencial como a palavra-passe da conta que usa para iniciar sessão ou a informação particular dos seus amigos ou contactos.

Passo 6 - Ative o seu produto

Observação
Este passo aparece se selecionar criar uma nova conta Bitdefender durante o passo anterior ou se iniciar sessão utilizando uma conta com uma subscrição expirada.

É necessária uma ligação à internet para completar a ativação do seu produto.

Proceda consoante a sua situação:

- Tenho um código de ativação
  Neste caso, ative o produto seguindo estas etapas:

  1. Introduza o código de ativação no campo Eu tenho um código de ativação, depois clique em **CONTINUAR**.

     Observação
     Pode encontrar o seu código de ativação:
     - na etiqueta do CD/DVD.
     - ou no cartão de registo do produto.
     - no e-mail da sua compra on-line.

  2. **Pretendo avaliar o Bitdefender**
     Neste caso, pode utilizar o produto durante um período de 30 dias. Para iniciar o período de avaliação, selecione **Não tenho uma subscrição; quero experimentar o produto de forma gratuita** e, em seguida, clique em **CONTINUAR**.

Passo 7 - Introdução

Na janela **Introdução**, pode ver os detalhes sobre a sua assinatura ativa.

Clique **TERMINAR** para acessar o Bitdefender Total Security interface.

3.2. Gerir a sua segurança

3.2.1. Proteção Antivírus

Bitdefender protege o seu dispositivo de todo o tipo de ameaças (malware, Trojans, spyware, rootkits, etc.). A protecção que BitDefender oferece está dividida em duas categorias:

- **Análise no acesso** - previne que novas ameaças entrem no seu sistema. Por exemplo, o Bitdefender irá analisar um documento word à procura de ameaças conhecidas quando o abrir, e uma mensagem de email quando recebe uma.
  A análise no acesso garante proteção em tempo real contra ameaças, sendo um componente essencial de qualquer programa informático de segurança.

  > **Importante**
  > Para prevenir a infeção de ameaças no seu dispositivo, mantenha ativada a **análise no acesso**.

- **Análise a pedido** - permite detetar e remover ameaças que já se encontram no sistema. Esta é uma análise clássica iniciada pelo utilizador – você escolhe qual a drive, pasta ou ficheiro o BitDefender deverá analisar, e o mesmo é analisado – a-pedido.

O Bitdefender analisa automaticamente qualquer media removível que esteja ligado ao dispositivo para garantir um acesso em segurança. Para mais informação, dirija-se a Análise automática de média removíveis (página 40).

Os utilizadores avançados poderão configurar excepções se não desejarem que ficheiros ou tipos de ficheiros específicos sejam analisados. Para mais informação, dirija-se a A configurar exceções de análise (página 42).

Quando deteta uma ameaça, o Bitdefender irá tentar remover automaticamente o código malicioso do ficheiro e reconstruir o ficheiro original. Esta operação é designada por desinfecção. Os ficheiros que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção. Para mais informação, dirija-se a Gerir ficheiros da quarentena (página 45).

Se o seu dispositivo estiver infetado com ameaças, consulte Remover ameaças do seu sistema (página 148). Para o ajudar a limpar as ameaças

do dispositivo que não podem ser removidas no sistema operativo Windows, o Bitdefender proporciona-lhe o Ambiente de Resgate (página 149). Este é um ambiente fiável, concebido sobretudo para a remoção de ameaças, que lhe permite arrancar o seu dispositivo independentemente do Windows. Quando o dispositivo é executado no Ambiente de Resgate, as ameaças do Windows estão inativas, tornando-as mais fáceis de remover.

Análise no acesso (proteção em tempo real)

O Bitdefender fornece uma proteção contínua e em tempo real contra uma ampla variedade de ameaças ao analisar todos os ficheiros e mensagens de e-mail acedidas.

Ligar ou desligar a proteção em tempo real

Para ativar ou desativar a proteção contra ameaças em tempo real:

1. Clique em **Proteção** no menu de navegação na **interface do Bitdefender**.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Avançado**, ative ou desative o **Bitdefender Shield**.
4. Se pretender desativar a proteção em tempo real, aparece uma janela de aviso. Tem de confirmar a sua escolha seleccionando no menu durante quanto tempo pretende desactivar a protecção em tempo real. Pode desativar a sua proteção em tempo real durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até ao reinício do sistema. A proteção em tempo real será ativada automaticamente quando o tempo selecionado expirar.

Aviso

Esta é uma incidência de segurança critica. Recomendamos que desactive a protecção em tempo-real o menos tempo possível. Quando a mesma está desactivada você deixa de estar protegido contra as ameaças.

Configuração das definições avançadas de proteção em tempo real

Os utilizadores avançados podem aproveitar as definições que o Bitdefender oferece. Pode configurar as definições da proteção em tempo real criando um nível de proteção personalizado.

Para configurar as definições avançadas de proteção em tempo real:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Na janela **Avançado**, pode configurar as definições da verificação conforme necessário.

Informação sobre as opções de análise

Poderá achar esta informação útil:

- **Analisar apenas as aplicações.** Pode definir o Bitdefender para verificar apenas as aplicações acedidas.
- **Analise aplicações potencialmente indesejadas.** Selecione esta opção para analisar aplicações indesejadas. Uma aplicação potencialmente indesejada (PUA) ou um programa potencialmente indesejado (PUP) é um software que normalmente vem com software freeware e irá mostrar pop-ups ou instalar uma barra de ferramentas no navegador predefinido. Alguns irão alterar a página inicial ou o motor de pesquisa e outros irão executar vários processos em segundo plano, deixando o seu PC lento, ou irão mostrar numerosos anúncios. Estes programas podem ser instalados sem o seu consentimento (também chamado adware) ou serão incluídos por predefinição no seu kit de instalação expresso (suportado por anúncios).
- **Verificar os scripts.** A função de Verificar Scripts permite que o Bitdefender verifique os scripts de PowerShell e documentos do Office que possam conter malware baseado em scripts.
- **Verificar os partilhas de rede.** Para aceder a uma rede remota com segurança no seu dispositivo, recomendamos que mantenha ativada a opção Verificar partilhas de rede.
- **Verificação da memória de processo.** Verifica atividades maliciosas na memória dos processos em execução.
- **Verificação da linha de comando.** Verifica a linha de comando das aplicações recém-iniciadas para evitar ataques sem ficheiros.
- **Verificar os ficheiros.** A verificação de ficheiros internos é um processo lento e com intensa exigência de recursos. Portanto, não é recomendada para uma proteção em tempo real. Pastas compactadas que contenham ficheiros infetados não constituem uma ameaça

imediata à segurança do seu sistema. A ameaça só afetará o seu sistema se o ficheiro infetado for extraído e executado sem que a proteção em tempo real seja ativada.
Se escolher esta opção, ative-a e, em seguida, arraste o marcador pela escala para excluir da análise ficheiros mais longos do que um valor dado em MB (Megabites).

- **Verificar os setores de arranque.** Pode definir o Bitdefender para verificar os setores de arranque do seu disco rígido. Este setor do disco rígido contém o código necessário para começar o processo de arranque. Quando uma ameaça infecta o setor de arranque, a drive pode tornar-se inacessível e não conseguirá iniciar o sistema e aceder aos seus dados.
- **Verificar as apenas os ficheiros novos e modificados.** Ao verificar apenas os ficheiros novos e modificados, pode melhorar significativamente a resposta geral do sistema com um comprometimento mínimo da segurança.
- **Verificação de keyloggers.** Selecione esta opção para verificar o seu sistema à procura de aplicações keyloggers. Os keyloggers registam o que é introduzido no seu teclado e enviam relatórios pela internet a uma pessoa com más intenções (hacker). O hacker pode descobrir informações confidenciais a partir dos dados roubados, tais como números de contas bancárias e palavras-passe, e utilizá-las para benefício próprio.
- **Verificação do arranque antecipada.** Selecione a opção **Verificação do arranque antecipada** para verificar o seu sistema no arranque assim que todos os serviços essenciais tenham sido carregados. A missão desta funcionalidade é melhorar o tempo e a deteção de ameaças no arranque do sistema.

Ações tomadas em ameaças detetadas

Pode configurar as ações a serem levadas a cabo pela proteção em tempo-real seguindo estes passos:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Na janela **Avançado**, rode para baixo até ver a opção **Ações de ameaça**.

4. Configure as definições de análise como necessário.

As seguintes ações podem ser levadas a cabo pela proteção em tempo real do Bitdefender:

Tomar medidas adequadas

Bitdefender tomará as ações recomendadas dependendo do tipo de ficheiro detetado:

- **Ficheiros infetados.** Os ficheiros detetados como estando infetados correspondem a uma informação de ameaça na Base de Dados de Informações sobre Ameaças do Bitdefender. O Bitdefender irá tentar remover automaticamente o código malicioso do ficheiro infetado e reconstruir o ficheiro original. Esta operação é referida como desinfeção.

  Os ficheiros que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece. Para mais informação, dirija-se a Gerir ficheiros da quarentena (página 45).

  > **Importante**
  > Para determinados tipos de ameaças, a desinfeção não é possível por o ficheiro detetado ser totalmente malicioso. Nestes casos, o ficheiro infectado é eliminado do disco.

- **Ficheiros suspeitos.** Os ficheiros são detetados como sendo suspeitos pela análise heurística. Não é possível desinfetar ficheiros suspeitos porque não há uma rotina de desinfeção disponível. Irão ser colocados em quarentena para evitar uma potencial infeção.

- **Pastas que contêm ficheiros infetados.**

  - Os arquivos que contêm apenas ficheiros infectados são eliminados automaticamente.

  - Se um arquivo tiver ficheiros infectados e limpos, o Bitdefender tentará eliminar os ficheiros infectados desde que possa reconstruir o arquivo com os ficheiros limpos. Se não for possível a reconstrução do arquivo, será informado de que não pode ser tomada qualquer ação, de forma a evitar perder ficheiros limpos.

Mover para a quarentena

Move os ficheiros infectados para a quarentena. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece. Para mais informação, dirija-se a Gerir ficheiros da quarentena (página 45).

Negar o acesso

Será negado o acesso de um ficheiro que se encontre infectado.

Restaurar as predefinições

As predefinições da proteção em tempo real asseguram uma ótima proteção contra ameaças, com um impacto mínimo no desempenho do seu sistema.

Para restaurar as definições da protecção em tempo real:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Na janela **Avançado**, role para baixo até ver a opção **Restaurar configurações avançadas**. Selecione esta opção para retornar às configurações de fábrica do antivírus.

Verificação por ordem

O objetivo principal do Bitdefender é manter o seu dispositivo livre de ameaças. Isto é feito ao manter as novas ameaças fora do seu dispositivo e ao analisar as suas mensagens de e-mail e quaisquer novos ficheiros transferidos ou copiados para o seu sistema.

Há o risco de a ameaça já ter acedido ao seu sistema, antes mesmo de ter instalado o Bitdefender. Este é o motivo pelo qual é uma excelente ideia verificar ameaças residentes no seu dispositivo depois de instalar o Bitdefender. E é definitivamente uma boa ideia analisar frequentemente o seu dispositivo quanto a ameaças.

A análise a-pedido está baseada em tarefas de análise. As tarefas de análise especificam as opções de análise e os objectos a serem analisados. Pode analisar o dispositivo sempre que quiser executar as tarefas por defeito ou as suas próprias tarefas de análise (tarefas definidas pelo utilizador). Se quer analisar localizações específicas no seu dispositivo ou configurar as opções de análise, pode configurar e executar uma análise personalizada.

Procurar ameaças num ficheiro ou pasta

Deve verificar os ficheiros e as pastas sempre que suspeitar que possam estar infetados. Clique com o botão direito do rato no ficheiro ou pasta que deseja verificar, aponte para o **Bitdefender** e selecione **Verificar com o Bitdefender**. O **Assistente de Verificação** aparecerá e irá guiá-lo através do processo de verificação. Ao final da verificação, será solicitado que escolha as ações a serem tomadas para os ficheiros detetados, se houver algum.

Executar uma Análise Rápida

A Análise Rápida utiliza a análise nas nuvens para detetar ameaças em execução no seu sistema. Normalmente, a realização de uma Análise Rápida demora menos de um minuto e utiliza uma fração dos recursos do sistema necessários para uma análise antivírus normal.

Para realizar uma análise rápida:

1. Clique em Proteção no menu de navegação da interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Na janela **Verificações**, clique no botão **Executar verificação** ao lado de **Verificação rápida**.
4. Siga o **assistente de Análise Antivírus** para completar a análise. O Bitdefender tomará automaticamente as ações recomendadas nos ficheiros detetados. Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

Executar uma Análise do Sistema

A tarefa de Análise do Sistema procura em todo o dispositivo todos os tipos de ameaças que prejudicam a sua segurança, tais como malware, spyware, adware, rookits, etc.

> **Observação**
> Porque a **Análise do Sistema** leva a cabo uma análise minuciosa de todo o seu computador, a mesma poderá levar algum tempo. Portanto, recomenda-se que execute esta tarefa quando não estiver a utilizar o seu dispositivo.

Antes de executar uma Análise do Sistema, recomendamos o seguinte:

- Certifique-se de que o Bitdefender está atualizado com a sua base de dados de informações de ameaças. Verificar o seu dispositivo utilizando bases de dados de informação de ameaças desatualizadas pode impedir que o Bitdefender detecte novas ameaças criadas desde a última atualização. Para mais informação, dirija-se a Manter o Bitdefender atualizado.
- Encerre todos os programas abertos.

Se quer analisar localizações específicas no seu dispositivo ou configurar as opções de análise, pode configurar e executar uma análise personalizada. Para mais informação, dirija-se a Configurar uma análise personalizada (página 33).

Para realizar uma análise do sistema:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Na janela **Verificações**, clique no botão **Executar verificação** ao lado de **Verificação do sistema**.
4. A primeira vez que executar uma Análise do Sistema, verá uma apresentação da função. Clique em **OK, entendi** para continuar.
5. Segue o Assistente de verificação antivírus para concluir a digitalização. O Bitdefender executará automaticamente as ações recomendadas nos arquivos detectados. Se houver ameaças não resolvidas, você será solicitado a escolher as ações a serem executadas.

Configurar uma análise personalizada

Sempre que achar que o seu dispositivo precisar de ser analisado quanto a ameaças potenciais, pode configurar a Bitdefender para realizar análises utilizando a janela **Gerir análises**. Pode programar uma **Análise de Sistema**, uma **Análise Rápida**, ou pode criar uma análise personalizada segundo as suas necessidades.

Para configurar uma nova análise personalizada detalhadamente:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Nas janelas de **Verificações**, clique em **+Criar verificação**.

4. No campo **Nome da tarefa**, introduza o nome da verificação, a seguir, selecione os locais que deseja verificar, e depois clique em **Próximo**.
5. Configure as seguintes opções gerais:
   - **Digitalizar apenas aplicativos.** Você pode configurar o Bitdefender para verificar apenas os aplicativos acessados.
   - **Prioridade da tarefa de verificação.** Pode escolher o impacto que um processo de verificação deve ter no desempenho do seu sistema.
     - Automática - A prioridade do processo de análise dependerá da atividade do sistema. Para que o processo de análise não afete a atividade do sistema, o Bitdefender decide se o processo de análise deve ser executado com prioridade alta ou baixa.
     - Alta - A prioridade do processo de análise será alta. Ao escolher esta opção, permite que outros programas sejam executados mais devagar, diminuindo o tempo necessário para o processo de análise ser concluído.
     - Baixa - A prioridade do processo de análise será baixa. Ao escolher essa opção, permite que outros programas sejam executados mais rápido, aumentando o tempo necessário para o processo de análise ser concluído.
   - **Ações de pós-verificação.** Escolha a ação que o Bitdefender deve tomar caso não sejam encontradas ameaças:
     - Mostrar janela de resumo
     - Desligar dispositivo
     - Fechar janela da Análise
6. Se deseja configurar as opções de análise detalhadamente, clique em **Mostrar opções avançadas**. Poderá encontrará informações sobre as análises listadas no final desta seção.
   Clique em **Próximo**.
7. Pode ativar a opção **Programar tarefa de análise** se quiser e, em seguida, escolha quando a análise personalizada que criou deve começar.
   - No iniciar do sistema

- Diária
- Mensal
- Semanal

Para escolher Diariamente, Mensalmente ou Semanalmente, arraste o marcador pela barra de frequência para definir o intervalo em que a análise programada deve começar.

8. Clique em **Guardar** para guardar as definições e fechar a janela de configuração.
   Dependendo das localizações a serem analisadas, a análise pode demorar um pouco. Se forem encontradas ameaças durante o processo de análise, deve escolher as ações a serem tomadas para os ficheiros detectados.

Informações sobre as opções de digitalização

Você pode achar esta informação útil:

- Se não está familiarizado com alguns dos termos, procure-os no **glossário**. Pode também encontrar informação útil pesquisando a Internet.
- **Examine aplicativos potencialmente indesejados.** Selecione esta opção para procurar aplicativos indesejados. Um aplicativo potencialmente indesejado (PUA) ou programa potencialmente indesejado (PUP) é um software que geralmente vem junto com o software freeware e exibe pop-ups ou instala uma barra de ferramentas no navegador padrão. Alguns deles mudarão a página inicial ou o mecanismo de pesquisa, outros executarão vários processos em segundo plano, tornando o PC mais lento ou exibirão vários anúncios. Esses programas podem ser instalados sem o seu consentimento (também chamados de adware) ou serão incluídos por padrão no kit de instalação expresso (suportado por anúncios).
- **Verificar os ficheiros.** Pastas compactadas que contenham ficheiros infetados não constituem uma ameaça imediata à segurança do seu sistema. A ameaça só afetará o seu sistema se o ficheiro infetado for extraído e executado sem que a proteção em tempo real seja ativada. Contudo, recomenda-se a utilização desta opção para detetar e remover qualquer ameaça potencial, mesmo que não seja uma ameaça imediata.

Arraste o marcador pela escala para excluir da análise ficheiros mais longos do que um dado valor em MB (Megabites).

> **Observação**
> Analisar ficheiros arquivados aumenta o tempo da análise e requer mais recursos do sistema.

- **Examine apenas arquivos novos e modificados.** Ao verificar apenas arquivos novos e modificados, você pode melhorar muito a capacidade de resposta geral do sistema com uma compensação mínima em segurança.
- **Verifique os setores de inicialização.** Você pode configurar o Bitdefender para verificar os setores de inicialização do seu disco rígido. Este setor do disco rígido contém o código de computador necessário para iniciar o processo de inicialização. Quando uma ameaça infecta o setor de inicialização, a unidade pode ficar inacessível e você pode não conseguir iniciar o sistema e acessar seus dados.
- **Analisar memória.** Selecione esta opção para analisar programas em execução na memória do seu sistema.
- **Verificar o registo.** Selecione esta opção para verificar as chaves de registo. O Registo do Windows é um banco de dados que armazena as configurações e opções para os componentes do sistema operacional Windows, bem como para as aplicações instaladas.
- **Verificar os cookies.** Selecione esta opção para verificar os cookies armazenados pelos navegadores do seu dispositivo.
- **Digitalizar keyloggers.** Selecione esta opção para escanear seu sistema em busca de aplicativos keylogger. Os keyloggers registram o que você digita no teclado e enviam relatórios pela internet para uma pessoa maliciosa (hacker). O hacker pode descobrir informações confidenciais dos dados roubados, como números de contas bancárias e senhas, e usá-los para obter benefícios pessoais.

Assistente de Análise Antivírus

Sempre que iniciar uma verificação a pedido (por exemplo, clique com o botão direito do rato numa pasta, aponte para o Bitdefender e selecione **Verificar com o Bitdefender**), o Assistente de Verificação aparecerá. Siga o assistente para concluir o processo de verificação.

Observação

Se o assistente de análise não surgir, a análise pode ser configurada para ser executada de forma silenciosa, em segundo plano. Procure o ícone de progresso de análise na **bandeja do sistema**. Pode clicar neste ícone para abrir a janela de análise e para ver o progresso da análise.

Passo 1 - Realizar Análise

BitDefender iniciará a análise dos objectos seleccionados. Pode ver informação em tempo real sobre o estado da análise e as estatísticas (incluindo o tempo decorrido, uma estimativa do tempo restante e o número de ameaças detetadas).

Espere que o BitDefender termine a análise. O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

Parar ou colocar em pausar a verificação. Pode parar a verificação sempre que quiser ao clicar em **PARAR**. Será direcionado ao último passo do assistente. Para parar temporariamente o processo de verificação, basta clicar em **PAUSA**. Terá que clicar em **RETOMAR** para retomar a verificação.

Ficheiros protegidos por palavra-passe. Quando um ficheiro protegido por palavra-passe é detetado, dependendo das definições de verificação, pode ser preciso fornecer a palavra-passe. Os ficheiros protegidos por palavra-passe não podem ser verificados, a menos que a mesma seja fornecida. As seguintes opções estão disponíveis:

- **Palavra-passe.** Se quiser que o Bitdefender verifique o ficheiro, selecione esta opção e escreva a palavra-passe. Se não souber a palavra-passe, escolha uma das outras opções.
- **Não peça uma palavra-passe e ignore este objeto na verificação.** Selecione esta opção para ignorar a verificação deste ficheiro.
- **Ignorar todos os itens protegidos por palavra -passe sem verificá-los.** Selecione esta opção se não quiser ser incomodado com ficheiros protegidos por palavra-passe. O Bitdefender não poderá verificá-los, mas um relatório será mantido no registo de verificação.

Escolha a opção desejada e clique em **OK** para continuar a analisar.

Passo 2 - Escolher Ações

No final da análise, será notificado para escolher as ações que devem ser tomadas nos ficheiros detetados, caso os haja.

> **Observação**
> Quando realiza uma verificação rápida ou do sistema, o Bitdefender automaticamente aplica as ações recomendadas nos ficheiros detetados durante a verificação. Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

Os objetos infetados são apresentados em grupos, baseados no tipo de ameaças com que estão infetados. Clique no link correspondente a uma ameaça para descobrir mais informação acerca dos objetos infectados.

Pode escolher uma ação geral a ser levada a cabo para todas as incidências ou pode escolher ações separadas para cada grupo de incidências. Uma ou várias das seguintes opções poderão aparecer no menu:

Tomar as medidas adequadas

O Bitdefender tomará as ações recomendadas dependendo do tipo de arquivo detectado:

- **Arquivos infectados.** Os arquivos detectados como infectados correspondem a uma informação sobre ameaças encontrada no Banco de Dados de Informações sobre Ameaças do Bitdefender. O Bitdefender tentará automaticamente remover o código malicioso do arquivo infectado e reconstruir o arquivo original. Esta operação é referida como desinfecção.
  Os arquivos que não podem ser desinfetados são movidos para a quarentena para conter a infecção. Arquivos em quarentena não podem ser executados ou abertos; portanto, o risco de infecção desaparece. Para mais informações, consulte Gerir ficheiros da quarentena (página 45).

  > **Importante**
  > Para determinados tipos de ameaças, a desinfecção não é possível porque o arquivo detectado é totalmente malicioso. Nesses casos, o arquivo infectado é excluído do disco.

- **Arquivos suspeitos.** Os arquivos são detectados como suspeitos pela análise heurística. Arquivos suspeitos não podem ser desinfetados

porque nenhuma rotina de desinfecção está disponível. Eles serão transferidos para a quarentena para evitar uma possível infecção.

- **Arquivos contendo arquivos infectados.**
  - Os arquivos que contêm apenas arquivos infectados são excluídos automaticamente.
  - Se um arquivo contém arquivos infectados e limpos, o Bitdefender tentará excluir os arquivos infectados desde que possa reconstruir o arquivo com os arquivos limpos. Se a reconstrução do arquivo não for possível, você será informado de que nenhuma ação pode ser tomada para evitar a perda de arquivos limpos.

Excluir

Remove os ficheiros detectados do disco.

Se os ficheiros infectados estiverem armazenados num arquivo junto com ficheiros limpos, o Bitdefender tentará eliminar os ficheiros infectados e reconstruir o arquivo com ficheiros limpos. Se não for possível a reconstrução do arquivo, será informado de que não pode ser tomada qualquer ação, de forma a evitar perder ficheiros limpos.

Não tomar medidas

Nenhuma acção será levada a cabo sobre os ficheiros detectados. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses ficheiros.

Clique em **Continuar** para aplicar as acções especificadas.

Passo 3 - Resumo

Quando o BitDefender termina de reparar estas incidências, o resultado da análise aparecerá numa nova janela. Se deseja uma informação completa sobre o processo de análise, clique em **MOSTRAR RELATÓRIO** para ver o relatório da análise.

Importante

Na maioria dos casos o BitDefender desinfecta com sucesso o ficheiro infectado ou isola a infecção. No entanto, há incidências que não podem ser automaticamente resolvidas. Se necessário, ser-lhe-à solicitado que reinicie o seu computador, para que o processo de limpeza seja completado. Para mais informações e instruções sobre como remover manualmente uma ameaça, consulte Remover ameaças do seu sistema (página 148).

Ver os relatórios da análise

Sempre que uma análise for efetuada, é criado um registo de análise e o Bitdefender regista as incidências detectadas na janela Antivírus. O relatório da análise contém informação detalhada acerca dos processos de análise registados, tal como as opções da análise, o alvo da análise, as ameaças encontradas e as acções tomadas sobre essas ameaças.

Pode abrir o relatório diretamente no assistente de análise, assim que esta terminar, clicando em **MOSTRAR RELATÓRIO**.

Para verificar um registo de análise ou qualquer infeção detetada posteriormente:

1. Clique **Notificações** no menu de navegação do Interface do Bitdefender.
2. No separador **Todas**, selecione a notificação referente à última análise.
   Aqui poderá encontrar todos os eventos de análise de ameaças, incluindo ameaças detectadas na análise no acesso, análises iniciadas pelo utilizador e alterações de estado para as análises automáticas.
3. Na lista de notificações, pode ver as análises que foram recentemente efectuadas. Clique numa notificação para visualizar detalhes sobre o mesmo.
4. Para abrir o relatório da análise, clique em **Ver Relatório**.

Análise automática de média removíveis

O Bitdefender deteta automaticamente quando um dispositivo de armazenamento removível é ligado ao dispositivo e analisa-o em segundo plano quando a opção de Análise automática está ativada. Isto é recomendado para evitar que ameaças infetem o seu dispositivo.

Os dispositivos detetados encaixam-se numa destas categorias:

- CDs/DVDs
- Dispositivos de armazenamento externos como pen USB e discos rígidos externos
- Unidades de Rede Mapeadas (remotas)

Você pode configurar a análise automática separadamente para cada categoria de dispositivos de armazenamento. Análise automática das drives de rede mapeadas está desativada por defeito.

Como funciona?

Ao detectar um dispositivo de armazenamento removível, o Bitdefender começa a analisá-lo à procura de ameaças (desde que a análise automática esteja ativa para esse tipo de dispositivo). Será notificado através de uma janela de pop-up que um novo dispositivo foi detetado e está a ser analisado.

Um ícone de progresso da verificação do Bitdefender aparecerá na **bandeja do sistema**. Pode clicar neste ícone para abrir a janela de verificação e para ver o progresso da verificação.

Quando a análise estiver concluída, é apresentada a janela dos resultados da análise para o informar se pode aceder em segurança aos ficheiros nos dispositivos removíveis.

Na maioria dos casos, o Bitdefender remove automaticamente as ameaças detetadas ou isola os ficheiros infetados na quarentena. Se houver ameaças não resolvidas depois da análise, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

> **Observação**
> Tenha em conta que nenhuma ação pode ser efetuada nos ficheiros que estiverem infetados ou suspeitos detetados em CDs / DVDs. Do mesmo modo, nenhuma ação pode ser tomada nos ficheiros infetados ou suspeitos detetados em unidades de rede mapeada se não tiver os privilégios adequados.

Esta informação pode ser útil para si:

- Tenha cuidado ao utilizar um CD/DVD infetado com ameaças porque as ameaças não podem ser removidas do disco (é apenas de leitura). Certifique-se que a proteção em tempo real está ativada para evitar que as ameaças se propaguem no seu sistema. É recomendado copiar quaisquer dados valiosos do disco no seu sistema e depois descartar o disco.
- Em alguns casos, o Bitdefender poderá não conseguir remover as ameaças de ficheiros específicos devido a restrições legais ou técnicas. Exemplo disso são os ficheiros guardados usando uma tecnologia proprietária (isto acontece porque o ficheiro não pode ser correctamente recriado).
  Para saber mais sobre como lidar com ameaças, consulte Remover ameaças do seu sistema (página 148).

Gerir análise de média removível

Para gerir a verificação automática de dispositivos multimédia amovíveis:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Selecione a janela **Definições**.

As opções de análise estão pré-configuradas para obter os melhores resultados de deteção. Se forem detctados ficheiros infetados, o Bitdefender tentará desinfetá-los (remover o código malicioso) ou movê-los para a quarentena. Se ambas as acções falharem, o assistente da Análise Antivírus permite especificar outras acções a serem tomadas com ficheiros infectados. As opções de análise são padronizadas e não as pode alterar.

Para uma melhor proteção, recomenda-se que deixe a opção **Análise automática** selecionada para todos os tipos de dispositivos de armazenamento removíveis.

Analisar ficheiro hosts

Os ficheiros anfitrião são fornecidos por predefinição com a instalação do seu sistema operativo e são utilizados para mapear os nomes de anfitrião nos endereços IP sempre que acede a uma nova página Web, ligue um FTP ou outros servidores de Internet. É um ficheiro de texto simples e os programas maliciosos podem modificá-lo. Os utilizadores avançados sabem como utilizá-lo para bloquear anúncios incómodos, separadores, cookies de terceiros ou hijackers.

Para configurar o ficheiro anfitrião de verificação:

1. Clique **Configurações** no menu de navegação do Interface do Bitdefender.
2. Selecione os **Avançado** aba.
3. Ligue ou desligue a **Análise do ficheiro do host**.

A configurar exceções de análise

O Bitdefender permite excluir ficheiros, pastas ou extensões de ficheiros específicos da análise. Esta característica visa evitar a interferência com o seu trabalho e também pode ajudar a melhorar o desempenho do sistema. As exceções devem ser utilizadas por utilizadores com

conhecimentos avançados de informática ou sob as recomendações de um representante da Bitdefender.

Pode configurar excepções para que sejam realizadas análises somente após acesso ou por demanda ou até mesmo ambas. Os objetos excetuados da análise após acesso não serão analisados, mesmo se forem acedidos por si ou por uma aplicação.

> **Observação**
> As exceções NÃO serão aplicadas à análise contextual. Análise Contextual é um tipo de análise a-pedido: você clica com o botão direito de rato sobre o ficheiro ou pasta que quer analisar e selecciona **Analisar com BitDefender**.

Excluindo ficheiros e pastas da análise

Para excluir ficheiros e pastas específicas da análise:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Na janela **Definições**, clique em **Gerir exceções**.
4. Clique em **+Adicionar uma exceção**.
5. Introduza no campo correspondente o caminho da pasta que pretende adicionar à lista de exceção da análise.
   Como alternativa, pode navegar até a pasta ao clicar no botão navegar no lado direito da interface, selecioná-la e clicar em **OK**.
6. Ligue o interruptor junto à funcionalidade de proteção que não deve analisar a pasta. Há três opções:
   - Antivírus
   - Prevenção de Ameaças Online
   - Advanced Threat Defense
7. Clique em **Guardar** para guardar as alterações e fechar a janela.

Exceto extensões de ficheiros de verificação

Quando exclui uma extensão de ficheiro da análise, o Bitdefender deixará de analisar ficheiros com essa extensão, independentemente da sua localização no seu dispositivo. A exceção também se aplica a ficheiros em

meios removíveis, tais como CDs, DVDs, dispositivos de armazenamento USB ou unidades de rede.

> **Importante**
> Tenha cuidado ao excluir as extensões da análise, porque essas exceções podem deixar o seu dispositivo vulnerável a ameaças.

Para excluir extensões de ficheiros da análise:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. No **Configurações** janela, clique **Gerenciar exceções**.
4. Clique **+Adicionar uma exceção**.
5. Escreva as extensões que deseja excluir da análise com um ponto antes e separando-as por ponto e vírgula (;).
   txt;avi;jpg
6. Ligue o interruptor junto à funcionalidade de proteção que não deve analisar a extensão.
7. Clique em **Guardar**.

Ativar exceções de análise

Se as exceções de análise configuradas já não forem necessárias, é recomendado que elimine ou desactive as exceções de análise.

Para gerir exceções da análise:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Na janela de **Definições**, clique em **Gerir exceções**. Uma lista com todas as suas exceções será exibida.
4. Para remover ou editar exceções da análise, clique num dos botões disponíveis. Proceder da seguinte forma:
   - Para remover um dado da lista, clique no botão próximo a ele.
   - Para editar uma entrada da tabela, clique no botão **Editar** ao lado dela. Uma nova janela aparece onde pode alterar a extensão ou o caminho a ser excluído e a funcionalidade de segurança do qual

deseja que eles sejam excluídos, conforme necessário. Faça as alterações necessárias e, em seguida, clique em **MODIFICAR**.

Gerir ficheiros da quarentena

O Bitdefender isola os ficheiros infetados por ameaças que não consegue desinfetar numa área segura denominada quarentena. Quando uma ameaça se encontra na quarentena não pode provocar nenhum mal, porque não pode ser nem lida nem executada.

Além disso, o Bitdefender analisa os ficheiros em quarentena sempre que a base de dados de informações de ameaças é atualizada. Os ficheiros limpos são automaticamente repostos no seu local de origem.

Para verificar e gerir os ficheiros em quarentena:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Vá para a janela **Definições**.
   Aqui pode ver o nome dos ficheiros em quarentena, a sua localização original e o nome das ameaças detetadas.
4. Os ficheiros da quarentena são geridos automaticamente pelo Bitdefender de acordo com as predefinições da quarentena.
   Embora não seja recomendado, pode ajustar as definições de quarentena de acordo com as suas preferências clicando em **Ver Definições**.
   Clique nos botões para ligar ou desligar:
   Verifique novamente a quarentena depois de atualizações às informações sobre ameaças
   Mantenha esta opção ligada para analisar automaticamente os ficheiros da quarentena após cada atualização da base de dados das informações de ameaças. Os ficheiros limpos são automaticamente repostos no seu local de origem.
   Apagar conteúdo com mais de 30 dias
   Os ficheiros em quarentena com mais de 30 dias são eliminados automaticamente.
   Criar exceções para ficheiros restaurados

Os ficheiros que você restaurar da quarentena serão colocados de volta na sua localização original sem que sejam reparados e excluídos automaticamente de análises futuras.

5. Para eliminar um ficheiro da quarentena, selecione-o e clique no botão **Eliminar**. Se pretende restaurar um ficheiro da quarentena para a respetiva localização original, selecione-o e clique em **Restaurar**.

3.2.2. Defesa Avançada contra Ameaças

A Defesa Avançada contra as Ameaças do Bitdefender é uma tecnologia de deteção inovadora e proativa que utiliza métodos heurísticos avançados para detetar ransomware e outras novas ameaças potenciais em tempo real.

Advanced Threat Defense monitoriza continuamente as aplicações executadas no dispositivo, procurando ações tipo ameaças. Cada uma destas acções é classificada e é calculada uma pontuação geral para cada processo.

Como medida de segurança, será notificado sempre que seja detectada e bloqueada uma ameaça ou um processo potencialmente malicioso.

Ativar ou desativar o Advanced Threat Defense

Para ativar ou desativar o Advanced Threat Defense:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No painel **DEFESA AVANÇADA CONTRA AMEAÇAS**, clique em **Abrir**.
3. Vá à janela **Definições** e clique no botão ao lado de **Defesa Avançada contra Ameaças do Bitdefender**.

> **Observação**
> Para manter o sistema protegido contra ransomware e outras ameaças, recomendamos que desative o Advanced Threat Defense o mínimo de tempo possível.

A verificar ataques maliciosos detectados

Cada vez que seja detectada uma ameaça ou um processo potencialmente malicioso, o Bitdefender irá bloqueá-lo para previr que o seu dispositivo seja infectado por ransomware ou outro malware. Pode comprovar a lista de ataques maliciosos detectados seguindo os seguintes passos:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **DEFESA AVANÇADA DE AMEAÇA** painel, clique **Abrir**.
3. Vá para a janela **Defesa contra Ameaças**.
   São apresentados os ataques detetados nos últimos 90 dias. Para obter informações sobre o tipo de um ransomware detetado, o caminho do processo malicioso ou se a desinfeção foi bem-sucedida, basta clicar neste.

A adicionar processos a exceções

Você pode configurar as regras de exceção para aplicações fidedignas para que a Defesa Avançada Contra Ameaças as bloqueie caso executem ações típicas de ameaças.

Para começar a adicionar processos à lista de exceções da Defesa Avançada Contra Ameaças:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **DEFESA AVANÇADA DE AMEAÇA** painel, clique **Abrir**.
3. No **Configurações** janela, clique **Gerenciar exceções**.
4. Clique **+Adicionar uma exceção**.
5. Insira o caminho da pasta que deseja excluir da digitalização no campo correspondente.
   Como alternativa, pode navegar para o executável ao clicar no botão navegar no lado direito da interface, selecioná-lo e clicar em **OK**.
6. Ligue o interruptor ao lado de **Defesa contra Ameaças Avançadas**.
7. Clique **Salvar**.

Deteção de exploits

Uma forma utilizada pelos hackers para invadir sistemas é aproveitarem-se de certos bugs ou vulnerabilidades no software (aplicações e plug-ins) e hardware dos computadores. O Bitdefender utiliza a mais moderna tecnologia antiexploit para evitar que o seu dispositivo seja vítima de um desses ataques, que se costumam espalhar muito rapidamente.

Ativar ou desativar a deteção de exploits

Para ativar ou desativar a deteção de exploits:

- Clique **Proteção** no menu de navegação do Interface do Bitdefender.
- No **DEFESA AVANÇADA DE AMEAÇA** painel, clique **Abrir**.
- Vá à janela de **Definições** e clique no botão ao lado de **Deteção de exploits** para ativar ou desativar a função.

> **Observação**
> A opção de Deteção de exploits está ativa por predefinição.

3.2.3. Prevenção de ameaças on-line

A Prevenção contra Ameaças Online do Bitdefender garante uma navegação segura ao alertá-lo sobre as páginas da web potencialmente maliciosas.

O Bitdefender fornece a prevenção de ameaças online em tempo real para:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Para configurar a Prevenção contra ameaças online:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No painel **PREVENÇÃO CONTRA AMEAÇAS ONLINE**, clique em **Definições**.

Na janela **Proteção na web** clique nos interruptores para ativar ou desativar:

- A prevenção contra ataques da web bloqueia ameaças provenientes da internet, incluindo downloads não autorizados.
- Consultor de pesquisa, um componente que qualifica os resultados do seu motor de pesquisa e dos links colocados nos websites das redes sociais ao colocar um icone ao lado de cada resultado:

Não deve visitar esta página da web.

Esta página web pode conter conteúdo perigoso. Tenha cuidado se decidir visitá-lo.

Esta é uma página segura de visitar.

O Consultor de Pesquisa qualifica os resultados da pesquisa dos seguintes motores de busca:

- Google
- Yahoo!
- Bing
- Baidu

O Consultor de Pesquisa classifica os links publicados nos seguintes serviços das redes sociais:

- Facebook
- 123

- Encrypted web scan.
  Ataques mais sofisticados podem usar tráfego da web seguro para enganar as suas vítimas. Logo, recomendamos que mantenha ativa a opção Análise da web encriptada.
- Proteção antifraude.
- Proteção Phishing.

Role para baixo e chegará à seção **Prevenção de ameaças em rede**. Aqui tem a opção **Prevenção de ameaças em rede**. Para manter o seu dispositivo longe de ataques feitos por malware complexos (como ransomware) através da exploração de vulnerabilidades, mantenha a opção ativada.

Pode criar uma lista de sites, domínios e endereços de IP que não serão analisados pelos mecanismos antiameaça, antiphishing e antifraude da Bitdefender. A lista deve conter apenas sites, domínios e endereços de IP nos quais confia plenamente.

Para configurar e gerir sites, domínios e endereços de IP utilizando a Prevenção Contra Ameaças Online fornecida pelo Bitdefender:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.

2. No **PREVENÇÃO DE AMEAÇAS ONLINE** painel, clique **Configurações**.
3. Clique em **Gerir exceções**.
4. Clique **+Adicionar uma exceção**.
5. No campo correspondente, escreva o nome do site, do domínio ou do endereço IP que deseja adicionar às excepções.
6. Clique no botão ao lado de **Prevenção de Ameaças Online**.
7. Para remover uma entrada da lista, clique no botão botão ao lado dele.
   Clique **Salvar** para salvar as alterações e fechar a janela.

Alertas do Bitdefender no navegador

Sempre que tenta visitar uma página Web classificada como insegura, esta é bloqueada e é apresentada uma página de aviso no seu navegador.

A página contém informações como a URL do site web e a ameaça detetada.

Tem de decidir o que fazer a seguir. Estão disponíveis as seguintes opções:

- Voltar ao site ao clicar em **VOLTAR À SEGURANÇA**.
- Seguir para o site Web, apesar do alerta, clicando em **Compreendo os riscos, continuar mesmo assim**.
- Se tem certeza de que o site detectado é seguro, clique em **ENVIAR** para adicioná-lo às exceções. Recomendamos apenas sites nos quais confia plenamente.

3.2.4. Antispam

Spam é o termo utilizado para descrever mensagens eletrónicas não solicitadas. O Spam é um problema crescente, tanto para indíviduos como para organizações. Não é bonito, não desejaria que os seus filhos o vissem, pode fazer com que seja despedido (por desperdiçar muito tempo, ou por receber pornografia no seu mail de trabalho) e não pode impedir que as pessoas o enviem. O melhor a fazer para impedir isso, é, obviamente, parar de o receber. Infelizmente, o Spam vem em muitos formatos e feitios, e é muito abundante.

O BitDefender Antispam emprega inovações tecnológicas surpreendentes e um conjunto de filtros de antispam standard para limpar o spam antes

de o mesmo chegar à caixa de correio A receber do utilizador. Para mais informação, dirija-se a Compreender o Antispam (página 51).

A proteção Bitdefender Antispam está disponível apenas para clientes de e-mail definidos para receber mensagens através do protocolo POP3. POP3 é um dos protocolos mais amplamente utilizados para fazer a transferência de mensagens através de um servidor de e-mail.

> **Observação**
> O Bitdefender não proporciona proteção antispam para contas de correio eletrónico a que acede através de sites Internet (webmail).

As mensagens de spam detetadas pelo Bitdefender são marcadas com o prefixo [spam] na linha do assunto. O Bitdefender move automaticamente as mensagens de spam para uma pasta específica, da seguinte forma:

- No Microsoft Outlook, as mensagens de spam são movidas para a pasta **Spam**, localizada na pasta **Itens Eliminados**. A pasta **Spam** fé criada quando um e-mail é indicado como spam.
- No Mozilla Thunderbird, as mensagens de spam são movidas para uma pasta de **Spam**, localizada no **Lixo**. A pasta de **Spam** é criada quando um e-mail é rotulado como spam.

Se utilizar outros clientes de e-mail, deve criar uma regra para mover as mensagens de e-mail marcadas pelo Bitdefender como [spam] para uma pasta de quarentena personalizada. Se os itens Excluídos ou os ficheiros do Lixo forem eliminados, a pasta de spam também será eliminada. No entanto, será criada uma nova pasta de spam assim que um e-mail for rotulado como spam.

Compreender o Antispam

A função antispam tem as seguintes funções e definições:

Filtros impeditivos da entrada de mails indesejados

O Bitdefender Antispam Engine incorpora proteção de nuvem e vários outros filtros diferentes que asseguram que a sua Caixa de Entrada esteja livre de SPAM, com a sua **Lista de amigos**, **Lista de spammers** e **Filtro charset**.

Lista de Amigos / Lista de Spammers

A maioria das pessoas comunica regularmente com um grupo de pessoas, ou até mesmo recebe mensagens de empresas ou organizações

no mesmo domínio. Ao utilizar as **listas de amigos ou spammers**, pode facilmente decidir de quem pretende receber e-mails (amigos) independentemente do conteúdo das mensagens, ou de quem nem sequer pretende ouvir falar novamente (spammers).

> **Observação**
> Recomendamos que adicone os nomes e endereços de e-mail dos seus amigos à **Lista de Amigos**. O BitDefender não bloqueia mensagens das pessoas dessa lista; logo, adicionar amigos ajuda a que as mensagens legítimas cheguem a si.

Filtro caracteres

A maioria das mensagens Spam é escrita em caracteres Cirílicos e/ou Asiáticos. O filtro de Caracteres deteta este tipo de mensagens e marca-as como SPAM.

Operação Antispam

O Bitdefender Antispam Engine utiliza todos os filtros antispam combinados para determinar se uma mensagem de e-mail deve entrar em sua **Caixa de Entrada** ou não.

Todos os e-mails vindos da Internet são verificados em primeiro lugar com o filtro **Lista de amigos** / **Lista de remetentes de spam**. Se o endereço do remetente for encontrado na **Lista de amigos**, o e-mail é movido diretamente para a sua **Caixa de entrada**.

Caso contrário, o filtro da **Lista de Spammers** irá apoderar-se do seu correio electrónico para verificar se o endereço do remetente se encontra na lista. Se for encontrada uma correspondência, a mensagem será marcada como SPAM e movida para a pasta de **Spam**.

Ainda, o **Filtro caracteres** irá verificar se o e-mail está escrito em caracteres Cirílicos ou Asiáticos. Se assim for, e-mail será marcado com Indesejado e movido para a pasta de **Spam**.

> **Observação**
> Se o email é marcado como SEXUALLY EXPLICIT na linha do assunto, o Bitdefender vai considerá-lo SPAM.

Clientes de email e protocolos suportados

A proteção Antispam é fornecida para todos os clientes de e-mail POP3/SMTP. No entanto a barra de ferramentas do Antispam BitDefender apenas se integra em:

- Microsoft Outlook 2007 / 2010 / 2013 / 2016 / 2019
- Mozilla Thunderbird 14 e as versões superiores

Ligar ou desligar a proteção antispam

A proteção AntiSpam está ativada por defeito.

Para ligar ou desligar a ferramenta Antispam:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No painel **ANTISPAM**, ative ou desative o botão.

Utilizar a barra de ferramentas Antispam na janela do seu cliente de email

No lado superior da janela do seu cliente de mail pode ver a barra de ferramentas do Antispam. A barra de ferramentas do Antispam ajuda-o a gerir a proteção antispam diretamente do seu cliente de e-mail. Pode facilmente corrigir o BitDefender se ele marcar uma mensagem legítima como SPAM.

> **Importante**
> O BiDefender integra uma barra antispam de facil utilização, nos clientes de email mais comuns. Para ver a lista completa de clientes de e-mail suportados, por favor consulte o Clientes de email e protocolos suportados (página 53).

Cada botão é explicado abaixo:

Definições - abre uma janela onde pode configurar os filtros antispam e as definições na barra de ferramentas.

É spam - indica que o e-mail selecionado é spam. O e-mail será movido imediatamente para a pasta de **spam**. Se os serviços de antispam em cloud forem ativados, a mensagem é enviada para o Bitdefender Cloud para uma análise mais aprofundada.

Não é spam - indica que o e-mail selecionado não é um spam e o Bitdefender não deveria tê-lo marcado. O e-mail será movido da pasta de

spam para a **Caixa de Entrada**. Se os serviços antispam em nuvem forem ativados, a mensagem é enviada para a Nuvem da Bitdefender para uma análise mais aprofundada.

> **Importante**
> O botão **Não é spam** é ativado quando seleciona uma mensagem marcada pelo Bitdefender como SPAM (normalmente estas mensagens estão localizadas na pasta de **spam**).

Adicionar spammer - adiciona o remetente do e-mail selecionado à Lista de spammers. Talvez tenha que clicar em **OK** para confirmar. As mensagens de e-mail recebidas dos endereços da Lista de spammers são automaticamente marcadas como [spam].

Adicionar amigo - adiciona o remetente do e-mail selecionado à Lista de amigos. Talvez tenha que clicar em **OK** para confirmar. Irá receber sempre as mensagens que venham deste endereço de e-mail, independentemente do seu conteúdo.

Remetentes de spam - abre a **Lista de remetentes de spam** que contém todos os endereços de e-mail dos quais não deseja receber mensagens, independentemente do seu conteúdo. Para mais informações, consulte Configurar a lista de Spammers (página 57).

Amigos - abre a **Lista de amigos** que contém todos os endereços de e-mail dos quais deseja sempre receber as mensagens, independentemente do seu conteúdo. Para mais informações, consulte Configurar a Lista de Amigos (página 56).

Indicar os erros de deteção

Caso esteja a utilizar um cliente de e-mail suportado, pode facilmente corrigir o filtro antispam (indicando quais mensagens de e-mail não deveriam ter sido marcadas como [spam]). Ao fazer isso, ajuda a melhorar a eficiência do filtro antispam. Siga estes passos:

1. Abra o mail de cliente.
2. Vá à pasta de lixo eletrónico, para onde são movidas as mensagens.
3. Selecione a mensagem incorretamente marcada como [spam] pelo Bitdefender.
4. Clique no botão **Adicionar amigo**, na barra de ferramentas antispam do Bitdefender, para adicionar o remetente à Lista de

amigos. Poderá ter de clicar em **OK** para confirmar. Irá sempre receber as mensagens que venham deste endereço de e-mail, independentemente do seu conteúdo.

5. Clique no botão **Não Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de mail do cliente). A mensagem de email será movida para a pasta de Entrada.

Indicar mensagens de spam não detetadas

Se estiver a utilizar um cliente de e-mail suportado, pode facilmente indicar quais as mensagens de e-mail que devem ser detectadas como spam. Se o fizer, ajuda a melhorar a eficiência do filtro antispam. Siga os seguintes passos:

1. Abra seu cliente de e-mail.
2. Vá à pasta Caixa de Entrada.
3. Selecione as mensagens spam não detetadas
4. Clique no botão **É spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela do cliente de e-mail). As mensagens serão marcadas imediatamente como [spam] e movidas para a pasta de e-mails de lixo.

Configurar definições da barra de ferramentas

Para configurar a barra de ferramentas antispam para o seu cliente de e-mail, clique no botão **Definições** na barra de ferramentas e, em seguida, no separador **Definições da barra de ferramentas**.

Tem as seguintes opções:

- **Marque as mensagens de e-mail indesejadas como 'ler'** - marca as mensagens indesejadas como ler automaticamente, para que não seja perturbador quando chegarem.
- Pode escolher se deseja ou não mostrar as janelas de confirmação ao clicar nos botões **Adicionar spammer** e **Adicionar amigo**, na barra de ferramentas antispam.
  As janelas de confirmação pode evitar a adição acidental de destinatários de email à lista de Amigos / Spammers.

Configurar a Lista de Amigos

A **Lista de Amigos** é uma lista de todos os endereços de e-mail dos quais deseja sempre receber mensagens, independentemente do seu conteúdo. As mensagens dos seus amigos não são marcadas como spam, mesmo que o conteúdo se assemelhe a spam.

> **Observação**
> Qualquer mail proveniente de um endereço presente na **Lista de amigos**, será automaticamente entregue na sua Caixa de Entrada, sem mais demora.

Para configurar e gerir a lista de Amigos:

- Se estiver a utilizar o Microsoft Outlook ou o Thunderbird, clique no botão Amigos na **barra de ferramentas do Bitdefender antispam**.
- Alternativa:
  1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
  2. No painel **ANTISPAM**, clique em **Definições**.
  3. Aceda à janela **Gerir amigos**.

Para adicionar um endereço de e-mail, selecione a opção **Endereço de e-mail**, introduza o endereço e clique em **ADICIONAR**. Sintaxe: nome@domain.com.

Para adicionar todos os endereços de e-mail de um domínio específico, selecione a opção **Nome do domínio**, insira o nome do domínio e clique em **ADICIONAR**. Sintaxe:

- @domain.come domain.com - todas as mensagens de e-mail recebidas de domain.com chegarão à sua **Caixa de entrada** independentemente do seu conteúdo;
- dominio - todos os mails provenientes de dominio (independentemente dos sufixos de domínio) serão marcados como INDESEJADOS;
- com - todos os mails tendo o sufixo de domínio com serão marcados como INDESEJADOS;

É recomendado que evite adicionar domínios completos, mas isto poderá ser útil em algumas situações. Por exemplo, pode adicionar o domínio do

endereço eletrónico da empresa para a qual trabalha ou de parceiros de confiança.

Para eliminar um item da lista, clique no botão correspondente ao lado. Para eliminar todas as entradas da lista, clique em **Limpar lista**.

Pode guardar a lista de Amigos num ficheiro para que mais tarde possa utilizá-lo noutro dispositivo ou quando reinstalar o produto. Para guarda a lista de Amigos, clique no botão Guardar e guarda no local desejado. O ficheiro terá a extensão .bwl

Para carregar uma lista de Amigos guardada anteriormente, clique em **Carregar** e abra o ficheiro .bwl correspondente. Para restabelecer o conteúdo da lista existente ao carregar uma lista previamente guardada, marque a caixa ao lado de **Sobrescrever lista atual**.

Configurar a lista de Spammers

A **Lista de indesejados** é uma lista de todos os endereços de e-mail, dos quais nunca pretende receber mensagens, independentemente do seu conteúdo. Todo o mail proveniente de um endereço presente na **Lista de indesejados**, será marcado automaticamente com indesejado, sem mais demora.

Para configurar e gerir a lista de Spammers:

- Se estiver a utilizar o Microsoft Outlook ou o Thunderbird, clique no botão **Remetentes de spam** na **barra de ferramentas antispam do Bitdefender** integrada ao seu cliente de e-mail.
- Alternativamente:
  1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
  2. No **ANTISPAM** painel, clique **Configurações**.
  3. Aceda à janela **Gerir Spammers**.

Para adicionar um endereço de e-mail, selecione o **Endereço de email** opção, insira o endereço e clique em **ADICIONAR**. Sintaxe: nome@dominio.com.

Para adicionar todos os endereços de e-mail de um domínio específico, selecione o **Nome do domínio** opção, insira o nome de domínio e clique em **ADICIONAR**. Sintaxe:

- @domain.comand domain.com - todas as mensagens de e-mail recebidas de domain.com chegarão à sua **Caixa de Entrada** independentemente de seu conteúdo;
- domínio - todas as mensagens de e-mail recebidas do domínio (independentemente dos sufixos do domínio) serão marcadas como SPAM;
- com - todos os mails tendo o sufixo de domínio com serão marcados como INDESEJADOS.

É recomendado que evite adicionar domínios completos, mas isto poderá ser útil em algumas situações.

> **Aviso**
> Não adicione domínios de serviços de e-mail legítimos da web (como o Yahoo, o Gmail, o Hotmail ou outros) à Lista de remetentes de spam. Se o fizer, as mensagens de e-mail recebidas de utilizadores registados em qualquer um destes serviços serão detetadas como spam. Se, por exemplo, adicionar **yahoo.com** à Lista de remetentes de spam, todas as mensagens de e-mail provenientes de endereços **yahoo.com** serão marcadas como [spam].

Para excluir um item da lista, clique no ícone correspondente botão ao lado dele. Para excluir todas as entradas da lista, clique em **Limpar lista**.

Pode guardar a lista de Spammers num ficheiro para que mais tarde possa utilizá-lo noutro dispositivo ou quando reinstalar o produto. Para guarda a lista de Spam, clique no botão **Guardar** e guarda no local desejado. O ficheiro terá a extensão .bwl

Para carregar uma lista de Spammers previamente guardada, clique em **CARREGAR** e abra o ficheiro .bwl correspondente. Para repor o conteúdo da lista existente ao carregar uma lista guardada anteriormente, selecione Sobrescrever lista atual.

A configurar os filtros locais Antispam

Como descrito em Compreender o Antispam (página 51), o Bitdefender utiliza um conjunto de diferentes filtros antispam para identificar o spam. Os filtros antispam são pré-configurados para uma proteção eficaz.

Importante

Dependendo se recebe ou não mensagens eletrónicas fiáveis ou não escrita com caracteres asiáticos ou cirílicos, desative ou ative a definição que bloqueia automaticamente estas mensagens. A respetiva definição está desativada nas versões localizadas do programa que utilizam conjuntos de caracteres (por exemplo, na versão russa ou chinesa).

Para configurar os filtros locais antispam:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTISPAM** painel, clique **Configurações**.
3. Vá para a janela **Definições** e clique nos interruptores ligar/desligar correspondentes.

Se estiver utilizar o Microsoft Outlook ou Thunderbird, pode configurar os filtros antispam locais diretamente no seu cliente de e-mail. Clique no botão **Definições** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela do cliente de e-mail) e depois, na aba **Filtros antispam**.

Configurar as definições da nuvem

A deteção em nuvem utiliza os serviços da Nuvem da Bitdefender para lhe proporcionar uma proteção antispam eficiente e sempre atualizada.

A proteção em nuvem funciona desde que mantenha o Bitdefender Antispam ativado.

Amostras de spam ou de e-mails legítimos podem ser enviados à Nuvem da Bitdefender quando indicar erros de deteção ou e-mails de spam não detetados. Isto ajuda a aprimorar a deteção do Bitdefender antispam.

Configure o envio de amostras de e-mail para a Nuvem da Bitdefender ao selecionar as opções desejadas nos passos a seguir:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTISPAM** painel, clique **Configurações**.
3. Vou ao **Configurações** janela e clique nos interruptores de ligar ou desligar correspondentes.

Se estiver a utilizar o Microsoft Outlook ou o Thunderbird, pode configurar a deteção por nuvem diretamente no seu cliente de e-mail. Clique no

botão **Definições** na barra de ferramentas do Bitdefender Antispam (normalmente localizada na parte superior da janela do cliente de e-mail) e, em seguida, no separador **Definições da nuvem**.

3.2.5. Firewall

O Firewall protege o seu dispositivo contra tentativas de ligação não autorizadas de entrada e saída, tanto em redes locais quanto na internet. É muito semelhante a um guarda no portão - ele controla as tentativas de ligação e decide quais permitir e quais bloquear.

O firewall da Bitdefender utiliza um conjunto de regras para filtrar os dados transmitidos de e para o seu sistema.

Em condições normais, o Bitdefender cria automaticamente uma regra sempre que uma aplicação tenta aceder à internet. Também pode adicionar ou editar manualmente as regras para as aplicações.

Como medida de segurança, será notificado sempre que uma aplicação potencialmente maliciosa for bloqueada de aceder à internet.

O Bitdefender atribui automaticamente um tipo de rede a cada ligação de rede detetada. Dependendo do tipo de rede, a proteção do firewall é definida para o nível apropriado para cada ligação.

Para saber mais sobre as definições de firewall para cada tipo de rede e como pode editar as definições de rede, consulte Gerir definições da ligação (página 63).

Ativação ou desativação da proteção do firewall

Para ativar ou desativar a proteção do firewall:

1. Clique em **Proteção** no menu de navegação da interface Bitdefender.
2. No painel **FIREWALL**, ative ou desative a chave.

> **Aviso**
> Como isto expõe o seu dispositivo a ligações não autorizadas, a desativação do firewall deve ser apenas uma medida temporária. Ative o firewall novamente assim que possível.

Gerir regras de aplicações

Para visualizar e gerir as regras da firewall de controlo do acesso a aplicações a recursos da rede e à Internet:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No painel **FIREWALL**, clique em **Definições**.
3. Vá para a janela **Acesso à aplicação**.

Poderá ver os últimos programas (processos) que passaram pelo Bitdefender Firewall e a rede de internet à qual está ligado. Para ver as regras criadas para uma aplicação específica, basta clicar nela e depois clicar no link **Ver regras da aplicação**. A janela **Regras** abrirá.

Para cada regra é apresentada a seguinte informação:

- **REDE** - o processo e os tipos de adaptador de rede (doméstico/escritório, público ou todos) aos quais a rede se aplica. As regras são automaticamente criadas para filtrar o acesso à rede ou à Internet através de qualquer adaptador. Por defeito, as regras aplicam-se a qualquer rede. Pode criar manualmente as regras ou editar as regras existentes para filtrar o acesso à rede ou à Internet de uma aplicação através de um determinado adaptador (por exemplo, um adaptador de rede wireless).
- **PROTOCOLO** - o protocolo IP ao qual a regra se aplica. Por defeito, as regras aplicam-se a qualquer protocolo.
- **TRÁFEGO** - a regra aplica-se em ambas as direções, entrada e saída.
- **PORTAS** - o protocolo PORTA ao qual a regra se aplica. Por predefinição, as regras aplicam-se a todas as portas.
- **IP** - o protocolo Internet (IP) ao qual a regra se aplica. Por predefinição, as regras aplicam-se a qualquer endereço IP.
- **ACESSO** - se a aplicação permite ou recusa acesso à rede ou Internet em circunstâncias específicas.

Para editar ou excluir as regras da aplicação selecionada, clique no ícone ⋯.

- **Editar regra** - abre uma janela onde é possível editar a regra atual.
- **Eliminar regra** - é possível optar por remover o conjunto de regras atual para a aplicação selecionada.

A adicionar regras de aplicações

Para adicionar uma regra de aplicação:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **FIREWALL** painel, clique **Configurações**.
3. Na janela **Regras**, clique em **Adicionar regra**.

Aqui pode aplicar as seguintes mudanças:

- **Aplique esta regra a todas as aplicações.** Ative este botão para aplicar a regra criada a todas as aplicações.
- **Caminho do programa.** Clique em **PROCURAR** e selecione a aplicação à qual a regra se aplica.
- **Permissão.** Selecione uma das permissões disponíveis:

Permissão	Descrição
Permitir	À aplicação especificada será permitido o acesso à rede / Internet nas circunstâncias determinadas.
Negar	À aplicação especificada será negado o acesso à rede / Internet nas circunstâncias determinadas.

- **Tipo de rede**. Selecione o tipo de rede à qual a regra se aplica. Pode alterar o tipo ao abrir o menu suspenso **Tipo de rede** e ao selecionar um dos tipos disponíveis a partir da lista.

Tipo de rede	Descrição
Qualquer rede	Permite todo o tráfego entre o seu dispositivo e outros dispositivos independentemente do tipo de rede.
Casa/Escritório	Permitir todo o tráfego entre o seu dispositivo e outros diferentes na rede local.
Pública	Todo o tráfego é filtrado.

- **Protocolo.** Selecione o protocolo IP ao qual a regra se aplica a partir do menu.
  - Se deseja que a regra se aplique a todos os protocolos, selecione **Todos**.
  - Se deseja que a regra se aplique ao TCP, selecione **TCP**.
  - Se deseja que a regra se aplique ao UDP, selecione **UDP**.
  - Se pretender que a regra se aplique a ICMP, selecione **ICMP**.
  - Se pretender que a regra se aplique a IGMP, selecione **IGMP**.

- Se deseja que a regra se aplique ao GRE, selecione **GRE**.
- Se quiser que a regra se aplique num protocolo específico, introduza o número atribuído ao protocolo que quiser filtrar no campo de edição em branco.

> **Observação**
> Os números de protocolo IP são atribuídos pela Internet Assigned Numbers Authority (IANA). Poderá encontrar a lista completa dos números de protocolo IP atribuídos em http://www.iana.org/assignments/protocol-numbers.

- **Direção.** Selecione a direção do tráfego à qual a regra se aplica a partir do menu.

Direção	Descrição
Saída	A regra aplica-se apenas ao tráfego de saída.
Entrada	A regra aplica-se apenas ao tráfego de entrada.
Ambos	A regra aplica-se em ambos os sentidos.

Clique no botão **Definições avançadas** na parte inferior da janela para personalizar as seguintes definições:

- **Endereço local personalizado.** Especifique o endereço IP local e a porta à qual a regra se aplica.
- **Endereço remoto personalizado.** Especifique o endereço IP remoto e a porta à qual a regra se aplica.

Para remover o atual conjunto de regras e restaurar as regras padrão, clique em **Redefinir regras** na janela **Regras**.

Gerir definições da ligação

Independentemente de se ligar à Internet por Wi-Fi ou adaptador Ethernet, pode configurar as definições que devem ser aplicadas para uma navegação segura. As opções disponíveis são:

- **Dinâmica** – o tipo de rede será definido automaticamente com base no perfil da rede ligada, doméstica/escritório ou pública. Quando isto acontece, só serão aplicadas as regras de firewall do tipo de rede específica ou as definidas para se aplicarem a todos so tipos de rede.
- **Doméstica/escritório** – o tipo de rede será sempre doméstica/escritório, independentemente do perfil da rede ligada. Quando isto

acontece, só serão aplicadas as regras de firewall para doméstica/escritório ou as definidas para se aplicarem a todos so tipos de rede.

- **Pública** – o tipo de rede será sempre pública, independentemente do perfil da rede ligada. Quando isto acontece, só serão aplicadas as regras de firewall para pública ou as definidas para se aplicarem a todos so tipos de rede.

Para configurar os adaptadores de rede:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **FIREWALL** painel, clique **Configurações**.
3. Selecione a janela **Adaptadores de rede**.
4. Selecione as definições que pretende aplicar ao estabelecer ligação com os seguintes adaptadores:
   - Wi-Fi
   - Ethernet

Configurar definições avançadas

Para definições avançadas da firewall:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **FIREWALL** painel, clique **Configurações**.
3. Selecione os **Configurações** janela.

É possível configurar as seguintes funcionalidades:

- **Proteção de verificação de porta** - detecta e bloqueia tentativas de descobrir quais portas estão abertas.
  Os scans de portas são frequentemente utilizados pelos hackers para descobrir que portas se encontram abertas no seu dispositivo. Então eles poderão entrar no seu dispositivo se descobrirem uma porta menos segura ou vulnerável.
- **Modo de alerta** - os alertas são exibidos sempre que uma aplicação tenta ligar-se à Internet. Selecione **Permitir** ou **Bloquear**. Quando o Modo de alerta está ativo, a função **Perfis** é desligada automaticamente. O Modo de alerta pode ser utilizado em simultâneo com o **Modo de bateria**.

- **Permitir acesso à rede do domínio** - aceite ou negue o acesso a recursos e itens compartilhados definidos pelos seus controladores de domínio.
- **Modo Invisível** - para não ser detetado por outros dispositivos. Clique em **Editar definições sigilosas** para escolher quando o seu dispositivo deve ou não ficar visível para outros dispositivos.
- **Comportamento predefinido da aplicação** - permite que o Bitdefender aplique definições automáticas às aplicações sem regras definidas. Clique em **Editar regras predefinidas** para escolher se as definições automáticas devem ser aplicadas ou não.
  - Automático - o acesso a aplicações será permitido ou recusado com base nas regras automáticas de firewall e utilizadores.
  - Permitir - as aplicações que não têm qualquer regra de firewall definidas serão permitidas automaticamente.
  - Bloquear - as aplicações que não têm qualquer regra de firewall definidas serão bloqueadas automaticamente.

3.2.6. Vulnerabilidade

Um passo importante na proteção do seu dispositivo contra as ações e aplicações maliciosas é manter atualizado o seu sistema operativo e as aplicações que utiliza regularmente. Além disso, para evitar o acesso físico não autorizado ao seu dispositivo, palavras-passe fortes (palavras-passe que não são facilmente descobertas) devem ser configuradas para cada conta de utilizador do Windows e também para as redes Wi-Fi às quais se liga.

O Bitdefender proporcionar duas formas fáceis de resolver as vulnerabilidades do seu sistema:

- Pode analisar o seu sistema por vulnerabilidades e repará-las passo a passo com a opção **Análise de Vulnerabilidades**.
- Utilizando a monitorização automática de vulnerabilidades, pode verificar e reparar as vulnerabilidades detetadas na janela **Notificações**.

Deve verificar e resolver as vulnerabilidades do sistema semanal ou quinzenalmente.

Procurar vulnerabilidades no seu sistema

Para detectar vulnerabilidades, o Bitdefender requer uma ligação ativa à internet.

Para analisar o seu sistema em busca de vulnerabilidades:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Abrir**.
3. Na aba **Verificação de vulnerabilidades**, clique em **Iniciar verificação** e então, aguarde que o Bitdefender verifique o seu sistema à procura de vulnerabilidades. As vulnerabilidades detetadas são agrupadas em três categorias:

   - **SISTEMA OPERACIONAL**

     - **Segurança do Sistema Operativo**
       Definições de sistema alteradas que podem comprometer o seu dispositivo e dados, como não exibir avisos quando ficheiros executados realizam alterações no seu sistema sem a sua permissão ou quando dispositivos MTP como telefones ou câmaras se conectam e executam operações diferentes sem o seu conhecimento.

     - **Atualizações críticas do Windows**
       Será mostrada uma lista de atualizações importantes para o Windows que não estão instaladas no seu sistema. Talvez seja preciso reiniciar o sistema para a Bitdefender finalizar a instalação. As atualizações podem demorar a serem instaladas.

     - **Contas do Windows fracas**
       Pode ver a lista dos utilizadores de contas Windows configurados no seu dispositivo e o nível de proteção que as suas palavras-passe garantem. Pode escolher entre pedir ao utilizador para alterar a palavra-passe da próxima vez que iniciar sessão ou o próprio alterar a palavra-passe imediatamente. Para definir uma nova palavra-passe para o seu sistema, selecione **Definir a palavra-passe agora**.
       Para criar uma palavra-passe segura, recomendamos a utilização de uma combinação de maiúsculas e minúsculas, números e caracteres especiais (como #, $ ou @).

- **APLICAÇÕES**
  - **Segurança do navegador**
    Altere as definições do seu dispositivo que permitem a execução de ficheiros e programas transferidos pelo Internet Explorer sem uma validação de integridade, o que pode levar ao comprometimento do seu dispositivo.
  - **Atualizações da aplicação**
    Para visualizar informação sobre a aplicação que precisa de ser atualizada, clique no nome dela na lista.
    Caso uma aplicação não esteja atualizada, clique na ligação **Transferir nova versão** para transferir a última versão.
- **REDE**
  - **Rede e credenciais**
    A alteração das definições do sistema, como a ligação automática a redes de hotspot abertas sem o seu conhecimento ou a não encriptação do tráfego de saída de canal seguro.
  - **Routers e redes Wi-Fi**
    Para obter mais informação sobre a rede Wi-Fi e o router ao qual está ligado, clique no seu nome da lista. Se receber uma recomendação para definir uma palavra-passe mais forte para a sua rede doméstica, siga as nossas instruções para continuar conectado sem se preocupar com a sua privacidade.
    Quando outras recomendações estiverem disponíveis, siga as instruções fornecidas para garantir que a rede da sua casa fica protegida contra hackers.

Usar monitorização de vulnerabilidade automática

O Bitdefender verifica o seu sistema quanto a vulnerabilidades regularmente, em segundo plano, e mantém os registos de problemas detetados na janela **Notificações**.

Para verificar e reparar os problemas detetados:

1. Clique **Notificações** no menu de navegação do Interface do Bitdefender.

2. No separador **Todas**, selecione a notificação referente à verificação de vulnerabilidades.
3. Pode ver a informação detalhada sobre as vulnerabilidades do sistema detetadas. Dependendo da incidencia, para reparar uma vulnerabilidade específica proceda da seguinte forma:
   - Se estiverem disponíveis atualizações para o Windows, clique em **Instalar**.
   - Se as atualizações automáticas do Windows estiverem desativadas, clique em **Ativar**.
   - Se uma aplicação estiver desatualizada, clique em **Atualizar agora** para obter a hiperligação para a página de Internet do fornecedor a partir da qual pode instalar a versão mais recente dessa aplicação.
   - Se uma conta de utilizador do Windows tiver uma palavra-passe fraca, clique em **Alterar palavra-passe** para obrigar o utilizador a mudar a palavra-passe no próximo início de sessão ou alterá-la por si mesmo. Para obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).
   - Se a funcionalidade de Execução Automática do Windows estiver ativada, clique em **Reparar** para a desativar.
   - Se o router que tem configurado tiver uma palavra-passe fraca, clique em **Alterar palavra-passe** para aceder à sua interface a partir da qual é possível definir uma palavra-passe forte.
   - Se a rede à qual está ligado apresentar vulnerabilidades que possam expor o seu sistema a riscos, clique em **Alterar definições de WI-FI**.

Para configurar as definições de monitorização de vulnerabilidades:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **VULNERABILIDADE** painel, clique **Abrir**.

> **Importante**
> Para ser notificado automaticamente sobre vulnerabilidades no sistema ou nas aplicações, mantenha a opção **Vulnerabilidade** ativada.

3. Vá para o separador **Definições**.
4. Escolha as vulnerabilidades do sistema que deseja que sejam regularmente verificadas usando os botões correspondentes.

   atualizações do Windows

   Verifique se o seu sistema operativo Windows possui as mais recentes e importantes atualizações de segurança da Microsoft.

   Atualizações de aplicativos

   Verifique se as aplicações instaladas no seu sistema estão atualizadas. As aplicações desatualizadas podem ser exploradas por software malicioso, tornando o PC vulnerável a ataques externos.

   Palavras-passa do utilizador

   Verifique se as palavras-passe dos routers e contas Windows configuradas no sistema são fáceis de descobrir ou não. A definição de palavras-passe difíceis de descobrir (palavras-passe fortes) torna muito difícil a invasão do seu sistema pelos hackers. Uma palavra-passe forte inclui maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

   Reprodução automática

   Verifique o estado do recurso Windows Autorun. Esta característica permite que as aplicações se iniciem automaticamente a partir dos CDs, DVDs, drives USB ou outros dispositivos externos.

   Alguns tipos de ameaças utilizam Autorun para se propagar automaticamente dos suportes multimédia removíveis do PC. Por isso, recomenda-se a desactivação desta janela.

   Consultor de Segurança do Wi-Fi

   Verifique se a rede doméstica sem fios à qual está ligado é segura ou não e se tem vulnerabilidades. Além disso, verifique se a palavra-passe do seu router doméstico é suficientemente e se pode torná-la mais segura.

   A maioria das redes não protegidas não são seguras, permitindo o fácil acesso de hackers às suas atividades privadas.

   Observação

   Se desativar a monitorização de uma vulnerabilidade específica, os problemas relacionados não serão mais registados na janela de notificações.

Consultor Segurança Wi-Fi

Enquanto caminha, trabalha num café ou aguarda no aeroporto, ligar-se a uma rede pública sem fios para realizar pagamentos, verificar e-mails ou aceder às contas de redes sociais pode ser a solução mais rápida. Enquanto isso, pessoas curiosas tentam roubar os seus dados pessoais vendo como as informações fluem ao longo da rede.

Dados pessoais consistem em palavras-passe e nomes de utilizadores que utilizar para aceder às suas contas online, tais como e-mails, contas bancárias, contas de redes sociais, mas também mensagens enviadas por si.

Geralmente, as redes públicas sem fios tendem a ser menos seguras uma vez que não necessitam de qualquer palavra-passe para efetuar a ligação ou, caso seja necessária uma palavra-passe, esta é disponibilizada a qualquer pessoa que pretenda ligar-se. Além disso, podem ser redes maliciosas ou "honeypot", que representam um alvo para criminosos informáticos.

O Bitdefender Wi-Fi Security Advisor dá informações sobre:

- **Redes Wi-Fi domésticas**
- **Redes Wi-Fi de escritório**
- **Redes Wi-Fi públicas**

Ativar ou desativar as notificações do Consultor de Segurança Wi-Fi

Para ativar ou desativar as notificações do Consultor de Segurança Wi-Fi:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **VULNERABILIDADE** painel, clique **Abrir**.
3. Vá para a janela **Definições** e ative ou desative a opção **Wi-Fi Security Advisor**.

Configurar a rede Wi-Fi doméstica

Para começar a configurar a sua rede doméstica:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **VULNERABILIDADE** painel, clique **Abrir**.
3. Vá para a janela **Wi-Fi Security Advisor** e clique em **Wi-Fi doméstico**.

4. No separador **Wi-Fi doméstico**, clique em **SELECIONAR WI-FI DOMÉSTICO**.
   Uma lista com redes sem fios às quais já esteve ligado é agora exibida.
5. Indique a sua rede doméstica e, em seguida, clique em **SELECIONAR**.

Se uma rede doméstica for considerada insegura ou desprotegida, são exibidas as recomendações de configuração para aumentar a sua segurança.

Para remover a rede sem fios definida como rede doméstica, clique no botão **REMOVER**.

Para adicionar uma nova rede Wi-Fi como doméstica, clique em **Selecionar nova rede WI-FI doméstica**.

Configurar a rede Wi-Fi do trabalho

Para começar a configurar sua rede de escritório:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **VULNERABILIDADE** painel, clique **Abrir**.
3. Vá à janela **Wi-Fi Security Advisor** e clique em **Wi-Fi de escritório**.
4. No separador **Wi-Fi de escritório**, clique em **SELECIONAR WI-FI DE ESCRITÓRIO**.
   Uma lista com as redes sem fio às quais você se conectou até agora é exibida.
5. Aponte para a sua rede de escritório e, em seguida, clique em **SELECIONAR**.

Se uma rede de escritório for considerada desprotegida ou não segura, serão exibidas recomendações para reforçar a sua segurança.

Para remover a rede sem fios que definiu como rede de escritório, clique no botão **REMOVER**.

Para remover a rede sem fios que definiu como rede de escritório, clique no botão **Selecionar nova rede WI-FI do escritório**.

Wi-Fi público

Enquanto está ligado a uma rede sem fios insegura ou desprotegida, o perfil de Wi-Fi pública é ativado. Ao executar neste perfil, o Bitdefender

Total Security é definido automaticamente de modo a obter as seguintes definições de programa:

- Advanced Threat Defense ativado
- As seguintes definições da Prevenção contra ameaças online são ativadas:
  - Verificação de web criptografada
  - Proteção contra fraudes
  - Proteção contra phishing
- Um botão que abre o Bitdefender Safepay™ está disponível. Neste caso, a proteção de pontos de acesso para redes desprotegidas é ativada por padrão.

Verificar informações sobre redes Wi-Fi

Para verificar as informações sobre as redes sem fios a que é habitual ligar-se:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **VULNERABILIDADE** painel, clique **Abrir**.
3. Vá para a janela **Consultor de Segurança do Wi-Fi**.
4. Dependendo das informações de que precisar, selecione um dos três separadores: **Wi-Fi doméstico**, **Wi-Fi de escritório** ou **Wi-Fi público**.
5. Clique em **Visualizar detalhes** junto à rede sobre a qual pretende obter mais informações.

Existem três tipos de redes sem fios filtrados por importância, sendo cada tipo indicado com um ícone específico:

Wi-Fi inseguro - indica que o nível de segurança da rede é baixo. Ou seja, é muito arriscado usá-la e não é recomendado fazer pagamentos ou verificar contas bancárias sem uma proteção extra. Nestas situações, recomendamos usar o Bitdefender Safepay™ com a proteção para pontos de acesso de redes não seguras ativada.

Wi-Fi inseguro - indica que o nível de segurança da rede é moderado. Ou seja, pode ter vulnerabilidades e não é recomendado fazer pagamentos nem conferir contas bancárias sem proteção adicional. Em

situações do género, recomendamos utilizar o Bitdefender Safepay™ com a proteção para pontos de acesso de redes não seguras ativada.

Wi-Fi seguro - indica que a rede que está a utilizar é segura. Neste caso, pode usar dados confidenciais para fazer operações online.

Ao clicar na ligação **Ver detalhes** na área de cada rede, são apresentados os seguintes detalhes:

- **Segura** - onde pode ver se a rede selecionada está segura ou não. As redes não encriptadas podem deixar os seus dados expostos.
- **Tipo de encriptação** - aqui pode visualizar o tipo de encriptação utilizado pela rede selecionada. Alguns tipos de encriptação podem não ser seguros. Assim, recomendamos vivamente verificar as informações sobre o tipo de encriptação exibido para garantir que está protegido ao navegar na Web.
- **Canal/Frequência** - aqui pode visualizar a frequência do canal utilizada pela rede selecionada.
- **Força da palavra-passe** - aqui pode visualizar a força da palavra-passe. Observe que as redes que têm palavras-passe fracas definidas representam um alvo para os cibernautas criminosos.
- **Tipo de início de sessão** - aqui pode visualizar se a rede selecionada está ou não protegida com uma palavra-passe. É altamente recomendado ligar-se apenas a redes que possuem palavras-passe fortes definidas.
- **Tipo de autenticação** - aqui pode visualizar o tipo de autenticação utilizado pela rede selecionada.

3.2.7. Proteção de Audio & Vídeo

Cada vez mais ameaças são criadas para aceder às webcams e microfones acoplados. Para evitar o acesso não autorizado à sua webcam e para informá-lo quais as aplicações não confiáveis que têm acesso ao microfone do seu dispositivo e quando, o Bitdefender Video & Audio incluiu:

- {1}Proteção da webcam{2}
- {1}Monitor de Microfone{2}

Proteção da Webcam

O facto de os hackers podem assumir o controlo da sua webcam para espiá-lo já não é uma novidade e as soluções para protegê-la, como a retirada de privilégios de aplicações, desativar a câmara incorporada do dispositivo ou cobri-la não são muito práticas. Para evitar novas tentativas de acesso à sua privacidade, o Bitdefender Webcam Protection monitoriza permanentemente as aplicações que tentam aceder à sua câmara e bloqueia as que não estão listadas como fidedignas.

Como uma medida de segurança, será notificado sempre que uma aplicação não fiável tentar ganhar acesso à sua câmara.

Ativar ou desativar a Proteção da Câmara Web

1. Clique em **Privacidade** no menu de navegação da interface da **Bitdefender**.
2. No painel **PROTEÇÃO DE VÍDEO E ÁUDIO**, clique em **Definições**.
3. Agora vá para a janela **Definições** e ative ou desative o interruptor correspondente.

Configuração da Proteção da Câmara Web

É possível configurar as regras que devem ser aplicadas quando uma aplicação tentar aceder à sua câmara ao seguir estes passos:

1. Clique **Privacidade** no menu de navegação do Interface do Bitdefender.
2. No **PROTEÇÃO DE VÍDEO E ÁUDIO** painel, clique **Configurações**.
3. Vou ao **Configurações** aba.

Estão disponíveis as seguintes opções:

Regras de bloqueio de aplicações

- **Bloquear todo o acesso à câmara Web** - nenhuma aplicação pode aceder à sua câmara Web.
- **Bloquear o acesso dos browsers à câmara Web** - nenhum browser exceto Internet Explorer e Microsoft Edge podem aceder à câmara Web. As aplicações da Windows Store são executados num único processo. Por isso, o Internet Explorer e o Microsoft Edge não podem

ser detectados pelo Bitdefender como navegadores, e, portanto, estão excluídos da lista.

- **Estabelecer permissões da aplicação com base na escolha da comunidade** - se a maioria dos utilizadores de Bitdefender considerar uma aplicação popular como sendo inofensiva, o seu acesso à câmara Web é automaticamente definido como Permitir. Se uma aplicação popular for considerada como perigosa por muitas pessoas, o seu acesso será automaticamente definido como Bloqueado.

Notificações

- **Notifique quando aplicações permitidas se ligam à webcam** - será notificado sempre que uma aplicação permitida aceder à sua câmara.

Adicionar aplicações à lista de Proteção da Câmara Web

As aplicações que tentam estabelecer ligação à sua câmara Web são detetadas automaticamente e, dependendo do respetivo comportamento e da escolha da comunidade, o acesso é permitido ou recusado. No entanto, é possível começar a configurar manualmente a ação que deve ter tomada ao seguir estes passos:

1. Clique **Privacidade** no menu de navegação do Interface do Bitdefender.
2. No **PROTEÇÃO DE VÍDEO E ÁUDIO** painel, clique **Configurações**.
3. Vá para a janela **Proteção da Webcam**.
4. Clique em **Adicionar aplicação**.
5. Clique na hiperligação pretendida:
   - **Na Windows Store** - será exibida uma lista com as aplicações do Windows Store detetados. Ative os botões perto das aplicações que pretende adicionar à lista.
   - **Das suas aplicações** - vá para o ficheiro .exe que deseja adicionar à lista e, em seguida, clique em **OK**.

Para ver o que os utilizadores do Bitdefender escolheram fazer com a aplicação ao selecionar, clique no ícone .

As aplicações que pedem acesso à câmara, assim como a hora da última atividade são apresentadas nesta janela.

Será notificado sempre que uma das aplicações permitidas for bloqueada pelos utilizadores do Bitdefender.

A fim de parar o acesso à sua webcam através de uma aplicação adicionado, clique no ícone .

O ícone muda para , o que significa que a aplicação selecionada não terá acesso à sua webcam.

Supervisor do microfone

Aplicações nocivas podem aceder ao seu microfone integrado de forma silenciosa ou em segundo plano sem o seu consentimento. Para que fique ciente de potenciais exploits maliciosos, o supervisor do microfone do Bitdefender irá notificá-lo sobre esses eventos. Assim, nenhuma aplicação conseguirá aceder ao seu microfone sem a sua permissão.

Ativar e desativar o Supervisor do microfone

1. Clique **Privacidade** no menu de navegação do Interface do Bitdefender.
2. No **PROTEÇÃO DE VÍDEO E ÁUDIO** painel, clique **Configurações**.
3. Selecione os **Configurações** janela.
4. Na janela **Definições**, ative ou desative o botão do **Monitor de Microfone**.

Configurar notificações para o Supervisor do microfone

Para configurar as notificações que devem aparecer quando aplicações tentarem obter acesso ao seu microfone, siga estes passos:

1. Clique **Privacidade** no menu de navegação do Interface do Bitdefender.
2. No **PROTEÇÃO DE VÍDEO E ÁUDIO** painel, clique **Configurações**.
3. Vou ao **Configurações** janela.

Notificações

- **Enviar notificação quando uma aplicação tentar aceder ao microfone**
- **Enviar notificação quando navegadores acederem ao microfone**

- **Enviar notificação quando aplicações não fiáveis acederem ao microfone**
- **Mostrar notificações baseadas na escolha do utilizador do produto Bitdefender**

Adicionar aplicações à lista do Supervisor do microfone

As aplicações que tentarem aceder ao seu microfone serão automaticamente detetadas e adicionadas à Lista de notificação. No entanto, pode configurar manualmente se uma notificação deve ser mostrada ou não, seguindo simplesmente estes passos:

1. Clique **Privacidade** no menu de navegação do Interface do Bitdefender.
2. No **PROTEÇÃO DE VÍDEO E ÁUDIO** painel, clique **Configurações**.
3. Vá para a janela **Proteção de áudio**.
4. Clique **Adicionar aplicativo** janela.
5. Clique no link desejado:
   - **Da loja do Windows** - uma lista com os aplicativos detectados da Windows Store é exibida. Ative os interruptores ao lado dos aplicativos que deseja adicionar à lista.
   - **Dos seus aplicativos** - vá para o arquivo .exe que deseja adicionar à lista e clique em **OK**.

Para ver o que os usuários do Bitdefender escolheram fazer com o aplicativo selecionado, clique no ícone.

As aplicações que irão solicitar acesso ao seu microfone e a hora da última atividade aparecerão nesta janela.

Para deixar de receber notificações referentes à atividade de uma aplicação adicionada, clique no ícone.

O ícone muda para, o que significa que nenhuma notificação do Bitdefender será exibida quando a aplicação selecionada tentar aceder ao microfone.

3.2.8. Remediação de Ransomware

A Remediação de Ransomware da Bitdefender faz um backup dos seus ficheiros, como documentos, fotos, vídeos ou música, para garantir que

eles estejam protegidos contra danos ou perda em caso de encriptação por ransomware. Cada vez que um ataque de ransomware for detetado, o Bitdefender bloqueia todos os processos envolvidos no ataque e inicia o processo de remediação. Assim, pode recuperar o conteúdo total dos seus ficheiros sem pagar qualquer resgate exigido.

Ativar ou desativar a Remediação de Ransomware

Para ativar ou desativar a Remediação de Ransomware:

1. 1. Clique em **Proteção** no menu de navegação na **interface do Bitdefender**.
2. No painel **REMEDIAÇÃO DE RANSOMWARE**, ative ou desative o botão.

> **Observação**
> Para garantir que os seus ficheiros estejam protegidos contra ransomware, recomendamos que mantenha a Remediação de Ransomware ativada.

A ativar ou desativar a restauração automática

A Restauração Automática assegura que seus ficheiros sejam restaurados automaticamente em caso de encriptação por ransomware.

Para ativar ou desativar a restauração automática:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No painel **REMEDIAÇÃO DE RANSOMWARE**, clique em **Gerir**.
3. Na janela Definições, ative ou desative o interruptor **Restauração automática**.

Ver ficheiros restaurados automaticamente

Quando o botão de **Restauração automática** esteja habilitado, o Bitdefender irá automaticamente restabelecer os ficheiros criptografados por ransomware. Assim, pode ter uma experiência na web sem preocupações, sabendo que os seus ficheiros estão seguros.

Para ver ficheiros restaurados automaticamente:

1. Clique **Notificações** no menu de navegação do Interface do Bitdefender.

2. Na aba **Todas**, selecione a notificação referente ao último comportamento de ransomware remediado e clique em **Ficheiros restaurados**.
   Será exibida a lista dos ficheiros restaurados. Neste local também pode ver o local onde seus ficheiros foram restaurados.

Restauração manual de ficheiros encriptados

Caso tenha que restaurar manualmente ficheiros criptografados por ransomware, siga estes passos:

1. Clique **Notificações** no menu de navegação do Interface do Bitdefender.
2. No separador **Todos**, selecione a notificação referente ao último comportamento de ransomware detetado e clique em **Ficheiros encriptados**.
3. Será exibida a lista dos ficheiros encriptados.
   Clique em **Recuperar Ficheiros** para continuar.
4. Caso o processo de recuperação falhe inteira ou parcialmente, deve escolher o local em que os ficheiros encriptados devem ser guardados. Clique em **Restaurar localização** e, em seguida, escolha uma localização no seu PC.
5. Aparece uma janela de confirmação.
   Clique em **Finalizar** para terminar o processo de restauração.

Ficheiros com as seguintes extensões podem ser restaurados caso sejam encriptados:

.3g2;.3gp;.7z;.ai;.aif;.arj;.asp;.aspx;.avi;.bat;.bin;.bmp;.c;.cda;.cgi;.class;.com;.cpp;.cs;.css;.csv;.dat;.db;.dbf;.deb;.doc;.docx;.gif;.gz;.h264;.h;.flv;.htm;.html;.ico;.jar;.java;.jpeg;.jpg;.js;.jsp;.key;.m4v;.mdb;.mid;.midi;.mkv;.mp3;.mp4;.mov;.mpg;.mpeg;.ods;.odp;.odt;.ogg;.pdf;.pkg;.php;.pl;.png;.pps;.ppt;.pptx;.ps;.psd;.py;.rar;.rm;.rtf;.sav;.sql;.sh;.svg;.swift;.swf;.tar;.tex;.tif;.tiff;.txt;.xlr;.xls;.xlsx;.xml;.wmv;.vb;.vob;.wav;.wks;.wma;.wpl;.wps;.wpd;.wsf;.z;.zip;

Adicionar aplicações às exceções

Pode configurar regras de excepção para aplicações de confiança para que a função de Remediação de Ameaças não bloqueie caso executem ações típicas de ransomware.

Para adicionar aplicações à lista de excepções de Remediação de Ransomware:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **REMEDIAÇÃO DE RANSOMWARE** painel, clique **Gerenciar**.
3. Na janela **Exceções**, clique em **+Adicionar uma exceção**.

3.2.9. Cryptomining Protection

O que é proteção contra criptomineração?

Com o uso de criptomineração, os invasores podem se beneficiar financeiramente sem arcar com os custos associados e as consequências legais.

O recurso Cryptomining Protection do Bitdefender defende os computadores Windows contra a ameaça crescente de atividades não autorizadas de mineração de criptografia, uma prática maliciosa que explora os recursos e a eletricidade de um usuário para gerar receita para os invasores.

> **Observação**
> A proteção contra criptomineração depende de:
>
> - Escudo Bitdefender
> - Prevenção de ataques na Web
>
> Para que a Proteção contra Criptomineração possa ser executada, esses dois recursos também devem estar habilitados.

Habilitando proteção contra criptomineração

O recurso Cryptomining Protection está localizado na guia Proteção.

Para habilitá-lo, basta alternar o botão correspondente.

> **Observação**
> A Proteção contra Criptomineração está desabilitada por padrão, garantindo que os usuários tenham controle sobre sua ativação.

Modos de operação

Uma vez ativado, o recurso Cryptomining Protection opera em 2 estados distintos, cada um adaptado às preferências do usuário:

1. **Bloqueie todas as atividades de criptomineração.** (bloqueia automaticamente quaisquer atividades de mineração de criptografia e toma as ações necessárias para evitar novas tentativas não autorizadas)
   Este modo é ideal para usuários que não têm intenção de se envolver em atividades de mineração de criptografia.
2. **Detecte atividades de criptomineração.** (emite alertas sempre que uma atividade de mineração de criptografia é detectada e requer a entrada do usuário para determinar a ação apropriada)
   Este modo é adequado para usuários ativamente envolvidos em suas próprias atividades de mineração de criptografia, mas que desejam monitorar e controlar quaisquer tentativas não autorizadas.

Gerenciar exceções

Exceções podem ser especificadas para aplicativos, com a capacidade adicional de definir linhas de comando específicas. Porém, exceções também podem ser estabelecidas sem a necessidade de fornecer parâmetros tão detalhados, oferecendo um equilíbrio entre customização e simplicidade.

Para adicionar uma exceção:

1. Clique**Proteção**no menu do lado esquerdo da interface do Bitdefender.
2. No**Proteção contra criptografia**painel, clique em**Configurações**.
3. Clique no**Gerenciar exceções**opção.
4. A seguir, clique no**Adicionar uma exceção**botão.
5. Uma nova janela se abrirá. Você pode excluir manualmente aplicativos, URLs e endereços IP.
6. Por fim, clique**Salvar**. A nova regra é adicionada à lista de exceções da Proteção contra Criptomineração.

> **Observação**
> Para remover uma exceção, basta clicar no ícone da lixeira próximo a ela.

3.2.10. Antitracker

Uma grande parte dos sites que utiliza monitorizadores para recolher informação sobre o seu comportamento para compartilhar com empresas

ou para mostrar publicidade direcionada para si. Devido a isso, os donos dos sites ganham dinheiro por proporcionar conteúdo de graça ou para continuarem a funcionar. Além de recolher informação, os monitorizadores podem desacelerar a sua navegação ou desperdiçar a sua banda larga.

Com a extensão Anti-rastreio Bitdefender ativada no seu navegador da web, evita que seja rastreado para que os seus dados permaneçam privados enquanto navega online e acelera o tempo que os sites precisam para carregar.

A extensão do Bitdefender é compatível com os seguintes navegadores de internet:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

Os monitorizadores que detectamos estão divididos nas seguintes categorias:

- **Publicidade** - utilizada para analisar o tráfego do site, o comportamento do utilizador ou os padrões de tráfego dos visitantes.
- **Interação com o cliente** - utilizados para medir a interação com o utilizador através de diferentes formas de entrada, como chat ou suporte.
- **Essenciais** - utilizados para monitorizar funcionalidades críticas do site.
- **Analíticas do site** - utilizadas para recolher dados sobre a utilização do site.
- **Redes Sociais** - utilizados para monitorizar o público em redes sociais, as suas atividades e o envolvimento dos utilizadores nas diferentes plataformas de redes sociais.

Interface do Antitracker

Quando a extensão Anti-rastreio Bitdefender é ativada, o ícone aparece ao lado da barra de pesquisa no seu navegador da web. Todas as vezes que visita um site, um contador pode ser observado no ícone, referente aos rastreadores detetados e bloqueados. Para ver mais detalhes sobre os rastreadores bloqueados, clique no ícone para abrir a interface.

Além do número de rastreadores bloqueados, pode visualizar o tempo necessário para a página carregar e as categorias às quais pertencem os rastreadores detetados. Para ver a lista dos sites que estão a rastrear, clique na categoria desejada.

Para impedir que a Bitdefender bloqueie monitorizadores no site que está a visitar, clique em **Pausar proteção neste site**. Esta definição só se aplica enquanto tiver o site aberto, e volta ao estado inicial quando fechar o site.

Para permitir que os monitorizadores de uma categoria específica monitorizem a sua atividade, clique na atividade desejada e, em seguida, no botão correspondente. Se mudar de ideias, clique no mesmo botão novamente.

Desligar o Anti-rastreio Bitdefender

Para desativar o Bitdefender Antitracker:

- No seu navegador da Web:
  1. Abra o seu navegador web.
  2. Clique no ícone ao lado da barra de endereços no seu navegador.
  3. Clique no ícone no canto superior direito.
  4. Utilize o interruptor correspondente para o desativar.
     O ícone do Bitdefender fica cinzento.

- Na interface do Bitdefender:
  1. Clique **Privacidade** no menu de navegação do Interface do Bitdefender.
  2. No painel **ANTITRACKER**, clique em **Definições**.
  3. Desligue o interruptor correspondente do lado do navegador web no qual deseja desativar a extensão.

Permitir a monitorização de um site

Se desejar ser monitorizado ao visitar um site em particular, pode adicionar o seu endereço às excepções da seguinte forma:

1. Abra seu navegador da web.

2. Clique no ícone ao lado da barra de pesquisa.
3. Clique no ícone no canto superior direito.
4. Se estiver no site que precisa de adicionar às exceções, clique em **Adicionar o site atual à lista**.
   Se desejar adicionar outro site, escreva o seu endereço no campo correspondente e, em seguida, clique em .

3.2.11. Segurança Safepay para transações online

O computador está a tornar-se na principal ferramenta para a realização de compras e operações bancárias. Pagar contas, transferir dinheiro, comprar praticamente qualquer coisa que possa imaginar nunca foi tão fácil e rápido.

Isto engloba enviar informação pessoal, de conta e de cartão de crédito, palavras-passe e outros tipos de informação privada pela Internet, por outras palavras exatamente o tipo de fluxo de informação que os cibercriminosos estão muito interessados em deitar a mão. Os hackers são incansáveis nos seus esforços para roubar esta informação, assim que nunca poderá ser demasiado cuidadoso em manter seguras as suas transações online.

O Bitdefender Safepay™ é, acima de tudo, um navegador protegido, um ambiente selado que foi feito para manter as suas operações bancárias, as suas compras e qualquer outro tipo de transação online privadas e seguras.

O Bitdefender Safepay™ oferece as seguintes funcionalidades:

- Bloqueia o acesso ao seu ambiente de trabalho e de qualquer tentativa de tirar fotografias do seu ecran.
- Vem com um teclado virtual que, quando usado, torna impossível para os hackers lerem as teclas que usar.
- É completamente independente dos outros navegadores.
- Vem com uma proteção hotspot embutida para ser utilizada quando o seu dispositivo se liga a redes Wi-fi não-seguras.
- Suporta bookmarks e permite-lhe navegar entre os seus sites favoritos de bancos/compras.

- Não está só limitado ao banking e às compras online. Qualquer website pode ser aberto no Bitdefender Safepay™.

A utilizar o Bitdefender Safepay™

Por defeito, o Bitdefender deteta quando entra numa página de um banco ou de compras em qualquer navegador do seu dispositivo e pergunta se gostaria de utilizar o Bitdefender Safepay™.

Para aceder à interface principal do Bitdefender Safepay™, utilize um dos métodos a seguir:

- Da interface do **Bitdefender**:
  1. Clique **Privacidade** no menu de navegação do Interface do Bitdefender.
  2. No painel **SAFEPAY**, clique em **Definições**.
  3. Na janela **Safepay**, clique em **Abrir Safepay**.
- Do Windows:
  - No **Windows 7**:
    1. Clique em **Iniciar** e vá para **Todos os programas**.
    2. Clique em **Bitdefender**.
    3. Clique em **Bitdefender Safepay™**.
  - No **Windows 8** e no **Windows 8.1**:
    Encontre o Bitdefender Safepay™ no Ecrã inicial do Windows (por exemplo, pode introduzir "Bitdefender Safepay™" diretamente no Ecrã Inicial) e, em seguida, clique no ícone.
  - No **Windows 10** e no **Windows 11**:
    Escreva "Bitdefender Safepay™" na caixa de pesquisa da barra de tarefas e, em seguida, clique no ícone correspondente.

Se está habituado a navegadores web, não terá qualquer problema em usar o Bitdefender Safepay ™- pois parece e comporta-se como um navegador normal:

- insira URLs que deseja ir na barra de endereços.

- adicione abas para visitar múltiplos sites na janela do Bitdefender Safepay™ ao clicar em ⊞.
- navegue para a frente e para trás e atualize as páginas usando ← → ↻ respetivamente.
- aceda as **Definições** do Bitdefender Safepay™ ao clicar e escolher **Definições**.
- gira os seus **marcadores** ao clicar em ☆ ao lado da barra de endereço.
- abra o teclado virtual ao clicar em ⌨.
- aumente ou diminua o tamanho do navegador ao pressionar simultaneamente **Ctrl** e as teclas **+/-** no teclado numérico.
- veja as informações sobre o seu produto Bitdefender ao clicar em ⋯ e escolher **Sobre**.
- imprima as informações importantes ao clicar em ⋯ e escolher **Imprimir**.

> **Observação**
> Para alternar entre o Bitdefender Safepay™ e o ambiente de trabalho do Windows, prima as teclas **Alt+Tab** ou clique na opção **Mudar para a área de trabalho** no lado superior esquerdo da janela.

Configurar definições

Clique em ⋯ e escolha **Definições** para configurar o Bitdefender Safepay™:

Aplicar regras do Bitdefender Safepay para domínios acedidos

Os sites que adicionou aos **Favoritos** com a opção **Abrir automaticamente no Safepay** ativa aparecerão aqui. Se quiser que um site da lista pare de abrir automaticamente com o Bitdefender Safepay™, clique em × do lado da entrada desejada na coluna **Remover**.

Bloquear pop-ups

Pode escolher para bloquear pop-ups clicando no botão correspondente.

Também pode criar uma lista de páginas que possa permitir pop-ups. A lista deve conter apenas os sites web em que confia plenamente.

Para adicionar uma página à lista, introduza o seu endereço no campo correspondente e clique em **Adicionar domínio**.

Para remover uma página da web da lista, selecione o X correspondente à entrada pretendida.

Gerir plugins

Pode escolher se pretende ativar ou desativar os plug-ins específicos no Bitdefender Safepay™.

Gerir certificados

Pode importar certificados do seu sistema para uma loja de certificados.

Clique em **IMPORTAR** e siga o assistente para utilizar os certificados no Bitdefender Safepay™.

Usar teclado virtual

O teclado virtual irá aparecer automaticamente quando o campo de palavra-passe for selecionado.

Utilize o botão correspondente para ativar ou desativar a função.

Confirmação de impressão

Ative esta opção se pretender dar a sua confirmação antes de iniciar o processo de impressão.

Gerir bookmarks

Se desativou a detecção automática de alguma ou de todas as páginas, ou o Bitdefendersimplesmente não detectar algumas páginas, pode adicionar bookmarks ao Bitdefender Safepay™ para que possa abrir facilmente as suas páginas favoritas no futuro.

Siga estes passos para adicionar um URL aos bookmarks do Bitdefender Safepay™

1. Clique em ⋯ e escolha **Marcadores** para abrir a página de Marcadores.

   > **Observação**
   > A página de Bookmarks abre por defeito quando executa o Bitdefender Safepay™.

2. Clique no botão **+** para adicionar um novo bookmark.
3. Introduza o URL e o título do favorito, e depois clique em **CRIAR**. Marque a opção **Abrir automaticamente no Safepay** se quiser que a

página marcada abra com o Bitdefender Safepay™ todas as vezes que acedê-la. O URL é também adicionado à lista de Domínios na página de definições.

Desligar as notificações do Safepay

Quando um site bancário for detectado, o produto Bitdefender é configurado para notificá-lo por meio de uma janela pop-up.

Para desligar as notificações do Safepay:

1. Clique **Privacidade** no menu de navegação do Interface do Bitdefender.
2. No **SAFEPAY** painel, clique **Configurações**.
3. Na janela **Definições**, desative o botão ao lado de **Notificações do Safepay**.

3.2.12. dispositivo antirroubo

O roubo de laptops é um problema importante que afeta indivíduos e organizações. Ainda mais do que perder o hardware em si, os dados perdidos com ele podem causar danos significativos, tanto financeira quanto emocionalmente.

No entanto, poucas pessoas tomam as medidas adequadas para proteger seus importantes dados pessoais, comerciais e financeiros em caso de roubo ou perda.

O Bitdefender Anti-Theft ajuda você a estar melhor preparado para tal evento, permitindo que você localize ou bloqueie remotamente seu laptop e até mesmo apague todos os dados dele, caso você separe seu laptop contra sua vontade.

Para usar os recursos Antifurto, os seguintes pré-requisitos devem ser atendidos:

- Os comandos só podem ser enviados da conta Bitdefender.
- O laptop deve estar conectado à internet para receber os comandos.

Os recursos antirroubo funcionam da seguinte maneira:

Localizar

Veja a localização do seu dispositivo no Google Maps.

A precisão da localização depende de como o Bitdefender é capaz de determiná-la. A localização é determinada com precisão de dezenas de metros se o Wi-fi estiver ativado em seu laptop e houver redes sem fio em seu alcance.

Se o laptop estiver conectado a uma LAN com fio sem localização baseada em Wi-fi disponível, a localização será determinada com base no endereço IP, que é consideravelmente menos preciso.

Alerta

Envie um alerta remoto no dispositivo.

O recurso está disponível apenas em dispositivos móveis.

Trancar

Bloqueie seu laptop e defina um PIN de 4 dígitos para desbloqueá-lo. Quando você enviar o **Trancar** comando, o sistema é reinicializado e o login no Windows só é possível depois de inserir o PIN que você definiu.

Se você deseja que o Bitdefender tire fotos de quem tenta acessar seu laptop, marque a caixa de seleção correspondente. As fotos tiradas são tiradas com a câmera frontal e exibidas junto com o carimbo de data/hora no painel Antirroubo. Apenas as duas fotos mais recentes serão salvas.

Esta ação está disponível apenas para laptops com câmera frontal.

Limpar

Remova todos os dados do seu sistema. Quando você enviar o **Limpar** comando, o laptop reinicia e os dados em todas as partições do disco rígido são apagados.

Mostrar IP

Exibe o último endereço IP do dispositivo selecionado. Clique **MOSTRAR IP** para torná-lo visível.

O Antifurto é ativado após a instalação e pode ser acessado exclusivamente por meio de sua conta Bitdefender de qualquer dispositivo conectado à internet, em qualquer lugar.

Usando recursos antirroubo

Para acessar os recursos do Antifurto, use uma das seguintes possibilidades:

- Na interface principal do Bitdefender:
  1. Clique **Serviços de utilidade pública** no menu de navegação do Interface do Bitdefender.
  2. Clique **IR PARA O CENTRO**.
     Você é redirecionado para a página Central do Bitdefender. Verifique se você está conectado com suas credenciais.
  3. Na janela do Bitdefender Central que se abre, clique no cartão do dispositivo desejado e selecione **Anti-roubo**.

- Em qualquer dispositivo com acesso à internet:
  1. Abra um navegador da Web e vá para: https://central.bitdefender.com.
  2. Entre na sua conta Bitdefender usando seu endereço de e-mail e senha.
  3. Selecione os **Meus dispositivos** painel.
  4. Clique no cartão do dispositivo desejado e selecione **Anti-roubo**.
  5. Selecione o recurso que deseja usar:
     Localizar - exibir a localização do seu dispositivo no Google Maps.
     Mostrar IP - exibir o último endereço IP do seu dispositivo.
     Alerta - enviar um alerta no dispositivo.
     Trancar - bloqueie seu laptop e defina um código PIN para desbloqueá-lo.
     Limpar - exclua todos os dados do seu laptop.

     Importante
     Depois de limpar um dispositivo, todos os recursos antirroubo param de funcionar.

3.3. Serviços de utilidade pública

3.3.1. Perfis

Atividades de trabalho diárias, ver filmes ou jogar podem provocar lentidão no sistema, especialmente se estes estiverem a ser executados simultaneamente com os processos de atualização do Windows e as

tarefas de manutenção. Com o Bitdefender, pode agora escolher e aplicar o seu perfil preferido; o que irá ajustar o sistema a melhorar o desempenho de aplicações específicas.

O Bitdefender fornece os seguintes perfis:

- Perfil de Trabalho
- Perfil do filme
- Perfil do jogo
- **Perfil de Wi-Fi público**
- Perfil do modo de bateria

Se decidir não usar os **Perfis**, um perfil padrão chamado **Padrão** é ativado e não faz nenhuma otimização no seu sistema.

De acordo com a sua atividade, as seguintes definições do produto serão aplicadas quando os perfis Trabalho, Filme ou Jogo são ativados:

- Todos os alertas e pop-ups do Bitdefender são desactivados.
- A Atualização Automática é adiada.
- As análises agendadas são adiadas.
- **Consultor de pesquisa** está desativado.
- As notificações de ofertas especiais estão desativadas.

De acordo com sua atividade, as seguintes definições do sistema são aplicadas quando os perfis Trabalho, Filme ou Jogo são ativados:

- As Atualizações Automáticas do Windows são adiadas.
- Os alertas e pop-ups do Windows são desativados.
- Os programas desnecessários em segundo plano são suspensos.
- Os efeitos visuais são ajustados para o melhor desempenho.
- As tarefas de manutenção são adiadas.
- As definições do plano de energia são ajustadas.

Ao executar neste perfil Wi-Fi público, o Bitdefender Total Security é definido automaticamente de modo a obter as seguintes definições de programa:

- A Defesa Avançada contra Ameaças está ativada

- As seguintes configurações do Online Threat Prevention estão ativadas:
  - Varredura da web criptografada
  - Proteção contra fraude
  - Proteção contra phishing

Perfil Trabalho

A execução de várias tarefas no trabalho, tais como o envio de e-mails, ter uma videoconferência com os seus colegas distantes ou trabalhar com aplicações de design pode afetar o desempenho do sistema. O Perfil de Trabalho foi desenhado para ajudá-lo a melhorar a sua eficiência no trabalho, desativando alguns dos serviços e tarefas de manutenção em segundo plano.

A configurar o Perfil de Trabalho

Para configurar as ações a executar enquanto está no Perfil de Trabalho:

1. Clique **Serviços de utilidade pública** no menu de navegação do Interface do Bitdefender.
2. No **Perfis** guia, clique **Configurações**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Trabalho.
4. Escolha os ajustes do sistema que quer que sejam aplicados selecionando as seguintes opções:
   - Aumente o desempenho das aplicações de trabalho
   - Otimize as definições do produto para o perfil Trabalho
   - Adie programas em segundo plano e tarefas de manutenção
   - Adiar as Atualizações Automáticas do Windows
5. Clique em **GUARDAR** para guardar as alterações e fechar a janela.

A adicionar aplicações manualmente à lista do Perfil de Trabalho

Se o Bitdefender não entrar automaticamente no Perfil de Trabalho quando abre uma determinada aplicação de trabalho, pode adicionar a aplicação manualmente à **Lista de aplicações de trabalho**.

Para adicionar aplicações manualmente à Lista de aplicações de trabalho do Perfil de Trabalho:

1. Clique **Serviços de utilidade pública** no menu de navegação do Interface do Bitdefender.
2. No **Perfis** guia, clique **Configurações**.
3. Clique no **CONFIGURAR** botão na área Perfil de trabalho.
4. Na janela **Definições do perfil de trabalho**, clique em **Lista de aplicações**.
5. Clique em **ADICIONAR**.
   Aparece uma nova janela. Vá até ao ficheiro executável da aplicação, selecione-o e clique em **OK** para o adicionar à lista.

Perfil de Filme

A exibição de conteúdo de vídeo de alta qualidade, como filmes de alta definição, exige recursos significativos do sistema. O Perfil de Filme ajusta as definições do sistema e do produto para que possa desfrutar de uma experiência cinematográfica agradável e sem interrupções.

A configurar o Perfil de Filme

Para configurar as ações a serem tomadas no Perfil de Filme:

1. Clique **Serviços de utilidade pública** no menu de navegação do Interface do Bitdefender.
2. No **Perfis** guia, clique **Configurações**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Filme.
4. Escolha os ajustes do sistema que você gostaria de aplicar marcando as seguintes opções:
   - Aumente o desempenho dos leitores de vídeo
   - Otimize as definições do produto para o perfil Filme
   - Adiar programas em segundo plano e tarefas de manutenção
   - Adiar atualizações automáticas do Windows
   - Ajustar as definições do esquema de energia para filmes
5. Clique **SALVAR** para salvar as alterações e fechar a janela.

A adicionar manualmente leitores de vídeo à lista do Perfil de Filme

Se o Bitdefender não entrar automaticamente no Perfil de Cinema quando abrir uma certa aplicação de reprodução de vídeo, pode adicioná-lo manualmente à **Lista de aplicações de filme**.

Para adicionar manualmente leitores de vídeo à Lista de aplicações de filme no Perfil de Filme:

1. Clique **Serviços de utilidade pública** no menu de navegação do Interface do Bitdefender.
2. No **Perfis** guia, clique **Configurações**.
3. Clique no **CONFIGURAR** botão na área Perfil do filme.
4. Na janela **Definições do Perfil de Filme**, clique em **Lista de aplicações de reprodução**.
5. Clique **ADICIONAR**.
   Uma nova janela aparece. Navegue até o arquivo executável do aplicativo, selecione-o e clique em **OK** para adicioná-lo à lista.

Perfil de Jogo

Para desfrutar de uma experiência de jogo sem interrupções, é importante reduzir a carga do sistema e diminuir a lentidão. Ao utilizar heurísticas comportamentais, juntamente com uma lista de jogos conhecidos, o Bitdefender pode detectar automaticamente os jogos em execução e otimizar os recursos do sistema para que possa aproveitar a sua pausa de jogo.

A configurar o Perfil de Jogo

Para configurar as ações a serem tomadas no Perfil de Jogos:

1. Clique **Serviços de utilidade pública** no menu de navegação do Interface do Bitdefender.
2. No **Perfis** guia, clique **Configurações**.
3. Clique no botão **Configurar** na área do Perfil de Jogos.
4. Escolha os ajustes do sistema que você gostaria de aplicar marcando as seguintes opções:
   - Aumente o desempenho dos jogos

- Otimize as definições do produto para o perfil Jogo
- Adiar programas em segundo plano e tarefas de manutenção
- Adiar atualizações automáticas do Windows
- Ajustar as definições do esquema de energia para jogos

5. Clique **SALVAR** para salvar as alterações e fechar a janela.

Adicionar os jogos manualmente à lista de Jogos

Se o Bitdefender não entrar automaticamente no Perfil de Jogo quando abre um certo jogo ou aplicação, pode adicioná-lo manualmente à **Lista de aplicações de jogos**.

Para adicionar jogos manualmente à lista de aplicações de jogos no Perfil de Jogo:

1. Clique **Serviços de utilidade pública** no menu de navegação do Interface do Bitdefender.
2. No **Perfis** guia, clique **Configurações**.
3. Clique no **configurar** botão na área Perfil do Jogo.
4. Na janela **Definições do Perfil de Jogo**, clique em **Lista de jogos**.
5. Clique **ADICIONAR**.
   Aparece uma nova janela. Navegue até o ficheiro executável do jogo, selecione-o e clique em **OK** para adicioná-lo à lista.

Perfil Wi-Fi Público

Enviar e-mails, digitar credenciais sensíveis ou fazer compras online enquanto ligado a uma rede sem fios insegura pode colocar os seus dados pessoais em risco. O perfil Wi-Fi Público ajusta as definições do produto para lhe dar a possibilidade de fazer pagamentos online e utilizar informações sensíveis num ambiente protegido.

A configurar o perfil Wi-Fi Público

Para configurar o Bitdefender para aplicar as definições do produto enquanto ligado a uma rede sem fios insegura:

1. Clique **Serviços de utilidade pública** no menu de navegação do Interface do Bitdefender.

2. No **Perfis** guia, clique **Configurações**.
3. Clique no botão **CONFIGURAR** na área do Perfil Wi-Fi Público.
4. Deixe a caixa de verificação **Ajusta as definições do produto para aumentar a proteção quando ligado a uma rede Wi-Fi pública insegura** marcada.
5. Clique **Salvar**.

Perfil do Modo de Bateria

O perfil Modo de Bateria foi concebido especialmente para utilizadores de portáteis e tablets. O seu objetivo é minimizar o impacto do sistema e do Bitdefender no consumo de energia quando o nível de bateria estiver abaixo do nível predefinido que selecionou.

Configurando o perfil Modo de Bateria

Para configurar o perfil Modo de Bateria:

1. Clique **Serviços de utilidade pública** no menu de navegação do Interface do Bitdefender.
2. No **Perfis** guia, clique **Configurações**.
3. Clique no botão **Configurar** na área do Perfil do Modo de Bateria.
4. Escolha os ajustes do sistema que serão aplicados selecionando as seguintes opções:
   - Otimize as definições do produto para o modo Bateria.
   - Adie programas em segundo plano e tarefas de manutenção.
   - Adiar as Atualizações Automáticas do Windows.
   - Ajuste as definições do plano de energia para o modo Bateria.
   - Desative os dispositivos externos e as portas de rede.
5. Clique **SALVAR** para salvar as alterações e fechar a janela.

Digite um valor válido na caixa de rotação ou selecione um valor utilizando os botões de setas para cima e para baixo para especificar quando o sistema deve começar a operar no Modo de Bateria. Por defeito, o modo é ativado quando o nível da bateria cai abaixo dos 30%.

As definições do produto seguinte são aplicadas quando o Bitdefender opera em Modo de Bateria:

- A Atualização Automática do Bitdefender é adiada.
- As varreduras agendadas são adiadas.

O Bitdefender deteta quando o portátil mudou para a energia da bateria e com base no nível de carga, ele entra automaticamente no Modo de Bateria. Da mesma forma, o Bitdefender sai automaticamente do Modo de Bateria ao detectar que o portátil já não está a funcionar pela bateria.

Otimização em tempo real

A otimização em tempo real do Bitdefender é um plugin que melhora o desempenho do seu sistema silenciosamente, em segundo plano, ao assegurar que não é interrompido enquanto está no modo de perfil. Dependendo da carga da CPU, o plugin monitoriza todos os processos, concentrando-se naqueles que absorvem uma carga mais elevada, para ajustá-los às suas necessidades.

Para ativar ou desativar a Otimização em Tempo Real:

1. Clique **Serviços de utilidade pública** no menu de navegação do Interface do Bitdefender.
2. No **Perfis** guia, clique **Configurações**.
3. Desloque-se para baixo até ver a opção de otimização em tempo real e utilize o botão correspondente para a ativar ou desativar.

3.3.2. Otimizador OneClick

Problemas como falhas no disco rígido, sobras de arquivos de registro e histórico do navegador podem tornar seu trabalho mais lento, o que pode se tornar incômodo para você. Tudo isso agora pode ser corrigido com um único clique de um botão.

O OneClick Optimizer permite identificar e remover arquivos inúteis executando várias tarefas de limpeza ao mesmo tempo.

Para iniciar o processo do OneClick Optimizer:

1. Clique **Serviços de utilidade pública** no menu de navegação do Interface do Bitdefender.
2. Clique no **otimizar** botão.
   a. **Analisando**
   Aguarde que o Bitdefender termine de procurar por problemas do sistema.

- Limpeza de disco - identifica arquivos e pastas desnecessários.
- Registry Cleanup - identifica referências inválidas ou desatualizadas no Registro do Windows.
- Limpeza de privacidade - identifica arquivos e cookies temporários da Internet, cache e histórico do navegador.

O número de problemas encontrados é exibido. Clique no link Exibir detalhes para analisá-los antes de prosseguir com o processo de limpeza. Clique em Otimizar para continuar.

b. **Otimizando**
Aguarde que o Bitdefender termine de otimizar seu sistema.

c. **Problemas**
Aqui é onde você pode ver o resultado da operação.
Se você deseja informações abrangentes sobre o processo de otimização, clique no **Ver relatório detalhado** botão.

3.3.3. Proteção de dados

Apagar ficheiros permanentemente

Quando apaga um ficheiro, o mesmo já não fica acessível por meios normais. No entanto o ficheiro continua armazenado no disco duro até que seja sobrescrito quando copiar para lá novos ficheiros.

O Bitdefender File Shredder ajuda você a excluir dados permanentemente, removendo-os fisicamente de seu disco rígido.

Pode rapidamente destruir ficheiros ou pastas do seu dispositivo utilizando o menu contextual Windows seguindo os seguintes passos:

1. Clique botão direito sobre o ficheiro ou pasta que deseja apagar permanentemente.
2. Selecione **Bitdefender > Destruidor de Ficheiros** no menu de contexto que aparece.
3. Clique em **Eliminar permanentemente** e, em seguida, confirme que deseja continuar com o processo.
Aguarde que o Bitdefender termine a destruição dos ficheiros.
4. Os resultados são apresentados. Clique em **Terminar** para sair do assistente.

Alternativamente pode destruir os ficheiros a partir da interface do Bitdefender, conforme o seguinte:

1. Clique **Serviços de utilidade pública** no menu de navegação do Interface do Bitdefender.
2. No painel **Proteção de dados**, clique em **Destruidor de Ficheiros**.
3. Siga o assistente do Destruidor de Ficheiros:
   a. Clique no botão **Adicionar pastas** para adicionar os ficheiros ou pastas que deseja remover permanentemente.
   Alternativamente, arraste estes ficheiros ou pastas para esta janela.
   b. Clique em **Eliminar permanentemente** e, em seguida, confirme que deseja continuar com o processo.
   Aguarde que o Bitdefender termine de triturar os arquivos.
   c. **Resumo de resultados**
   Os resultados são exibidos. Clique **Terminar** para sair do assistente.

3.4. Como

3.4.1. Instalação

Como instalo o Bitdefender num segundo dispositivo?

Caso a subscrição que comprou cubra mais do que um dispositivo, pode utilizar a sua conta Bitdefender para ativar um segundo PC.

Para instalar o Bitdefender num segundo dispositivo:

1. Clique na hiperligação **Instalar noutro dispositivo** no canto inferior esquerdo da **interface do Bitdefender**.
   Uma nova janela aparece em sua tela.
2. Clique **COMPARTILHAR LINK DE DOWNLOAD**.
3. Siga as instruções no ecrã para instalar o Bitdefender.

O novo dispositivo no qual instalou o produto Bitdefender aparece no painel do Bitdefender Central.

Como posso reinstalar o Bitdefender?

As situações típicas em que deve reinstalar Bitdefender são as seguintes:

- você reinstalou o sistema operativo.
- pretende corrigir problemas que causaram abrandamentos e falhas.
- o seu produto Bitdefender não começa ou funciona corretamente.

Na eventualidade de uma das situações mencionadas ser o seu caso, siga estes passos:

- Em **windows 7**:
  1. Clique **Começar** e vai para **Todos os programas**.
  2. Localize Bitdefender Total Security e selecione **Desinstalar**.
  3. Clique em **REINSTALAR** na janela que aparece.
  4. Precisa de reiniciar o dispositivo para concluir o processo.

- Em **Windows 8** e **Windows 8.1**:
  1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
  2. Clique em **Desinstalar** um programa ou **Programas e Funcionalidades**.
  3. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique **REINSTALAR** na janela que aparece.
  5. Você precisa reiniciar o dispositivo para concluir o processo.

- Em **Windows 10** e **Windows 11**:
  1. Clique em **Iniciar** e, em seguida, clique em **Definições**.
  2. Clique no ícone **Sistema** na área de Definições e então selecione **Aplicações e funcionalidades**.
  3. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
  5. Clique em **REINSTALAR**.
  6. Você precisa reiniciar o dispositivo para concluir o processo.

> **Observação**
> Ao seguir este procedimento de reinstalação, as definições personalizadas são guardadas e estão disponíveis no novo produto instalado. As outras definições podem ser alteradas novamente para a configuração predefinida.

De onde é que posso transferir o meu produto Bitdefender?

Pode instalar o Bitdefender do disco de instalação ou através do instalador transferido no seu dispositivo da plataforma Bitdefender Central.

> **Observação**
> Antes de executar o kit, é recomendada a remoção de qualquer solução de segurança instalada no seu sistema. Quando utiliza mais do que uma solução de segurança no mesmo dispositivo, o sistema torna-se instável.

Para instalar o Bitdefender a partir da Central Bitdefender:

1. Acesso Bitdefender Central.
2. Selecione os **Meus dispositivos** painel e, em seguida, clique em **INSTALAR PROTEÇÃO**.
3. Escolha uma das duas opções disponíveis:
   - **Proteger este dispositivo**
     Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, clique no botão correspondente.
   - **Proteger outros dispositivos**
     Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, clique no botão correspondente.
     Clique **ENVIAR LINK DE DOWNLOAD**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR EMAIL**. Observe que o link de download gerado é válido apenas pelas próximas 24 horas. Se o link expirar, você terá que gerar um novo seguindo os mesmos passos.

No dispositivo em que deseja instalar seu produto Bitdefender, verifique a conta de e-mail que você digitou e clique no botão de download correspondente.

4. Execute o Bitdefender que transferiu.

Como utilizo a minha subscrição do Bitdefender após uma atualização do Windows?

Esta situação ocorre quando atualiza o sistema operativo e pretende continuar a utilizar a subscrição do Bitdefender.

Se estiver a utilizar uma versão anterior do Bitdefender, pode atualizá-la, gratuitamente, para a última versão, conforme segue:

- De uma versão anterior do Bitdefender Antivirus até à sua versão mais recente que esteja disponível.
- De uma versão anterior do Bitdefender Internet Security até à sua versão mais recente que esteja disponível.
- De uma versão anterior do Bitdefender Total Security até à sua versão mais recente que esteja disponível.

Há dois tipos de caso que podem aparecer:

- Atualizou o sistema operativo utilizando o Windows Update e constata que o Bitdefender já não funciona.
  Neste caso, é necessário reinstalar o produto ao seguir estes passos:
  - Em **windows 7**:
    1. Clique em **Iniciar**, vá ao **Painel de Controlo** e dê um clique duplo em **Programas e Recursos**.
    2. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
    3. Clique **REINSTALAR** na janela que aparece.
    4. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.
       Abra a interface do produto Bitdefender recentemente instalado para ter acesso às respetivas funcionalidades.
  - Em **Windows 8** e **Windows 8.1**:

1. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
2. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
3. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
4. Clique **REINSTALAR** na janela que aparece.
5. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.
   Abra a interface do seu novo produto Bitdefender instalado para ter acesso aos seus recursos.

- Em **Windows 10** e **Windows 11**:
  1. Clique **Começar**, então clique **Configurações**.
  2. Clique no ícone **Sistema** na área Definições e, em seguida, selecione **Aplicações**.
  3. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique **Desinstalar** novamente para confirmar sua escolha.
  5. Clique **REINSTALAR** na janela que aparece.
  6. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.
     Abra a interface do seu novo produto Bitdefender instalado para ter acesso aos seus recursos.

  Observação
  Ao seguir este procedimento de reinstalação, as configurações personalizadas são salvas e disponibilizadas no novo produto instalado. Outras configurações podem ser alteradas de volta para sua configuração padrão.

- Alterou o seu sistema e pretende continuar a utilizar a proteção Bitdefender. Portanto, será necessário reinstalar o produto utilizando a versão mais recente.
  Para resolver este problema:
  1. Transfira o ficheiro de instalação:

a. Acesso Bitdefender Central.

b. Selecione os **Meus dispositivos** painel e, em seguida, clique em **INSTALAR PROTEÇÃO**.

c. Escolha uma das duas opções disponíveis:

- **Proteger este dispositivo**
  Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, clique no botão correspondente.
- **Proteger outro dispositivo**
  Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, clique no botão correspondente.
  Clique **ENVIAR LINK DE DOWNLOAD**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR EMAIL**. Observe que o link de download gerado é válido apenas pelas próximas 24 horas. Se o link expirar, você terá que gerar um novo seguindo os mesmos passos.
  No dispositivo em que deseja instalar seu produto Bitdefender, verifique a conta de e-mail que você digitou e clique no botão de download correspondente.

2. Execute o produto Bitdefender que você baixou.

Para obter mais informações sobre o processo de instalação do Bitdefender, consulte Instalação do seu produto Bitdefender (página 18).

Como posso atualizar o Bitdefender para a versão mais recente?

A partir de agora, a atualização para a versão mais recente é possível sem seguir o procedimento manual de desinstalação e reinstalação. Mais exatamente, o novo produto que inclui novas funcionalidades e melhorias de produto importantes é fornecido por atualização do produto e, se já tiver uma subscrição de Bitdefender ativa, o produto é ativado automaticamente.

Se estiver a utilizar a versão de 2020, é possível atualizar para a versão mais recente ao seguir estes passos:

1. Clique em **REINICIAR AGORA** na notificação recebida com as informações sobre a atualização. Se a perder, aceda à janela

Notificações, aponte para a atualização mais recente e clique no botão **REINICIAR AGORA**. Espere que o dispositivo seja reiniciado.
É apresentada a janela **Novidades** com informações sobre as novas e melhoradas funcionalidades.

2. Clique nas hiperligações **Ler mais** para ser redirecionado para a nossa página dedicada com mais detalhes e artigos úteis.
3. Feche a janela **Novidades** para aceder à interface da nova versão instalada.

Os utilizadores que desejam atualizar gratuitamente da versão 2016 ou inferior para a versão mais recente do Bitdefender, devem remover a sua versão atual no Painel de Controlo, e depois transferir o ficheiro de instalação mais recente do site do Bitdefender no seguinte endereço: https://www.bitdefender.com/Downloads/. A ativação é possível apenas com uma subscrição válida

3.4.2. Bitdefender Central

Como faço para aceder o Bitdefender com outra conta?

Criou uma nova conta Bitdefender e deseja utilizá-la a partir de agora.

Para iniciar sessão com outra conta da Bitdefender:

1. Clique no nome da sua conta no canto superior da **interface do Bitdefender**.
2. Clique em **Alterar Conta** no canto superior direito do ecrã para trocar a conta vinculada ao dispositivo.
3. Digite o endereço de e-mail no campo correspondente e clique em **PRÓXIMO**.
4. Digite sua senha e clique em **ENTRAR**.

> **Observação**
> O produto Bitdefender do seu dispositivo muda automaticamente de acordo com a subscrição associada à nova conta Bitdefender. Se não houver uma subscrição associada à nova conta Bitdefender ou caso pretenda transferi-la da conta anterior, pode contatar o Bitdefender para obter suporte, como descrito na secção Pedir Ajuda (página 261).

Como desligar as mensagens de ajuda da Central Bitdefender?

As mensagens de ajuda são exibidas no painel para ajudá-lo a entender como cada opção na Bitdefender Central é útil.

Se pretender deixar de ver este tipo de mensagens:

1. Acesso Bitdefender Central.
2. Clique no ícone no canto superior direito da tela.
3. Clique em **A Minha Conta** no menu deslizante.
4. Clique em **Definições** no menu deslizante.
5. Desative a opção **Ativar/desativar mensagens de ajuda**.

Esqueci-me da palavra-passe que defini para a minha conta Bitdefender. Como é que a reponho?

Existem duas possibilidades para definir uma nova palavra-passe para a sua conta do Bitdefender:

- De Interface do Bitdefender:
  1. Clique **Minha conta** no menu de navegação do Interface do Bitdefender.
  2. Clique no botão **Alterar Conta** no canto superior direito do ecrã. Aparece uma nova janela.
  3. Introduza o seu endereço de e-mail e clique em **PRÓXIMO**. Uma nova janela aparece.
  4. Clique **Esqueceu sua senha?**.
  5. Clique em **PRÓXIMO**.
  6. Verifique sua conta de e-mail, digite o código de segurança que você recebeu e clique em **PRÓXIMO**. Alternativamente, você pode clicar **Alterar a senha** no e-mail que lhe enviamos.
  7. Digite a nova senha que deseja definir e digite-a novamente. Clique **SALVAR**.
- No seu navegador da Web:
  1. Vá para: https://central.bitdefender.com.

2. Clique em **ENTRAR**.
3. Digite seu endereço de e-mail e clique em **PRÓXIMO**.
4. Clique **Esqueceu sua senha?**.
5. Clique **PRÓXIMO**.
6. Verifique a sua conta de e-mail e siga as instruções fornecidas para definir a nova palavra-passe da sua conta Bitdefender.

A partir de agora, para aceder à sua conta Bitdefender, escreva o seu endereço de e-mail e a nova palavra-passe que acabou de definir.

Como posso gerir os inícios de sessão associados à minha conta do Bitdefender?

Na sua conta do Bitdefender tem a possibilidade de ver os últimos inícios de sessão inativos e ativos a funcionar em dispositivos associados à sua conta. Além disso, pode terminar sessão remotamente seguindo os seguintes passos:

1. Acesso Bitdefender Central.
2. Clique no ícone no canto superior direito da tela.
3. Clique em **Sessões** no menu deslizante.
4. Na área de **Sessões ativas**, selecione a opção **SAIR** próxima ao dispositivo em que deseja encerrar sessão.

3.4.3. A analisar com BitDefender

Como posso analisar um ficheiro ou uma pasta?

A forma mais fácil para verificar um ficheiro ou pasta é clicando com o botão direito no objeto que deseja verificar, apontar para o Bitdefender e selecionar no menu **Verificar com o Bitdefender**.

Para concluir a análise, siga o assistente de Análise Antivírus. O Bitdefender tomará automaticamente as ações recomendadas nos ficheiros detetados.

Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

Situações típicas em que deve de usar este método de análise são as seguintes:

- Suspeita que um determinado ficheiro ou pasta está infectado.
- Sempre que descarrega ficheiros da Internet que julga serem perigosos.
- Verifique uma partilha de rede antes de copiar os ficheiros para o seu dispositivo.

Como posso analisar o seu sistema

Para realizar uma análise completa no sistema:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Clique no botão **Executar verificação** ao lado de **Verificação do sistema**.
4. Siga as instruções do assistente de Verificação do Sistema para concluir a verificação. O Bitdefender tomará automaticamente as ações recomendadas nos ficheiros detetados.
   Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas. Para mais informação, dirija-se a .

Como programar uma verificação?

Pode configurar o seu produto Bitdefender para iniciar a verificação de locais importantes do sistema quando não estiver a utilizar o dispositivo.

Para agendar uma análise:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Clique em ··· ao lado do tipo de verificação que deseja programar, Análise de Sistema ou Análise Rápida na parte inferior da interface e, em seguida, selecione **Editar**.
   Também pode criar um tipo de verificação que atenda às suas necessidades clicando em **+Criar verificação** ao lado de **Gerir verificações**.
4. Personalize a análise de acordo com as suas necessidades e, em seguida, clique em **Seguinte**.

5. Marque a caixa ao lado de **Escolha quando agendar esta tarefa**. Selecione uma das opções correspondentes para definir uma agenda:
   - Na inicialização do sistema
   - Diário
   - Semanalmente
   - Por mês

   Se você escolher Diariamente, Mensalmente ou Semanalmente, arraste o controle deslizante ao longo da escala para definir o período de tempo desejado quando a verificação agendada deve começar.

Se escolher criar uma nova análise personalizada, a janela **Tarefa de análise** aparecerá. Aqui, pode selecionar os locais que deseja analisar.

Como posso criar uma tarefa de análise personalizada?

Se quer analisar localizações específicas no seu dispositivo ou configurar as opções de análise, pode configurar e executar uma tarefa personalizada.

Para criar uma tarefa de análise personalizada, proceda da seguinte forma:

1. No **ANTIVÍRUS** painel, clique **Abrir**.
2. Clique em **+Criar verificação** ao lado de **Gerir verificações**.
3. No campo de nome da tarefa, introduza o nome da verificação e selecione os locais que deseja analisar e, em seguida, clique em **SEGUINTE**.
4. Configure estas opções gerais:
   - **Verificar apenas aplicações.** Pode configurar o Bitdefender para verificar apenas aplicações acedidas.
   - **Verificar prioridade de tarefas.** Pode escolher o impacto que o processo de verificação tem no desempenho do seu sistema.
     - Auto - A prioridade do processo de verificação dependerá da atividade do sistema. Para garantir que o processo de verificação não afetará a atividade do sistema, o Bitdefender decidirá se o processo de verificação deve ser executado com alta ou baixa prioridade.

- Alta - A prioridade do processo de verificação será alta. Ao escolher esta opção, você permitirá que outros programas sejam executados mais lentamente e diminuirá o tempo necessário para que o processo de verificação seja concluído.
- Baixa - A prioridade do processo de verificação será baixa. Ao escolher esta opção, você permitirá que outros programas sejam executados mais rapidamente e aumentará o tempo necessário para a conclusão do processo de verificação.

- **Medidas pós-verificação.** Escolha a ação que o Bitdefender deve realizar se não forem encontradas ameaças:
  - Mostrar janela de resumo
  - Dispositivo de desligamento
  - Fechar janela de digitalização

5. Se deseja configurar as opções de análise detalhadamente, clique em **Mostrar opções avançadas**.
   Clique **Próximo**.
6. Pode ativar a opção **Programar tarefa de análise** e, se quiser, escolha quando a análise personalizada que criou deve começar.
   - Na inicialização do sistema
   - Diário
   - Por mês
   - Semanalmente

   Se você escolher Diariamente, Mensalmente ou Semanalmente, arraste o controle deslizante ao longo da escala para definir o período de tempo desejado quando a verificação agendada deve começar.
7. Clique **Salvar** para salvar as configurações e fechar a janela de configuração.
   Dependendo dos locais a serem verificados, a verificação pode demorar um pouco. Se forem encontradas ameaças durante o processo de verificação, você será solicitado a escolher as ações a serem executadas nos arquivos detectados.

Se quiser, pode voltar a executar rapidamente uma análise personalizada anterior ao clicar na entrada correspondente na lista disponível.

Como excluir uma pasta da análise?

O Bitdefender permite excluir ficheiros, pastas ou extensões de ficheiros específicos da análise.

As exceções devem ser usadas pelos utilizadores que possuem conhecimento informáticos avançados e apenas nas seguintes situações:

- Você tem uma pasta grande no seu sistema onde guarda filmes e música.
- Você tem um ficheiro grande no seu sistema onde guarda diferentes dados.
- Você tem uma pasta onde instala diferentes tipos de software e aplicações para testar. A análise da pasta pode resultar na perda de alguns dados.

Para adicionar uma pasta à lista de Exceções:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Clique na aba **Definições**.
4. Clique em **Gerir exceções**.
5. Clique **+Adicionar uma exceção**.
6. Insira o caminho da pasta que deseja excluir da digitalização no campo correspondente.
   Como alternativa, você pode navegar até a pasta clicando no botão Procurar no lado direito da interface, selecioná-la e clicar em **OK**.
7. Ligue o interruptor ao lado do recurso de proteção que não deve verificar a pasta. Existem três opções:
   - antivírus
   - Prevenção de ameaças on-line
   - Defesa Avançada contra Ameaças
8. Clique **Salvar** para salvar as alterações e fechar a janela.

O que fazer se o Bitdefender identificar um ficheiro limpo como infectado?

Pode haver casos em que o Bitdefender marque erroneamente um ficheiro legítimo como sendo uma ameaça (um falso positivo). Para corrigir este erro, adicione o ficheiros à área de exceções do Bitdefender:

1. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
   b. No **ANTIVÍRUS** painel, clique **Abrir**.
   c. Na janela **Avançado**, desative o **Bitdefender Shield**.
   Aparece uma janela de aviso. Tem de confirmar a sua escolha seleccionando no menu durante quanto tempo pretende desactivar a protecção em tempo real. Pode desativar a sua proteção em tempo real durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até ao reinício do sistema.
2. Mostrar ficheiros ocultos no Windows. Para saber mais sobre como fazer isto, aceda a Como posso mostrar objetos ocultos no Windows? (página 124).
3. Restaurar o ficheiro da área de Quarentena:
   a. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
   b. No **ANTIVÍRUS** painel, clique **Abrir**.
   c. Vá para a janela **Definições** e clique em **Gerir a quarentena**.
   d. Selecione o ficheiro e, em seguida, clique em **Restaurar**.
4. Adicione o ficheiro à Lista de exceções. Para saber mais sobre como fazer isso, aceda Como excluir uma pasta da análise? (página 111).
5. Ligue a proteção antivírus em tempo real do Bitdefender.
6. Entre em contacto com os nossos representantes do apoio para que possamos remover a deteção da atualização da informação de ameaça. Para saber mais sobre como fazer isto, aceda a Pedir Ajuda (página 261).

Como posso saber que ameaças o Bitdefender detetou?

Cada vez que uma análise é levada a cabo, um registo de análise é criado e o Bitdefender regista as incidências detetadas.

O relatório da análise contém informação detalhada acerca dos processos de análise registados, tal como as opções da análise, o alvo da análise, as ameaças encontradas e as acções tomadas sobre essas ameaças.

Você pode abrir o log de verificação diretamente do assistente de verificação, uma vez que a verificação for concluída, clicando em **MOSTRAR LOG**.

Para verificar um log de verificação ou qualquer infecção detectada posteriormente:

1. Clique **Notificações** no menu de navegação do Interface do Bitdefender.
2. No **Todos** guia, selecione a notificação sobre a verificação mais recente.
   É aqui que você pode encontrar todos os eventos de varredura de ameaças, incluindo ameaças detectadas por varredura no acesso, varreduras iniciadas pelo usuário e alterações de status para varreduras automáticas.
3. Na lista de notificações, você pode verificar quais verificações foram realizadas recentemente. Clique em uma notificação para ver os detalhes sobre ela.
4. Para abrir um relatório da análise, clique em **Ver Relatório**.

3.4.4. Controlo de Privacidade

Como posso ter a certeza de que a minha transação online é segura?

Para ter a certeza de que as suas operações online se mantém privadas, pode usar o browser fornecido pelo Bitdefender para proteger as suas transações e as suas aplicações bancárias.

O Bitdefender Safepay™ é um navegador desenhado para proteger as informações do seu cartão de crédito, número de conta ou qualquer outro dado pessoal que possa utilizar enquanto acede a diferentes localizações online.

Para manter a sua atividade online segura e privada:

1. Clique **Privacidade** no menu de navegação do Interface do Bitdefender.
2. No **SAFEPAY** painel, clique **Configurações**.
3. No **Safepay** janela, clique **Lançar Safepay**.
4. Clique no botão para aceder ao **Teclado virtual**.
   Use o **Teclado Virtual** quando inserir informação sensível tal como palavras-passe.

O que posso fazer se o meu dispositivo tiver sido roubado?

O roubo de dispositivos móveis, seja um smartphone, um tablet ou um portátil é um dos principais problemas que afetam os indivíduos e as organizações de todo o mundo nos dias de hoje.

O Bitdefender Antirroubo permite não só localizar e bloquear o dispositivo roubado, mas também limpar todos os dados para garantir que ele não será utilizado pelo ladrão.

Para aceder às funções anti-furto da sua conta:

1. Acesso Bitdefender Central.
2. Selecione os **Meus dispositivos** painel.
3. Clique no cartão do dispositivo pretendido e, em seguida, selecione **Anti-furto**.
4. Selecione a funcionalidade que deseja usar:
   - **LOCALIZAR** - exibe a localização do seu dispositivo no Google Maps.
     Mostrar IP - exibe o último endereço de IP para o dispositivo selecionado.
   - **Alerta** - envie um alerta ao dispositivo.
   - **Bloqueio** - bloqueie o seu dispositivo e defina um código PIN para desbloqueá-lo. De forma alternativa, ative a opção correspondente para permitir que o Bitdefender tire fotos da pessoa que está a tentar aceder ao seu dispositivo.
   - **Limpeza** - apague todos os dados do seu dispositivo.

Importante

Após apagar toda a informação de um dispositivo, todas as funcionalidades Anti-Roubo deixam de funcionar.

Como removo um ficheiro permanentemente com o Bitdefender?

Se deseja remover um ficheiro permanentemente do seu sistema, necessita de apagar a informação fisicamente do seu disco duro.

O Destruidor de Ficheiros da Bitdefender irá ajudá-lo a destruir rapidamente os ficheiros ou as pastas do seu dispositivo ao utilizar o menu de contexto do Windows ao realizar os passos a seguir:

1. Clique com o botão direito do rato no ficheiro ou pasta que quer apagar permanentemente, selecione Bitdefender e clique em **Destruidor de Ficheiros**.
2. Clique **Apagar permanentemente**e, em seguida, confirme que deseja continuar com o processo.
   Aguarde que o Bitdefender termine de triturar os arquivos.
3. Os resultados são apresentados. Clique em **TERMINAR** para sair do assistente.

Como protejo a minha câmara Web contra hacking?

Pode configurar o produto Bitdefender para permitir ou negar o acesso das aplicações instaladas à sua câmara Web ao seguir estes passos:

1. Clique **Privacidade** no menu de navegação do Interface do Bitdefender.
2. No **PROTEÇÃO DE VÍDEO E ÁUDIO** painel, clique **Configurações**.
3. Vá para a janela **Proteção da Webcam** e verá a lista com as aplicações que solicitaram acesso à sua câmara.
4. Indique a aplicação cujo acesso deseja permitir ou proibir e, em seguida, clique no botão representado por uma câmara de vídeo, situada ao lado dele.
   Para ver o que os outros utilizadores do Bitdefender escolheram fazer com a aplicação selecionada, clique no ícone . Será notificado sempre que uma das aplicações listados for bloqueada por utilizadores do Bitdefender.

Para adicionar aplicações manualmente a esta lista, clique no botão **Adicionar aplicação** e selecione uma das duas opções.

- Da Windows Store
- Das suas aplicações

Como posso restaurar manualmente ficheiros encriptados quando o processo de restauração falhar?

Caso ficheiros encriptados não possam ser automaticamente restaurados, pode restaurá-los manualmente seguindo estes passos:

1. Clique **Notificações** no menu de navegação do Interface do Bitdefender.
2. No **Todos** guia, selecione a notificação sobre o último comportamento de ransomware detectado e clique em **Arquivos Criptografados**.
3. A lista com os arquivos criptografados é exibida.
   Clique em **Recuperar ficheiros** para continuar.
4. Caso todo ou parte do processo de restauração falhe, você deve escolher o local onde os arquivos descriptografados devem ser salvos.
   Clique **Restaurar localização**e, em seguida, escolha um local no seu PC.
5. Uma janela de confirmação é exibida.
   Clique **Terminar** para finalizar o processo de restauração.

Arquivos com as seguintes extensões podem ser restaurados caso sejam criptografados:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com ; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

3.4.5. Ferramentas de otimização

Como melhorar o desempenho do meu sistema?

O desempenho do sistema não depende apenas da configuração do hardware, como carga da CPU, uso de memória e espaço no disco rígido. Também está diretamente conectado à sua configuração de software e ao seu gerenciamento de dados.

Estas são as principais ações que você pode realizar com o Bitdefender para melhorar a velocidade e o desempenho do seu sistema:

- Otimize o desempenho do seu sistema com um único clique (página 117)
- Escaneie seu sistema periodicamente (página 117)

Otimize o desempenho do seu sistema com um único clique

A opção OneClick Optimizer economiza um tempo valioso quando você deseja uma maneira rápida de melhorar o desempenho do sistema, verificando, detectando e limpando rapidamente arquivos inúteis.

Para iniciar o processo do OneClick Optimizer:

1. Clique **Serviços de utilidade pública** no menu de navegação do Interface do Bitdefender.
2. Clique no **otimizar** botão.
3. Deixe o Bitdefender procurar por arquivos que podem ser excluídos e, em seguida, clique no botão **otimizar** botão para finalizar o processo.

Escaneie seu sistema periodicamente

A velocidade do sistema e seu comportamento geral também podem ser afetados por ameaças.

Certifique-se de verificar seu sistema periodicamente, pelo menos uma vez por semana.

É recomendável usar o System Scan porque ele verifica todos os tipos de ameaças que colocam em risco a segurança do seu sistema e também verifica dentro de arquivos.

Para iniciar a verificação do sistema:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Clique **Executar verificação** ao lado de **Verificação do sistema**.
4. Siga as etapas do assistente.

3.4.6. Informações Úteis

Como posso testar a minha solução de segurança?

Para garantir que o seu produto Bitdefender está a funcionar corretamente, recomendamos a utilização do teste Eicar.

O teste Eicar permite que verifique a sua solução de segurança utilizando um ficheiro de segurança desenvolvido para este fim.

Para testar a sua solução de segurança:

1. Transfira o teste da página oficial da organização EICAR http://www.eicar.org/.
2. Clique no separador **Ficheiro de teste antimalware**.
3. Clique em **Transferir** no menu do lado esquerdo.
4. A partir da **Área de transferência utilizando o protocolo padrão http**, clique no ficheiro de teste **eicar.com**.
5. Receberá informações de que a página a que está a tentar aceder contém o Ficheiro de Teste EICAR (não é uma ameaça).
   Caso clique em **Compreendo os riscos, leve-me até lá mesmo assim**, a transferência do teste irá iniciar e um pop-up do Bitdefender irá informá-lo da deteção de uma ameaça.
   Clique em **Mais Detalhes** para obter mais informações sobre esta ação.

Caso não receba qualquer alerta de Bitdefender, recomendamos que entre em contacto com Bitdefender para suporte conforme descrito na secção Pedir Ajuda (página 261).

Como removo o Bitdefender?

Se deseja remover o seu Bitdefender Total Security:

- Em **windows 7**:

1. Clique **Começar**, Vá para **Painel de controle** e clique duas vezes **Programas e características**.
2. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
3. Clique em **REMOVER** na janela que aparece.
4. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

- Em **Windows 8** e **Windows 8.1**:
  1. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
  2. Clique **Desinstalar um programa** ou **Programas e características**.
  3. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique **REMOVER** na janela que aparece.
  5. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

- Em **Windows 10** e **Windows 11**:
  1. Clique em **Iniciar**, em seguida, clique em Definições.
  2. Clique no **Sistema** ícone na área Configurações e selecione **aplicativos**.
  3. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique **Desinstalar** novamente para confirmar sua escolha.
  5. Clique **REMOVER** na janela que aparece.
  6. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

  Observação
  Este procedimento de reinstalação irá eliminar permanentemente as definições personalizadas.

Como removo o Bitdefender VPN?

O procedimento de remoção do Bitdefender VPN é semelhante ao que usa para remover outros programas do seu dispositivo:

- Em **windows 7**:
  1. Clique **Começar**, Vá para **Painel de controle** e clique duas vezes **Programas e características**.
  2. Localize o **Bitdefender VPN** e selecione **Desinstalar**.
     Aguarde até que o processo de desinstalação seja concluído.
- Em **Windows 8** e **Windows 8.1**:
  1. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
  2. Clique **Desinstalar** um programa ou **Programas e características**.
  3. Encontrar **Bitdefender VPN** e selecione **Desinstalar**.
     Aguarde a conclusão do processo de desinstalação.
- Em **Windows 10** e **Windows 11**:
  1. Clique **Começar**e clique em Configurações.
  2. Clique no ícone **Sistema** na área de Definições e, em seguida, selecione **Aplicações instaladas**.
  3. Encontrar **Bitdefender VPN** e selecione **Desinstalar**.
  4. Clique **Desinstalar** novamente para confirmar sua escolha.
     Aguarde a conclusão do processo de desinstalação.

Como remover a extensão do Bitdefender Antitracker?

Dependendo do navegador que esteja a utilizar, siga estes passos para desinstalar a extensão do Bitdefender Antitracker:

- Internet Explorer
  1. Clique em ⚙ ao lado da barra de pesquisa e, em seguida, selecione Gerir suplementos. Será exibida a lista das extensões instaladas.
  2. Clique em Bitdefender Antitracker.
  3. Clique em **Desativar** no canto inferior direito.
- Google Chrome
  1. Clique em ⋮ ao lado da barra de pesquisa.

2. Selecione **Mais ferramentas** e, em seguida, **Extensões**.
   Será exibida a lista das extensões instaladas.
3. Clique em **Remover** no cartão Bitdefender Antitracker.
4. Clique em **Remover** na janela pop-up que aparece.

- Mozilla Firefox

  1. Clique ☰ ao lado da barra de pesquisa.
  2. Selecione **Suplementos** e, em seguida, selecione **Extensões**.
     Uma lista com as extensões instaladas é exibida.
  3. Clique em ··· e, em seguida, selecione **Remover**.

Como desligo automaticamente o meu dispositivo após terminar a análise?

O Bitdefender oferece múltiplas tarefas de análise que pode usar para se certificar que o seu sistema não está infectado com ameaças. Analisar todo o dispositivo pode demorar muito mais tempo a concluir dependendo do hardware do seu sistema e da configuração do seu software.

Por este motivo, o Bitdefender permite-lhe configurar o produto para desligar o computador assim que a análise terminar.

Considere este exemplo: terminou o seu trabalho e quer ir dormir. Gostaria que o seu sistema fosse completamente analisado quanto a ameaças pelo Bitdefender.

Para desligar o dispositivo uma vez finalizada a Análise Rápida ou a Análise de Sistema:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Na janela **Análises**, clique em ···, ao lado da Análise Rápida ou Análise do Sistema, e selecione **Editar**.
4. Personalize a análise de acordo com as suas necessidades e clique em **Seguinte**.
5. Marque a caixa ao lado de **Escolher quando agendar esta tarefa** e, em seguida, escolha quando a tarefa deve começar.

Se você escolher Diariamente, Mensalmente ou Semanalmente, arraste o controle deslizante ao longo da escala para definir o período de tempo desejado quando a verificação agendada deve começar.

6. Clique **Salvar**.

Para desligar o dispositivo ao finalizar uma análise personalizada:

1. Clique em ⋯ ao lado da análise personalizada que criou.
2. Clique em **Seguinte** e, em seguida, clique em **Seguinte** novamente.
3. marque a caixa ao lado de **Escolher quando agendar esta tarefa** e, em seguida, escolha quando a tarefa deve ser iniciada.
4. Clique **Salvar**.

Se não forem encontradas ameaças, o dispositivo desligar-se-á.

Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas. Para mais informação, dirija-se a Assistente de Análise Antivírus (página 36).

Como posso configurar o Bitdefender para utilizar uma ligação à internet com proxy?

Se o seu dispositivo se ligar à Internet através de um servidor proxy, deve configurar as definições do proxy do Bitdefender. Normalmente, o Bitdefender deteta e importa automaticamente as definições proxy do seu sistema.

> **Importante**
> As ligações à Internet domésticas normalmente não usam um servidor proxy. Como regra de ouro, verifique e configure as definições da ligação proxy do seu programa Bitdefender quando as atualizações não funcionam. Se o Bitdefender atualizar, então está corretamente configurado à Internet.

Para gerir as definições de proxy:

1. Clique **Configurações** no menu de navegação do Interface do Bitdefender.
2. Selecione os **Avançado** aba.
3. Ative o **Servidor proxy**.
4. Clique em **Alteração de proxy**.

5. Existem duas opções para as definições do proxy:
   - **Importe as definições de proxy do navegador por defeito** - as definições de proxy do utilizador atual, extraídas do explorador por defeito. Se o servidor proxy requer um nome de utilizador e uma palavra-passe, deverá inseri-los nos campos correspondentes.

     > **Observação**
     > O Bitdefender pode importar definições de proxy dos browsers mais populares, incluindo as mais recentes versões do Microsoft Edge, Internet Explorer, Mozilla Firefox e Google Chrome.

   - **Definições de proxy personalizadas** - definições de proxy que você pode configurar.
     As seguintes definições devem ser especificadas:
     - **Endereço** - introduza o IP do servidor proxy.
     - **Porta** - introduza a porta que o Bitdefender utiliza para estabelecer ligação ao servidor proxy.
     - **Nome de usuário** - introduza um nome de utilizador reconhecido pelo proxy.
     - **Palavra-passe** - introduza a palavra-passe válida do utilizador previamente especificado.

6. Clique em **OK** para guardar as alterações e fechar a janela.

O Bitdefender usará as definições de proxy disponíveis até conseguir ligar à Internet.

Estou a utilizar uma versão de 32 ou 64 Bit do Windows?

Para descobrir se possui sistema operativo de 32 bits ou 64 bits:

- Em **windows 7**:
  1. Clique em **Iniciar**.
  2. Localize **Computador** no menu **Iniciar**.
  3. Clique com o botão direito do rato em **Computador** e selecione **Propriedades**.
  4. Procure na secção **Sistema** a informação sobre o seu sistema.

- No **Windows 8**:
  1. A partir do ecrã Iniciar do Windows, localize **Computador** (por exemplo, pode começar a digitar "Computador" diretamente no menu Iniciar) e, em seguida, clique com o botão direito do rato no seu ícone.
  2. Selecione **Propriedades** no menu inferior.
  3. Procure na área do Sistema o seu tipo de sistema.
- Em **Windows 10** e **Windows 11**:
  1. Introduza "Sistema" na caixa de pesquisa da barra de tarefas e, em seguida, clique no ícone correspondente.
  2. Procure por informações sobre o tipo do sistema na área do Sistema.

Como posso mostrar objetos ocultos no Windows?

Estes passos são úteis nos casos de ameaças e se tiver de encontrar e remover os ficheiros infectados, que poderão estar ocultos.

Siga os seguintes passos para mostrar objetos ocultos no Windows:

1. Clique em **Iniciar**, vá para o **Painel de Controlo**.
   No **Windows 8** e no **Windows 8.1**: No ecrã inicial do Windows, localize o **Painel de Controlo** (por exemplo, pode começar a introduzir "Painel de Controlo" diretamente no ecrã inicial) e depois clique no ícone.
2. Selecione **Opções de pasta**.
3. Aceda ao separador **Visualizar**.
4. Selecione **Mostrar ficheiros e pastas ocultos**.
5. Desmarque **Ocultar extensões nos tipos de ficheiro conhecidos**.
6. Desmarque **Ocultar ficheiros protegidos do sistema operativo**.
7. Clique em **Aplicar** e, em seguida, clique em **OK**.

Em **Windows 10** e **Windows 11**:

1. Introduza "Mostrar ficheiros e pastas ocultos" na caixa de pesquisa da barra de tarefas e, em seguida, clique no ícone correspondente.
2. Selecione **Mostrar ficheiros, pastas e unidades ocultos**.

3. Claro **Ocultar extensões de ficheiros conhecidos**.
4. Claro **Ocultar arquivos protegidos do sistema operacional**.
5. Clique **Aplicar**, então clique **OK**.

Como posso remover outras soluções de segurança?

A principal razão para utilizar uma solução de segurança é proporcionar proteção e segurança aos seus dados. Mas o que acontece quando tem mais do que um produto de segurança no mesmo sistema?

Quando utiliza mais do que uma solução de segurança no mesmo dispositivo, o sistema torna-se instável. O instalador do Bitdefender Total Security deteta automaticamente outros programas de segurança e oferece-lhe a opção de os desinstalar.

Se não tiver removido as outras soluções de segurança durante a instalação inicial:

- Em **windows 7**:
  1. Clique **Começar**, Vá para **Painel de controle** e clique duas vezes **Programas e características**.
  2. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
  3. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.
  4. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

- Em **Windows 8** e **Windows 8.1**:
  1. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
  2. Clique **Desinstalar um programa** ou **Programas e características**.
  3. Aguarde alguns instantes até que a lista de softwares instalados seja exibida.
  4. Encontre o nome do programa que deseja remover e selecione **Desinstalar**.

5. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

- Em **Windows 10** e **Windows 11**:
  1. Clique **Começar**e clique em Configurações.
  2. Clique no **Sistema** ícone na área Configurações e selecione **aplicativos**.
  3. Encontre o nome do programa que deseja remover e selecione **Desinstalar**.
  4. Clique **Desinstalar** novamente para confirmar sua escolha.
  5. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

Se não conseguir remover as outras soluções de segurança do seu sistema, obtenha a ferramenta de desinstalação do site Internet do fornecedor ou contacte-o diretamente para receber instruções de desinstalação.

Como posso reiniciar no Modo de Segurança?

O Modo de Segurança é um modo operativo de diagnóstico, utilizado principalmente para detetar e resolver problemas que estejam a afetar o funcionamento normal do Windows. As causas destes problemas vão desde a incompatibilidade de controladores a ameaças que impedem o arranque normal do Windows. No Modo de Segurança funcionam apenas algumas aplicações e o Windows só carrega os controladores básicos e os componentes mínimos do sistema operativo. É por isso que a maioria das ameaças está inativa quando o Windows está no Modo de Segurança e podem ser facilmente removidos.

Para iniciar o Windows no Modo de Segurança:

- Em **windows 7**:
  1. Reinicie o dispositivo.
  2. Prima a tecla **F8** várias vezes antes de o Windows iniciar para aceder ao menu de arranque.
  3. Selecione **Modo de Segurança** no menu de arranque ou **Modo de segurança com rede**, se quiser ter acesso à internet.

4. Prima em **Enter** e aguarde enquanto o Windows carrega o Modo Seguro.
5. Este processo termina com uma mensagem de confirmação. Clique em **OK** para confirmar.
6. Para iniciar o Windows normalmente, basta reiniciar o sistema.

- No **Windows 8**, **Windows 8.1**, **Windows 10** e **Windows 11**:
  1. Execute a **Configuração do sistema** no Windows pressionando simultaneamente as teclas **Windows + R** no seu teclado.
  2. Escreva **msconfig** na caixa de diálogo **Abrir** e, em seguida, clique em **OK**.
  3. Selecione o separador **Arranque**.
  4. Na área **Opções de arranque** selecione a caixa **Arranque seguro**.
  5. Clique em **Rede** e, em seguida, clique em **OK**.
  6. Clique em **OK** na janela **Configuração do Sistema** que informa que o sistema tem de ser reiniciado para poder implementar as alterações que definiu.
     O seu sistema será reiniciado no Modo Seguro com rede.

Para arrancar novamente no modo normal, reverta as definições executando novamente a **Operação do Sistema** e desmarcando a caixa de verificação **Arranque seguro**. Clique em **OK** e, em seguida, em **Reiniciar**. Aguarde ate que as novas definições sejam aplicadas.

3.5. Solução de problemas

3.5.1. Resolver incidências comuns

Este capítulo apresenta alguns dos problemas que poderão surgir enquanto utiliza o BitDefender, e providencia possiveis soluções. A maioria destes problemas podem ser resolvidos através da configuração adequada das definições do produto.

- O meu sistema parece estar lento (página 128)
- A análise não inicia (página 129)
- Já não posso utilizar uma aplicação (página 132)

- O que fazer quando o Bitdefender bloqueia um site, domínio, endereço IP ou aplicação online que é seguro (página 133)
- Como atualizar o Bitdefender numa ligação à Internet lenta (página 138)
- Os serviços do Bitdefender não estão a responder (página 138)
- A remoção Bitdefender falhou (página 144)
- O meu sistema não reinicia após a instalação de Bitdefender (página 145)

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contacta os representantes do suporte técnico da BitDefender como está representado no capítulo Pedir Ajuda (página 261).

O meu sistema parece estar lento

Normalmente, após a instalação de um software de segurança, o sistema poderá abrandar ligeiramente, o que é, até um certo nível, normal.

Se notar um abrandamento significativo, este problema pode dever-se às seguintes razões:

- **O Bitdefender não é o único programa de segurança instalado no sistema.**
  Apesar de o Bitdefender procurar e remover os programas de segurança encontrados durante a instalação, é recomendado que remova todas as outras soluções de segurança utilizadas antes de instalar o Bitdefender. Para mais informação, dirija-se a Como posso remover outras soluções de segurança? (página 125).
- **Não estão cumpridos os requisitos do sistema para executar o Bitdefender.**
  Se o seu dispositivo não cumprir os Requisitos do Sistema, ficará lento, especialmente se estiver a executar várias aplicações ao mesmo tempo. Para mais informação, dirija-se a Requisitos do sistema (página 16).
- **Instalou aplicações que não utiliza.**
  Qualquer dispositivo tem programas ou aplicações que não utiliza. E quaisquer programas indesejados são executados em segundo plano, ocupando espaço no disco rígido e na memória. Caso não utilize um

programa, desinstale-o. Também se aplica a qualquer outro software pré-instalado ou aplicação de teste que se esqueceu de remover.

> **Importante**
> Se suspeitar que um programa ou uma aplicação é uma parte essencial do seu sistema operativo, não o remova e contacte o Serviço de Apoio ao Cliente da Bitdefender para obter assistência.

- **O seu sistema pode estar infetado.**
  A velocidade do seu sistema e do seu comportamento geral também podem ser afetados por ameaças. Spyware, malware, trojans e adware, todos afetam o desempenho do seu dispositivo. Certifique-se de verificar o seu sistema periodicamente, ao menos uma vez por semana. É recomendado utilizar a Verificação de Sistema da Bitdefender porque ela verifica todos os tipos de ameaça que colocam em risco a segurança do seu sistema.
  Para iniciar a Verificação do Sistema:

  1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
  2. No **ANTIVÍRUS** painel, clique **Abrir**.
  3. Na janela **Análises**, clique em **Executar análise** ao lado de **Análise do sistema**.
  4. Siga os passos do assistente.

A análise não inicia

Este tipo de problema pode ter duas causas principais:

- **Uma instalação anterior do Bitdefender que não foi totalmente removida ou uma instalação do Bitdefender mal sucedida.**
  Neste caso, reinstale o Bitdefender:
  - Em **windows 7**:
    1. Clique **Começar**, Vá para **Painel de controle** e clique duas vezes **Programas e características**.
    2. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
    3. Clique **REINSTALAR** na janela que aparece.

4. Aguarde pela conclusão do processo de reinstalação e reinicie o sistema.

- Em **Windows 8** e **Windows 8.1**:

  1. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
  2. Clique **Desinstalar** um programa ou **Programas e características**.
  3. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique **REINSTALAR** na janela que aparece.
  5. Aguarde a conclusão do processo de reinstalação e reinicie o sistema.

- Em **Windows 10** e **Windows 11**:

  1. Clique **Começar**, então clique **Configurações**.
  2. Clique no **Sistema** ícone na área Configurações e selecione **Aplicativos instalados**.
  3. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique **Desinstalar** novamente para confirmar sua escolha.
  5. Clique **REINSTALAR** na janela que aparece.
  6. Aguarde a conclusão do processo de reinstalação e reinicie o sistema.

  Observação
  Ao seguir este procedimento de reinstalação, as configurações personalizadas são salvas e disponibilizadas no novo produto instalado. Outras configurações podem ser alteradas de volta para sua configuração padrão.

- **O Bitdefender não é a única solução de segurança instalada no seu sistema.**
  Neste caso:

1. Remover a outra solução de segurança. Para mais informação, dirija-se a Como posso remover outras soluções de segurança? (página 125).
2. Reinstale o Bitdefender:
   - Em **windows 7**:
     a. Clique **Começar**, Vá para **Painel de controle** e clique duas vezes **Programas e características**.
     b. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
     c. Clique **REINSTALAR** na janela que aparece.
     d. Aguarde a conclusão do processo de reinstalação e reinicie o sistema.
   - Em **Windows 8** e **Windows 8.1**:
     a. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
     b. Clique **Desinstalar** um programa ou **Programas e características**.
     c. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
     d. Clique **REINSTALAR** na janela que aparece.
     e. Aguarde a conclusão do processo de reinstalação e reinicie o sistema.
   - Em **Windows 10** e **Windows 11**:
     a. Clique **Começar**, então clique **Configurações**.
     b. Clique no **Sistema** ícone na área Configurações e selecione **Aplicativos instalados**.
     c. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
     d. Clique **Desinstalar** novamente para confirmar sua escolha.
     e. Clique em **REINSTALAR** na janela que aparece

f. Aguarde a conclusão do processo de reinstalação e reinicie o sistema.

> **Observação**
> Ao seguir este procedimento de reinstalação, as configurações personalizadas são salvas e disponibilizadas no novo produto instalado. Outras configurações podem ser alteradas de volta para sua configuração padrão.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção Pedir Ajuda (página 261).

Já não posso utilizar uma aplicação

Este problema ocorre quando está a tentar utilizar um programa que estava a funcionar normalmente antes de instalar o Bitdefender.

Após instalar o Bitdefender pode deparar-se com uma das seguintes situações:

- Poderá receber uma mensagem do Bitdefender a informar que o programa está a tentar modificar o sistema.
- Pode receber uma mensagem de erro do programa que está a tentar utilizar.

Este tipo de situação ocorre quando o Advanced Threat Defense deteta erradamente algumas aplicações como maliciosas.

Advanced Threat Defense é uma funcionalidade do Bitdefender que monitoriza constantemente as aplicações executadas no seu sistema e comunica o comportamento potencialmente malicioso. Como esta funcionalidade se baseia num sistema heurístico, pode haver casos em que as aplicações legítimas são comunicadas pelo Advanced Threat Defense.

Quando isso acontecer, poderá excluir a respectiva aplicação para que não seja monitorizada pela Defesa Avançada Contra Ameaças.

Para adicionar o programa à lista de exceções:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **DEFESA AVANÇADA DE AMEAÇA** painel, clique **Abrir**.
3. No **Configurações** janela, clique **Gerenciar exceções**.

4. Clique **+Adicionar uma exceção**.
5. Introduza o caminho do executável que deseja adicionar à lista de exceção da verificação no campo correspondente.
   Como alternativa, você pode navegar até o executável clicando no botão de navegação no lado direito da interface, selecione-o e clique em **OK**.
6. Ligue o interruptor ao lado de **Defesa Avançada contra Ameaças**.
7. Clique **Salvar**.

Se esta informação não for útil, você pode entrar em contato com a Bitdefender para obter suporte conforme descrito na seção Pedir Ajuda (página 261).

O que fazer quando o Bitdefender bloqueia um site, domínio, endereço IP ou aplicação online que é seguro

O Bitdefender oferece uma experiência de navegação segura na web, ao filtrar todo o tráfego da web e ao bloquear qualquer conteúdo malicioso. No entanto, é possível que o Bitdefender considere um site, domínio, endereço IP ou uma aplicação online seguro como inseguro, o que poderá fazer com que a verificação de tráfego HTTP do Bitdefender o bloqueie incorretamente.

Caso a mesma página, domínio, endereço de IP ou aplicação online estejam a ser bloqueados repetidamente, eles poderão ser adicionados para não serem analisados pelos mecanismos da Bitdefender, assegurando uma experiência de navegação mais tranquila.

Para adicionar uma página web a **Exceções**:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **PREVENÇÃO DE AMEAÇAS ONLINE** painel, clique **Configurações**.
3. Clique **Gerenciar exceções**.
4. Clique **+Adicionar uma exceção**.
5. Digite no campo correspondente o nome do site, o nome do domínio ou o endereço IP que deseja adicionar às exceções.
6. Clique no botão ao lado de **Prevenção de ameaças on-line**.
7. Clique **Salvar** para salvar as alterações e fechar a janela.

Apenas sites, domínios, endereços de IP e aplicações nos quais confia plenamente devem ser adicionados à lista. Estes serão excluídos da análise pelos seguintes mecanismos: ameaças, phishing e fraude.

Se esta informação não for útil, você pode entrar em contato com a Bitdefender para obter suporte conforme descrito na seção Pedir Ajuda (página 261).

Não consigo ligar-me à Internet

Poderá verificar que um programa ou navegador da web já não consegue ligar à Internet ou aceder aos serviços em rede após a instalação do Bitdefender.

Neste caso, a melhor solução é configurar o Bitdefender para permitir automaticamente as ligações de e para a respetiva aplicação de software:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **FIREWALL** painel, clique **Configurações**.
3. No **Regras** janela, clique **Adicionar regra**.
4. Abrirá uma nova janela onde poderá adicionar os detalhes. Certifique-se de selecionar todos os tipos de rede disponíveis e na seção **Permissão**, selecione **Permitir**.

Feche o Bitdefender, abra a aplicação de software e tente de novo ligar-se à Internet.

Se esta informação não for útil, você pode entrar em contato com a Bitdefender para obter suporte conforme descrito na seção Pedir Ajuda (página 261).

Não consigo aceder a um dispositivo na minha rede

Dependendo da rede a que está ligado, a firewall do Bitdefender poderá bloquear a ligação entre o seu sistema e outro dispositivo (como outro PC ou uma impressora). Como resultado, já não poderá partilhar ou imprimir ficheiros.

Neste caso, a melhor solução é configurar o Bitdefender para permitir automaticamente as ligações de e para o respetivo dispositivo como se segue:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.

2. No **FIREWALL** painel, clique **Configurações**.
3. No **Regras** janela, clique **Adicionar regra**.
4. Ative a opção **Aplicar esta regra a todas as aplicações**.
5. Clique no botão **Configuração Avançada**.
6. Na caixa **Endereço remoto personalizado**, digite o endereço de IP do PC ou da impressora aos quais deseja ter acesso ilimitado.

Se ainda não conegue ligar-se ao dispositivo, a incidência poderá não ser causada pelo Bitdefender.

Procure por outras potenciais causas, tais como as seguintes:

- O Firewall do outro dispositivo pode bloquear a partilha de ficheiros e impressoras com o seu PC.
  - Se a Firewall do Windows estiver a utilizada, pode ser configurada para permitir a partilha de ficheiros e impressora da seguinte forma:
    - Em **windows 7**:
      1. Clique em **Iniciar**, vá para o **Painel de Controlo** e selecione **Sistema e segurança**.
      2. Vá à **Firewall do Windows**, depois clique em **Permitir um programa por meio do Firewall do Windows**.
      3. Selecione a caixa de verificação **Partilha de ficheiros e impressoras**.
    - Em **Windows 8** e **Windows 8.1**:
      1. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
      2. Clique em **Sistema e segurança**, vá até à **Firewall do Windows** e selecione **Permitir uma aplicação através do Firewall do Windows**.
      3. Marque a caixa de verificação **Partilha de ficheiros e impressora** e depois clique em **OK**.
    - Em **Windows 10** e **Windows 11**:

1. Introduza "Permitir uma aplicação através do Firewall do Windows" na caixa de pesquisa da barra de tarefas e clique no ícone correspondente.
2. Clique em **Alterar as definições**.
3. Na lista de **Aplicações e recursos permitidos**, marque a caixa de verificação **Partilha de ficheiros e impressoras**, depois clique em **OK**.

- Se outro programa de firewall estiver a ser utilizado, por favor consulte a documentação e ficheiro de ajuda.

- Condições gerais que podem impedir a utilização ou conexão com a impressora compartilhada:
  - Poderá precisar de se ligar com uma conta de administrador do Windows para aceder à impressora compartilhada.
  - As permissões são definidas para a impressora partilhada para permitir acesso a um dispositivo específico e apenas utilizadores. Se está a partilhar a sua impressora, verifique as permissões definidas para a impressora para saber se o utilizador do outro dispositivo está autorizado a aceder à impressora. Se está a tentar ligar-se a uma impressora partilhada, verifique com o utilizador do outro dispositivo se tem permissão para se ligar com a impressora.
  - A impressora ligada ao seu dispositivo ou ao outro não é partilhada.
  - A impressora partilhada não está adicionada ao dispositivo.

    Observação
    Para aprender como gerir o compartilhamento de impressoras (compartilhar uma impressora, definir ou remover permissões para a impressora, conecta-se a uma rede de impressora ou a uma impressora partilhada), vá à Ajuda e Suporte do Windows (no menu Iniciar, clique em **Ajuda e Suporte**).

- O acesso a uma impressora em rede pode ser restringido a dispositivo ou apenas a utilizadores. Deverá verificar com o administrador da rede se tem ou não permissão para aceder à impressora.

Se esta informação não for útil, você pode entrar em contato com a Bitdefender para obter suporte conforme descrito na seção Pedir Ajuda (página 261).

A minha Internet está lenta

Esta situação poderá surgir depois de instalar o Bitdefender. Este problema poderá ser causado por erros na configuração da firewall do Bitdefender.

Para resolver esta situação:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No painel da **FIREWALL**, clique no botão desligar para desativar a função.
3. Verifique se a sua ligação à Internet melhorou com a firewall do Bitdefender desativada.
   - ❍ Se ainda tem uma ligação à Internet lenta, a incidência poderá não ser causada pelo Bitdefender. Deve contactar o seu Fornecedor de Serviço de Internet para confirmar se a ligação está operacional.
     Se receber a confirmação do seu Fornecedor de Serviços de Internet que a ligação está operacional e o problema persistir, contacte a Bitdefender como indicado na secção Pedir Ajuda (página 261).
   - ❍ Se a ligação à Internet melhorou depois de desativar a firewall do Bitdefender:
     a. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
     b. No **FIREWALL** painel, clique **Configurações**.
     c. Vá para a aba **Adaptadores de rede** e defina a sua ligação com a internet como **Doméstica/Escritório**.
     d. Na aba **Definições**, desative a **Proteção de verificação de porta**.
        Na área de **Modo Sigiloso**, clique em **Editar as definições de sigilo**. Ligue o Modo Sigiloso para o adaptador de rede ao qual está ligado.
     e. Feche o Bitdefender, reinicie o sistema e verifique a velocidade de ligação à Internet.

Se esta informação não for útil, você pode entrar em contato com a Bitdefender para obter suporte conforme descrito na seção Pedir Ajuda (página 261).

Como atualizar o Bitdefender numa ligação à Internet lenta

Se tiver uma ligação à Internet lenta (por exemplo, ligação telefónica), poderão ocorrer erros durante o processo de atualização.

Para manter o seu sistema atualizado com a base de dados de informações de ameaças mais recente do Bitdefender:

1. Clique **Configurações** no menu de navegação do Interface do Bitdefender.
2. Selecione os **Atualizar** aba.
3. Desligar o botão **Atualização silenciosa**.
4. A próxima vez que uma atualização estiver disponível, será pedido para selecionar a atualização que deseja transferir. Selecionar apenas **Atualização das subscrições**.
5. O Bitdefender transfere e instala apenas a base de dados de informações de ameaças.

Os serviços do Bitdefender não estão a responder

Este artigo ajuda-o a troubleshoot os erros de **Os Serviços BitDefender não estão a responder**. Pode encontrar esse erro da seguinte forma:

- O ícone do Bitdefender na **bandeja do sistema** está em cinzento e informa que os serviços do Bitdefender não estão a responder.
- A janela do BitDefender indica que os serviços do BitDefender não estão a responder.

O erro pode ter ocorrido devido a um dos seguintes fatores:

- problemas temporários de comunicação entre os serviços da BitDefender.
- alguns dos serviços da BitDefender estão parados.
- outras soluções de segurança em execução no seu dispositivo, ao mesmo tempo que o Bitdefender.

Para solucionar este erro, tente estas soluções:

1. Espere uns momentos e verifique se existe alguma alteração. Este erro pode ser temporário.

2. Reinicie o dispositivo e aguarde alguns momentos até o Bitdefender iniciar. Abra o BitDefender e veja se o erro se mantém. Reiniciar o dispositivo normalmente resolve o problema.
3. Verifique se tem qualquer outra solução de segurança instalada na medida em que possam interferir no funcionamento normal do BitDefender. Se for este o caso, recomendamos que remova todas as outras soluções de segurança e reinstale BitDefender.
   Para mais informação, dirija-se a Como posso remover outras soluções de segurança? (página 125).

Se o erro persistir, por favor contacte os nossos representantes do suporte conforme descrito na secção Pedir Ajuda (página 261).

O filtro Antispam não está a funcionar corretamente

Este artigo ajuda a solucionar os seguintes problemas relacionados com a operação de filtragem do Antispam do BitDefender:

- **Um número de mensagens de e-mail legítimas são marcadas como [spam].**
- **Muitas mensagens spam não estão marcadas de acordo com o filtro antispam.**
- **O filtro antispam não deteta qualquer mensagem de spam.**

Mensagens legítimas são marcadas como [spam]

As mensagens legítimas são marcadas como [spam] simplesmente porque, para o filtro antispam do Bitdefender, elas parecem-se com um spam. Pode resolver este problema ao configurar adequadamente o filtro Antispam.

O Bitdefender adiciona automaticamente os destinatários das suas mensagens de e-mail a uma Lista de amigos. As mensagens de e-mail recebidas dos contactos da Lista de amigos são consideradas legítimas. Elas não são verificadas pelo filtro antispam e, portanto, nunca são marcadas como [spam].

A configuração automática da lista de Amigos não impede a deteção de erros que podem ocorrer nestas situações:

- Recebeu muitos e-mails publicitários solicitados como resultado de se inscrever em vários sites. Neste caso, a solução é adicionar à Lista de Amigos o endereço de e-mail do qual recebeu esses e-mails.
- Uma parte significativa dos seus mails legítimos são de pessoas com quem nunca trocou e-mails antes, tais como clientes, potenciais parceiros empresariais e outros. Outras soluções são requeridas neste caso.

Se estiver a utilizar um dos clientes de e-mail com integração com o Bitdefender, **indique os erros de deteção**.

> **Observação**
> O Bitdefender se integra aos clientes de e-mail mais usados por meio de uma barra de ferramentas antispam fácil de usar. Para obter uma lista completa de clientes de e-mail compatíveis, consulte Clientes de email e protocolos suportados (página 53).

Adicionar contactos à Lista de Amigos

Se está a utilizar um cliente de mail suportado, pode facilmente adicionar os remetentes das mensagens legítimas à lista de Amigos. Siga os seguintes passos:

1. No seu cliente de mail, selecione a mensagem de e-mail do remetente que quer adicionar à lista de Amigos.
2. Clique no botão **Adicionar amigo** na barra de ferramentas antispam do Bitdefender.
3. Poderá ser convidado a reconhecer os endereços adicionados à lista de Amigos. Selecione **Não mostrar esta mensagem outra vez** e clique **OK**.

Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.

Se está a utilizar um cliente de mail diferente, poderá adicionar os contactos à lista Amigos a partir do interface do BitDefender. Siga os seguintes passos:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No painel **ANTISPAM**, clique em **Gerir amigos**.
   Aparece uma janela de configuração.

3. Digite o endereço de email onde quer sempre receber as mensagens de email e depois clique em **Adicionar**. Pode adicionar quantos endereços de email desejar.
4. Clique **OK** para salvar as alterações e fechar a janela.

Indique os erros de deteção

Se estiver a usar um cliente de e-mail suportado, pode facilmente corrigir o filtro antispam (indicando mensagens de correio eletrónico que não deveriam ter sido marcadas como [spam]). Se o fizer, ajuda a melhorar a eficiência do filtro antispam. Siga os seguintes passos:

1. Abra seu cliente de e-mail.
2. Vá para a pasta de lixo eletrônico para onde as mensagens de spam são movidas.
3. Selecione a mensagem legítima incorretamente marcada como [spam] pelo Bitdefender.
4. Clique no botão **Adicionar amigo** na barra de ferramentas antispam do Bitdefender para adicionar o remetente à Lista de amigos. Talvez tenha que clicar em **OK** para confirmar. Receberá sempre as mensagens que venham deste endereço de e-mail, independentemente de seu conteúdo.
5. Clique no **Não é spam** botão na barra de ferramentas antispam do Bitdefender (normalmente localizado na parte superior da janela do cliente de e-mail). A mensagem de e-mail será movida para a pasta Caixa de entrada.

Muitas mensagens de spam não são detetadas

Se está a receber muitas mensagens spam que não estão marcadas como [spam], tem de configurar o filtro antispam BitDefender de modo a melhorar a sua eficiência.

Tente as seguintes soluções:

1. Se está a utilizar um dos clientes de e-mail com integração com o Bitdefender, **indique as mensagens de spam não detetadas**.

> **Observação**
> O Bitdefender se integra aos clientes de e-mail mais usados por meio de uma barra de ferramentas antispam fácil de usar. Para obter uma lista completa de clientes de e-mail compatíveis, consulte Clientes de email e protocolos suportados (página 53).

2. **Adicione spammers à Lista de spammers**. As mensagens de e-mail recebidas de endereços da Lista de spammers são automaticamente marcadas como [spam].

Indique as mensagens de spam não detetadas

Se você estiver usando um cliente de e-mail compatível, poderá indicar facilmente quais mensagens de e-mail deveriam ter sido detectadas como spam. Isso ajuda a melhorar a eficiência do filtro antispam. Siga esses passos:

1. Abra seu cliente de e-mail.
2. Vá para a pasta Caixa de entrada.
3. Selecione as mensagens de spam não detectadas.
4. Clique no botão **É Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela do cliente de correio eletrónico). São imediatamente marcados como [spam] e movidos para a pasta junk.

Adicionar spammers à lista de Spammers

Se está a utilizar um cliente de mail suportado, pode facilmente adicionar os remetentes das mensagens spam à lista Spammers. Siga os seguintes passos:

1. Abra seu cliente de e-mail.
2. Vá para a pasta de lixo eletrônico para onde as mensagens de spam são movidas.
3. Seleccione a mensagem marcada como [spam] pela BitDefender.
4. Clique no botão **Adicionar spammers** na barra de ferramentas do Bitdefender antispam.
5. Poderá ser convidado a reconhecer os endereços como Spammers. Selecione **Não mostrar esta mensagem outra vez** e clique **OK**.

Se está a utilizar um cliente de mail diferente, poderá adicionar manualmente os spammers à lista de Spammers a partir do interface

do Bitdefender. É conveniente que o faça apenas quando receber várias mensagens spam do mesmo endereço e-mail. Siga os seguintes passos:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTISPAM** painel, clique **Configurações**.
3. Vá para a janela **Gerir Spammers**.
4. Digite o endereço de email do spammer e depois clique em **Adicionar**. Pode adicionar quantos endereços de email desejar.
5. Clique **OK** para salvar as alterações e fechar a janela.

O Filtro Antispam não deteta nenhuma mensagem spam

Se nenhuma mensagem spam for marcada como [spam], poderá haver algum problema como o filtro Antispam do BitDefender. Antes de resolver este problema, certifique-se de que não é causado por nenhuma das seguintes condições:

- A proteção antispam poderá estar desligada. Para verificar o estado da proteção antispam, clique em **Proteção** no menu de navegação da interface do **Bitdefender**. Verifique o painel **Antispam** para comprovar se a função está ativa
  Se o Antispam estava desligado, era isso que estava a causar o problema. Clique no botão correspondente para ativar a sua proteção antispam.
- A proteção Bitdefender Antispam está disponível apenas para clientes de e-mail definidos para receber mensagens através do protocolo POP3. Isto quer dizer o seguinte:
  - As mensagens de Email obtidas através de Webmail (Yahoo, Gmail, Hotmail ou outros) não são filtradas como spam pelo Bitdefender.
  - Se o seu cliente de e-mail está configurado para receber mensagens de e-mail através de outro protocolo além de POP3 (por exemplo, IMAP4), o filtro Antispam do BitDefender não os verifica por envio de spam.

> **Observação**
> POP3 é um dos protocolos mais utilizados para fazer o download de mensagens de e-mail a partir de um servidor de correio. Se você não sabe o protocolo que o seu cliente de e-mail utiliza para importar mensagens de e-mail, solicite à pessoa que o configurou.

- Bitdefender Total Security não analisa o tráfego do Lotus Notes POP3.

Uma solução possivel é reparar ou reinstalar o produto. Contudo, poderá contacta a BitDefender para suporte, como descrito na secção Pedir Ajuda (página 261).

A remoção Bitdefender falhou

Caso pretenda remover o seu produto Bitdefender e constate que o processo demora ou o sistema bloqueia, clique em **Cancelar** para interromper a ação. Se isso não funcionar, reinicie o sistema.

Se a remoção falhar, algumas chaves de registo e ficheiros do Bitdefender poderão permanecer no seu sistema. Esses resquícios podem impedir uma nova instalação do Bitdefender. Podem também afectar o desempenho e a estabilidade do sistema.

Para remover o Bitdefender completamente do seu sistema:

- Em **windows 7**:
  1. Clique **Começar**, Vá para **Painel de controle** e clique duas vezes **Programas e características**.
  2. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
  3. Clique **REMOVER** na janela que aparece.
  4. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

- Em **Windows 8** e **Windows 8.1**:
  1. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
  2. Clique **Desinstalar um programa** ou **Programas e características**.
  3. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique **REMOVER** na janela que aparece.

5. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

- Em **Windows 10** e **Windows 11**:
  1. Clique **Começar**e clique em Configurações.
  2. Clique no **Sistema** ícone na área Configurações e selecione **Aplicativos instalados**.
  3. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique **Desinstalar** novamente para confirmar sua escolha.
  5. Clique **REMOVER** na janela que aparece.
  6. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

O meu sistema não reinicia após a instalação de Bitdefender

Se instalou o Bitdefender e não consegue reiniciar o seu sistema no modo normal, podem existir vários motivos para este problema.

Isto é muito provavelmente causado por uma instalação anterior de Bitdefender que não foi removida adequadamente ou por outra solução de segurança que ainda se encontra no sistema.

Eis como pode resolver cada situação:

- **Tinha o Bitdefender e não o removeu corretamente.**
  Para resolver isto:
  1. Reinicie o seu sistema e entre no Modo de Segurança. Para saber mais sobre como fazer isto, aceda a Como posso reiniciar no Modo de Segurança? (página 126).
  2. Remova o Bitdefender do seu sistema:
     - Em **windows 7**:
       a. Clique **Começar**, Vá para **Painel de controle** e clique duas vezes **Programas e características**.
       b. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
       c. Clique **REMOVER** na janela que aparece.

d. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

e. Reinicie o sistema no modo normal.

- Em **Windows 8** e **Windows 8.1**:

  a. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.

  b. Clique **Desinstalar um programa** ou **Programas e características**.

  c. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.

  d. Clique **REMOVER** na janela que aparece.

  e. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

  f. Reinicie seu sistema no modo normal.

- Em **Windows 10** e **Windows 11**:

  a. Clique **Começar**e clique em Configurações.

  b. Clique no **Sistema** ícone na área Configurações e selecione **Aplicativos instalados**.

  c. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.

  d. Clique **Desinstalar** novamente para confirmar sua escolha.

  e. Clique **REMOVER** na janela que aparece.

  f. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

  g. Reinicie seu sistema no modo normal.

3. Reinstale o seu produto Bitdefender.

- **Você tinha uma solução de segurança diferente anteriormente e não a eliminou corretamente.**
  Para resolver isso:

1. Reinicie seu sistema e entre no modo de segurança. Para saber como fazer isso, consulte Como posso reiniciar no Modo de Segurança? (página 126).
2. Remova as outras soluções de segurança do seu sistema:
   - Em **windows 7**:
     a. Clique **Começar**, Vá para **Painel de controle** e clique duas vezes **Programas e características**.
     b. Encontre o nome do programa que pretende remover e selecione **Remover**.
     c. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.
   - Em **Windows 8** e **Windows 8.1**:
     a. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
     b. Clique **Desinstalar um programa** ou **Programas e características**.
     c. Encontre o nome do programa que deseja remover e selecione **Remover**.
     d. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.
   - Em **Windows 10** e **Windows 11**:
     a. Clique **Começar**e clique em Configurações.
     b. Clique no **Sistema** ícone na área Configurações e selecione **Aplicativos instalados**.
     c. Encontre o nome do programa que deseja remover e selecione **Desinstalar**.
     d. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

   Para desinstalar corretamente outro software, aceda ao site Web do fornecedor e execute a ferramenta de desinstalação

ou contacte-o para diretamente, para que lhe indiquem os procedimentos de desinstalação.

3. Reinicie o seu sistema no modo normal e reinstale o Bitdefender.

Já seguiu os passos acima e o problema não está resolvido.

Para resolver isso:

1. Reinicie seu sistema e entre no modo de segurança. Para saber como fazer isso, consulte Como posso reiniciar no Modo de Segurança? (página 126).
2. Utilizar a opção de Restauração do Sistema do Windows para restaurar o dispositivo para uma data anterior antes de instalar o produto Bitdefender.
3. Reinicie o sistema no modo normal e contacte os nossos representantes do suporte conforme descrito na secção Pedir Ajuda (página 261).

3.5.2. Remover ameaças do seu sistema

As ameaças podem afetar o seu sistema de várias formas e a atuação do Bitdefender depende do tipo de ataque da ameaça. Como as ameaças alteram frequentemente o modo de ação, é difícil estabelecer um padrão com base no comportamento e nas ações.

Há situações em que o Bitdefender não consegue remover automaticamente a infecção de ameaças do seu sistema. Nestes casos, a sua intervenção é necessária.

- Ambiente de Resgate (página 149)
- O que fazer quando o Bitdefender encontrar ameaças no seu dispositivo? (página 150)
- Como posso limpar uma ameaça num ficheiro? (página 151)
- Como posso limpar uma ameaça num ficheiro de e-mail? (página 152)
- O que fazer se suspeitar que um ficheiro é perigoso? (página 153)
- O que são os ficheiros protegidos por palavra-passe no relatório de análise? (página 154)
- O que são os itens ignorados no relatório de análise? (página 154)

- O que são os ficheiros muito comprimidos no relatório de análise? (página 154)
- Por que é que Bitdefender eliminou automaticamente um ficheiro infectado? (página 155)

Se você não conseguir encontrar seu problema aqui, ou se as soluções apresentadas não resolverem, você pode entrar em contato com os representantes de suporte técnico da Bitdefender conforme apresentado no capítulo Pedir Ajuda (página 261).

Ambiente de Resgate

O **Modo de Recuperação** é uma funcionalidade do Bitdefender que permite analisar e desinfetar todas as partições existentes do disco rígido dentro e fora do sistema operativo.

O Ambiente de Resgate do Bitdefender está integrado com o Windows RE,

Arranque do sistema no Ambiente de Recuperação

Só pode aceder ao Ambiente de Recuperação a partir do produto Bitdefender como se segue:

1. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Clique em **Abrir** ao lado de **Ambiente de Resgate**.
4. Clique em **REINICIAR** na janela que aparece.
   O Ambiente de Resgate do Bitdefender carrega em alguns instantes.

Analisar o seu sistema no Ambiente de Recuperação

Para analisar o seu sistema no Ambiente de Recuperação:

1. Aceda ao Ambiente de Recuperação como descrito em Arranque do sistema no Ambiente de Recuperação (página 149).
2. O processo de análise do Bitdefender começa automaticamente assim que o sistema é carregado no Ambiente de Recuperação.
3. Aguarde que a análise termine. Se for detetada qualquer ameaça, siga as instruções para a remover.

4. Para sair do Ambiente de Recuperação, clique no botão Fechar na janela com os resultados da análise.

O que fazer quando o Bitdefender encontrar ameaças no seu dispositivo?

Pode descobrir que há uma ameaça no seu dispositivo numa dessas formas:

- O Bitdefender analisou o seu dispositivo e encontrou itens infetados.
- Um alerta de ameaças avisa que o Bitdefender bloqueou uma ou várias ameaças no seu dispositivo.

Nessas situações, atualize o Bitdefender para se certificar de que possui a base de dados mais recente de informações sobre a ameaça e realize uma Análise de Sistema.

Assim que a análise do sistema terminar, selecione a ação pretendida para os itens infetados (Desinfetar, Eliminar, Mover para a Quarentena).

> **Aviso**
> Se suspeitar que o ficheiro faz parte do sistema operativo do Windows ou que não é um ficheiro infetado, não siga estes passos e contacte e Apoio ao Cliente do Bitdefender assim que possível.

Se não for possível efetuar a ação selecionada e o relatório da análise indicar uma infecção que não foi possível eliminar, tem de remover o(s) ficheiro(s) manualmente:

O primeiro método pode ser utilizado no modo normal:

1. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique **Proteção** no menu de navegação do Interface do Bitdefender.
   b. No **ANTIVÍRUS** painel, clique **Abrir**.
   c. No **Avançado** janela, desligue **Escudo Bitdefender**.
2. Exibir objetos ocultos no Windows. Para saber como fazer isso, consulte Como posso mostrar objetos ocultos no Windows? (página 124).
3. Procure a localização do ficheiro infectado (veja no relatório da análise) e elimine-o.

4. Ative a proteção antivírus em tempo real do Bitdefender.

Caso o primeiro método para remover a infeção falhe:

1. Reinicie seu sistema e entre no modo de segurança. Para saber como fazer isso, consulte Como posso reiniciar no Modo de Segurança? (página 126).
2. Exibir objetos ocultos no Windows. Para saber como fazer isso, consulte Como posso mostrar objetos ocultos no Windows? (página 124).
3. Navegue até o local do arquivo infectado (verifique o log de verificação) e exclua-o.
4. Reinicie o seu sistema e inicie sessão no modo normal.

Se esta informação não for útil, você pode entrar em contato com a Bitdefender para obter suporte conforme descrito na seção Pedir Ajuda (página 261).

Como posso limpar uma ameaça num ficheiro?

Um arquivo é um ficheiro ou um conjunto de ficheiros comprimidos num formato especial para reduzir o espaço no disco necessário para armazenar os ficheiros.

Alguns destes formatos são formatos livres, possibilitando ao Bitdefender a opção de analisar o conteúdo e aplicar as ações adequadas para os remover.

Outros formatos de arquivo estão parcial ou totalmente fechados, mas o Bitdefender só pode detetar a presença de ameaças no interior, mas não pode aplicar outras ações.

Se o Bitdefender avisar que foi detetada uma ameaça dentro de um arquivo e não estiver disponível uma ação, significa que não é possível remover a ameaça devido a restrições nas definições de permissão do arquivo.

Eis como pode limpar uma ameaça armazenada num arquivo:

1. Identifique o arquivo que inclui a ameaça ao executar uma Análise do Sistema.
2. Desative a proteção antivírus em tempo real do Bitdefender:

a. Clique **Proteção** no menu de navegação do Interface do Bitdefender.

b. No **ANTIVÍRUS** painel, clique **Abrir**.

c. No **Avançado** janela, desligue **Escudo Bitdefender**.

3. Vá à localização do arquivo e descomprima-o com uma aplicação de arquivo, como o WinZip.
4. Identifique e elimine o ficheiro infectado.
5. Elimine o arquivo original de modo a garantir que a infecção é totalmente removida.
6. Comprima novamente os ficheiros num novo arquivo com uma aplicação de arquivo, como o WinZip.
7. Ative a proteção antivírus em tempo real do Bitdefender e execute uma análise ao sistema para se certificar que não há outras infeções no sistema.

> **Observação**
> É importante observar que uma ameaça armazenada num arquivo não é uma ameaça imediata para o seu sistema pois a ameaça tem de ser descomprimida e executada para infetar o seu sistema.

Se esta informação não for útil, você pode entrar em contato com a Bitdefender para obter suporte conforme descrito na seção Pedir Ajuda (página 261).

Como posso limpar uma ameaça num ficheiro de e-mail?

O Bitdefender também pode identificar ameaças em bases de dados de correio eletrónico e arquivos de correio eletrónico armazenados no disco.

Por vezes, é necessário identificar a mensagem infectada com a informação fornecida no relatório da análise, e elimine-o manualmente.

Eis como pode limpar uma ameaça armazenada num arquivo de e-mail:

1. Verifique o banco de dados de e-mail com o Bitdefender.
2. Desative a proteção antivírus em tempo real do Bitdefender:

a. Clique **Proteção** no menu de navegação do Interface do Bitdefender.

b. No **ANTIVÍRUS** painel, clique **Abrir**.

c. No **Avançado** janela, desligue **Escudo Bitdefender**.

3. Abra o relatório da análise e utilize a informação de identificação (Assunto, De, Para) das mensagens infectadas para localizá-las no cliente de correio eletrónico.
4. Elimine as mensagens infectadas. A maioria dos clientes de correio eletrónico move a mensagem eliminada para uma pasta de recuperação, a partir da qual pode ser recuperada. Deve certificar-se que a mensagem também é eliminada desta pasta de recuperação.
5. Compactar a pasta com a mensagem infectada.
   - No Microsoft Outlook 2007: No menu do Ficheiro, clique em Gestão de ficheiros de dados. Selecione as pastas pessoais (.pst) de ficheiros que pretende compactar e clique em Definições. Clique em Compactar agora.
   - No Microsoft Outlook 2010/2013/2016: No menu Ficheiro, clique em informações, depois em Definições da conta (adicione ou remova contas ou modifique as definições de ligação existentes). Depois clique em Ficheiros de dados, selecione as pastas pessoais (.pst) de ficheiros que pretende compactar e clique em Definições. Clique em Compactar agora.
6. Ative a proteção antivírus em tempo real do Bitdefender.

Se esta informação não for útil, você pode entrar em contato com a Bitdefender para obter suporte conforme descrito na seção Pedir Ajuda (página 261).

O que fazer se suspeitar que um ficheiro é perigoso?

Pode suspeitar que um ficheiro do seu sistema é perigoso, embora o seu produto Bitdefender não o tenha detetado.

Para garantir que o seu sistema está protegido:

1. Executar uma **Verificação do sistema** com o Bitdefender. Para saber mais sobre como fazer isto, aceda a How do I scan my system?.
2. Se no resultado da análise parece estar limpo, mas você ainda tem dúvidas e quer verificar o ficheiro, contacte os representantes do suporte para que o possamos ajudar.

Para saber mais sobre como fazer isto, aceda a Pedir Ajuda (página 261).

O que são os ficheiros protegidos por palavra-passe no relatório de análise?

Isto é apenas uma notificação que indica que o Bitdefender detetou que estes ficheiros estão protegidos por palavra-passe ou por outra forma de encriptação.

Normalmente, os itens protegidos por palavra-passe são:

- Ficheiros que pertencem a outras solução de segurança.
- Ficheiros que pertencem ao sistema operativo.

Para analisar verdadeiramente os conteúdos, estes ficheiros têm de ser extraídos ou descodificados.

Se esses conteúdos pudessem ser extraídos, o analisador em tempo real do Bitdefender analisaria-os automaticamente para manter o seu dispositivo protegido. Se pretende analisar esses ficheiros com o Bitdefender, terá de contactar o fabricante do produto para receber mais informações sobre esses ficheiros.

Recomendamos que ignore estes ficheiros pois não constituem uma ameaça ao seu sistema.

O que são os itens ignorados no relatório de análise?

Todos os ficheiros que aparecem como Ignorados no relatório de análise estão limpos.

Para um melhor desempenho, o Bitdefender não analisa ficheiros que não tenham sido alterados desde a última análise.

O que são os ficheiros muito comprimidos no relatório de análise?

Os itens sobre-comprimidos são elementos que não puderam ser extraídos pelo motor de análise ou elementos para os quais a desencriptação levaria demasiado tempo, tornando o sistema instável.

Sobre-comprimido significa que o Bitdefender não realizou a análise a esse arquivo pois a descompactação iria consumir demasiados recursos do sistema. O conteúdo será analisado aquando o acesso em tempo real, se necessário.

Por que é que Bitdefender eliminou automaticamente um ficheiro infectado?

Se for detetado um ficheiro infectado, o Bitdefender tentará automaticamente desinfectá-lo. Se a desinfecção falhar, o ficheiro é movido para a quarentena de modo a restringir a infecção.

Para determinados tipos de ameaças, a desinfecção não é possível porque o arquivo detectado é totalmente malicioso. Nesses casos, o arquivo infectado é excluído do disco.

Este é, normalmente, o caso de ficheiros de instalação que são transferidos de sites Internet suspeitos. Se se deparar numa situação assim, transfira o ficheiro de instalação do site Internet do fabricante ou de outro site fidedigno.

4. ANTIVÍRUS PARA MAC

4.1. O que é Bitdefender Antivirus for Mac

O Bitdefender Antivirus for Mac é um detetor antivírus poderoso, que pode detetar e remover todos os tipos de software malicioso ("ameaças"), incluindo:

- ransomware
- Adware
- vírus
- spyware
- Trojans
- keyloggers
- worms

Esta aplicação deteta e remove não só ameaças no Mac, mas também ameaças no Windows, prevenindo, assim, que envie ficheiros infetados para a sua família, amigos e colegas utilizando PC.

4.2. Instalação e remoção

Este capítulo inclui os seguintes tópicos:

- Requisitos do sistema (página 156)
- A instalar o Bitdefender Antivirus for Mac (página 157)
- Ao remover o Bitdefender Antivirus para Mac (página 161)

4.2.1. Requisitos do sistema

Pode instalar o Bitdefender Antivirus for Mac em computadores Macintosh com sistema operativo X Yosemite (10.10) ou versões mais recentes.

O seu Mac tem de ter um espaço mínimo de 1 GB disponível no disco rígido.

É necessária uma ligação à Internet para registar e atualizar Bitdefender Antivirus for Mac.

Observação

O anti-rastreador da Bitdefender e o VPN da Bitdefender apenas podem ser instalados em sistemas macOS 10.12 ou versões mais recentes.

Como obter a versão do seu macOS e informações de hardware do seu Mac

Clique no icon da Apple no canto superior esquerdo no ecrã e escolha Sobre **Este Mac**. Na janela que aparece pode ver a versão do seu sistema operativo e outras informações uteis. Clique em **Relatório do Sistema** para informações detalhadas sobre o hardware.

4.2.2. A instalar o Bitdefender Antivirus for Mac

A aplicação de Bitdefender Antivirus for Mac pode ser instalada a partir da sua conta Bitdefender da seguinte forma:

1. Inicie sessão como administrador.
2. Vá a: https://central.bitdefender.com.
3. Inicie a sessão na seu conta Bitdefender com o seu endereço de e-mail e palavra-passe.
4. Selecione o painel **Os meus dispositivos** e, em seguida, clique em **INSTALAR PROTEÇÃO**.
5. Escolha uma das duas opções disponíveis:
   - **Proteger este dispositivo**
     a. Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
     b. Guarde o ficheiro de instalação.
   - **Proteger outros dispositivos**
     a. Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, clique no botão correspondente.
     b. Clique em **ENVIAR LINK PARA A TRANSFERÊNCIA**.
     c. Escreva um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**.

Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

d. No dispositivo em que deseja instalar o seu produto Bitdefender, verifique a conta de e-mail que escreveu e clique no botão de download correspondente.

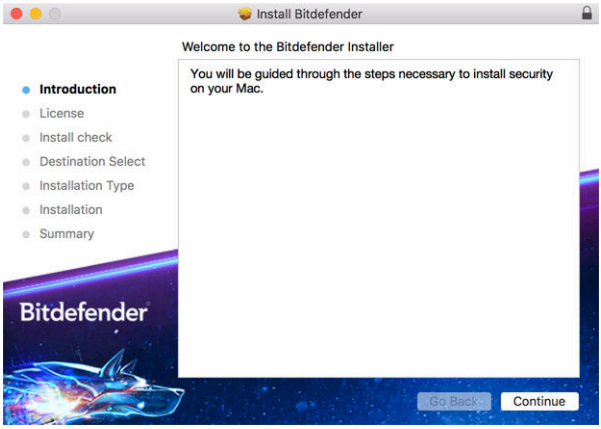
6. Execute o Bitdefender que transferiu.
7. Conclua os passos de instalação.

Processo de instalação

Para instalar o Bitdefender Antivirus for Mac:

1. Clique no ficheiro transferido. O instalador será iniciado e será orientado pelo processo de instalação.
2. Siga o assistente de instalação.

Passo 1 - Janela de Boas-vindas



Clique em {1}Continuar{2}.

Passo 2 - Ler o Acordo da Subscrição

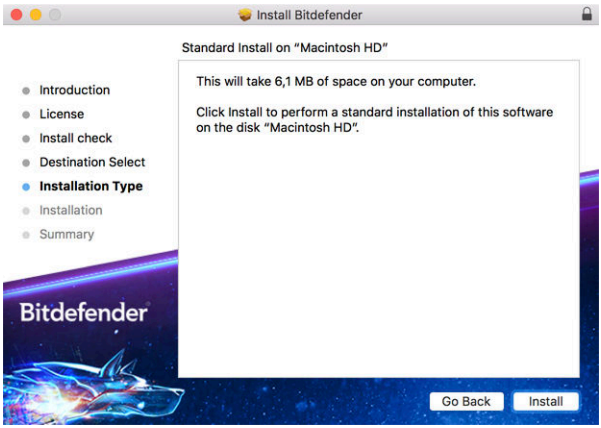
Antes de continuar com a instalação, tem de concordar com o Contrato de Subscrição. Leia o Contrato de Subscrição com calma pois contém os termos e condições que regem a utilização do Bitdefender Antivirus for Mac.

Nesta janela pode também selecionar o idioma em que quer instalar o produto.

Clique em **Continuar** e depois clique em **Aceitar**.

> **Importante**
> Caso não concorde com estes termos, clique em **Continuar** e depois em **Discordar** para cancelar a instalação e sair do instalador.

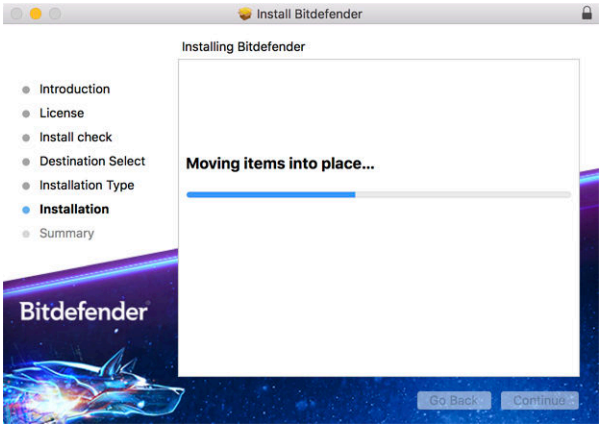
Passo 3 - Iniciar instalação



O Bitdefender Antivirus para Mac será instalado no Macintosh HD/Library/Bitdefender. A localização de instalação não pode ser alterada.

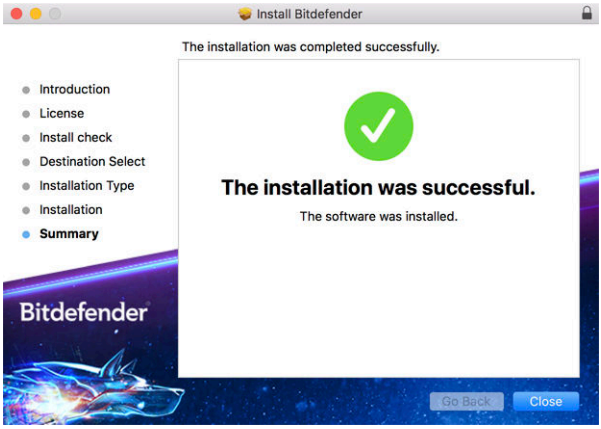
Clique em **Instalar** para iniciar a instalação.

Passo 4 - Instalar o Bitdefender Antivirus para Mac



Aguarde a instalação concluir e clique em **Continuar**.

Passo 5 - Terminar



Clique em **Fechar** para fechar a janela do instalador.

O processo de instalação agora está concluído.

Importante

- Se estiver a instalar o Bitdefender Antivirus para Mac no macOS High Sierra 10.13.0 ou uma versão mais recente, a notificação da **Extensão do Sistema Bloqueada** aparece. Esta notificação informa que as extensões assinadas pela Bitdefender foram bloqueadas e devem ser ativadas manualmente. Clique em OK para continuar. Na janela Bitdefender Antivirus para Mac que aparece, clique no link **Segurança e Privacidade**. Clique em **Permitir** na parte inferior da janela, ou selecione Bitdefender SRL na lista e clique em **OK**.
- Se estiver a instalar o Bitdefender Antivirus para Mac no macOS Mojave 10.14 ou numa versão mais recente, uma nova janela será exibida, ao informar que deve **Conceder acesso total ao disco à Bitdefender** e **Permita que o Bitdefender carregue**. Siga as instruções no ecrã para configurar corretamente o produto.

4.2.3. Ao remover o Bitdefender Antivirus para Mac

Por ser uma aplicação complexa, o Bitdefender Antivirus for Mac não pode ser removido da forma convencional, ou seja, ao arrastar o ícone da aplicação da pasta **Aplicações** para a Reciclagem.

Para remover o Bitdefender Antivirus para Mac, siga os seguintes passos:

1. Abra uma janela **Finder** e aceda à pasta **Aplicações**.
2. Abra a pasta da Bitdefender em **Aplicações** e depois faça duplo clique em **Desinstalar o Bitdefender**.
3. Selecione a opção de desinstalar preferida.

   Observação
   Se estiver a tentar remover apenas a aplicação Bitdefender VPN selecione apenas **Desinstalar o VPN**.

4. Clique em **Desinstalar** e aguarde pela conclusão do processo.
5. Clique em **Fechar** para terminar.

   Importante
   Se houver um erro, pode contactar Atendimento ao Consumidor da Bitdefender como descrito em Pedir Ajuda (página 261).

4.3. Introdução

Este capítulo inclui os seguintes tópicos:

- A abrir o Bitdefender Antivirus para Mac (página 162)
- Janela principal da aplicação (página 163)
- Ícone da aplicação no Dock (página 164)
- Menu de navegação (página 164)
- Modo Escuro (página 165)

4.3.1. A abrir o Bitdefender Antivirus para Mac

Tem diversas formas para abrir o Bitdefender Antivirus para Mac.

- Clique no ícone Bitdefender Antivirus para Mac no Painel de Iniciação.
- Clique no ícone na barra de menu e escolha **Abrir a interface de Antivirus**.
- Abra a janela de Pesquisa, vá a Aplicações e faça duplo clique no ícone **Bitdefender Antivirus para Mac**.

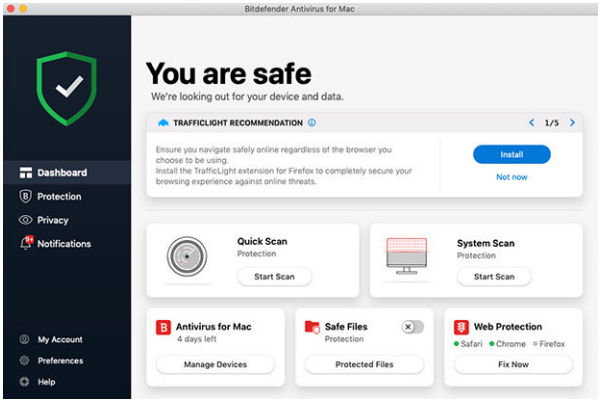
Importante

A primeira vez que abrir o Bitdefender Antivirus for Mac no macOS Mojave 10.14 ou superior, aparece uma recomendação de segurança. Esta recomendação aparece porque precisamos de permissões para fazer uma análise completa do seu sistema em busca de ameaças. Para dar permissões, precisa de ter iniciado sessão como administrador e seguir estes passos:

1. Clique na hiperligação **Preferências do Sistema**.
2. Clique no ícone e depois introduza as suas credenciais de administrador.
3. Uma nova janela aparece. Arraste o ficheiro **BDLDaemon** para a lista de aplicações permitidas.

4.3.2. Janela principal da aplicação

O Bitdefender Antivirus for Mac vai de encontro às necessidades quer dos principiantes quer dos utilizadores mais técnicos. Assim, o interface gráfico do utilizador foi desenhado para servir quer uns quer outros.



Vá à interface do Bitdefender, encontra-se exibido no canto superior esquerdo um assistente de introdução que contém detalhes sobre como interagir com o produto e como o configurar. Selecione o ícone do ângulo direito para continuar a ser guiado ou **Ignorar** para fechar o assistente.

A barra de estado na parte superior da janela informa sobre o estado de segurança do sistema através de mensagens explícitas e cores sugestivas.

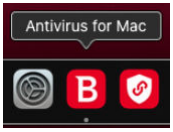
Se o Bitdefender Antivirus para Mac não tiver avisos, a barra de estado estará a verde. Quando um problema de segurança for detetado, a barra de estado muda para vermelho. Para obter informações detalhadas sobre os problemas e como corrigi-los, consulte Reparar Incidência (página 178).

Para lhe oferecer uma operação eficaz e maior proteção durante a realização de diferentes atividades, o **Bitdefender Autopilot** atuará como o seu consultor de segurança pessoal. Dependendo da atividade que realiza, trabalha ou faz pagamentos online, o Bitdefender Autopilot apresentará recomendações contextuais com base na utilização e nas necessidades do seu dispositivo. Isto irá ajudá-lo a descobrir e a beneficiar das vantagens trazidas pelos recursos incluídos na aplicação do Bitdefender Antivirus para Mac.

No menu de navegação à esquerda, pode aceder às secções do Bitdefender para uma configuração detalhada e tarefas administrativas avançadas (Separadores de **Proteção** e **Privacidade**), notificações, a sua **Conta Bitdefender** e a área de **Preferências**. Além disto, pode entrar em contato connosco (Separador **Ajuda**) para obter suporte caso tenha dúvidas ou ocorra algo inesperado.

4.3.3. Ícone da aplicação no Dock

O ícone do Bitdefender Antivirus para Mac pode ser notado no Dock assim que abrir a aplicação. O ícone no Dock fornece uma maneira fácil de verificar ficheiros e pastas quanto a ameaças. Basta arrastar e soltar o ficheiro ou pasta sobre o ícone do Dock e a verificação começará imediatamente.



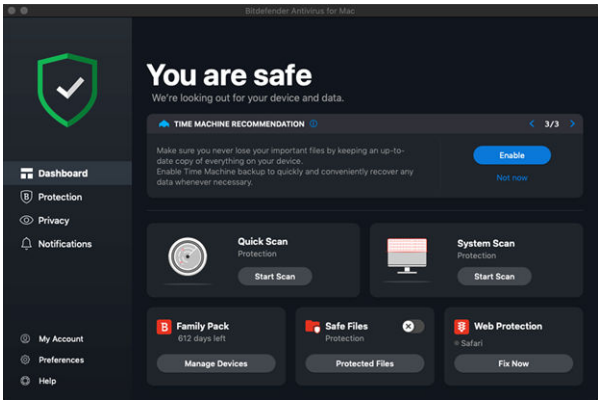
4.3.4. Menu de navegação

À esquerda, na interface da Bitdefender, encontra-se o menu de navegação, que lhe permite aceder rapidamente às funcionalidades da Bitdefender necessárias para utilizar o seu produto. Os separadores disponíveis nesta área são:

- **Painel de controlo**. A partir daqui, pode resolver rapidamente problemas de segurança, ver recomendações de acordo com os requisitos do seu sistema e padrões de utilização, realizar ações rápidas, e aceder à sua conta da Bitdefender para gerir os dispositivos que adicionou à sua subscrição da Bitdefender.
- **Proteção**. A partir daqui, pode executar análises de antivírus , adicione ficheiros à lista de exceções, proteger ficheiros e aplicações contra ataques de ransomware, proteger as suas cópias de segurança do Time Machine e configurar a proteção enquanto navega na Internet.
- **Privacidade**. A partir daqui, pode abrir a aplicação do Bitdefender VPN e instalar a extensão de Anti-rastreio no seu navegador de internet.
- **Notificações**. A partir daqui, pode ser detalhes sobre as ações tomadas relativamente aos ficheiros verificados.
- **A minha conta**. A partir daqui, pode consultar a conta e a subscrição Bitdefender pelas quais o seu dispositivo está a ser protegido, bem como mudar de conta se necessário.
- **Preferências**. A partir daqui, pode configurar as definições do Bitdefender.
- **Ajuda**. Aqui, pode entrar em contacto com o departamento de Assistência Técnica sempre que precisar de ajuda com o seu produto Bitdefender. Pode também enviar feedback para melhorar o produto.

4.3.5. Modo Escuro

Para proteger a vista de brilho e luzes durante a noite ou em locais pouco iluminados, o Bitdefender Antivirus for Mac possui um Modo Escuro para o Mojave 10.14 e daí em diante. As cores da interface foram optimizadas para que possa utilizar o seu Mac sem forçar a vista. A interface do Bitdefender Antivirus for Mac ajusta-se automaticamente consoante as definições do seu dispositivo.



4.4. Proteger contra software malicioso

Este capítulo inclui os seguintes tópicos:

4.4.1. Melhores Práticas

Para manter o seu sistema protegido contra ameaças e evitar infeções acidentais de outros sistemas, siga estas práticas:

- Mantenha o **Bitdefender Shield** ativado, de forma a permitir que os ficheiros do sistema sejam automaticamente verificados pelo Bitdefender Antivirus para Mac.
- Mantenha o seu Bitdefender Antivirus for Mac atualizado com as informações sobre as ameaças e atualizações de produto mais recentes.
- Verifique e corrija os problemas regularmente relatados pelo Bitdefender Antivirus para Mac. Para mais informações, consulte o Reparar Incidência (página 178).
- Verifique o registo detalhado de eventos relacionados à atividade do Bitdefender Antivirus para Mac no seu computador. Sempre que algo relevante para a segurança do seu sistema ou dados ocorrer, uma mensagem nova é adicionada à área de Notificações do Bitdefender. Para mais detalhes, aceda a Notificações (página 179).
- É recomendável que também siga estas práticas:
  - Crie o hábito de verificar ficheiros que baixa de uma memória de armazenamento externa (como uma unidade USB ou CD), especialmente quando desconhecer a fonte.
  - Se tiver um ficheiro DMG, monte-o e analise o seu conteúdo (os ficheiros no volume/imagem montada).

  A forma mais fácil de verificar um ficheiro, uma pasta ou um volume é ao arrastar e largar sobre a janela Bitdefender Antivirus para Mac ou no ícone na Dock

Nenhuma outra configuração ou ação é necessária. No entanto, se pretender, é possível ajustar as definições e preferências da aplicação para melhor satisfazer as suas necessidades. Para mais informação, dirija-se a Configurar preferências (página 182).

4.4.2. Analisar o seu Mac

Além do recurso **Bitdefender Shield**, que monitoriza regularmente as aplicações instaladas, ao procurar ações semelhantes a ameaças e evita que novas ameaças entrem no seu sistema, pode verificar o seu Mac ou ficheiros específicos a qualquer momento que queira.

A maneira mais fácil de verificar um ficheiro, uma pasta ou um volume é arrastá-lo e soltá-lo sobre a janela do Bitdefender Antivirus para Mac ou

ícone do Dock. O assistente de verificação irá aparecer e guiá-lo através do processo de verificação.

Também pode iniciar uma análise como se segue:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. Selecione o separador **Antivírus**.
3. Clique num dos três botões para iniciar a análise desejada.
   - **Análise Rápida** - procura por ameaças nos locais mais vulneráveis no seu sistema (por exemplo, as pastas que contêm os documentos, transferências, transferências de e-mail e ficheiros temporários de cada utilizador).
   - **Verificação do Sistema** - realize uma verificação completa por ameaças em todo o sistema. Todas as montagens ligadas também serão verificadas.

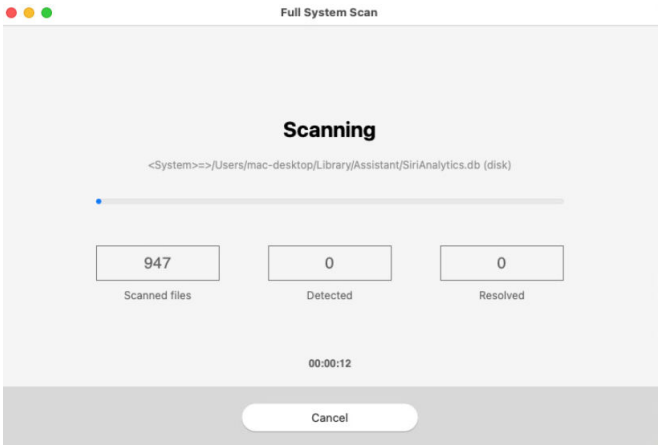
     > **Observação**
     > Dependendo do tamanho do seu disco rígido, analisar todo o sistema pode demorar (até uma hora ou mais). Para um desempenho melhor, é recomendável não executar esta tarefa ao executar outras tarefas intensivas (como edição de vídeo).
     >
     > Se preferir, pode optar por não analisar volumes montados específicos adicionando-os à lista **Exceções** na janela de Proteção.

   - **Análise Personalizada** - ajuda a verificar ameaças em ficheiros, pastas ou volumes específicos.

Pode também iniciar uma Análise de Sistema ou Análise Rápida no painel de controlo.

4.4.3. Assistente de Análise

Sempre que iniciar uma verificação, o assistente de análise do Bitdefender Antivirus for Mac aparece.



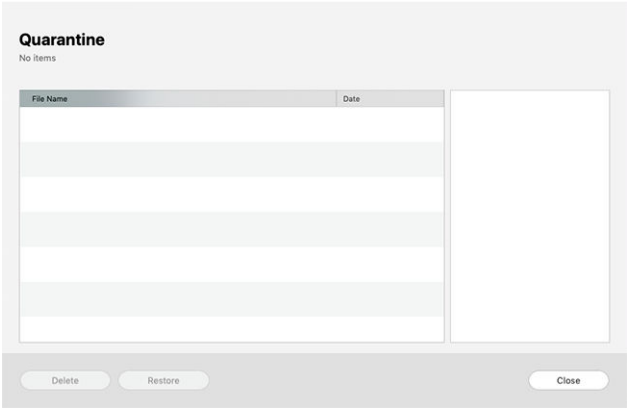
Informações em tempo real sobre as ameaças detetadas e resolvidas são apresentadas durante cada análise.

Espere que o Bitdefender Antivirus para Mac termine a verificação

> **Observação**
> O processo de verificação pode demorar algum tempo, dependendo da complexidade da mesma.

4.4.4. Quarentena

O Bitdefender Antivirus for Mac permite o isolamento de ficheiros infectados ou suspeitos numa área segura, chamada de quarentena. Quando uma ameaça se encontra na quarentena não pode provocar nenhum mal, porque não pode ser nem lida nem executada.



A secção de Quarentena mostra todos os ficheiros atualmente isolados na pasta de Quarentena.

Para eliminar um ficheiro da quarentena, selecione-o e clique em **Eliminar**. Se pretende restaurar um ficheiro da quarentena para a respetiva localização original, selecione-o e clique em **Restaurar**.

Para visualizar a lista de itens adicionados à quarentena:

1. Clique **Proteção** no menu de navegação na interface do Bitdefender.
2. Clique em **Abrir** no painel de **Quarentena**.

4.4.5. Bitdefender Shield (proteção em tempo real)

O Bitdefender fornece uma proteção contínua e em tempo real contra uma ampla variedade de ameaças ao verificar todos os ficheiros instalados, as suas versões atualizadas e ficheiros novos e modificados.

Para desativar a proteção em tempo real:

1. Clique em **Preferências** no menu de navegação da interface da Bitdefender.
2. Desligue o **Bitdefender Shield** na janela de **Proteção**.

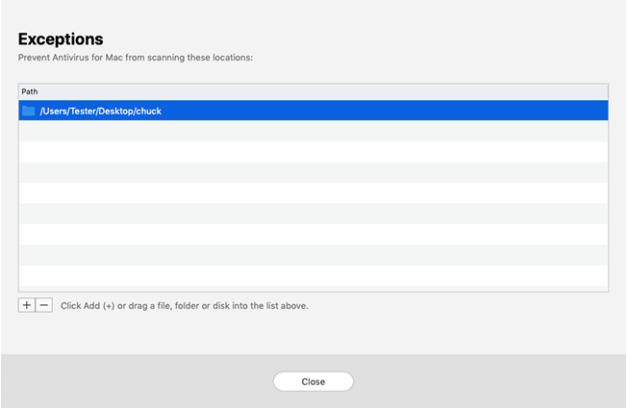
Aviso

Esta é uma incidência de segurança critica. Recomendamos que desactive a protecção em tempo-real o menos tempo possível. Quando a mesma está desactivada você deixa de estar protegido contra as ameaças.

4.4.6. Exceções de Análise

Se quiser, pode configurar o Bitdefender Antivirus for Mac para não analisar ficheiros, pastas ou até mesmo um volume inteiro específicos. Por exemplo, pode pretender eliminar da análise:

- Ficheiros que são erroneamente identificados como infetados (conhecidos como falsos positivos)
- Ficheiros que causam erros de análise
- Volumes de cópia de segurança



A lista de exceções contém os caminhos que foram excluídos da verificação.

Para aceder à lista de exceções:

1. Clique **Proteção** no menu de navegação na interface do Bitdefender.
2. Clique em **Abrir** no painel de **Exceções**.

Há duas formas de configurar uma exceção de análise:

- Arraste e largue um ficheiro, pasta ou volume sobre a lista de exceções.
- Clique no botão com o sinal mais (+), localizado sob a lista de exceções. De seguida, escolha o ficheiro, pasta ou volume a ser excluído da análise.

Para remover uma exceção de análise, selecione-a na lista e clique no botão com o sinal menos (-), localizado na lista de exceções.

4.4.7. Proteção da Internet

O Bitdefender Antivirus for Mac utiliza as extensões do TrafficLight para tornar a sua experiência de navegação na Web completamente segura. As extensões do TrafficLight intercetam, processam e filtram todo o tráfego na Web, bloqueando conteúdo malicioso.

As extensões funcionam e integram-se com os seguintes browsers: Mozilla Firefox, Google Chrome e Safari.

Ativar extensões do TrafficLight

Para ativar as extensões do TrafficLight:

1. Clique em **Resolver agora** no cartão de **Proteção da web** no Painel de Controlo.
2. É aberta a janela **Proteção na Web**.
   O navegador detetado que tem instalado no seu sistema aparecerá. Clique em **Obter extensão** para instalar a extensão do TrafficLight no seu navegador.
3. Vai ser redirecionado para:
   https://bitdefender.com/solutions/trafficlight.html
4. Selecione **Transferência Gratuita**.
5. Siga os passos para instalar a extensão do TrafficLight correspondente ao seu browser.

Gerir definições da extensões

Está disponível uma variedade de funcionalidades para o proteger de todas as formas de ameaças que pode encontrar enquanto navega na Internet. Para acedê-los, clique no ícone do TrafficLight próximo

das definições do seu navegador e, em seguida, clique no botão **Definições**:

- **Definições Bitdefender TrafficLight**
  - Proteção na Web - previne que aceda a sites utilizados para ataques de malware, phishing e fraude.
  - Analisador de Resultados de Pesquisa - proporciona alertas antecipados de websites de risco nos seus resultados de pesquisa.

- **Exceções**
  Se estiver no site que precisa de adicionar às exceções, clique em **Adicionar o site atual à lista**.
  Se desejar adicionar outro site, escreva o seu endereço no campo correspondente e, em seguida, clique em .
  Nenhum aviso será exibido caso ameaças estejam presentes nas páginas excluídas. É por esta razão que apenas as páginas em que confia totalmente devem ser adicionadas a esta lista.

Classificação de página e alertas

Dependendo de como o TrafficLight classifica a página que está a ver, é apresentado um dos seguintes ícones nessa área:

Esta é uma página segura de visitar. Pode continuar o seu trabalho.

Esta página web pode conter conteúdo perigoso. Tenha cuidado se decidir visitá-lo.

Deve abandonar esta página web imediatamente pois contém malware e outras ameaças.

No Safari, o fundo dos ícones do TrafficLight é preto.

4.4.8. Antitracker

Uma grande parte dos sites que utiliza monitorizadores para recolher informação sobre o seu comportamento para compartilhar com empresas ou para mostrar publicidade direcionada para si. Devido a isso, os donos dos sites ganham dinheiro por proporcionar conteúdo de graça ou para continuarem a funcionar. Além de recolher informação, os monitorizadores podem desacelerar a sua navegação ou desperdiçar a sua banda larga.

Com a extensão Anti-rastreio Bitdefender ativada no seu navegador da web, evita que seja rastreado para que os seus dados permaneçam privados enquanto navega online e acelera o tempo que os sites precisam para carregar.

A extensão do Bitdefender é compatível com os seguintes navegadores de internet:

- Google Chrome
- Mozilla Firefox
- Safari

Os monitorizadores que detectamos estão divididos nas seguintes categorias:

- **Publicidade** - utilizada para analisar o tráfego do site, o comportamento do utilizador ou os padrões de tráfego dos visitantes.
- **Interação com o cliente** - utilizados para medir a interação com o utilizador através de diferentes formas de entrada, como chat ou suporte.
- **Essenciais** - utilizados para monitorizar funcionalidades críticas do site.
- **Analíticas do site** - utilizadas para recolher dados sobre a utilização do site.
- **Redes Sociais** - utilizados para monitorizar o público em redes sociais, as suas atividades e o envolvimento dos utilizadores nas diferentes plataformas de redes sociais.

A ativar o Anti-rastreio Bitdefender

Para ativar a extensão Anti-rastreio Bitdefender no seu navegador da web:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. Selecione o separador **Anti-tracker**.
3. Clique **Permitir extensão** no browser em que pretende activar a extensão.

Interface do Antitracker

Quando a extensão Anti-rastreio Bitdefender é ativada, o ícone aparece ao lado da barra de pesquisa no seu navegador da web. Todas as vezes

que visita um site, um contador pode ser observado no ícone, referente aos rastreadores detetados e bloqueados. Para ver mais detalhes sobre os rastreadores bloqueados, clique no ícone para abrir a interface. Além do número de rastreadores bloqueados, pode visualizar o tempo necessário para a página carregar e as categorias às quais pertencem os rastreadores detetados. Para ver a lista dos sites que estão a rastrear, clique na categoria desejada.

Para impedir que a Bitdefender bloqueie monitorizadores no site que está a visitar, clique em **Pausar proteção neste site**. Esta definição só se aplica enquanto tiver o site aberto, e volta ao estado inicial quando fechar o site.

Para permitir que os monitorizadores de uma categoria específica monitorizem a sua atividade, clique na atividade desejada e, em seguida, no botão correspondente. Se mudar de ideias, clique no mesmo botão novamente.

Desligar o Anti-rastreio Bitdefender

Para desligar o Anti-rastreio Bitdefender do seu navegador da internet:

1. Abra o seu navegador web.
2. Clique no ícone ao lado da barra de endereço no seu navegador da web.
3. Clique no ícone no canto superior direito.
4. Utilize o interruptor correspondente para o desativar.
   O ícone do Bitdefender fica cinzento.

Permitir a monitorização de um site

Se desejar ser monitorizado ao visitar um site em particular, pode adicionar o seu endereço às excepções da seguinte forma:

1. Abra seu navegador da web.
2. Clique no ícone ao lado da barra de pesquisa.
3. Clique no ícone no canto superior direito.
4. Se você estiver no site que deseja adicionar às exceções, clique em **Adicionar site atual à lista**.

Se você deseja adicionar outro site, digite seu endereço no campo correspondente e clique em ⊕.

4.4.9. Safe Files

Ransomwares são softwares maliciosos que atacam sistemas vulneráveis bloqueando-os e exigindo dinheiro para permitir que o utilizador volte a ter controlo do seu sistema. Este software malicioso finge ser inteligente ao exibir mensagens falsas para assustar o utilizador, persuadindo-o a realizar o pagamento solicitado.

Utilizando a tecnologia mais recente, a Bitdefender assegura a integridade do sistema ao proteger as suas áreas essenciais contra ataques de ransomware sem ter impacto no sistema. Contudo, pode desejar proteger os seus ficheiros pessoais, como documentos, fotos ou filmes, contra o acesso de aplicações não fiáveis. Com o Safe Files da Bitdefender pode colocar os seus ficheiros pessoais sob proteção e configurar quais aplicações devem ou não ter permissão para fazer alterações nos ficheiros protegidos.

Para adicionar ficheiros ao ambiente protegido posteriormente:

1. Clique **Proteção** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Antiransomware**.
3. Clique em **Ficheiros protegidos** na área de ficheiros seguros.
4. Clique no botão com o sinal mais (+), localizado sob a lista de ficheiros protegidos. Em seguida, escolha o ficheiro, pasta ou volume a proteger no caso de ataques de ransomware que tentam aceder aos mesmos.

Para evitar o abrandamento do sistema, recomendamos que adicione no máximo 30 pastas ou guarde vários ficheiros numa única pasta.

Por predefinição, as pastas Imagens, Documentos, Ambiente de Trabalho e Transferências estão protegidas contra ataques de ameaças.

> **Observação**
> Pastas personalizadas apenas podem ser protegidas para os utilizadores atuais. Unidades externas, ficheiros do sistema e de aplicações não podem ser adicionados ao ambiente de proteção.

Será informador sempre que uma aplicação desconhecida com um comportamento incomum tente modificar os ficheiros adicionados. Clique em **Permitir** ou **Bloquear** para adicioná-la à lista **Gerir aplicações**.

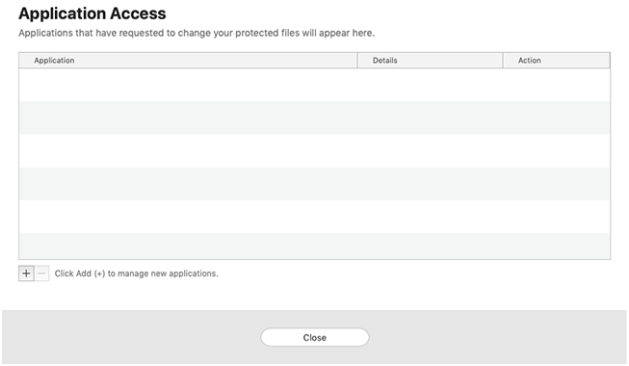
Acesso à aplicação

As aplicações que tentam mudar ou apagar ficheiros protegidos podem ser sinalizadas como potencialmente inseguras e adicionadas à lista de aplicações bloqueadas. Se uma aplicação como esta estiver bloqueada e não tiver a certeza se o respetivo comportamento é normal, pode autorizá-la ao seguir estes passos:

1. Clique **Proteção** no menu de navegação na interface do Bitdefender.
2. Selecione os **Anti-Ransomware** aba.
3. Clique em **Acesso à aplicação** na área de ficheiros seguros.
4. Altere o estado para Permitir, ao lado da aplicação bloqueada.

As aplicações definidas como Permitidas também podem ser definidas como Bloqueadas.

Utilize o método arraste&largar ou clique no sinal positivo (+) para adicionar mais aplicações à lista.



4.4.10. Time Machine Protection

A Proteção da Máquina do Tempo da Bitdefender funciona como uma camada de segurança adicional para a sua unidade de cópia de segurança, ao incluir todos os ficheiros nela armazenados, através do bloqueio do acesso de qualquer fonte externa. Caso os ficheiros da sua unidade da Máquina do Tempo sejam encriptados por ransomware, poderá recuperá-los sem pagar pelo resgate.

Caso precise de restaurar os itens de uma cópia de segurança da Máquina do Tempo, verifique a página de apoio da Apple para ver as instruções.

Ativar ou desativar a Proteção da Máquina do Tempo

Para ligar ou desligar desative a Proteção da Máquina do Tempo:

1. Clique em **Proteção** no menu de navegação da interface do **Bitdefender**.
2. Selecione os **Anti-Ransomware** aba.
3. Ative ou desative o botão de **Proteção Time Machine**.

4.4.11. Reparar Incidência

O Bitdefender Antivirus for Mac deteta automaticamente e informa-o sobre uma série de problemas que podem afetar a segurança do seu sistema e dados. Desta forma, pode reparar riscos de segurança facilmente e a tempo.

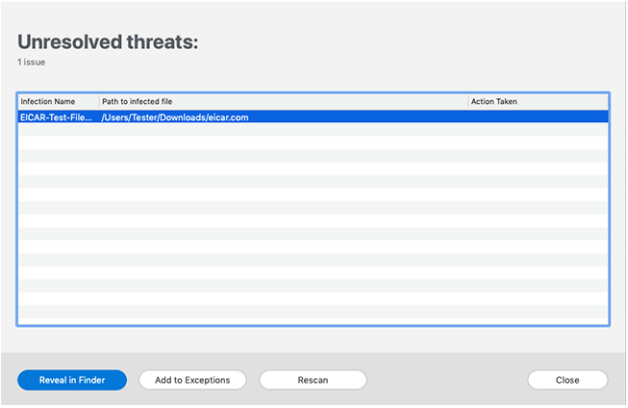
Reparar os problemas indicados pelo Bitdefender Antivirus for Mac é uma forma rápida e fácil de garantir a melhor proteção do seu sistema e dados.

Os problemas detetados incluem:

- A nova atualização de informações sobre ameaças não foi descarregada dos nossos servidores.
- Foram detectadas ameaças no seu sistema e o produto não pode desinfectá-las automaticamente.
- A proteção em tempo real está desativada.

Para verificar e reparar os problemas detetados:

1. Se o Bitdefender não tiver alertas, a barra de estado é verde. Quando um problema de segurança é detectado, a cor da barra de estado muda para vermelho.
2. Verifique a descrição para obter mais informações.
3. Quando um problema for detectado, clique no botão correspondente para realizar uma ação.



A lista de ameaças não resolvidas é atualizada após cada verificação de sistema, independentemente de se a verificação é feita de forma automática em segundo plano ou iniciada por si.

Pode escolher as seguintes ações para ameaças não resolvidas:

- **Eliminar manualmente**. Tome esta ação para remover as infeções manualmente.
- **Adicionar às Exceções**. Esta ação não está disponível para ameaças encontradas dentro dos ficheiros.

4.4.12. Notificações

A Bitdefender mantém um registo detalhado de eventos em relação à sua atividade no seu computador. Sempre que acontece algo relevante para a segurança do seu sistema ou dados, é adicionada uma nova mensagem à área de Notificações da Bitdefender, de forma semelhante a um novo e-mail a aparecer na sua caixa de entrada.

As notificações são uma ferramenta importante na monitorização e gestão da proteção do seu Bitdefender. Por exemplo, pode verificar com facilidade se a atualização foi realizada com sucesso, se foram encontradas ameaças ou vulnerabilidades no seu computador, etc. Adicionalmente, pode realizar outras ações, se necessário, ou alterar ações tomadas pelo Bitdefender.

Para aceder ao registo de notificações, clique em **Notificações** no menu de navegação da interface do Bitdefender. Sempre que acontecer este evento crítico, pode ser observado um contador no ícone .

Dependendo do tipo e da gravidade, as notificações são agrupadas em:

- Os eventos **críticos** indicam problemas críticos. Deve verificá-los imediatamente.
- O eventos de **Aviso** indicam incidências não críticas. Dev verificar e resolvê-los quando puder.
- Eventos de **Informação** indicam operações bem sucedidas.

Clique em cada separador para ver mais detalhes sobre os eventos gerados. São apresentados breves detalhes com um único clique em cada título de evento, como uma descrição curta, a ação tomada pelo Bitdefender quando o evento ocorreu e a data e hora do evento. Pode ser fornecidas opções para tomar mais ações, caso seja necessário.

Para o ajudar a gerir com facilidade os eventos registados, a janela de notificações oferece opções para eliminar ou marcar como lidos todos os eventos naquela secção.

4.4.13. Atualizações

Novas ameaças são encontradas e identificadas todos os dias. É por isto que é muito importante manter Bitdefender Antivirus for Mac atualizado com as atualizações de informação mais recentes.

As atualizações de informações sobre ameaças são executadas imediatamente, ou seja, os ficheiros que precisam de ser atualizados são substituídos progressivamente. Deste modo, a atualização não afetará o funcionamento do produto e, ao mesmo tempo, qualquer vulnerabilidade será eliminada.

- Se o Bitdefender Antivirus for Mac estiver atualizado, pode detetar as ameaças mais recentes descobertas e limpar os ficheiros infetados.
- Se o Bitdefender Antivirus para Mac não estiver atualizado, não será capaz de detetar e remover as ameaças mais recentes descobertas pelo Bitdefender Labs.

Solicitar uma Atualização

Pode solicitar uma atualização manualmente sempre que quiser.

É necessária uma ligação à Internet ativa para verificar atualizações disponíveis e transferi-las.

Para solicitar uma atualização manualmente:

1. Clique no botão **Ações** na barra de menu.
2. Escolha **Atualizar base de dados de informações sobre ameaças**.

Em alternativa, pode solicitar uma atualização manualmente ao premir CMD + U.

Pode ver o progresso de atualização e ficheiros transferidos.

A obter atualizações através de um servidor proxy

O Bitdefender Antivirus for Mac só pode ser atualizado através de servidores proxy que não requerem autenticação. Não precisa de modificar quaisquer definições do programa.

Caso se ligue à Internet através de um servidor proxy que requer autenticação, é necessário mudar para uma ligação direta regularmente para obter atualizações de informações sobre as ameaças.

Atualizar para uma nova versão

Ocasionalmente, lançamos atualizações do produto para adicionar novas funcionalidades e melhorias ou reparar problemas. Estas atualizações podem exigem um reinício do sistema para iniciar a instalação de ficheiros novos. Por predefinição, se uma atualização requer a reinicialização do sistema, o Bitdefender Antivirus for Mac continuará a trabalhar com os ficheiros anteriores até reiniciar o sistema. Neste caso, o processo de atualização não interferirá com o trabalho do utilizador.

Quando uma atualização do produto é concluída, uma janela pop-up irá informar para reiniciar o sistema. Se perder a notificação, pode clicar em **Reiniciar para atualizar** na barra de menus ou reiniciar o sistema manualmente.

Descobrir informação sobre o Bitdefender Antivirus para Mac

Para mais informações sobre a versão do Bitdefender Antivirus for Mac que tem instalada, aceda à janela **Informações**. Na mesma janela, pode obter acesso e visualizar as licenças de código aberto do Contrato de Subscrição e a Política de Privacidade.

Para aceder à janela Sobre:

1. Abra o Bitdefender Antivirus para Mac.

2. Clique em Bitdefender Antivirus para Mac na barra de menu e selecione **Sobre o Antivirus para Mac**.

4.5. Configurar preferências

Este capítulo inclui os seguintes tópicos:

4.5.1. Aceder às preferências

Para abrir a janela de Preferências do Bitdefender Antivirus para Mac:

- Faça qualquer uma das seguintes:
  - Clique **Preferências** no menu de navegação na interface do Bitdefender.
  - Clique em Bitdefender Antivirus para Mac na barra de menu e selecione **Preferências**.

4.5.2. Preferências de proteção

As preferências de proteção permitem que configure a abordagem geral de análise. Pode configurar as ações para ficheiros infectados e suspeitos detetados e outras definições gerais.

- **Bitdefender Shield.** A Bitdefender Shield oferece proteção em tempo real contra uma ampla gama de ameaças, verificando todas as aplicações instaladas, suas versões atualizadas e ficheiros novos e modificados. Não recomendamos que desative a Bitdefender Shield, mas se for necessário, faça-o pelo menor tempo possível. Se a Bitdefender Shield for desativada, não estará protegido contra ameaças.
- **Apenas Analise ficheiros novos e alterados.** Selecione esta caixa de seleção para configurar o Bitdefender Antivirus para Mac para analisar apenas ficheiros que não foram verificados antes ou que foram modificados desde a última análise.

Pode optar por não aplicar esta configuração para a verificação personalizada por meio de arrastar e soltar ao desmarcar a caixa de seleção correspondente.

- **Não analise conteúdo em cópias de segurança.** Selecione esta caixa para eliminar ficheiros de cópia de segurança da análise. Se os ficheiros infetados forem restaurados posteriormente, o Bitdefender Antivirus para Mac irá detetá-los automaticamente e tomará a ação apropriada.

4.5.3. Preferências avançadas

Pode escolher uma ação coletiva para todos os problemas e itens suspeitos encontrados durante o processo de análise.

Ação para itens infetados

- **Tente desinfetar ou mover para quarentena** - Se forem detetados ficheiros infetados, a Bitdefender tentará desinfetá-los (eliminar o código malicioso) ou colocá-los em quarentena.
- **Não fazer nada** - Nada será realizada qualquer ação em relação aos ficheiros detetados.

Ação para itens suspeitos

- **Mover os ficheiros para quarentena** - Se forem detetados ficheiros suspeitos, a Bitdefender irá colocá-los em quarentena.
- **Não faça nada** - Nenhuma ação será tomada nos arquivos detectados.

4.5.4. Ofertas Especiais

Quando as ofertas promocionais forem disponibilizadas, o produto Bitdefender está configurado para notificá-lo através de uma janela pop-up. Isto dar-lhe-á a oportunidade de aproveitar os preços vantajosos e manter os dispositivos protegidos por um período mais longo.

Para ativar ou desativar notificações de ofertas especiais:

1. Clique **Preferências** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Outros**.
3. Ative ou desative o botão **As minhas ofertas**.

Observação
A opção **As minhas ofertas** aparece ativada como definição padrão.

4.6. Perguntas Frequentes

Como posso experimentar o Bitdefender Antivirus for Mac antes de realizar a subscrição?

É um novo cliente Bitdefender e gostaria de experimentar o nosso produto antes de o comprar. O período de avaliação é de 30 dias e pode continuar a utilizar o produto instalado apenas se comprar uma subscrição Bitdefender. Para avaliar o Bitdefender Antivirus for Mac, precisa de:

1. Criar uma conta Bitdefender seguindo os seguintes passos:
   a. Vá para: https://central.bitdefender.com.
   b. Digite as informações solicitadas nos campos correspondentes. Os dados que nos fornecer serão mantidos confidenciais.
   c. Antes de continuar, deve concordar com os Termos de utilização. Aceda aos Termos de Utilização e leia-os com atenção, pois eles contêm os termos e condições segundo os quais pode utilizar o Bitdefender.
      Além disso, pode aceder e ler a Política de Privacidade.
   d. Clique em **CRIAR CONTA**.

2. Tranfira o Bitdefender Antivirus for Mac seguindo as instruções abaixo:
   a. Selecione os **Meus dispositivos** painel e, em seguida, clique em **INSTALAR PROTEÇÃO**.
   b. Escolha uma das duas opções disponíveis:
      - **Proteger este dispositivo**
        i. Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, clique no botão correspondente.
        ii. Salve o arquivo de instalação.
      - **Proteger outros dispositivos**

i. Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, clique no botão correspondente.

ii. Clique **ENVIAR LINK DE DOWNLOAD**.

iii. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR EMAIL**.
Observe que o link de download gerado é válido apenas pelas próximas 24 horas. Se o link expirar, você terá que gerar um novo seguindo os mesmos passos.

iv. No dispositivo em que deseja instalar seu produto Bitdefender, verifique a conta de e-mail que você digitou e clique no botão de download correspondente.

c. Execute o produto Bitdefender que você baixou.

Tenho um código de ativação. Como adiciono a sua validade à minha subscrição?

Se você comprou um código de ativação de um de nossos revendedores ou o recebeu de presente, pode adicionar sua disponibilidade à sua assinatura do Bitdefender.

Para ativar uma assinatura usando um código de ativação, siga estas etapas:

1. Acesso Bitdefender Central.
2. Selecione os **Minhas assinaturas** painel.
3. Clique no **CÓDIGO DE ATIVAÇÃO** botão e digite o código no campo correspondente.
4. Clique **ATIVAR** continuar.

A extensão agora é visível na sua conta da Bitdefender, e no seu produto Bitdefender Antivirus para Mac instalado, na parte inferior direita do ecrã.

O registo de análise indica que ainda há itens não resolvidos. Como os removo?

Os itens não resolvidos no registo de análise podem ser:

- ficheiros de acesso restrito (xar, rar, etc.)

Solução: Utilize a opção {3}Revelar no Finder{4} para encontrar o ficheiro e apagá-lo manualmente. Certifique-se de esvaziar a Lixeira.

- caixas de correio de acesso restrito (Thunderbird, etc.)
  Solução: utilize a aplicação para remover a entrada que contém o ficheiro infetado.
- O conteúdo nas cópias
  Solução: Ative a opção **Não verificar o conteúdo nas cópias de segurança** nas Preferências de Proteção ou **Adicione a Exceções** os os ficheiros detetados.
  Se os ficheiros infetados forem restaurados posteriormente, o Bitdefender Antivirus for Mac os detetará automaticamente e tomará a ação necessária.

> **Observação**
> Ficheiros de acesso restrito significam que o Bitdefender Antivirus for Mac só os pode abrir, mas não pode modificá-los.

Onde posso ver detalhes sobre a atividade do produto?

O Bitdefender mantém um registo de todas as ações importantes, mudanças de estado e outras mensagens críticas relacionadas com a sua atividade. Para aceder a essas informações, clique em **Notificações** no menu de navegação na interface da Bitdefender.

Posso atualizar o Bitdefender Antivirus for Mac através de um servidor proxy?

O Bitdefender Antivirus for Mac pode atualizar apenas através de servidores proxy que não requerem autenticação. Você não precisa definir nenhuma configuração do programa.

Se você se conectar à Internet por meio de um servidor proxy que exija autenticação, deverá alternar para uma conexão direta à Internet regularmente para obter atualizações de informações sobre ameaças.

Como faço para remover o Bitdefender Antivirus para Mac?

Para remover o Bitdefender Antivirus for Mac, siga estes passos:

1. Abra uma janela **Finder** e aceda à pasta Aplicações.
2. Abra a pasta da Bitdefender e depois clique duas vezes em Desinstalador Bitdefender.

3. Clique **Desinstalar** e aguarde a conclusão do processo.
4. Clique **Fechar** terminar.

> **Importante**
> Se houver um erro, você pode entrar em contato com o Atendimento ao Cliente da Bitdefender conforme descrito em Pedir Ajuda (página 261).

Como removo as extensões do TrafficLight do meu browser?

- Para remover as extensões do TrafficLight do Mozilla Firefox, siga estes passos:
  1. Vá para **Ferramentas** e selecione **Add-ons**.
  2. Selecione **Extensões** na coluna da esquerda.
  3. Selecione a extensão e clique em **Remover**.
  4. Reinicie o browser para concluir o processo de remoção.
- Para remover as extensões do TrafficLight do Google Chrome, siga estes passos:
  1. Na parte superior direita, clique em **Mais** ⋮.
  2. Vá para **Mais ferramentas** e selecione **Extensões**.
  3. Clique no ícone **Remover** 🗑 ao lado da extensão que deseja remover.
  4. Clique em **Desinstalar** para confirmar o processo de remoção.
- Para remover o Bitdefender TrafficLight do Safari, siga estes passos:
  1. Vá para **Preferências** ou pressione **Command-Comma(,)**.
  2. Selecione as **Extensões**.
     Será exibida a lista das extensões instaladas.
  3. Selecione a extensão do Bitdefender TrafficLight, e depois clique em **Desinstalar**.
  4. Clique outra vez em **Desinstalar** para confirmar a desinstalação.

Quando devo utilizar o Bitdefender VPN?

Tem de ter cuidado quando aceder, transferir ou enviar conteúdos na internet. Para garantir que fica em segurança enquanto navega na Web, recomendamos que utilize o Bitdefender VPN quando:

- quiser ligar-se a redes sem fios públicas
- quiser aceder a conteúdos que normalmente são restritos em áreas específicas, não importa se estiver em casa ou fora
- quiser manter os seus dados pessoais privados (nomes de utilizador, palavras-passe, informações de cartão de crédito, etc.)
- desejar esconder o seu endereço IP

O Bitdefender VPN terá um impacto negativo na bateria do meu dispositivo?

O Bitdefender VPN foi concebido para proteger os seus dados pessoais, esconder o seu endereço IP enquanto estiver ligado a redes sem fios não seguras e aceder a conteúdo restrito em certos países. Para evitar um consumo desnecessário de bateria do seu dispositivo, recomendamos que use o VPN apenas quando precisar, e que o desconecte quando estiver offline.

Por que estou a deparar-me com lentidão na Internet enquanto uso o Bitdefender VPN?

O Bitdefender VPN foi concebido para suavizar a sua experiência enquanto navega na Internet. No entanto, a lentidão pode ser causada pela sua conectividade com a internet ou pela distância do servidor ao qual está ligado. Nesse caso, se não for uma necessidade ligar a um servidor distante com respeito à sua localização (por exemplo, dos EUA ou China), recomendamos que permita ao Bitdefender VPN ligá-lo automaticamente ao servidor mais próximo, ou encontrar um servidor próximo da sua localização atual.

5. SEGURANÇA MÓVEL PARA ANDROID

5.1. O que é o Bitdefender Mobile Security

Atividades online, como pagar contas, fazer reservas para as férias ou comprar bens e serviços são convenientes e práticas. Mas, como muitas atividades realizadas na Internet, fazem-se acompanhar de elevados riscos e, se os detalhes de segurança forem ignorados, os dados pessoais podem ser hackeados. E o que é mais importante do que proteger os dados armazenados em contas online e no seu smartphone?

O **Bitdefender Mobile Security** permite-lhe:

- Obtenha a melhor proteção para o seu smartphone e tablet Android com impacto mínimo na duração da bateria
- Proteja-se contra a ameaça de virar vítima de fraudes com base em ligações
- Ganhe acesso ao nosso VPN seguro para uma experiência rápida, anónima e segura enquanto navega na internet
- Localize, bloqueie e limpe o seu dispositivo Android remotamente em caso de perda ou furto
- Verifique se a sua conta de e-mail esteve envolvida em vazamentos ou violações de dados

5.2. Introdução

5.2.1. Requisitos do Aparelho

O Bitdefender Mobile Security funciona em qualquer dispositivo que execute o Android 5.0 ou em qualquer versão posterior do sistema operativo. É necessária uma ligação ativa à internet para a verificação de ameaças na nuvem.

5.2.2. Instalar o Bitdefender Mobile Security

- **Na Central Bitdefender**
  - Android
    1. Vá a: https://central.bitdefender.com.

2. Entre na sua conta Bitdefender.
3. Selecione o painel **Os Meus Dispositivos**.
4. Toque em **INSTALAR PROTEÇÃO** e, em seguida, toque em **Proteger este dispositivo**.
5. Selecione o dono do dispositivo. Se o dispositivo pertencer a outra pessoa, pressione o respetivo botão.
6. Você será redirecionado para a aplicação do **Google Play**. No ecrã do Google Play, pressione a opção de instalação.

- No Windows, macOS e iOS
  1. Vá para: https://central.bitdefender.com.
  2. Entre na sua conta Bitdefender.
  3. Selecione os **Meus dispositivos** painel.
  4. Prima **INSTALAR PROTEÇÃO** e, em seguida, prima **Proteger outros dispositivos**.
  5. Selecione o dono do dispositivo. Se o dispositivo pertencer a outra pessoa, pressione o respetivo botão.
  6. Prima **ENVIAR LIGAÇÃO DE TRANSFERÊNCIA**.
  7. Escreva um endereço de e-mail no campo correspondente e pressione **ENVIAR E-MAIL**. Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.
  8. No dispositivo em que deseja instalar o Bitdefender verifique a conta de e-mail que escreveu e pressione o botão de download correspondente.

- **No Google Play**
  Procure o Bitdefender Mobile Security para localizar e instalar a aplicação.
  Alternativamente, analise o código QR:

  Antes de passar pelos passos de validação, deve concordar com o Acordo de Subscrição. Leia o acordo de Subscrição com calma, já que

ele contém os termos e condições segundo os quais pode utilizar o Bitdefender Mobile Security.
Toque em **CONTINUAR** para avançar para a janela seguinte.

5.2.3. Entre na sua conta Bitdefender

Para utilizar o Bitdefender Mobile Security, deve associar o seu dispositivo a uma conta Bitdefender do Facebook, Google, Apple ou Microsoft iniciando sessão na conta a partir da aplicação. A primeira vez que abrir a aplicação, será pedido que inicie sessão numa conta.

Se instalou o Bitdefender Mobile Security a partir da sua conta Bitdefender, a aplicação tentará entrar automaticamente nessa conta.

Para vincular o seu dispositivo a uma conta Bitdefender:

1. Introduza o endereço de e-mail e palavra-passe da sua conta Bitdefender nos campos correspondentes. Caso não tenha uma conta Bitdefender e deseje criar uma, pressione o link correspondente para criar uma.
2. Toque em **INICIAR SESSÃO**.

Para entrar usando uma conta do Facebook, Google ou Microsoft, pressione o serviço que deseja usar na área Ou entrar com. Será redirecionado para a página de login do serviço selecionado. Siga as instruções para vincular a sua conta ao Bitdefender Mobile Security.

> **Observação**
> O Bitdefender não obtém acesso a qualquer informação confidencial como a palavra-passe da conta que usa para iniciar sessão ou a informação particular dos seus amigos ou contactos.

5.2.4. Configurar proteção

Uma vez que consiga entrar na aplicação, a janela Configurar proteção aparecerá. Nós recomendamos que realize estes passos para proteger o seu dispositivo:

- **Estado de subscrição**. Para obter a proteção do Bitdefender Mobile Security, deve ativar o seu produto com uma subscrição, que especificará por quanto tempo poderá utilizar o produto. Assim que esse período acabar, a aplicação irá parar de realizar as suas funções e de proteger o seu dispositivo.

Se tiver um código de ativação, toque em **TENHO UM CÓDIGO**, e depois toque em **ATIVAR**.

Se tiver entrado com uma nova conta Bitdefender e não tiver um código de ativação, poderá utilizar o produto por 14 dias gratuitamente.

- **Proteção na Web**. Se o seu dispositivo requer Acessibilidade para ativar a Proteção na Web, toque em **ATIVAR**. Será redirecionado para o menu de Acessibilidade. Toque em Bitdefender Mobile Security e depois ative o botão correspondente.
- **Analisador de malware**. Realize uma análise única do seu dispositivo para se certificar que ele esteja livre de ameaças. Para iniciar o processo de análise, toque em **ANALISAR AGORA**.

  Assim que o processo de análise começar, o painel aparecerá. Aqui vê o estado de segurança do seu dispositivo.

5.2.5. Painel

Toque no ícone do Bitdefender Mobile Security nas aplicações do seu dispositivo para abrir a interface da aplicação.

O Painel fornece informações sobre o estado de segurança do seu dispositivo e através do Autopilot, ele ajuda a reforçar a segurança do seu dispositivo oferecendo recomendações de funcionalidades.

O cartão de estado no topo da janela informa sobre o estado de segurança do dispositivo utilizando mensagens explícitas e cores sugestivas. Se o Bitdefender Mobile Security não tiver alertas, o cartão de estado será verde. Quando um problema de segurança é detectado, a cor do cartão de estado muda para vermelho.

Para oferecer uma operação eficaz e uma proteção aprimorada enquanto realiza diferentes atividades, o **Bitdefender Autopilot** atuará como seu consultor pessoal de segurança. Dependendo da atividade que você realizar, o Bitdefender Autopilot fornecerá recomendações contextuais com base na utilização e necessidades do seu dispositivo. Isso irá ajudá-lo a descobrir e se beneficiar das vantagens trazidas pelos recursos incluídos na aplicação do Bitdefender Mobile Security.

Quando houver um processo em curso ou uma função solicitar uma ação sua, é exibido um cartão com mais informações e ações possíveis no Painel de Controlo.

É possível aceder às funcionalidades de Bitdefender Mobile Security e navegar facilmente da barra de navegação inferior:

Analisador de malware

Permite que inicie uma análise sob demanda e que ative o Armazenamento da Análise. Para mais informação, dirija-se a Analisador de Malware (página 194).

Proteção da Internet

Garante uma experiência de navegação segura alertando-lhe sobre páginas Web potencialmente maliciosas. Para mais informação, dirija-se a Proteção da Internet (página 197).

VPN

Encripta a comunicação na Internet, ajudando-o a manter a sua privacidade, não importando a rede à qual está ligado. Para mais informação, dirija-se a VPN (página 198).

Scam Alert

Garante a sua segurança ao alertá-lo sobre hiperligações maliciosas que chegam via SMS, aplicações de mensagens e qualquer tipo de notificação. Para mais informações, consulte Scam Alert (página 201).

Antifurto

Permite que ative ou desative as características Anti Furto e configure as definições Anti Furto. Para mais informação, dirija-se a Funcionalidades Anti Furto (página 203).

Privacidade de Conta

Verifique se houve fuga de dados nas suas contas online. Para mais informação, dirija-se a Privacidade de conta (página 207).

Bloqueio da aplicação

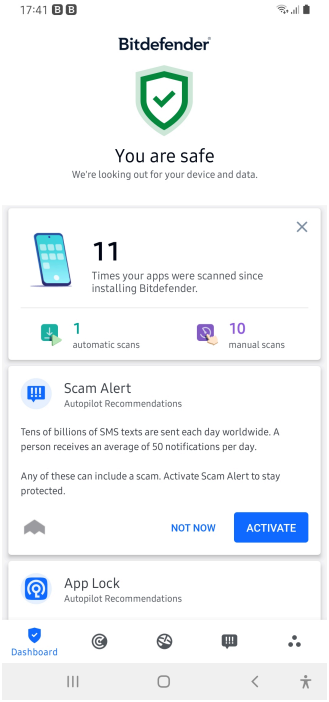
Permite que proteja as suas aplicações instaladas, através da configuração de um código PIN de acesso. Para mais informação, dirija-se a Bloqueio de Aplicativo (página 209).

Relatórios

Mantém um registro de todas as ações importantes, mudanças de estado e outras mensagens críticas relacionadas à atividade do seu dispositivo. Para mais informações, consulte Relatórios (página 213).

WearON

Comunica com o seu smartwatch para ajudá-lo a encontrar o seu telefone, caso o tenha perdido ou caso se tenha esquecido onde o deixou. Para mais informação, dirija-se a WearON (página 214).



5.3. Características e Funcionalidades

5.3.1. Analisador de Malware

Bitdefender protege o seu aparelho e dados de aplicações maliciosas utilizando a análise na instalação e análise sob pedido.

A interface do Verificador de Malware oferece uma lista de todos os tipos de ameaças analisadas pela Bitdefender, acompanhadas das suas definições. Basta tocar em qualquer ameaça para ver a sua definição.

> **Observação**
> Certifique-se de que o seu dispositivo móvel está ligado à internet. Se o seu dispositivo não estiver ligado à internet, o processo de análise não será iniciado.

- **Verificação na instalação**
  Sempre que instala uma aplicação, o Bitdefender Mobile Security verifica-o automaticamente utilizando a tecnologia na nuvem. O mesmo processo de verificação é iniciado toda vez que as aplicações instaladas são atualizadas.
  Se a aplicação for considerada maliciosa, irá aparecer um alerta solicitando que a desinstale. Toque em **Desinstalar** para aceder ao ecrã de desinstalação da aplicação.

- **Análise a pedido**
  Sempre que quiser saber se as aplicações instaladas no seu dispositivo são seguras para utilização, pode executar uma análise.
  Para iniciar uma análise sob demanda:

  1. Toque em **Verificador de Malware** na barra de navegação inferior.
  2. Toque em **COMEÇAR A ANÁLISE**.

  > **Observação**
  > Permissões adicionais são necessárias no Android 6 para a função do Verificador de Malware. Depois de tocar em **COMEÇAR VARREDURA**, selecione **Permitir** para o seguinte:
  >
  > - Permitir que o **Antivírus** faça e administre chamadas?
  > - Permitir que o **Antivírus** aceda a fotos, multimédia e ficheiros no seu dispositivo?

  O processo da análise é exibido e poderá interrompê-lo a qualquer momento.

O Bitdefender Mobile Security já vem configurado para analisar o armazenamento interno do seu dispositivo, incluindo qualquer cartão SD ligado. Desta forma, quaisquer aplicações perigosas que estejam no cartão podem ser detetadas antes de causar danos.

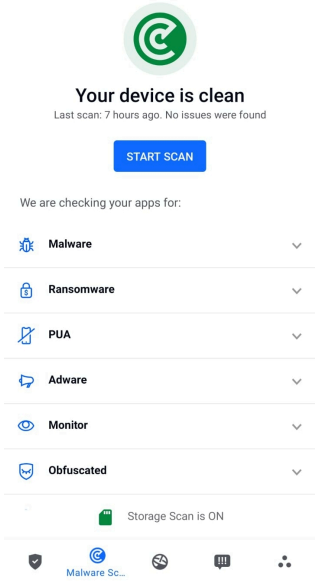
Para desativar a definição Análise do armazenamento:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Definições**.
3. Desative o interruptor **Análise do armazenamento** na área Scanner de Malware.

Caso sejam detetadas quaisquer aplicações maliciosas, serão exibidas informações sobre elas e poderá removê-las tocando no botão **DESINSTALAR**.

O cartão do analisador de Malware exibe o estado do seu dispositivo. Quando está seguro, o cartão fica verde. Quando o dispositivo necessitar de análise ou de alguma ação sua, o cartão ficará vermelho.

Se a sua versão do Android é a 7.1 ou posterior, pode aceder a um atalho para o Verificador de Malware, para poder executar as verificações de forma mais rápida, sem ter de abrir a interface do Bitdefender Mobile Security. Para isso, carregue continuamente no ícone do Bitdefender no seu ecrã de Início ou na gaveta de aplicações e, de seguida, selecione o ícone .



Detecção de anomalias em aplicativos

O Bitdefender App Anomaly Detection é uma nova tecnologia integrada ao Bitdefender Malware Scanner para fornecer uma camada adicional de proteção, monitorando e detectando continuamente quaisquer comportamentos maliciosos e alertando o usuário se atividades suspeitas forem identificadas.

A Detecção de Anomalias em Aplicativos Bitdefender protege os usuários mesmo quando eles instalam inadvertidamente um aplicativo perigoso que fica inativo por um período de tempo ou um aplicativo aparentemente confiável que quebra sua funcionalidade e se torna nocivo.

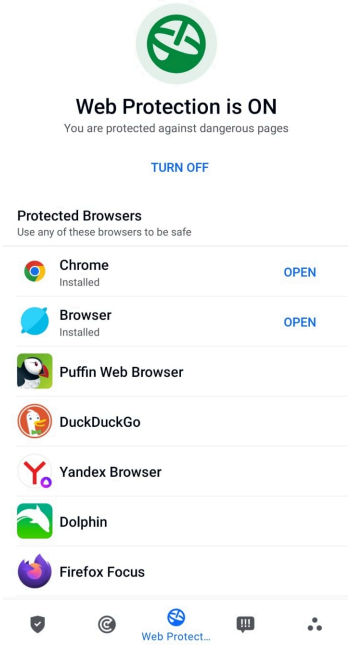
5.3.2. Proteção da Internet

A Proteção na Web verifica ao utilizar o Bitdefender páginas web de serviços em nuvem que você acede com o navegador padrão do Android, Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser e Dolphin.

Observação

São necessárias permissões adicionais no Android 6 para a função Web Protection.

Ative a permissão para registar como serviço de Acessibilidade e pressione **LIGAR** quando solicitado. Toque em **Antivírus** e ative o botão, depois confirme que concorda com o acesso às permissões do seu dispositivo.



Cada vez que acede a um site bancário, a Proteção na Web da Bitdefender é configurada para notificá-lo para utilizar o Bitdefender VPN. A notificação aparece na barra de estado. Recomendamos a utilização do Bitdefender VPN enquanto estiver conectado à sua conta bancária, para que os seus dados possam ficar a salvo de possíveis violações de segurança.

Para desativar a notificação Proteção Web:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Desligue o interruptor correspondente na área de Proteção Web.

5.3.3. VPN

Com o Bitdefender VPN , pode manter os seus dados privados sempre que se ligar a redes sem fios não seguras em aeroportos, shoppings, cafés ou hotéis. Assim, poderá evitar situações inoportunas, como roubo de dados

pessoais ou tentativas de tornar o endereço de IP do seu dispositivo acessível a hackers.

A VPN funciona como um túnel entre o seu dispositivo e a rede à qual se liga, protegendo a sua ligação, encriptando os seus dados utilizando uma encriptação de nível bancário e escondendo o seu endereço IP onde quer que esteja. O seu tráfego é redirecionado por meio de um servidor separado, tornando o seu dispositivo quase impossível de ser identificado entre os incontáveis dispositivos que usam os nossos serviços. Além disso, enquanto estiver ligado à Internet com o VPN, pode aceder a conteúdos que normalmente são restritos em áreas específicas.

> **Observação**
> Alguns países censuram a Internet e, portanto, a utilização de VPN nos seus territórios foi banido por lei. Para evitar consequências legais, pode ser apresentada uma mensagem de aviso ao tentar utilizar a aplicação Bitdefender VPN pela primeira vez. Ao continuar a utilizar a aplicação, confirma que está ciente dos regulamentos aplicáveis e dos riscos aos quais pode estar exposto.

Há duas formas de ativar ou desativar o Bitdefender VPN:

- Toque em **LIGAR** na placa VPN do Painel.
  O estado do Bitdefender VPN é exibido.
- Toque em **VPN** na barra de navegação inferior e, em seguida, toque em **CONECTAR**.
  Pressione **CONECTAR** sempre que quiser permanecer protegido enquanto estiver conectado a redes sem fios não seguras.
  Pressione **DESCONECTAR** quando desejar desativar a ligação.

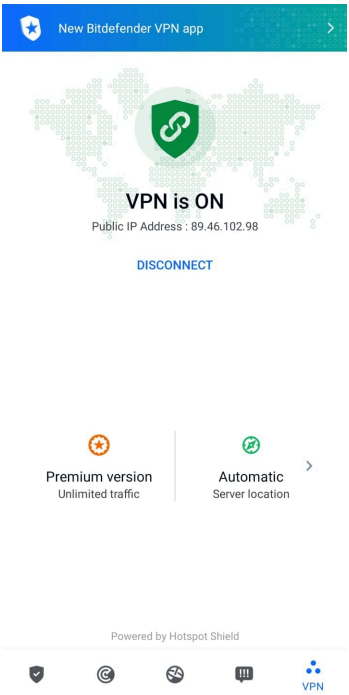
> **Observação**
> Na primeira vez que ligar o VPN, deve permitir a solicitação do Bitdefender para configurar uma ligação VPN que monitorizará o tráfego de rede. Prima **OK** para continuar.

Se a versão do seu Android for 7.1 ou superior, pode aceder a um atalho para o Bitdefender VPN, sem abrir a interface do Bitdefender Mobile Security.

Para isso, carregue continuamente no ícone do Bitdefender no seu ecrã de Início ou na gaveta de aplicações e, de seguida, selecione o ícone .

Para economizar bateria, recomendamos que desligue a VPN quando não precisar de usá-la.

Se tiver uma subscrição Premium e quiser ligar-se a um servidor da sua escolha, pressione Localização do servidor na ferramenta de VPN e, em seguida, selecione o local desejado. Para detalhes sobre as subscrições de VPN, aceda a



Definições da VPN

Para uma configuração avançada da sua VPN:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.

Nas área VPN, pode configurar as seguintes opções:

- Acesso rápido ao VPN - uma notificação aparecerá na barra de estado do seu dispositivo permitindo que ligue o VPN rapidamente.

- Alerta de Wi-Fi aberto - sempre que se ligar a uma rede Wi-Fi aberta, a barra de estado do seu dispositivo vai pedir-lhe para utilizar o VPN.

Assinaturas

O Bitdefender VPN oferece gratuitamente uma cota de tráfego diária de 200 MB por dispositivo para garantir a sua ligação sempre que precisar, ao ligá-lo automaticamente à localização ideal do servidor.

Para obter tráfego ilimitado e acesso irrestrito a conteúdos no mundo inteiro escolhendo um local da sua preferência, atualize para a versão Premium.

Pode atualizar para a versão do Bitdefender Premium VPN a qualquer momento tocando em **Ativar Premium** na janela do VPN.

A subscrição do Bitdefender Premium VPN é independente da subscrição do Bitdefender Mobile Security, o que significa que poderá utilizá-la enquanto estiver disponível, independentemente do estado da sua subscrição de segurança. Caso a subscrição do Bitdefender Premium VPN expire, mas a do Bitdefender Mobile Security ainda estiver ativa, será revertido para o plano gratuito.

O Bitdefender VPN é um produto multiplataforma, disponível nos produtos Bitdefender compatíveis com Windows, MacOS, Android e iOS. Quando atualizar para o plano premium, poderá utilizar a sua subscrição em todos os seus produtos, desde que inicie a sessão com a mesma conta da Bitdefender.

Observação

O Bitdefender VPN também funciona como uma aplicação autónoma em todos os sistemas operativos suportados, incluindo Windows, macOS, Android e iOS.

5.3.4. Scam Alert

A funcionalidade Scam Alert toma medidas preventivas em primeiro plano, lidando com situações potencialmente perigosas antes mesmo que elas tenham a oportunidade de se tornar um problema, incluindo ameaças de malware. O Scam Alert monitoriza todas as mensagens SMS recebidas e notificações do Android em tempo real.

Quando um link perigoso chegar por mensagem no seu telefone, um aviso irá aparecer no seu ecrã. A Bitdefender irá oferecer duas opções.

A primeira opção é ignorar a informação. A segunda opção é **VISUALIZAR DETALHES**. Isso fornece mais informações sobre o incidente, bem como conselhos essenciais, como por exemplo:

- Não abra ou encaminhe o link detetado.
- No caso dos SMS, elimine a mensagem, se possível.
- Bloqueie o remetente se não for um contacto de confiança.
- Elimine a aplicação que envia links perigosos em notificações.

> **Observação**
> Devido a limitações do sistema operativo Android, a Bitdefender não pode apagar mensagens de texto ou tomar quaisquer medidas diretas relacionadas com as mensagens SMS, ou qualquer outra fonte de notificações maliciosas. Se ignorar o aviso de Scam Alert e tentar abrir um link perigoso, a funcionalidade da Proteção na Web da Bitdefender captura-o automaticamente, ao impedir que o seu dispositivo seja infetado.

Ativar o Scam Alert

Para ativar o Scam Alert, é necessário conceder o acesso às mensagens SMS e ao sistema de notificação à aplicação da Bitdefender Mobile Security:

1. Abra a aplicação do Bitdefender Mobile Security instalado no seu telefone ou tablet Android.
2. No ecrã principal da aplicação da Bitdefender, toque na opção **Scam Alert** na barra de navegação inferior, depois toque em **ATIVAR**.
3. Toque no botão **PERMITIR**.
4. Na lista de Acesso à Notificação, mude o Bitdefender Security para a posição **ON**.
5. Confirme a ação ao tocar em **PERMITIR**.
6. Volte ao ecrã de Scam Alert e toque em **PERMITIR** para dar ao Bitdefender a capacidade de verificar as mensagens SMS recebidas.

Proteção de chat em tempo real

As mensagens de chat são o nosso meio mais confortável de manter contacto, mas são também uma forma fácil para que links perigosos cheguem até si.

Com o recurso de Proteção de Chat ativo, o módulo Scam Alert vai além da proteção das suas mensagens de texto e notificações para manter os seus chats seguros também contra ataques baseados em links, ao detetar os links perigosos que envia ou recebe durante o chat.

Para ativar a Proteção de Chat:

1. Abra o aplicativo Bitdefender Mobile Security instalado em seu telefone ou tablet Android.
2. No ecrã principal da aplicação da Bitdefender, toque na opção **Scam Alert** na barra de navegação inferior.
3. Verá a funcionalidade de Proteção de Chat no topo da aba do Scam Alert. Mude o interruptor correspondente para a posição **ON**.

> **Observação**
> Atualmente, a Proteção de Chat é compatível com as seguintes aplicações:
>
> - WhatsApp
> - Facebook Messenger
> - Telegram
> - Discord

5.3.5. Funcionalidades Anti Furto

Bitdefender pode ajudá-lo a localizar o seu dispositivo e impedir que os seus dados pessoais caiam nas mãos erradas.

Tudo o que necessita de fazer é ativar o Anti-roubo a partir do dispositivo e, quando necessário, aceder à **Bitdefender Central** a partir de qualquer Web browser, em qualquer lugar.

> **Observação**
> A interface do Antifurto também inclui uma hiperligação para a nossa aplicação da Central Bitdefender no Google Play Store. Pode utilizar esta hiperligação para transferir a aplicação, caso ainda não o tenha feito.

O Bitdefender Mobile Security oferece as seguintes características Antifurto:

Localização remota

Visualize a localização atual do seu dispositivo no Google Maps. A localização é atualizada a cada 5 segundos para que possa controlá-lo se estiver em movimento.

A precisão da localização depende do quanto o Bitdefender é capaz de o determinar:

- Caso o GPS esteja ativado no dispositivo, a sua localização pode ser determinada no alcance de dois metros, desde que esteja ao alcance dos satélites GPS (ou seja, fora de um edifício).
- Se o dispositivo estiver dentro de um edifício, a sua localização pode ser determinada no alcance de 10 metros caso o Wi-Fi esteja ativado e existam rede sem fios disponíveis no seu alcance.
- Caso contrário, a localização será determinada utilizando apenas as informações da rede móvel, que pode oferecer uma precisão não melhor que várias centenas de metros.

Bloqueio remoto

Bloqueie o ecrã do seu dispositivo e defina uma palavra-passe para desbloquear o mesmo.

Limpeza remota

Remova todos os dados pessoais do seu dispositivo roubado.

Enviar alerta para o dispositivo (Scream)

Envie uma mensagem remotamente para ser exibida no ecrã do dispositivo ou para emitir um som alto no altifalante do dispositivo.

Caso venha a perder o seu dispositivo, pode informar a quem o encontrar como pode ser devolvido, exibindo uma mensagem no ecrã do dispositivo.

Caso tenha perdido o seu dispositivo e exista a possibilidade de não estar longe de si (por exemplo, em algum lugar em casa ou no escritório), que melhor maneira de encontrá-lo do que fazê-lo tocar um som alto? O som será reproduzido mesmo se o dispositivo estiver no modo silencioso.

A ativar o Anti Furto

Para ativar a função Anti Furto, basta completar o processo de configuração do cartão Anti Furto disponível no Painel de Controlo.

Também pode ativar a função Anti Furto seguindo estas instruções:

1. Tocar **Mais** na barra de navegação inferior.
2. Toque em **Antifurto**.
3. Toque em **ATIVAR**.
4. O seguinte procedimento será iniciado para ajudá-lo na ativação desta função:

   > **Observação**
   > São necessárias permissões adicionais no Android 6 para a função Anti Furto.
   >
   > Para o ativar, siga estes passos:
   >
   > a. Toque em **Ativar Antifurto** e, em seguida, toque em **ATIVAR**.
   > b. Permite que o **Antivírus** aceda à localização deste dispositivo

   a. **Conferir Privilégios de Administrador**
   Estes privilégios são essenciais para o funcionamento da função Anti Furto e devem ser concedidas antes de continuar.

   b. **Definir o PIN da Aplicação**
   Para evitar o acesso não autorizado ao seu dispositivo, tem de definir um código PIN. Sempre que for feita uma tentativa de acesso ao seu dispositivo, é necessário introduzir o PIN primeiro. Em alternativa, nos dispositivos que suportam a autenticação com impressão digital, pode utilizar uma confirmação de impressão digital em vez do código PIN configurado.
   O mesmo código PIN é utilizado pelo Bloqueio de Aplicação para proteger as suas aplicações instaladas.

   c. **Ativar Foto Instantânea**
   Sempre que alguém tentar desbloquear o seu dispositivo sem sucesso enquanto Tirar Foto estiver ativado, o Bitdefender tira uma foto.
   Dokładniej, za każdym razem, gdy kod PIN, hasło lub potwierdzenie odcisku palca, które ustawiłeś, aby chronić urządzenie, jest trzykrotnie błędnie wpisane, robione jest zdjęcie przy użyciu przedniego aparatu. A foto é guardada com o carimbo de data/hora e o motivo e pode ser vista quando abre Bitdefender Mobile Security da janela Antirroubo.
   Alternatywnie można wyświetlić zrobione zdjęcie w koncie Bitdefender:

i. Vá para: https://central.bitdefender.com.
ii. Aceda à sua conta.
iii. Selecione os **Meus dispositivos** painel.
iv. Selecione o dispositivo Android e o separador **Antirroubo**.
v. Toque em ⋮ ao lado de **Verificar suas fotos** para ver as últimas fotografias que foram tiradas.
Só são guardadas as duas fotografias mais recentes.

Ao ativar o recurso Anti-roubo, pode ativar ou desativar os comandos de Controlo Web de maneira individual na janela de Anti-roubo tocando nas opções correspondentes.

Usar as funcionalidades Anti-Roubo a partir da Bitdefender Central

> **Observação**
> Todas as funcionalidades de Anti Furto necessitam que a opção **Dados em segundo plano** esteja ativa nas configurações de Dados do seu dispositivo.

Para aceder às funções anti-furto da sua conta Bitdefender:

1. Aceda a **Central da Bitdefender**.
2. Selecione os **Meus dispositivos** painel.
3. Na janela **OS MEUS DISPOSITIVOS**, selecione o cartão de dispositivo desejado tocando no botão **Ver detalhes** correspondente.
4. Selecione o separador **Anti Furto**.
5. Toque no botão correspondente à funcionalidade que pretende utilizar:
   Localizar - exibe a localização do seu dispositivo no Google Maps.
   MOSTRAR IP - exibe o último endereço de IP para o dispositivo selecionado.
   Alerta - escreva uma mensagem para ser exibida no ecrã do seu dispositivo e/ou para fazer com que o seu dispositivo emita um alarme sonoro.
   Bloqueio - bloqueie o seu dispositivo e defina um código PIN para desbloqueá-lo.
   Limpeza - apague todos os dados do seu dispositivo.

> **Importante**
> Após apagar toda a informação de um dispositivo, todas as funcionalidades Anti-Roubo deixam de funcionar.

Funcionalidades Antirroubo

Se pretender ativar ou desativar os comandos remotos:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Anti-roubo**.
3. Ative ou desative as opções pretendidas.

5.3.6. Privacidade de conta

O Bitdefender Account Privacy deteta se houve alguma violação de dados nas contas que utiliza para fazer pagamentos online, compras ou iniciar sessão em diferentes aplicações ou sites Web. Os dados armazenados numa conta podem ser palavras-passe, informações de cartão de crédito ou informações de conta bancária e, se não forem devidamente protegidos, pode sofrer roubo de identidade ou invasão de privacidade.

O estado de privacidade de uma conta é apresentado depois da validação.

A novas verificações automáticas são definidas para serem executadas em segundo plano, mas é possível executar análises manuais diariamente.

As notificações serão apresentadas sempre que são detetadas novas quebras que incluam qualquer uma das contas de e-mail validadas.

Para começar a proteger informações pessoais:

1. Tocar **Mais** na barra de navegação inferior.
2. Toque em **Privacidade da conta**.
3. Toque em **INICIAR**.
4. O endereço de e-mail utilizado para criar a sua conta da Bitdefender aparece e é automaticamente adicionado à lista de contas monitorizadas.
5. Para adicionar outra conta, toque em **ADICIONAR CONTA** na janela de Privacidade da Conta e escreva o endereço de e-mail.

Toque em **ADICIONAR** para continuar.

Bitdefender necessita de validar esta conta antes de apresentar informações privadas. Portanto, é enviado um e-mail com um código de validação para o endereço de e-mail fornecido.

Verifique a caixa de entrada e digite o código recebido na área **Privacidade de Conta** da aplicação. Se não conseguir encontrar o e-mail de validação na pasta Caixa de Entrada, verifique a pasta Spam.

O estado de privacidade da conta validada é apresentado.

Se forem detetadas quebras nas suas contas, recomendamos que altere as palavras-passe assim que possível. Para criar uma palavra-passe forte e segura, tenha em mente estas dicas:

- Oito carateres no mínimo.
- Carateres maiúsculos e minúsculos.
- Pelo menos um número ou símbolo, como #, @, % ou !.

Ao proteger uma conta que constava de uma violação de privacidade, pode confirmar as alterações ao marcar a(s) quebra(s) identificada(s) como Resolvido. Para tal:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Privacidade da conta**.
3. Toque na conta que acabou de proteger.
4. Toque na quebra de onde protegeu a conta.
5. Toque em **RESOLVIDO** para confirmar que a conta está protegida.

Quando todas as quebras detetadas estiverem marcadas como **Resolvido**, a conta já não aparece como quebra, pelo menos até à deteção de uma nova quebra.

Para parar de ser notificado sempre que são realizadas análises automáticas:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Desligue o interruptor correspondente na área Privacidade da conta.

5.3.7. Bloqueio de Aplicativo

Aplicações instaladas, como e-mails, fotos ou mensagens, podem conter dados pessoais que gostaria que permanecessem privados, limitando o acesso a estes de forma seletiva.

O Bloqueio de Aplicação ajuda-o a bloquear o acesso indesejado às aplicações, através da configuração de um código PIN de acesso de segurança. O código PIN deve ter no mínimo 4 dígitos e no máximo 8 e será solicitado sempre que pretender aceder às aplicações restritas.

A autenticação biométrica (tal como confirmação de impressão digital ou reconhecimento facial) pode ser utilizada em vez do código PIN configurado.

A ativar o Bloqueio de Aplicação

Para restringir o acesso a aplicações específicas, configure o Bloqueio de Aplicação através do cartão exibido no Painel de Controlo após a ativação da função Anti Furto.

Também pode ativar o Bloqueio de Aplicação seguindo estas instruções:

1. Tocar **Mais** na barra de navegação inferior.
2. Toque em **Bloqueio de aplicações**.
3. Tocar **LIGAR**.
4. Permitir o acesso aos dados de utilização para o Bitdefender Security.
5. Permitir **prioridade em relação a outras aplicações**.
6. Volte à aplicação, configure o código de acesso e pressione **DEFINIR PIN**.

   > **Observação**
   > Este passo será apenas necessário se não tiver configurado o PIN na função Anti Furto.

7. Permite que a opção Tirar Foto apanhe qualquer intruso que tente aceder aos seus dados pessoais.

Observação

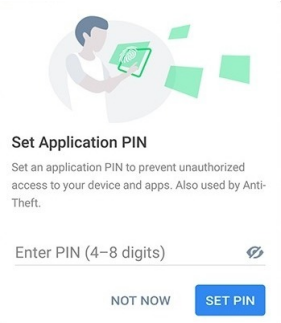
São necessárias permissões adicionais no Android 6 para a função Tirar Foto. Para ativá-la, permita que o **Antivírus** tire fotos e grave vídeos.

8. Selecione as aplicações que gostaria de proteger:

Utilizar o PIN ou a impressão digital errada cinco vez seguidas ativará uma pausa de 30 segundos. Dessa forma, qualquer tentativa de aceder às aplicações protegidas será bloqueada.

Observação

O mesmo código PIN é utilizado pelo Anti Furto para ajudá-lo a localizar o seu dispositivo.



MODO DE BLOQUEIO

A primeira vez que adicionar uma aplicação ao Bloqueio de aplicação, o ecrã Modo de bloqueio de aplicação aparece. Daqui é possível escolher quando a função Bloqueio de aplicação deve proteger as aplicações intaladas no seu dispositivo.

Pode selecionar entre uma das seguintes opções:

- **Necessita sempre de desbloqueio** - sempre que as aplicações bloqueadas são acedidas, o código PIN ou impressão digital que configurou será utilizado.
- **Manter desbloqueado até o ecrã apagar** - o acesso às suas aplicações será válido até o ecrã apagar.
- **Bloquear após 30 segundos** - é possível sair e aceder novamente às suas aplicações desbloqueadas num espaço de 30 segundos.

Caso pretenda alterar a definição selecionada:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Toque em **Requer sempre desbloqueio** na área Bloqueio de aplicação.
4. Escolha a opção desejada.

Definições do Bloqueio de Aplicação

Para uma configuração avançada do Bloqueio de aplicação:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.

Na área Bloqueio de aplicação, é possível configurar as opções seguintes:

- **Sugestão de aplicação confidencial** - receba uma notificação de bloqueio sempre que instalar uma aplicação confidencial.
- **Requer sempre desbloqueio** - escolha uma das opções de bloqueio e desbloqueio disponíveis.
- **Desbloqueio inteligente** - mantenha as aplicações desbloqueadas enquanto estiver ligado a redes Wi-Fi de confiança.
- **Teclado aleatório** - previne a leitura do PIN ao mostrar os números de forma aleatória.

Tirar foto

Com o Bitdefender Snap Photo, pode apanhar os seus amigos ou parentes rapidamente. Desta forma, pode educar os olhos curiosos deles para não passarem os olhos pelos seus ficheiros pessoais ou pelas aplicações que utiliza.

A função funciona de forma fácil: sempre que o código PIN ou a confirmação por impressão digital que definiu para proteger as suas aplicações for inserido de forma errada três vezes seguidas, será tirada uma foto com a câmara frontal. A foto será guardada com a informação sobre o dia, hora e motivo, e poderá ser visualizada quando abrir o Bitdefender Mobile Security e aceder à função do Bloqueio de Aplicação.

> **Observação**
> Esta função está disponível apenas para telefones que têm uma câmara frontal.

Para configurar a função de Instantâneo para Bloqueio de aplicação:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Ative o interruptor correspondente na área Instantâneo.

As fotos tiradas quando é introduzido o PIN incorreto são exibidas na janela de Bloqueio de Aplicação e podem ser visualizadas em ecrã completo.

De forma alternativa, eles podem ser vistos na sua conta Bitdefender:

1. Vá para: https://central.bitdefender.com.
2. Faça login em sua conta.
3. Selecione o painel **Os meus dispositivos**.
4. Selecione seu dispositivo Android e, em seguida, o **Anti-roubo** aba.
5. Tocar ao lado de **Verifique seus instantâneos** para ver as fotos mais recentes que foram tiradas.

Apenas as duas fotos mais recentes são salvas.

Para parar o carregamento de fotos tiradas na sua conta Bitdefender:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Desative **Carregar fotos** na área Instantâneo.

Desbloqueio Inteligente

Um método fácil para que a função Desbloqueio de Aplicação deixe de solicitar o código PIN ou a confirmação por impressão digital para as aplicações protegidas sempre que acede é ativar o Desbloqueio Inteligente.

Com o Desbloqueio Inteligente pode configurar as redes Wi-Fi que costuma utilizar como fiáveis e quando estiver ligado a elas, as definições de bloqueio do Bloqueio de Aplicação serão desativadas para as aplicações protegidas.

Para configurar a função Desbloqueio inteligente:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Bloqueio do aplicativo**.
3. Toque no botão .
4. Toque no interruptor ao lado do **Smart Unlock**, caso a funcionalidade ainda não esteja ativada
   Valide utilizando a sua impressão digital ou o seu PIN.
   A primeira vez que ativar a funcionalidade, deverá ativar a permissão de localização. Toque no botão **PERMITIR** e, em seguida, prima **PERMITIR** novamente.
5. Toque em **ADICIONAR** para configurar a ligação Wi-Fi que está a utilizar atualmente como sendo de confiança.

Sempre que mudar de opinião, desative a função e as redes Wi-Fi que configurou como fiáveis serão tratadas como não fiáveis.

5.3.8. Relatórios

O recurso Relatórios mantém um registo detalhado de eventos relacionados com a atividade de análise do seu dispositivo.

Sempre que acontecer algo relevante para a segurança do seu dispositivo, será adicionada uma nova mensagem aos Relatórios.

Para aceder à secção Relatórios:

1. Tocar **Mais** na barra de navegação inferior.
2. Toque em **Relatórios**.

Os seguintes separadores estão disponíveis na janela Relatórios:

- **RELATÓRIOS SEMANAIS** - aqui tem acesso ao estado de segurança e às tarefas executadas da semana atual e anterior. O relatório semanal é gerado todos os domingos e receberá uma notificação informando-o acerca da sua disponibilidade.
  Todas as semanas será exibida uma nova dica nesta secção, então lembre-se de conferir regularmente para obter o máximo do que a sua aplicação pode oferecer.
  Para parar de receber notificações sempre que um relatório é gerado:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Desative o interruptor **Notificação de novo relatório** na área Relatórios.

- **REGISTO DE ATIVIDADES** - aqui poderá aceder a informações detalhadas sobre as atividades da sua aplicação Bitdefender Mobile Security, desde quando foi instalada no seu dispositivo Android.
  Para eliminar o relatório de atividade disponível:

  1. Tocar **Mais** na barra de navegação inferior.
  2. Tocar **Configurações**.
  3. Toque em **Apagar registo de atividades**, e depois toque em **APAGAR**.

5.3.9. WearON

Com Bitdefender WearON, pode encontrar facilmente o seu smartphone, esteja ele na sala de reunião do escritório ou sob uma almofada no sofá. O dispositivo pode ser encontrado mesmo se o modo silencioso estiver ativado.

Mantenha esta função ativada para garantir que terá sempre o seu smartphone por perto.

> **Observação**
> A função funciona com Android 4.3 e Android Wear.

A ativar o WearON

Para utilizar o WearON, só precisa de ligar o seu smartwatch à aplicação do Bitdefender Mobile Security e ativar a função com o seguinte comando de voz:

Início:<Onde está o meu telefone>

O **Bitdefender WearON** tem dois comandos:

1. **Alerta de telefone**
   Com o recurso Alerta do Telefone encontra rapidamente o seu smartphone, sempre que se afastar muito dele.

Se estiver com o seu smartwatch, ele detectará automaticamente a aplicação no seu telefone e irá vibrar sempre que estiver muito longe do seu relógio, mais precisamente, quando a ligação de Bluetooth for perdida.
Para ativar esta função, abra o Bitdefender Mobile Security, toque em **Configurações Globais** no menu e selecione o botão correspondente na secção WearON.

2. **Grito**
   Encontrar o seu telefone nunca foi tão fácil. Quando se esquecer onde deixou o seu telefone, toque no comando Apitar no seu relógio para fazer o seu telefone apitar.

5.3.10. Sobre

Para mais informações sobre a versão do Bitdefender Mobile Security que tem instalada, para aceder e ler o Acordo de subscrição e Política de privacidade, e visualizar as licenças Open-source:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Toque na opção desejada na área Sobre.

5.4. Perguntas Frequentes

Porque é que o Bitdefender Mobile Security requer uma ligação à Internet?

A aplicação precisa de comunicar com os servidores do Bitdefender para determinar o estado de segurança das aplicações que analisa e das páginas web que visita e também para receber os comandos da sua conta Bitdefender quando utilizar a função Anti Furto.

Para que é que o Bitdefender Mobile Security precisa de cada permissão?

- Acesso à internet -> utilizado para comunicação com a nuvem.
- Ler o estado e a identidade do telefone -> utilizado para detetar se o dispositivo está ligado à internet e extrair certas informações do dispositivo necessárias para criar uma identificação única ao comunicar com a nuvem da Bitdefender.

- Ler e escrever marcadores do navegador -> O módulo Proteção da Web apaga sites maliciosos do seu histórico de navegação.
- Ler os dados de registo -> O Bitdefender Mobile Security deteta vestígios de atividades de ameaças a partir dos registos do Android.
- Localização -> necessária para a localização remota.
- Câmera -> necessária para Tirar foto.
- Armazenamento -> utilizado para permitir que o Analisador de Malware verifique o cartão SD.

Como é que posso parar de submeter informações de Bitdefender sobre aplicações suspeitas?

Por predefinição, o Bitdefender Mobile Security envia relatórios aos servidores Bitdefender sobre aplicações suspeitas que esteja a instalar. Estas informações são essenciais para melhorar a deteção de ameaças e pode ajudar-nos a oferecer-lhe uma melhor experiência no futuro. Caso queira parar de nos enviar informações sobre aplicações suspeitas:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Desligue **Deteção dentro da nuvem** na área Scanner de Malware.

Onde posso ver mais informações sobre a atividade do aplicação?

O Bitdefender Mobile Security mantém um registo de todas as ações importantes, mudanças de estado e outras mensagens críticas relacionadas com a sua atividade. Para aceder, consulte a atividade da aplicação:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Relatórios**.
   Na janela de RELATÓRIOS SEMANAIS, é possível aceder aos relatórios que foram gerados todas as semanas e na janela REGISTO DE ATIVIDADE, pode visualizar as informações sobre a atividade da sua aplicação Bitdefender.

Esqueci-me do código PIN que defini para proteger a minha aplicação. O que devo fazer?

1. Acesso Bitdefender Central.

2. Selecione os **Meus dispositivos** painel.
3. Toque no cartão de dispositivo pretendido e, em seguida, toque em ⋮ no canto superior direito do ecrã.
4. Selecione **Configurações**.
5. Recupere o PIN no campo **PIN da Aplicação**.

Como é que posso alterar o código PIN que definir para Bloqueio de aplicação e Antirroubo?

Se pretende alterar o código PIN que definir para Bloqueio de aplicação e Antirroubo:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Toque em **CÓDIGO PIN** de segurança na área Antirroubo.
4. Introduza o código PIN atual.
5. Introduza o novo código PIN que pretende definir.

Como posso desligar a função Bloqueio de Aplicação?

Não há qualquer opção para desligar a função Bloqueio de Aplicação, mas pode desativá-la facilmente ao desmarcar as caixas próximas às aplicações selecionadas depois que validar o PIN ou impressão digital definida.

Como posso definir outra rede sem fios como fiável?

Em primeiro, tem de ligar o seu dispositivo à rede sem fios que pretende definir como de confiança. Em seguida, siga estes passos:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Bloqueio do aplicativo**.
3. Toque em no canto superior direito.
4. Toque em **ADICIONAR** ao lado da rede que pretende definir como de confiança.

Como posso parar de ver fotografias associadas tiradas nos meus dispositivos?

Para parar de tornar visíveis as fotografias associadas tiradas nos seus dispositivos:

1. Acesso Bitdefender Central.
2. Toque em no canto superior direito do ecrã.
3. Toque em **Definições** no menu deslizante.
4. Desative a Opção **Mostrar/Não mostrar fotos instantâneas tiradas nos seus dispositivos**.

Como posso manter as minhas compras online seguras?

As compras online têm riscos elevados quando alguns detalhes são ignorados. Para não ser vítima de fraude, recomendamos o seguinte:

- Matenha a aplicação de segurança atualizada.
- Efetue pagamentos online apenas com proteção do comprador.
- Utilize uma VPN ao estabelecer ligação com a internet a partir de redes sem fios não protegidas e públicas.
- Preste atenção às palavras-passe que atribuiu às suas contas online. Têm de ser fortes e incluir letras maiúsculas e minúsculas, números e símbolos (@, !, %, #, etc.).
- Certifique-se de que as informações são enviadas por ligações seguras. A extensão do site Web online tem de ser HTTPS:// e não HTTP://.

Quando devo utilizar o Bitdefender VPN?

Tem de ter cuidado quando aceder, transferir ou enviar conteúdos na internet. Para garantir que fica em segurança enquanto navega na Web, recomendamos que utilize o Bitdefender VPN quando:

- quiser ligar-se a redes sem fios públicas
- quiser aceder a conteúdos que normalmente são restritos em áreas específicas, não importa se estiver em casa ou fora
- quiser manter os seus dados pessoais privados (nomes de utilizador, palavras-passe, informações de cartão de crédito, etc.)
- desejar esconder o seu endereço IP

O Bitdefender VPN terá um impacto negativo na bateria do meu dispositivo?

O Bitdefender VPN foi concebido para proteger os seus dados pessoais, esconder o seu endereço IP enquanto estiver ligado a redes sem fios não

seguras e aceder a conteúdo restrito em certos países. Para evitar um consumo desnecessário de bateria do seu dispositivo, recomendamos que use o VPN apenas quando precisar, e que o desconecte quando estiver offline.

Por que estou a deparar-me com lentidão na Internet enquanto uso o Bitdefender VPN?

O Bitdefender VPN foi concebido para suavizar a sua experiência enquanto navega na Internet. No entanto, a lentidão pode ser causada pela sua conectividade com a internet ou pela distância do servidor ao qual está ligado. Nesse caso, se não for uma necessidade ligar a um servidor distante com respeito à sua localização (por exemplo, dos EUA ou China), recomendamos que permita ao Bitdefender VPN ligá-lo automaticamente ao servidor mais próximo, ou encontrar um servidor próximo da sua localização atual.

Posso alterar a conta da Bitdefender ligada ao meu dispositivo?

Sim, pode alterar facilmente a conta Bitdefender associada ao seu dispositivo seguindo estes passos:

1. Tocar **Mais** na barra de navegação inferior.
2. Toque no seu endereço de e-mail.
3. Toque em **Terminar sessão na sua conta**. Se tiver sido definido um código PIN, será solicitado a inseri-lo.
4. Confirme sua escolha.
5. Escreva o endereço de e-mail e a palavra-passe da sua conta nos campos correspondentes e, em seguida, toque em **ENTRAR**.

Como o Bitdefender Mobile Security influencia o desempenho e a bateria do meu aparelho?

O impacto é muito baixo. A aplicação só é executada quando é fundamental — inclusive durante a instalação e quando navega pela interface da aplicação — ou quando pretende realizar uma verificação de segurança. O Bitdefender Mobile Security não funciona em plano de fundo quando liga para amigos, envia mensagens ou joga.

O que é o Administrador de Dispositivos?

O Administrador de Dispositivos é um recurso do Android que dá ao Bitdefender Mobile Security as permissões necessárias para executar

certas tarefas remotamente. Sem estes privilégios, o bloqueio remoto não funcionaria e a limpeza do dispositivo não seria capaz de remover completamente os seus dados. Se quiser remover aplicação, certifique-se de revogar estes privilégios antes de tentar desinstalar em **Configurações > Segurança > Selecionar administradores dos dispositivos**.

Como resolver o erro "Sem token Google" que aparece quando inicia a sessão no Bitdefender Mobile Security.

Este erro ocorre quando o dispositivo não está associado a uma conta Google, ou está associado, mas um problema temporário está a evitar que se ligue ao Google. Tente uma das seguintes soluções:

- Vá às Definições do Android > Aplicações > Gerir aplicações > Bitdefender Mobile Security e toque em **Apagar dados**. Depois tente entrar novamente.
- Certifique-se de que o seu dispositivo está associado a uma conta Google.
  Para verificar isso, vá a Definições > Contas e sincronização e veja se uma conta do Google aparece listada em **Gerir contas**. Adicione a sua conta se uma não estiver listada, reinicie o seu dispositivo e depois tente entrar no Bitdefender Mobile Security.
- Reinicie o seu dispositivo e, em seguida, tente iniciar sessão novamente.

Em quais idiomas o Bitdefender Mobile Security está disponível?

O Bitdefender Mobile Security está atualmente disponível nos seguintes idiomas:

- Brasileiro
- Checo
- Holandês
- Inglês
- Francês
- German
- Grego
- Húngaro
- Italiano

- Japonês
- Coreano
- Polaco
- Português
- Romanian
- Russo
- Spanish
- Sueco
- Tailandês
- Turco
- Vietnamita

Outros idiomas serão acrescentadas em futuros lançamentos. Para alterar o idioma da interface do Bitdefender Mobile Security, vá a Definições **Idiomas e teclado**, no seu dispositivo e defina o idioma que pretende utilizar no dispositivo.

6. SEGURANÇA MÓVEL PARA IOS

6.1. O que é o Bitdefender Mobile Security para iOS

Atividades online, como pagar contas, fazer reservas para as férias ou comprar bens e serviços são convenientes e práticas. Mas, como muitas atividades realizadas na Internet, fazem-se acompanhar de elevados riscos e, se os detalhes de segurança forem ignorados, os dados pessoais podem ser hackeados. E o que é mais importante do que proteger os dados armazenados em contas online e no seu smartphone?

O Bitdefender Mobile Security para iOS permite que:

- Oferece a proteção mais poderosa contra as ameaças com o menor impacto sobre a bateria do dispositivo
- Proteja os seus dados pessoais: palavras-passe, endereço, informações sociais e financeiras
- Verifique facilmente a segurança do seu telemóvel para detetar e corrigir configurações erradas que a possam expor
- Evite a exposição acidental de dados e a utilização indevida para todas as aplicações instaladas
- Analise o seu dispositivo para obter definições de segurança e privacidade ideais
- Obtenha informações de utilização da sua atividade online e o histórico de incidentes prevenidos
- Verifique as suas contas online contra violações de dados ou fugas de dados
- Encripte o tráfego da internet com o VPN incluído

Bitdefender Mobile Security para iOS é entregue gratuitamente e requer ativação com uma conta **Bitdefender**. Contudo, algumas funcionalidades importantes da Bitdefender, tais como o nosso módulo "Proteção da Internet", requerem uma subscrição paga para que seja acessível aos nossos utilizadores.

6.2. Introdução

6.2.1. Requisitos do Aparelho

O Bitdefender Mobile Security para iOS funciona em qualquer dispositivo a executar o iOS 12 ou versões posteriores do sistema operativo e necessita de uma ligação ativa à Internet para ser ativado e para detetar se ocorreu alguma fuga de dados nas suas contas online.

6.2.2. Instalar o Bitdefender Mobile Security para iOS

- **Na Central Bitdefender**
  - Em iOS
    1. Aceda à **Central da Bitdefender**.
    2. Selecione o painel **Os Meus Dispositivos**.
    3. Toque em **INSTALAR PROTEÇÃO** e, em seguida, toque em **Proteger este dispositivo**.
    4. Selecione o dono do dispositivo. Se o dispositivo pertencer a outra pessoa, pressione o respetivo botão.
    5. Foi redirecionado para a aplicação da **App Store**. No ecrã da App Store, toque na opção de instalação.
  - No Windows, macOS e Android
    1. Acesso Bitdefender Central.
    2. Selecione os **Meus dispositivos** painel.
    3. Prima **INSTALAR PROTEÇÃO** e, em seguida, prima **Proteger outros dispositivos**.
    4. Selecione o dono do dispositivo. Se o dispositivo pertencer a outra pessoa, pressione o respetivo botão.
    5. Prima **ENVIAR LIGAÇÃO DE TRANSFERÊNCIA**.
    6. Escreva um endereço de e-mail no campo correspondente e pressione **ENVIAR E-MAIL**. Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

7. No dispositivo em que deseja instalar o Bitdefender verifique a conta de e-mail que escreveu e pressione o botão de download correspondente.

- **Da App Store**
  Procure o Bitdefender Mobile Security para iOS e instale a aplicação.

É exibida uma janela introdutória com detalhes sobre as funções do produto na primeira vez que abrir a aplicação. Pressione Começar para avançar para o próximo passo.

Antes de passar pelos passos de validação, deve concordar com o Acordo de Subscrição. Leia o acordo de Subscrição com calma, já que ele contém os termos e condições segundo os quais pode utilizar o Bitdefender Mobile Security for iOS.

Toque em **Continuar** para avançar para a janela seguinte.

6.2.3. Entre na sua conta Bitdefender

Para utilizar o Bitdefender Mobile Security for iOS, deve associar o seu dispositivo a uma conta Bitdefender do Facebook, Google, Apple ou Microsoft iniciando sessão na conta a partir da aplicação. A primeira vez que abrir a aplicação, será pedido que inicie sessão numa conta.

Para vincular o seu dispositivo a uma conta Bitdefender:

1. Introduza o seu endereço de e-mail da sua conta da Bitdefender no respetivo campo e clique em **PRÓXIMO**. Se não tem uma conta da Bitdefender e pretende criar uma, selecione a respetiva hiperligação e depois siga as instruções no ecrã até a conta ser ativada.
   Para entrar usando uma conta do Facebook, Google, Apple ou Microsoft, pressione o serviço que deseja usar na área **Ou entrar com**. Será redirecionado para a página de login do serviço selecionado. Siga as instruções para vincular a sua conta ao Bitdefender Mobile Security for iOS.

   > **Observação**
   > O Bitdefender não obtém acesso a qualquer informação confidencial como a palavra-passe da conta que usa para iniciar sessão ou a informação particular dos seus amigos ou contactos.

2. Introduza a sua palavra-passe e depois toque em **ENTRAR**.

A partir daqui pode também aceder à Política de Privacidade da Bitdefender.

6.2.4. Painel de instrumentos

Toque no ícone do Bitdefender Mobile Security for iOS nas aplicações do seu dispositivo para abrir a interface da aplicação.

Na primeira vez que abrir a aplicação, será solicitado a permitir ao Bitdefender o envio de notificações. Prima **Permitir** para permanecer informado sempre que o Bitdefender tiver de comunicar algo relevante para a sua aplicação. Para gerir as notificações do Bitdefender, aceda a Definições > Notificações > Segurança móvel.

Para ter acesso à secção de que necessita, toque no ícone correspondente a partir da parte inferior do ecrã.

Proteção da Internet

Fique seguro(a) enquanto navega na Internet e quando aplicações menos seguras tentarem aceder a domínios não fiáveis. Para obter mais informações, aceda a Proteção da Internet (página 229).

VPN

Mantenha a sua privacidade independentemente da rede à qual estiver ligado(a) para manter a sua comunicação pela Internet encriptada. Para mais informações, aceda a VPN (página 231).

Privacidade de Conta

Saiba se as suas contas de e-mail foram invadidas ou não. Para mais informação, dirija-se a Privacidade da conta (página 234).

Para ver mais opções, toque no ícone ••• no dispositivo enquanto estiver no ecrã inicial da aplicação. São apresentadas as seguintes opções:

- **Restaurar compras** - aqui pode restaurar as antigas subscrições que comprou através da conta do iTunes.
- **Definições** - aqui tem acesso a:
  - **Definições de VPN**
    - **Contrato** - pode ler os termos de utilização do serviço VPN de Bitdefender. Caso selecione **Já não concordo**, não poderá utiliza a VPN de Bitdefender até carregar em **Concordo**.

- **Abrir aviso de Wi-Fi** - pode ativar ou desativar a notificação do produto que é apresentada sempre que estabelecer ligação a uma rede Wi-Fi não segura.
  O objetivo desta notificação é ajudá-lo a manter os seus dados privados e seguros utilizando a VPN de Bitdefender.

- **Definições de proteção da Internet**
  - **Contrato** - pode ler os termos de utilização da Proteção Bitdefender na Web. Caso selecione **Já não concordo**, não poderá utiliza a VPN de Bitdefender até carregar em **Concordo**.
  - **Ativar notificações da Proteção na Web** - Será notificado(a) para lembrar que a Proteção na Web pode ser ativada após o fim de uma sessão VPN.

- **Relatórios do produto**

- **Comentários** — aqui pode iniciar o cliente de e-mail predefinido para nos enviar comentários sobre a aplicação.
- **Informações sobre a aplicação** — aqui tem acesso a informações sobre a versão instalada e o Contrato de Subscrição, Política de Privacidade e conformidade com licenças de código aberto.

6.3. Análise

O Bitdefender Mobile Security para iOS permite-lhe verificar no seu dispositivo quaisquer vulnerabilidades de segurança e potenciais ameaças no seu dispositivo. A realização da análise irá verificar a existência de:

- **Versão do SO:** a verificar as atualizações mais recentes da sua versão iOS.
- **Código de acesso/Biometria:** verificar o nível de segurança em relação ao acesso ao seu dispositivo.
- **Proteção da Internet:** verificar o estado do módulo de Proteção da Internet
- **Privacidade da conta:** verificar a presença de contas monitorizadas listadas no módulo Privacidade da conta.

- **Analisar Wi-Fi:** verificar o estado de segurança da rede atualmente ligada.

O estado de proteção é determinado depois de executar uma análise manual.

Depois de executar a primeira análise, verá as **Recomendações do Autopilot** da Bitdefender. Este é o seu conselheiro de segurança pessoal, que lhe fornece recomendações contextuais com base na utilização e necessidades do seu dispositivo. Desta forma, poderá beneficiar de tudo o que a sua aplicação tem para oferecer.

> **Observação**
> Ao entrar na aplicação pela primeira vez, ser-lhe-á pedido que realize uma análise.

6.4. Alerta de fraude

O recurso Alerta de Golpe disponível no Bitdefender Mobile Security para iOS protege proativamente os usuários da Apple contra golpes de phishing. O Scam Alert para iOS inclui duas camadas de proteção que monitoram golpes entregues por meio de mensagens SMS/MMS e convites de calendário:

- **Filtro de mensagens de texto (SMS, MMS)**
  Este recurso identifica e filtra mensagens SMS e MMS indesejadas.
  Um SMS/MMS (serviço de mensagens curtas/serviço de mensagens multimídia) malicioso refere-se a um tipo de mensagem enviada a dispositivos móveis com intenções prejudiciais. Essas mensagens são projetadas para explorar vulnerabilidades, enganar destinatários ou causar danos ao dispositivo, às informações pessoais ou à segurança do alvo.
- **Scanner de link de convite de calendário**
  Este recurso detecta calendários de spam e eventos que contêm links perigosos. O vírus de calendário é um tipo de spam que afeta o aplicativo Calendário do seu iPhone, o que pode ser irritante e potencialmente perigoso:
  - Você recebe convites de calendário ou notificações de eventos indesejados quando aceita acidentalmente um convite de calendário falso enviado para seu endereço de e-mail por hackers ou spammers.

- Ao clicar no link do convite, você inadvertidamente se inscreve no calendário do remetente, o que permite que ele envie mais eventos de spam.
- Os eventos de spam podem conter links ou anexos que podem levar você a páginas de phishing ou outras ameaças cibernéticas, caso você os abra.

6.4.1. Como configurar o Alerta de Golpe

Para ativar o Alerta de Fraude, você precisa conceder ao aplicativo Bitdefender Mobile Security acesso a notificações de calendário e mensagens SMS:

Como ativar a filtragem de SMS:

Para que o Bitdefender comece a filtrar mensagens, você deve ativar manualmente a opção Filtrar Remetentes Desconhecidos nas configurações do aplicativo Mensagens:

1. Abra o **Configurações** aplicativo no seu iPhone ou iPad.
2. Role para baixo e selecione **Mensagens** na lista.
3. Toque em **Desconhecido e spam** seção.
4. Alternar **Filtrar remetentes desconhecidos** para a posição ligado.
5. Selecione **Segurança para celulares** na seção Filtragem de SMS e escolha **Habilitar**.

O Bitdefender agora será capaz de filtrar mensagens indesejadas no seu iPhone/iPad.

> **Observação**
> Devido às restrições do iOS, a filtragem de SMS do Bitdefender só pode ser usada para mensagens SMS e MMS provenientes de pessoas que você não salvou em seus contatos. Isso significa que ele não filtrará mensagens de pessoas que já estão na sua lista de contatos ou mensagens do iMessage de ninguém.

Como ativar a verificação de calendário:

1. Abra o **Segurança Móvel Bitdefender** aplicativo instalado no seu iPhone ou iPad.

2. Vou ao **Alerta de fraude** opção na barra de navegação inferior e pressione **Configurar agora**.
3. Tocar **Continuar** e toque em **Habilitar**.
4. Escolher **OK** para conceder ao Bitdefender acesso ao seu calendário. Uma verificação do calendário começará imediatamente.

6.5. Proteção da Internet

A Proteção da Web do Bitdefender garante uma experiência de navegação segura alertando-o sobre páginas da Internet maliciosas e quando aplicações instaladas menos seguras tentam aceder a domínios não fiáveis.

Quando um URL sinalizar uma página da Internet conhecida como phishing ou fraudulenta, ou como tendo conteúdo malicioso como spyware ou vírus, a página da Internet é bloqueada e é exibido um alerta. Acontece a mesma coisa quando aplicações instaladas tentam aceder a domínios maliciosos.

> **Importante**
> Se está numa área onde a utilização de um serviço VPN é limitado por lei, a função de Proteção na Internet não estará disponível.

Para ativar a Proteção na Internet:

1. Toque no ícone na parte inferior do ecrã.
2. Toque em **Concordo**.
3. Ativar a chave de Proteção na Internet.

> **Observação**
> A primeira vez que ligar a Proteção na Internet, deverá permitir ao Bitdefender definir as configuração de VPN que irão monitorizar o tráfego de rede. Pressione **Permitir** para continuar. Se tiver sido configurado um método de autenticação (leitura de impressão digital ou código PIN) para proteger o seu smartphone, será solicitado que o utilize. Para poder detetar o acesso a domínios não fiáveis, a Proteção na Internet trabalha em conjunto com os serviços VPN.

Importante

A funcionalidade de Proteção na Web e o VPN não podem funcionar ao mesmo tempo. Sempre que um deles for ativado, o outro (caso esteja ativo nessa altura) será desativado.

6.5.1. Alertas Bitdefender

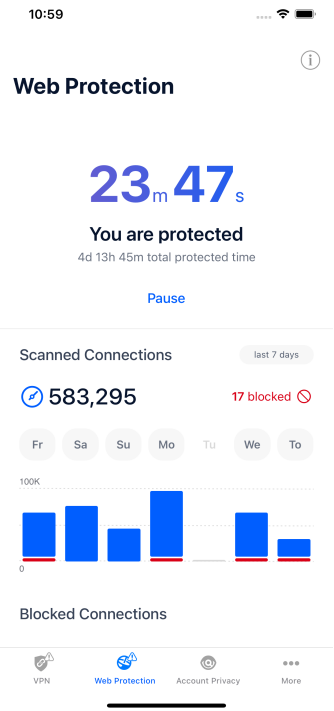
Sempre que tentar visitar um site classificado como não seguro, será bloqueado. Para avisá-lo sobre o evento, será notificado pelo Bitdefender no centro de Notificações e no seu navegador. A página de alertas contém informações como o URL do site e a ameaça detetada. Tem de decidir o que fazer a seguir.

Além disso, receberá notificações no Centro de Notificações quando uma aplicação menos segura tentar aceder a domínios não fiáveis. Clique na notificação exibida para ser redirecionado(a) para a janela onde poderá decidir o que fazer a seguir.

As seguintes opções estão disponíveis para os dois casos:

- Sair do site tocando em **VOLTAR À SEGURANÇA**.
- Ir para o site apesar do aviso tocando na notificação mostrada e, em seguida, em **Quero aceder à página**.

Confirme a sua escolha.



6.6. VPN

Com o Bitdefender VPN , pode manter os seus dados privados sempre que se ligar a redes sem fios não seguras em aeroportos, shoppings, cafés ou hotéis. Assim, poderá evitar situações inoportunas, como roubo de dados pessoais ou tentativas de tornar o endereço de IP do seu dispositivo acessível a hackers.

A VPN funciona como um túnel entre o seu dispositivo e a rede à qual está ligado, protegendo a sua ligação, encriptando os seus dados com encriptação de nível militar e ocultando o seu endereço IP onde quer que esteja. O seu tráfego é redirecionado através de um servidor separado, fazendo com que o seu dispositivo seja impossível de identificar pelo seu ISP, entre os incontáveis dispositivos que utilizam os nossos serviços. Além disso, enquanto estiver ligado à internet através do Bitdefender Total Security, poderá aceder a conteúdos que normalmente são restritos em áreas específicas.

> **Observação**
> Alguns países censuram a Internet e, portanto, a utilização de VPN nos seus territórios foi banido por lei. Para evitar consequências legais, pode ser apresentada uma mensagem de aviso ao tentar utilizar a aplicação Bitdefender VPN pela primeira vez. Ao continuar a utilizar a aplicação, confirma que está ciente dos regulamentos aplicáveis e dos riscos aos quais pode estar exposto.

Para ativar o Bitdefender VPN:

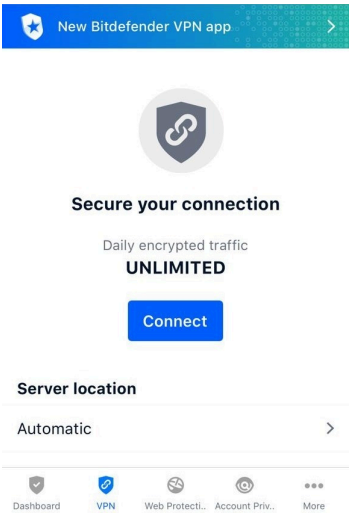
1. Toque em ícone na parte inferior da tela.
2. Pressione **Ligarr** sempre que quiser permanecer protegido enquanto estiver ligado às redes sem fios não seguras.
   Pressione **Desconectar** quando desejar desativar a ligação.

> **Observação**
> Na primeira vez que ligar o VPN, será solicitado a permitir que o Bitdefender faça configurações de VPN que monitorizarão o tráfego de rede. Prima **Permitir** para continuar. Se tiver sido configurado um método de autenticação (leitura de digital ou código PIN) para proteger o seu smartphone, será solicitado que o utilize.

O ícone do VPN aparece na barra de estado quando a VPN está ativa.

Para economizar bateria, recomendamos que desligue a VPN quando não precisar de usá-la.

Se tiver uma subscrição Premium e quiser ligar-se a um servidor da sua escolha, pressione Automático na interface de VPN e, em seguida, selecione o local desejado. Para detalhes sobre as subscrições de VPN, aceda a Subscrições (página 233).



6.6.1. Subscrições

O Bitdefender VPN oferece gratuitamente 200 MB de franquia por dispositivo para proteger a sua ligação sempre que precisar e liga-o automaticamente ao melhor local de servidor.

Para obter tráfego ilimitado e acesso irrestrito a conteúdos no mundo inteiro escolhendo um local da sua preferência, atualize para a versão Premium.

Pode atualizar a versão do Bitdefender VPN Premium a qualquer momento tocando no botão **Ativar VPN Premium** disponível na janela do VPN. Existem dois tipos de subscrição disponíveis: anual e mensal.

A subscrição Bitdefender Premium VPN é independente da subscrição grátis do Bitdefender Mobile Security for iOS, ou seja, poderá usá-lo por todo o seu período de disponibilidade. Caso a subscrição Bitdefender Premium VPN expire, voltará automaticamente para o plano gratuito.

O Bitdefender VPN é um produto multiplataforma, disponível nos produtos Bitdefender compatíveis com Windows, macOS, Android e iOS. Ao atualizar para o plano premium, pode utilizar a sua subscrição em todos os produtos, desde que inicie sessão com a mesma conta da Bitdefender.

> **Observação**
> O Bitdefender VPN também funciona como uma aplicação autónoma em todos os sistemas operativos suportados, incluindo Windows, macOS, Android e iOS.

6.7. Privacidade da conta

A Privacidade de Conta do Bitdefender deteta se ocorreu qualquer fuga de dados nas contas que utiliza para fazer pagamentos, compras ou subscrições online em diferentes aplicações e websites. Os dados armazenados numa conta podem ser palavras-passe, informações de cartão de crédito ou informações de conta bancária e, se não forem devidamente protegidos, pode sofrer roubo de identidade ou invasão de privacidade.

O estado de privacidade de uma conta é apresentado depois da validação.

Para verificar se qualquer conta foi invadida, toque em **Procurar fugas**.

Para começar a proteger informações pessoais:

1. Toque em ícone na parte inferior da tela.
2. Toque em **Adicionar conta**.
3. Digite o seu endereço de e-mail no campo correspondente e toque em **Seguinte**.
   Bitdefender necessita de validar esta conta antes de apresentar informações privadas. Portanto, é enviado um e-mail com um código de validação para o endereço de e-mail fornecido.
4. Verifique a caixa de entrada e digite o código recebido na área **Privacidade de Conta** da aplicação. Se não conseguir encontrar o e-mail de validação na pasta Caixa de Entrada, verifique a pasta Spam.
   O estado de privacidade da conta validada é apresentado.

Se forem detetadas fugas nas suas contas, recomendamos que altere as palavras-passe assim que possível. Para criar uma palavra-passe forte e segura, tenha em mente estas dicas:

- Oito carateres no mínimo.
- Carateres maiúsculos e minúsculos.
- Pelo menos um número ou símbolo, como #, @, % ou !.

Ao proteger uma conta que constava de uma violação de privacidade, pode confirmar as alterações ao marcar a(s) fuga(s) identificada(s) como **Resolvido**. Para tal:

1. Toque em ··· ao lado da infração que resolveu.
2. Toque em **Marcar como resolvido**.

Quando todas as fugas detetadas estiverem marcadas como Resolvido, a conta já não aparece como fuga, pelo menos até à deteção de uma nova fuga.

6.8. Perguntas frequentes

Como é que o Bitdefender Mobile Security for iOS me protege contra vírus, malware e ciberameaças?

O Bitdefender Mobile Security for iOS fornece proteção absoluta contra todas as ciberameaças e está especialmente concebido para manter os seus dados sensíveis protegidos contra olhares curiosos.

Obtém uma ampla variedade de funcionalidades de segurança e privacidade para o seu iPhone e iPad - além de muitas funcionalidades de bónus, incluindo o VPN e a Proteção na Web.

O Bitdefender Mobile Security for iOS reage instantaneamente ao vírus e malware sem comprometer o desempenho do seu sistema.

Que tipo de dispositivos e sistemas operativos são abrangidos pelo Bitdefender Mobile Security for iOS?

O Bitdefender Mobile Security for iOS protegerá os seus smartphones e tablets com iOS contra todas as ciberameaças.

Por que é que eu preciso do Bitdefender Mobile Security for iOS no sistema operativo da Apple?

Alguns dos seus dados mais pessoais estão armazenados no seu iPhone ou iPad - e precisa de saber se eles estão seguros a qualquer momento. O Bitdefender Mobile Security for iOS oferece proteção absoluta e informações privadas sem interferência nas suas atividades diárias.

Recebo uma VPN juntamente com a minha subscrição do Bitdefender Mobile Security for iOS?

O Bitdefender Mobile Security para iOS inclui uma versão básica do Bitdefender VPN que inclui uma quantidade generosa de tráfego (200 MB/dia, um total de 6 GB/mês) gratuitamente.

7. VPN

7.1. O que é Bitdefender Total Security

A VPN serve como um túnel entre o seu dispositivo e a rede à qual você se conecta para proteger sua conexão, criptografando os dados usando criptografia de nível militar e ocultando seu endereço IP onde quer que você esteja. Seu tráfego é redirecionado através de um servidor separado; impossibilitando assim a identificação do seu dispositivo pelo seu ISP, através da infinidade de outros dispositivos que utilizam os nossos serviços. Além disso, enquanto estiver conectado à Internet através do Bitdefender VPN, você poderá acessar conteúdo que normalmente é restrito em áreas específicas.

> **Observação**
> Alguns países censuram a Internet e, portanto, a utilização de VPN nos seus territórios foi banido por lei. Para evitar consequências legais, pode ser apresentada uma mensagem de aviso ao tentar utilizar a funcionalidade Bitdefender Total Security pela primeira vez. Ao continuar a utilizar a funcionalidade, confirma que está ciente dos regulamentos aplicáveis e dos riscos aos quais pode estar exposto.

7.1.1. Protocolos de encriptação

O conjunto de encriptação predefinido ativado no cliente e servidor Hydra é fornecido abaixo. Todos os outros conjuntos de encriptação estão desativados.

Conjunto de encriptação de cliente Hydra:

- ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA:DES-CBC3-SHA

Observação

A configuração da parte do servidor é muito mais restritiva e tanto o cliente como o servidor Hydra rejeitarão um modo diferente do GCM que utiliza AES. O servidor Hydra reforça a prioridade do lado do servidor de conjuntos de encriptação mais fortes e rejeitará o handshake TLS se um conjunto mais fraco for solicitado por parte de um cliente. Esta lista também é configurável no tempo de execução do servidor.

7.2. Subscrições de VPN

Com o Bitdefender Total Security, pode escolher dois tipos de subscrições:

- A subscrição Básica
- A subscrição Premium

7.2.1. Subscrição Básica

O Bitdefender Total Security oferece gratuitamente uma quota de 200 MB de tráfego diário por dispositivo para proteger a sua ligação sempre que precisar e permite-lhe estabelecer ligação com uma única localização, que não pode ser alterada.

A subscrição Básica está disponível para qualquer utilizador que transferir o Bitdefender Total Security.

7.2.2. Subscrição Premium

Para obter acesso ilimitado a todas as funcionalidades incluídas no Bitdefender Total Security, faça a atualização para a versão Premium. Os utilizadores com uma subscrição ativa da VPN Premium têm tráfego ilimitado protegido, podendo estabelecer ligação com qualquer um dos nossos servidores em todo o mundo.

Existem dois planos disponíveis para a subscrição Premium: o Plano Mensal e o Plano Anual.

- Plano Mensal: com este plano, os serviços VPN Premium ser-lhe-ão cobrados todos os meses. Pode cancelar este plano quando quiser.
- Plano Anual: requer um pagamento único, garantindo o acesso aos nossos serviços VPN Premium durante um ano inteiro.

7.2.3. Como atualizar para a VPN Premium

A forma mais fácil de atualizar para a versão Premium do Bitdefender Total Security é clicar no botão **Atualizar** situado na parte inferior da interface principal. Selecione o modelo de subscrição desejado e, em seguida, siga as instruções no ecrã.

Se já tem um código de ativação, siga as instruções abaixo:

- **Para os utilizadores de Windows:**
  1. Clique no ícone A Minha Conta no lado esquerdo da interface da VPN.
  2. Clique em **Adicione-o aqui**.
  3. Introduza o código recebido por e-mail e, depois, clique no botão **Ativar código**.

- **Para utilizadores de macOS**
  1. Clique no símbolo da roda dentada no canto superior direito da interface da VPN e selecione **A Minha Conta**.
  2. Clique **Adicione aqui**.
  3. Digite o código recebido por e-mail e clique no botão **Código de Ativação** botão.

- **Para utilizadores de Android**
  1. Toque no símbolo da roda dentada no canto superior direito da interface da VPN e selecione **A Minha Conta**.
  2. Toque em **Adicionar código**.
  3. Digite o código recebido por e-mail e clique no botão **Código de Ativação** botão.

- **Para utilizadores de iOS**
  1. Toque na roda dentada no canto superior direito da interface VPN e selecione **Minha conta**.
  2. Tocar **Adicionar código**.
  3. Digite o código recebido por e-mail e clique no botão **Código de Ativação** botão.

7.3. Instalação

7.3.1. A preparar a instalação

Antes de instalar o Bitdefender Total Security, complete estes procedimentos para assegurar uma boa instalação:

- Assegure-se que o dispositivo onde deseja instalar o Bitdefender tem os requisitos de sistema mínimos. Caso o dispositivo não cumpra os requisitos de sistema, o Bitdefender não será instalado ou caso seja instalado, não irá trabalhar de forma apropriada e irá causar lentidão e instabilidade do sistema.
  Para a lista completa dos requisitos mínimos dos sistema, consulte o Requisitos do sistema (página 240)
- Ligue-se ao dispositivo utilizando uma conta de Administrador.
- Recomenda-se que o seu dispositivo esteja ligado à Internet durante a instalação, mesmo quando realizar a instalação a partir de um CD/DVD. Se estiverem disponíveis versões mais recentes dos ficheiros da aplicação incluidos no pacote de instalação, o Bitdefender irá descarregá-las e instalá-las.

7.3.2. Requisitos do sistema

- **Para usuários do Windows**
  - **Sistema operativo:** Windows 7 com Service Pack 1, Windows 8, Windows 8.1 Windows 10 e Windows 11
  - **Memória (RAM):** 1 GB
  - **Espaço de disco rígido disponivel:** 500 MB de espaço livre
  - **Net Framework:** versão mín 4.5.2

    Importante
    O desempenho do sistema pode ser afetado em dispositivos com CPUs de geração antiga.

- **Para usuários macOS**
  - **Sistema operativo:** macOS Sierra (10.12) ou superior
  - **Espaço de disco rígido disponivel:** 100 MB de espaço livre

- **Para usuários do Android**
  - **Sistema operativo:** Android 5.0 ou superior
  - **Armazenamento:** 100MB
  - Uma ligação à Internet ativa
- **Para usuários de iOS**
  - **Sistema operativo:** iOS 12 ou superior
  - **Armazenamento no Iphone:** 50MB
  - **Armazenamento no iPad:** 100MB
  - Uma conexão ativa com a Internet

7.3.3. A instalar o Bitdefender Total Security

Para iniciar a instalação, siga as instruções correspondentes ao sistema operativo que utiliza:

- **Para usuários do Windows**
  1. Para iniciar a instalação do Bitdefender Total Security no PC Windows, inicie simplesmente ao transferir o kit de instalação do https://www.bitdefender.com/solutions/vpn/download ou a partir do e-mail recebido após a compra.
  2. Faça duplo clique no instalador transferido para o executar.
  3. Escolha Sim caso seja apresentada uma caixa de diálogo do Controlo de Conta de Utilizador.
  4. Aguarde até que a transferência seja concluída.
  5. Selecione o idioma do produto utilizando o menu suspenso no instalador.
  6. Marque a caixa "Eu confirmo que li e concordo com o Acordo de Subscrição e a Política de Privacidade" e, em seguida, clique em **INICIAR INSTALAÇÃO**.
  7. Espere que a instalação termine.
  8. **INICIE A SESSÃO** com a sua conta da Central Bitdefender. Se não tiver uma conta da Central, registe uma ao clicar no botão **CRIAR UMA CONTA**.

9. Selecione **Eu tenho um Código de Ativação** se comprou a subscrição do Premium VPN.
   Caso contrário, pode escolher **INICIAR VERSÃO DE TESTE** para experimentar o produto gratuitamente durante 7 dias antes de se comprometer a pagar por ele.
10. Introduza o código recebido por e-mail e, em seguida, clique no botão **ATIVAR PREMIUM**.
11. Após uma pequena espera, Bitdefender Total Security é instalado e fica pronto para ser utilizado no computador.

❍ **Para usuários macOS**

1. Para iniciar a instalação do Bitdefender Total Security no macOS, inicie simplesmente ao transferir o kit de instalação do https://www.bitdefender.com/solutions/vpn/download ou a partir do e-mail recebido após a compra.
2. O instalador será guardado no Mac. Na pasta Transferências, clique duas vezes no ficheiro do pacote .
3. Siga as instruções no ecrã. Selecione **Continuar**.
4. Será guiado através dos passos necessários para instalar Bitdefender Total Security no seu Mac. Clique duas vezes no botão **Continuar**.
5. Clique em **Eu concordo**, depois de ler e concordar com os termos do acordo de licença do software.
6. Clique em **Instalar**.
7. Introduza um nome de utilizador e palavra-passe de administrador e, em seguida, clique em **Instalar software**.
8. Receberá a notificação de que uma extensão assinada pela Bitdefender foi bloqueada. Isto não é um erro, apenas uma verificação de segurança. Clique em **Abri Preferências de segurança**.
9. Clique no ícone de bloqueio para o desbloquear.
   Introduza um nome e palavra-passe de administrador e, em seguida, prima **Desbloquear**.

10. Clique em **Permitir** para carregar a extensão do sistema BitdefenderBitdefender. Em seguida, feche a janela de Segurança e Privacidade e o instalador.
11. Aceda ao ícone do escudo na barra de menu e, em seguida, **Entre** na sua conta da Central Bitdefender. Se ainda não tiver uma conta da Central, crie uma.
12. Selecione Eu tenho um **Código de ativação** caso tenha adquirido a subscrição do VPN Premium.
    Caso contrário, você pode escolher **INICIAR TESTE** para testar o produto gratuitamente por 7 dias antes de se comprometer a pagar por ele.
13. Digite o código recebido por e-mail e clique no botão **Código de Ativação** botão.
14. Após uma pequena espera, Bitdefender Total Security será instalado e ficará pronto a utilizar no seu Mac.

❍ **Para usuários do Android**

1. Para instalar o Bitdefender Total Security no Android, abra primeiro a aplicação do **Google Play Store** no seu smartphone ou tablet.
2. Pesquise por Bitdefender Total Security e selecione esta aplicação.
3. Clique no botão **Instalar** e aguarde que a transferência termine.
4. Toque em **Abrir** para executar a aplicação.
5. Marque a caixa "Eu concordo com o Acordo de Subscrição e a Política de Privacidade" e, em seguida, toque em **Continuar**.
6. **Inicie a Sessão** com a sua conta da Central Bitdefender. Se não tiver uma conta da Central, registe uma ao tocar em **Criar uma Conta**.
7. Selecione **Eu tenho um código de ativação** caso tenha comprado uma subscrição Premium VPN.
   Caso contrário, pode escolher Iniciar uma versão de teste de 7 dias para experimentar o produto gratuitamente durante 7 dias antes de se comprometer a pagar por ele.
8. Introduza o código recebido por e-mail e, depois, clique em **Ativar código**.

- **Para usuários de iOS**

  1. Para instalar o Bitdefender Total Security no iOS, primeiro abra a **App Store** no seu iPhone ou iPad.
  2. Procurar Bitdefender Total Security e selecione este aplicativo.
  3. Toque no ícone **Obter** e aguarde até que a transferência termine.
  4. Tocar **Abrir** para executar o aplicativo.
  5. Marque a caixa **Eu concordo com o Acordo de Subscrição e a Política de Privacidade** e, em seguida, toque em **Continuar**.
  6. **Inicie a Sessão** com a sua conta da Central Bitdefender. Se não tiver uma conta, registe uma ao tocar em **Criar uma Conta**.
  7. Toque em **Permitir** se desejar receber notificações do Bitdefender Total Security.
  8. Escolher **Eu tenho um código de ativação** se você comprou uma assinatura VPN Premium.
     Caso contrário, você pode escolher Iniciar 7 dias de teste para testar o produto gratuitamente por 7 dias antes de se comprometer a pagar por ele.
  9. Digite o código recebido por e-mail e toque em **Código de Ativação**.

7.4. Utilizar o Bitdefender VPN

7.4.1. A abrir o Bitdefender VPN

- **Para Windows**
  Para aceder a **interface principal do Bitdefender VPN**, utilize um dos seguintes métodos:

  - **A partir da bandeja do sistema**
    Clique com o botão direito no ícone do escudo vermelho e depois selecione **Mostrar** no menu.

  - **Da interface doBitdefender**
    Se um produto de segurança da Bitdefender tal como o Bitdefender Total Security ou o Bitdefender Antivirus Plus etc. já estiver instalado no seu computador Windows, pode abrir o Bitdefender VPN a partir de lá:

1. Clique em **Privacidade** na barra do lado esquerdo da interface do Bitdefender.
2. Clique em **Abrir o VPN** no painel do VPN.

- **A partir do seu ambiente de trabalho**
  Faça duplo-clique no atalho Bitdefender VPN no seu Ambiente de trabalho.

- **Para macOS**

  Pode abrir a aplicação do Bitdefender VPN ao clicar no ícone da barra de menu no lado superior direito do ecrã.
  Se o escudo do Bitdefender não puder ser encontrado na barra de menu, utilize o Launchpad ou o Finder do Mac para recuperá-lo:

  - **A partir do Launchpad**

    1. Prima **F4** no seu teclado para introduzir o Launchpad no seu Mac.
    2. Navegue pelas páginas das aplicações instaladas até localizar a aplicação do Bitdefender VPN. Como alternativa, pode introduzir **Bitdefender VPN** no Launchpad para começar a filtrar os seus resultados.
    3. Assim que visualizar a aplicação Bitdefender VPN, clique no ícone para fixá-lo na barra de menu.

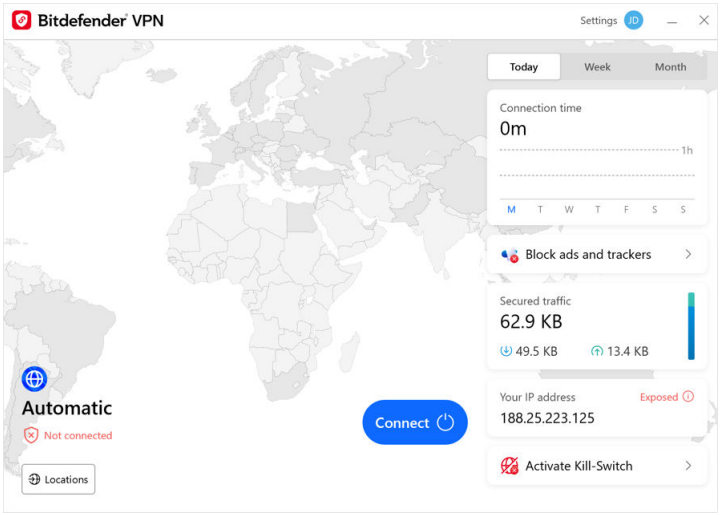
  - **A partir do Finder**

    1. Clique no **Finder** na parte inferior esquerda do Dock (Finder é o ícone que se parece com um quadrado azul com um rosto sorridente).
    2. Em seguida, clique em **Ir** no canto superior esquerdo do ecrã, na barra de menus.
    3. Selecione **Aplicações** a partir do menu para entrar na pasta das Aplicações no seu Mac.
    4. Na pasta de Aplicações, abra a pasta **Bitdefender** e clique duas vezes na aplicação **Bitdefender VPN**.

> **Observação**
> Para aceder ao Bitdefender VPN nos seus dispositivos móveis Android ou iOS, basta abrir a aplicação Bitdefender VPN depois de instalá-la.

7.4.2. Como ligar o Bitdefender Total Security

A interface VPN exibe o estado da aplicação: ligar ou desligar. A localização do servidor para utilizadores com a versão gratuita é definida automaticamente pelo Bitdefender para o servidor mais apropriado, enquanto os utilizadores premium têm a possibilidade de alterar a localização do servidor que desejam ligar-se ao selecioná-lo na lista de localização virtual. Para ligar ou desligar, basta clicar no botão liga/desliga na interface VPN.



- **Para Windows:** o ícone da bandeja do sistema exibe uma marca de seleção verde quando a VPN está ligado e uma marca preta quando a VPN está desligada. Enquanto ligado a um local selecionado manualmente, o endereço IP é exibido na interface principal.
- **Para macOS:** o ícone da barra de menus fica preto quando a VPN está ligada e branco quando a VPN é desligada. Clique no botão circular no meio da interface e aguarde o estabelecimento da ligação.
- **Para Android e iOS:** Para se ligar ao Bitdefender VPN para Android, iOS e iPadOS:

- **Na aplicação Bitdefender VPN:** Para ligar ou desligar, basta tocar no botão liga/desliga na interface VPN. O estado do Bitdefender VPN é exibido.
- **Na aplicação Bitdefender Mobile Security:**
  1. Aceda o ícone VPN na barra de navegação inferior do Bitdefender Mobile Security.
  2. Toque em **LIGAR** sempre que desejar permanecer protegido enquanto estiver ligado a redes sem fio não seguras. Toque em **DESLIGAR** sempre que desejar desativar a ligação VPN.

7.4.3. Como se ligar a um servidor diferente

Com uma subscrição Premium, Bitdefender Total Security permite-lhe ligar-se a qualquer um dos nossos servidores em todo o mundo, a qualquer momento. Para fazer isto, terá que:

1. Abrir a aplicação Bitdefender Total Security.
2. Toque no botão **Localização virtual** na parte inferior da interface.
3. Selecione o país que desejar.
4. Clique no botão **Ligar a [país]** na parte inferior da interface.

- O ícone da bandeja do sistema exibe uma marca de seleção verde quando a VPN está conectada.
- O endereço IP do servidor virtual é mostrado na tela inicial enquanto estiver conectado ao Bitdefender VPN.
- Um resumo do seu tempo de conexão, a quantidade de tráfego seguro e os últimos 5 locais aos quais você se conectou também são mostrados no painel principal.

7.5. Bitdefender Total Security Definições e Características

7.5.1. A aceder às Definições

Para aceder às definições do Bitdefender Total Security, deverá seguir os passos descritos abaixo:

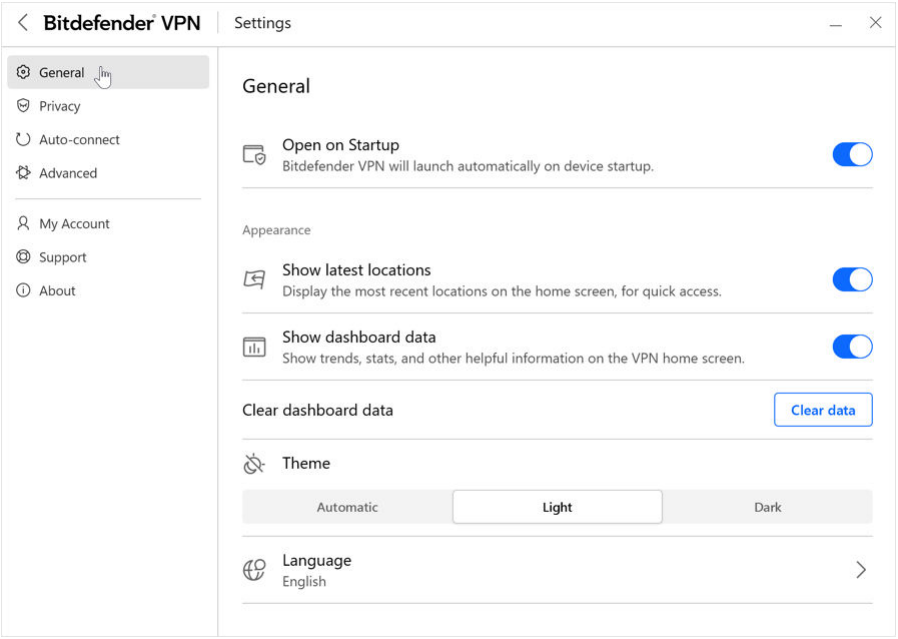
- **No Windows:**
  1. Abra a aplicação do Bitdefender Total Security no seu dispositivo clicando duas vezes no seu ícone no sistema ou clicando com o botão direito do rato nele e selecionando Mostrar.
  2. Clique no botão de **Definições** (representado por um símbolo de engrenagem) no lado esquerdo da interface.
- **No macOS:**
  1. Abra a aplicação do Bitdefender Total Security no seu dispositivo macOS ao clicar no seu ícone na barra de menu.
  2. Clique no botão da engrenagem no canto superior direito da interface do Bitdefender Total Security e selecione Definições.
- **No Android:**
  1. Abra a aplicação Bitdefender Total Security no seu dispositivo.
  2. Clique no botão de engrenagem no canto esquerdo superior da interface do Bitdefender Total Security.
- **No iOS:**
  1. Abra o Bitdefender Total Security aplicativo em seu dispositivo.
  2. Clique no botão roda dentada no canto superior direito do Bitdefender Total Security interface.

7.5.2. Em geral

Aqui você pode modificar o seguinte:

- **Abrir na inicialização**– O Bitdefender VPN será iniciado automaticamente na inicialização do dispositivo.
- **Mostrar locais mais recentes**– Exiba os locais mais recentes na tela inicial, para acesso rápido.
- **Mostrar dados do painel** – Mostre tendências, estatísticas e outras informações úteis na tela inicial da VPN.
- **Limpar dados do painel**– Todos os dados do seu painel serão apagados e todos os contadores serão redefinidos.
- **Tema**– Tema claro/escuro

- **Linguagem**– Altere o idioma do Bitdefender VPN.
- **Notificações**– Gerencie suas preferências de notificações.
- **Ajude a melhorar a VPN Bitdefender**– Envie relatórios anônimos de produtos para nos ajudar a melhorar sua experiência.
- **Redefinir todas as configurações**– Redefina a VPN para suas configurações originais sem reinstalá-la.



7.5.3. Características

Privacidade

Kill-Switch da Internet

O Kill-Switch é uma nova funcionalidade implementada no Bitdefender Total Security. Quando, ativado, ele suspende temporariamente todo o tráfego da internet se a ligação VPN cair acidentalmente. Assim que estiver online novamente, a ligação VPN é restabelecida.

Para ativar o Kill-Switch, siga os passos abaixo:

- **No Windows**
  1. Abra a aplicação Bitdefender Total Security no seu dispositivo ao clicar duas vezes no seu ícone na tentativa do sistema ou ao clicar com o botão direito nele e ao selecionar **Mostrar**.
  2. Clique no **Configurações** botão (representado por uma roda dentada) no lado esquerdo da interface.
  3. Selecione **Avançado**.
  4. Ative a opção **Kill-Switch da internet**.

- **No Android**
  1. Abra o Bitdefender Total Security aplicativo em seu dispositivo.
  2. Clique no botão roda dentada no canto superior direito do Bitdefender Total Security interface.
  3. Nas **Definições**, ative a opção **Kill-Switch**.

- **No iOS**
  1. Abra o Bitdefender Total Security aplicativo em seu dispositivo.
  2. Clique no botão roda dentada no canto superior direito do Bitdefender Total Security interface.
  3. Sob **Configurações**, habilite o **Botão de desligar** opção.

> **Observação**
> Este recurso também está disponível para dispositivos macOS com os sistemas operativos 10.15.4 ou versões posteriores.

Bloqueador de anúncios e antitracker

Estas funcionalidades são projetados para ajudá-lo a manter a privacidade e aproveitar a web sem anúncios irritantes ou empresas a espiá-lo. Eles ajudam a bloquear anúncios e parar rastreá-lo online.

Bloqueador de anúncios

O **Bloqueador de anúncios** é utiliza para bloquear anúncios, pop-ups, anúncios em vídeo altos ou abas de anúncios durante a navegação. Isto ajuda os sites a carregarem mais depressa e ficarem mais limpos, além de serem mais seguros para interagir.

Para ativar o Bloqueador de anúncios:

1. Localize a funcionalidade do **Bloqueador de anúncios e antirastreamento** na **Definições**.
2. Mude o interruptor para a posição **ON**.

Antitracker

O **Anti-rastreador** é utilizado para bloquear rastreadores definidos por anunciantes para seguir e traçar o seu perfil online. Alguns sites podem apresentar mau funcionamento ao bloquear rastreadores, mas adicionar o URL à lista de permissões pode corrigir isso.

Para ativar o Anti-tracker:

1. Localize o **Bloqueador de anúncios e Antitracker** recurso em **Configurações**.
2. Mude o interruptor para o **SOBRE** posição.

Lista de confiança

Alguns websites podem não carregar corretamente se bloquear o seu código localizador e de anúncios. Adicionar os URLs destes domínios específicos à lista de permissões pode resolver este problema, mas tenha em mente que, enquanto navega nestes websites, verá anúncios e o seu código localizador estará ativo.

Adicione os sites que deseja permitir a exibição de anúncios e o utilize os rastreadores:

1. Localize o **Bloqueador de anúncios e Antitracker** recurso em **Configurações**.
2. Clique na ligação **Gerir**. Em seguida, vá para a secção da Lista de permissões da janela e clique na ligação **Gerir** correspondente.
3. Clique em **Adicionar site** e insira o URL desejado.

Auto-conectar

Enquanto caminha, trabalha num café ou aguarda no aeroporto, ligar-se a uma rede pública sem fios para realizar pagamentos, verificar e-mails ou aceder às contas de redes sociais pode ser a solução mais rápida. Enquanto isso, pessoas curiosas tentam roubar os seus dados pessoais vendo como as informações fluem ao longo da rede.

Para o(a) proteger contra os perigos de hotspots públicos não seguros ou não encriptados, o Bitdefender Total Security inclui uma funcionalidade de auto-conexão. Isto significa que o Bitdefender Total Security pode ser ativado automaticamente em determinadas situações, dependendo das suas preferências e do sistema operativo que estiver a utilizar.

- No **Windows**, a funcionalidade de ligação automática pode ser ativado nas seguintes situações:
  - **Arranque:** Ligue-se ao VPN no arranque do Windows.
  - **Wi-Fi não seguro:** Utilize a VPN sempre que se ligar a redes Wi-Fi públicas ou não seguras.
  - **Aplicações ponto a ponto:** Ligue-se ao VPN ao iniciar uma aplicação de partilha de ficheiros ponto a ponto.
  - **Aplicações e domínios:** Utilize sempre o VPN para determinadas aplicações e sites.

    Observação

    1. Clique na ligação **Gerir**.
    2. Navegue até à localização da aplicação para o qual deseja utilizar o VPN, selecione o nome da aplicação e clique em **Adicionar**.

  - **Categorias de sites:** Ligue-se ao VPN ao visitar as categorias específicas dos sites. Bitdefender VPN pode-se ligar automaticamente para as seguintes categorias de sites:
    - Finanças
    - Pagamentos online
    - Saúde
    - Partilha de ficheiros
    - Encontros Online
    - Conteúdo para adultos

    Observação

    Para cada categoria, pode selecionar um servidor diferente para o VPN se ligar.

- No **macOS**, o recurso de ligação automática pode ser ativado nas seguintes situações:
  - **Arranque:** Ligue o VPN no arranque do macOS.
  - **Wi-Fi não seguro:** Use a VPN sempre que se conectar a redes Wi-Fi públicas ou não seguras.
  - **Aplicativos ponto a ponto:** Conecte-se à VPN ao iniciar um aplicativo de compartilhamento de arquivos ponto a ponto.
  - **Aplicações:** Ligue-se sempre ao VPN para determinadas aplicações.
- No **Android** e **iOS**, Bitdefender Total Security pode ser definido para se ligar automaticamente apenas quando estiver num Wi-Fi não seguro ou público.

Avançado

Túnel dividido

O túnel dividido da rede privada virtual (VPN) permite que direcione parte do tráfego da sua aplicação ou dispositivo por meio de um VPN encriptado, enquanto outras aplicações ou dispositivos têm acesso direto à Internet. Isto é particularmente útil se deseja beneficiar dos serviços que funcionam melhor quando a sua localização é conhecida, além de desfrutar de acesso seguro a comunicações e dados potencialmente confidenciais.

Ao ativar o recurso **Split tunneling**, as aplicações e os sites selecionados ignorarão a VPN e acederão a Internet diretamente.

Para gerir as aplicações e os sites que ignoram o VPN:

1. Clique no link **Gerir** assim que o recurso estiver ativado.
2. Clique no botão **Adicionar**.
3. Navegue até o local da aplicação em questão ou insira o URL do site desejado e clique em **Adicionar**.

> **Observação**
> Ao adicionar um site, todo o domínio, ao incluir todos os subdomínios, será ignorado.

Importante

Em dispositivos **macOS**, o recurso Split tunneling está disponível apenas para os sites.

App Traffic Optimizer

O App Traffic Optimizer do Bitdefender Total Security permite que priorize o tráfego para as aplicações mais importantes no seu dispositivo sem expor a sua ligação a riscos de privacidade. As VPNs redirecionam o tráfego da Internet através de um túnel seguro enquanto utilizam algoritmos de encriptação robustos para protegê-lo.

No entanto, esta combinação de técnicas pode ter algumas desvantagens, principalmente no que diz respeito à velocidade da ligação. Vários fatores podem desencadear lentidão na ligação, ao ser o mais comum a distância até o servidor ao qual está a ligar-se, congestionamento da rede e alta utilização de largura de banda. Se já sentiu que às vezes Bitdefender Total Security coloca uma carga desnecessária na sua ligação e lentidão constantemente atrapalha, pode haver uma resposta melhor do que desligar.

Como funciona o App Traffic Optimizer?

Certas aplicações e serviços, como plataformas de streaming, clientes de torrent e jogos, exigem mais largura de banda. A utilização constante deles pode afetar a velocidade da sua ligação com a Internet. O encaminhamento do seu tráfego através de um túnel VPN já sujeita a sua ligação a uma lentidão relativa. Ao colocar tensão adicional na sua ligaão pode degradar seriamente a sua experiência online.

A funcionalidade App Traffic Optimizer do Bitdefender Total Security pode ajudá-lo a lidar com a lentidão da ligação VPN, ao priorizá-lo para a aplicação da sua escolha. O recurso permite que decida quais as aplicações que devem receber a maior parte do seu tráfego e, em seguida, aloca o recursos de acordo. Por exemplo, se estiver numa reunião e perceber que a qualidade da sua chamada está abaixo da média, o App Traffic Optimizer permite que dê prioridade o tráfego para a aplicação de videoconferência para obter melhores resultados.

Normalmente, os utilizadores de VPN recorrem ao encerramento de todos os processos de interferência nos seus dispositivos ou até mesmo à desativação da sua ligação VPN para obter uma velocidade de Internet

mais rápida. O App Traffic Optimizer permite que desfrute de proteção de privacidade ininterrupta sem comprometer a velocidade da sua ligação.

Utilizar a Aplicação Traffic Optimizer

Atualmente, o recurso está disponível apenas em dispositivos Windows e permite priorizar o tráfego para até 3 aplicações.

Siga estas etapas para ativá-la e configurá-lo com o mínimo de esforço:

1. Inicie a aplicação Bitdefender VPN no seu computador Windows.
2. Clique no botão na barra lateral para aceder as definições da VPN.
3. Vá para à guia **Geral** e ative o recurso **App Traffic Optimizer**. A cor da chave mudará de cinza para azul.

Para gerir as aplicações priorizadas por este recurso:

1. Clique no**Gerenciar**link.
2. Navegue até ao local da aplicação para a qual deseja otimizar o tráfego, selecione o nome da aplicação e clique em **Adicionar**. A aplicação aparecerá na secção **Priorizado**.

   Observação
   Como alternativa, abriu-se recentemente a aplicação que deseja priorizar, ao pressionar o botão + na janela do App Traffic Optimizer.

3. Desligue e volte a ligar ao Bitdefender VPN após adicionar ou remover as aplicações da lista.

Para remover uma aplicação do App Traffic Optimizer, basta clicar no ícone ao lado do nome da aplicação.

Observação
O App Traffic Optimizer não está disponível no macOS.

Protocolo

Aqui você pode escolher o tipo de protocolo que deseja usar para transferência de dados. As seguintes opções estão disponíveis:

- **Automático** - O Bitdefender VPN selecionará o protocolo ideal para seu dispositivo e rede específicos.

- **Catapulta Hidra** - Rápido e seguro, ideal para streaming e jogos.
- **OpenVPN UDP** - Otimizado para velocidades rápidas. No entanto, este protocolo não é tão confiável em termos de perda de dados como outros protocolos da lista.
- **OpenVPN TCP** - Projetado para confiabilidade. Garante que seus dados sejam entregues integralmente, mas não é tão rápido quanto o OpenVPN UDP.
- **Proteção de arame** - Protocolo mais recente, proporcionando forte segurança e alto nível de desempenho.

Salto duplo

Com esse recurso você pode gerenciar os servidores através dos quais enviar e criptografar duas vezes o tráfego da Internet. Seus dados passarão por dois servidores VPN em vez de um, dificultando o rastreamento de sua atividade na Internet.

Observação
Você só pode adicionar um total de 5 locais de salto duplo. No entanto, você pode excluir os saltos duplos personalizados da sua lista e criar outros a qualquer momento.

Importante
Usar servidores localizados em continentes diferentes no mesmo salto duplo pode diminuir a velocidade da sua conexão.

7.6. Desinstalar Bitdefender Total Security

O procedimento de remoção do Bitdefender Total Security é similar ao que utiliza para remover outros programas do seu computador:

- **Ao desinstalado Bitdefender Total Security de dispositivos Windows**
  - No **Windows 7**:
    1. Clique em **Iniciar**, vá ao **Painel de Controlo** e dê um clique duplo em **Programas e Recursos**.
    2. Localize **Bitdefender Total Security** e selecione **Desinstalar**. Aguarde até que o processo de desinstalação seja concluído.

- No **Windows 8** e no **Windows 8.1**:
  1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
  2. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
  3. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
     Aguarde a conclusão do processo de desinstalação.

- No **Windows 10** e no **Windows 11**:
  1. Clique em **Iniciar**, depois clique em **Definições**.
  2. Clique no ícone **Sistema** na área de Definições e, em seguida, selecione **Aplicações instaladas**.
  3. Encontrar **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
     Aguarde a conclusão do processo de desinstalação.

- **Desinstalação dos dispositivos macOS**
  1. Clique no **Ir** na barra de menu e selecione **Aplicações**.
  2. Clique duas vezes na pasta **Bitdefender**.
  3. Execute **BitdefenderUninstaller**.
  4. Na nova janela, marque a caixa ao lado de **Bitdefender Total Security** e, em seguida, clique em **Desinstalar**.
  5. Introduza um nome de conta de administrador válido e uma palavra-passe e, em seguida, clique em **OK**.
  6. Finalmente, receberá uma notificação de que o Bitdefender Total Security foi desinstalado com sucesso. Clique em **Fechar**.

- **Desinstalação dos dispositivos Android**
  1. Abra a aplicação **Play Store**.
  2. Procurar por **Bitdefender Total Security**.

3. Na Bitdefender Total Security página da loja de aplicações, selecione **Desinstalar**.
4. Confirme ao tocar em **OK**.

- **Desinstalação de dispositivos iOS**
  1. Mantenha o dedo na aplicação Bitdefender Total Security.
  2. Selecione **Apagar a Aplicação**.
  3. Toque em **Excluir**.

7.7. Perguntas frequentes

Quando devo utilizar o Bitdefender VPN?

Deve ter cuidado ao aceder, transferir ou carregar conteúdo na Internet. Para garantir a sua segurança ao navegar na Web, recomendamos que utilize a VPN quando:

- quiser ligar-se a redes sem fios públicas
- quiser aceder a conteúdos que normalmente são restritos em áreas específicas, não importa se estiver em casa ou fora
- quiser manter os seus dados pessoais privados (nomes de utilizador, palavras-passe, endereços de email, informações de cartão de crédito, etc.)
- desejar esconder o seu endereço IP

Posso escolher uma cidade com o Bitdefender VPN?

Sim. Atualmente, a Bitdefender VPN para Windows, macOS, Android e iOS podem ser utilizados para selecionar uma cidade específica. Aqui está a lista de cidades atualmente disponíveis:

- **EUA:** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Angeles, Miami, Nova York, Newark, Phoenix, Portland, San Jose, Seattle, Washington
- **Canada:** Montreal, Toronto, Vancouver
- **RU:** Londres, Manchester

O Bitdefender VPN pode ser instalado como uma aplicação independente?

A aplicação VPN é instalada automaticamente em conjunto com a sua solução de segurança Bitdefender. Também pode ser instalado como uma aplicação independente na página do produto, da Google Play Store e App Store.

O Bitdefender partilhará o meu endereço IP e dados pessoais com terceiros?

Não, com o Bitdefender VPN a sua privacidade é 100% segura. Ninguém (agências de publicidade, ISPs, seguradoras, etc.) terá acesso aos seus registos online.

Qual algoritmo de encriptação ele utilizar?

Bitdefender VPN utiliza o protocolo Hydra em todas as plataformas, encriptação AES de 256 bits ou a cifra mais alta disponível suportada por cliente e servidor, com Perfect Forward Secrecy. Isto significa que as chaves de encriptação são geradas para cada nova sessão VPN e apagadas da memória quando a sessão terminar.

Posso ter acesso ao conteúdo restrito GEO-IP?

Com o VPN Premium, tem acesso a uma extensa rede de localizações virtuais em todo o mundo.

Isto terá um impacto negativo na duração da bateria do meu dispositivo?

Bitdefender VPN é projetado para proteger os seus dados pessoais, ocultar o seu endereço IP enquanto estiver ligado a redes sem fio não seguras e aceder a conteúdos restritos em determinados países. Para evitar o consumo desnecessário de bateria do seu dispositivo, recomendamos que utilize apenas a VPN quando precisar e desligar quando estiver offline.

Porque é que a VPN torna a minha ligação com a Internet mais lenta?

O Bitdefender VPN foi projetado para oferecer uma experiência leve ao navegar na web. Dependendo da distância entre a sua localização atual e a localização que selecionou do servidor para se ligar, alguma penalidade na velocidade é esperada, no entanto é por norma suficientemente pequena para não ser sentida durante a atividade online normal. Além disso, contamos com uma das infraestruturas de VPN mais rápidas do mundo. Se não for obrigatório ligar-se da sua localização a um servidor hospedado distante (por exemplo, do EUA para a França), recomendamos

que permita que a VPN o ligue automaticamente ao servidor mais próximo ou encontre um servidor mais próximo da sua localização atual.

8. CONSEGUINDO AJUDA

8.1. Pedir Ajuda

O Bitdefender se empenha em oferecer aos seus clientes um nível incomparável de apoio preciso e rápido. Se tiver qualquer problema ou pergunta sobre o seu produto Bitdefender, pode utilizar vários recursos online para encontrar uma solução ou uma resposta. Ao mesmo tempo, pode entrar em contacto com a equipe de Atendimento ao Cliente da Bitdefender. Os nossos representantes de apoio responderão às suas perguntas em tempo hábil e oferecerão a assistência de que precisa.

8.2. Recursos Em Linha

Estão disponíveis vários recursos online para o ajudar a resolver problemas e a responder a questões relacionados com o Bitdefender.

- Centro de Suporte da Bitdefender:
  https://www.bitdefender.pt/consumer/support/
- A Comunidade de Especialistas da Bitdefender:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Também pode utilizar o seu motor de busca favorito para saber mais sobre a segurança de computadores, os produtos Bitdefender e a empresa.

8.2.1. Centro de Suporte da Bitdefender

A Bitdefender Support Center é um repositório de informação online acerca dos produtos BitDefender. Armazena, num formato de relatório facilmente acessível, os resultados das atividades de reparação de erros por parte da equipa técnica do suporte BitDefender e da equipa de desenvolvimento, isto juntamente com artigos gerais acerca de prevenção de ameaças, a administração de soluções BitDefender e explicações pormenorizadas e muitos outros artigos.

A Bitdefender Support Center encontra-se aberta ao público e pode ser utilizada gratuitamente. Esta abundância de informação é uma

outra forma de dar aos clientes BitDefender o conhecimento e o aprofundamento que eles necessitam. Todos os pedidos de informação ou relatórios de erro válidos originários de clientes BitDefender são incluídos na Bitdefender Support Center, como relatórios de reparação de erros, ou artigos informativos como suplementos aos ficheiros de ajuda dos produtos.

O Centro de Suporte Bitdefender está disponível a qualquer momento no seguinte endereço: https://www.bitdefender.pt/consumer/support/.

8.2.2. A Comunidade de Especialistas da Bitdefender

A Comunidade de Especialistas da Bitdefender é um ambiente onde os utilizadores, entusiastas e fãs da Bitdefender podem interagir, trocar ideias, apoiar-se mutuamente e partilhar os seus conhecimentos e soluções. É também um lugar de criação de ideias que fornece um feedback valioso para as nossas equipas de desenvolvimento. Os membros da comunidade são utilizadores experientes da Bitdefender que têm todo o prazer em ajudar outros colegas no seu tempo livre. Com a sua imensa contribuição e os seus esforços genuínos e voluntários, criámos uma base de conhecimento onde os utilizadores podem encontrar respostas e orientação, mas com um toque humano.

Aqui encontrará conversas significativas com pessoas que utilizam a Bitdefender nos seus dispositivos. A comunidade oferece uma verdadeira ligação com os nossos membros e faz com que sua voz seja ouvida. É um lugar onde é encorajado a participar sabendo que sua opinião e sua contribuição são respeitadas e bem recebidas. Ao ser um fornecedor valioso, esforçamo-nos para oferecer um nível inigualável de apoio rápido e preciso e desejamos aproximar os nossos utilizadores de nós. Projetamos a nossa comunidade com este propósito em mente.

Pode encontrar a nossa página da Comunidade de Especialistas aqui:

https://community.bitdefender.com/en/

8.2.3. Bitdefender Cyberpedia

A Bitdefender Cyberpedia tem toda a informação de que precisa sobre as últimas ameaças cibernéticas. Este é o lugar onde os especialistas da Bitdefender partilham dicas e truques sobre como se protegerem contra hackers, violações de dados, roubo de identidade e tentativas de personificação social.

A página da Bitdefender Cyberpedia pode ser encontrada aqui:

https://www.bitdefender.com/cyberpedia/.

8.3. Informações de Contato

Uma comunicação eficiente é a chave para um negócio de sucesso. Desde 2001 a BITDEFENDER estabeleceu uma reputação inquestionável por buscar constantemente uma melhor comunicação para superar as expectativas de nossos clientes e parceiros. Se você tiver alguma dúvida, não hesite em nos contatar diretamente através do nosso Centro de Suporte da Bitdefender (página 261).

https://www.bitdefender.pt/consumer/support/

8.3.1. Distribuidores locais

Os distribuidores locais BitDefender estão preparados para responder a quaiquer dúvidas relacionadas com as suas áreas de operação, quer sejam comerciais ou assuntos gerais.

Para encontrar um distribuidor da Bitdefender no seu país:

1. Vá para https://www.bitdefender.com/partners/partner-locator.html.
2. Escolha o seu país e cidade utilizando as opções correspondentes.

GLOSSÁRIO

Código de ativação

É um código exclusivo que pode ser comprado no varejo e usado para ativar um produto ou serviço específico. Um código de ativação permite a ativação de uma assinatura válida por um determinado período de tempo e determinados dispositivos e também pode ser usado para estender uma assinatura com a condição de ser gerada para o mesmo produto ou serviço.

ActiveX

ActiveX é um modelo para escrever programas para que outros programas e o sistema operacional possam chamá-los. A tecnologia ActiveX é usada com o Microsoft Internet Explorer para criar páginas da Web interativas que se parecem e se comportam como programas de computador, em vez de páginas estáticas. Com o ActiveX, os usuários podem fazer ou responder perguntas, usar botões de pressão e interagir de outras maneiras com a página da web. Os controles ActiveX geralmente são escritos usando o Visual Basic. Active X é notável por uma completa falta de controles de segurança; especialistas em segurança de computadores desencorajam seu uso pela internet.

Ameaça persistente avançada

Ameaça persistente avançada (APT) explora vulnerabilidades de sistemas para roubar informações importantes para entregá-las à fonte. Grandes grupos, como organizações, empresas ou governos, são alvo dessa ameaça. O objetivo de uma ameaça persistente avançada é permanecer indetectável por muito tempo, sendo capaz de monitorar e coletar informações importantes sem danificar as máquinas visadas. O método usado para injetar a ameaça na rede é por meio de um arquivo PDF ou documento do Office que pareça inofensivo para que todos os usuários possam executar os arquivos.

Adware

O adware geralmente é combinado com um aplicativo host fornecido gratuitamente, desde que o usuário concorde em aceitar o adware. Como os aplicativos de adware geralmente são instalados depois que o usuário concorda com um contrato de licenciamento que declara a finalidade do aplicativo, nenhuma ofensa é cometida. No entanto, anúncios pop-

up podem se tornar um aborrecimento e, em alguns casos, degradar o desempenho do sistema. Além disso, as informações que alguns desses aplicativos coletam podem causar problemas de privacidade para usuários que não estavam totalmente cientes dos termos do contrato de licença.

Arquivo

Um disco, cassete, ou diretório que contém ficheiros que foram armazenados.

Um arquivo que contém um ou mais arquivos em um formato compactado.

Porta dos fundos

Uma brecha na segurança de um sistema deliberadamente deixada por designers ou mantenedores. A motivação para tais buracos nem sempre é sinistra; alguns sistemas operacionais, por exemplo, vêm com contas privilegiadas destinadas ao uso por técnicos de serviço de campo ou programadores de manutenção do fornecedor.

Setor de inicialização

Um setor no início de cada disco que identifica a arquitetura do disco (tamanho do setor, tamanho do cluster e assim por diante). Para discos de inicialização, o setor de inicialização também contém um programa que carrega o sistema operacional.

Vírus de inicialização

Uma ameaça que infecta o setor de inicialização de um disco fixo ou disquete. Uma tentativa de inicializar a partir de um disquete infectado com um vírus do setor de inicialização fará com que a ameaça se torne ativa na memória. Toda vez que você inicializar seu sistema a partir desse ponto, você terá a ameaça ativa na memória.

botnet

O termo “botnet” é composto pelas palavras “robô” e “rede”. Botnets são dispositivos conectados à Internet infectados com ameaças e podem ser usados para enviar e-mails de spam, roubar dados, controlar remotamente dispositivos vulneráveis ou espalhar spyware, ransomware e outros tipos de ameaças. Seu objetivo é infectar o maior número possível de dispositivos conectados, como PCs, servidores, dispositivos móveis ou IoT pertencentes a grandes empresas ou indústrias.

Navegador

Abreviação de navegador da web, um aplicativo de software usado para localizar e exibir páginas da web. Os navegadores populares incluem Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Estes são navegadores gráficos, o que significa que eles podem exibir gráficos, bem como texto. Além disso, a maioria dos navegadores modernos pode apresentar informações multimídia, incluindo som e vídeo, embora exijam plug-ins para alguns formatos.

Ataque de força bruta

Ataque de adivinhação de senha usado para invadir um sistema de computador inserindo possíveis combinações de senha, geralmente começando com a senha mais fácil de adivinhar.

Linha de comando

Em uma interface de linha de comando, o usuário digita comandos no espaço fornecido diretamente na tela usando a linguagem de comando.

Biscoitos

Na indústria da Internet, os cookies são descritos como pequenos arquivos contendo informações sobre computadores individuais que podem ser analisados e usados por anunciantes para rastrear seus interesses e gostos online. Neste domínio, a tecnologia de cookies ainda está sendo desenvolvida e a intenção é direcionar os anúncios diretamente para o que você disse que são seus interesses. É uma faca de dois gumes para muitas pessoas porque, por um lado, é eficiente e pertinente, pois você só vê anúncios sobre o que está interessado. Por outro lado, envolve realmente "rastrear" e "seguir" onde você vai e o que você clicar. Compreensivelmente, há um debate sobre privacidade e muitas pessoas se sentem ofendidas com a noção de que são vistas como um "número SKU" (você sabe, o código de barras no verso dos pacotes que é escaneado na fila do caixa do supermercado) . Embora esse ponto de vista possa ser extremo, em alguns casos é preciso.

Cyberbullying

Quando colegas ou estranhos estão cometendo atos abusivos contra crianças com o propósito de machucá-las fisicamente. Para prejudicar emocionalmente, os agressores estão enviando mensagens maldosas ou fotos pouco lisonjeiras, fazendo com que suas vítimas se isolem dos outros ou se sintam frustradas.

Ataque de dicionário

Ataques de adivinhação de senha usados para invadir um sistema de computador inserindo uma combinação de palavras comuns para gerar senhas em potencial. O mesmo método é usado para adivinhar as chaves de descriptografia de mensagens ou documentos criptografados. Os ataques de dicionário são bem-sucedidos porque muitas pessoas tendem a escolher senhas curtas e simples que são fáceis de adivinhar.

Unidade de disco

É uma máquina que lê e grava dados em um disco. Uma unidade de disco rígido lê e grava discos rígidos. Uma unidade de disquete acessa disquetes. As unidades de disco podem ser internas (alojadas em um computador) ou externas (alojadas em uma caixa separada que se conecta ao computador).

Download

Copiar dados (geralmente um arquivo inteiro) de uma fonte principal para um dispositivo periférico. O termo é frequentemente usado para descrever o processo de copiar um arquivo de um serviço online para o próprio computador. O download também pode se referir à cópia de um arquivo de um servidor de arquivos de rede para um computador na rede.

E-mail

Correio eletrônico. Um serviço que envia mensagens em computadores através de redes locais ou globais.

Eventos

Uma ação ou ocorrência detectada por um programa. Os eventos podem ser ações do usuário, como clicar em um botão do mouse ou pressionar uma tecla, ou ocorrências do sistema, como falta de memória.

Exploits

Uma forma de aproveitar diferentes bugs ou vulnerabilidades que estão presentes em um computador (software ou hardware). Assim, os hackers podem obter o controle de computadores ou redes.

Falso positivo

Ocorre quando um mecanismo de varredura identifica um arquivo como infectado quando, na verdade, não está.

Extensão de nome de arquivo

A parte de um nome de arquivo, após o ponto final, que indica o tipo de dados armazenados no arquivo. Muitos sistemas operacionais usam extensões de nome de arquivo, por exemplo, Unix, VMS e MS-DOS. Eles geralmente têm de uma a três letras (alguns sistemas operacionais antigos e tristes não suportam mais do que três). Os exemplos incluem "c" para código-fonte C, "ps" para PostScript, "txt" para texto arbitrário.

Heurística

Um método baseado em regras para identificar novas ameaças. Este método de verificação não depende de um banco de dados de informações de ameaças específico. A vantagem da verificação heurística é que ela não é enganada por uma nova variante de uma ameaça existente. No entanto, ocasionalmente pode relatar códigos suspeitos em programas normais, gerando o chamado "falso positivo".

Pote de mel

Um sistema de computador isca criado para atrair hackers para estudar a maneira como eles agem e identificar os métodos heréticos que usam para coletar informações do sistema. Empresas e corporações estão mais interessadas em implementar e usar honeypots para melhorar seu estado geral de segurança.

IP

Protocolo de Internet - Um protocolo roteável no conjunto de protocolos TCP/IP que é responsável pelo endereçamento IP, roteamento e fragmentação e remontagem de pacotes IP.

miniaplicativo Java

Um programa Java projetado para ser executado apenas em uma página da Web. Para usar um applet em uma página da web, você deve especificar o nome do applet e o tamanho (comprimento e largura, em pixels) que o applet pode utilizar. Quando a página é acessada, o navegador baixa o applet de um servidor e o executa na máquina do usuário (o cliente). Os applets diferem dos aplicativos porque são regidos por um protocolo de segurança estrito.

Por exemplo, embora os applets sejam executados no cliente, eles não podem ler ou gravar dados na máquina do cliente. Além disso, os applets são ainda mais restritos para que possam apenas ler e gravar dados do mesmo domínio do qual são servidos.

Keylogger

Um keylogger é um aplicativo que registra tudo o que você digita. Keyloggers não são maliciosos por natureza. Eles podem ser usados para fins legítimos, como monitorar atividades de funcionários ou crianças. No entanto, eles estão sendo cada vez mais usados por cibercriminosos para fins maliciosos (por exemplo, para coletar dados privados, como credenciais de login e números de CPF).

Vírus de macro

Um tipo de ameaça de computador codificada como uma macro incorporada a um documento. Muitos aplicativos, como Microsoft Word e Excel, oferecem suporte a poderosas linguagens de macro. Esses aplicativos permitem que você incorpore uma macro em um documento e execute a macro sempre que o documento for aberto.

cliente de e-mail

Um cliente de e-mail é um aplicativo que permite enviar e receber e-mails.

Memória

Áreas de armazenamento interno no computador. O termo memória identifica o armazenamento de dados que vem na forma de chips, e a palavra armazenamento é usada para memória que existe em fitas ou discos. Todo computador vem com uma certa quantidade de memória física, geralmente chamada de memória principal ou RAM.

Não heurístico

Este método de verificação depende de um banco de dados de informações de ameaças específico. A vantagem da verificação não heurística é que ela não é enganada pelo que pode parecer uma ameaça e não gera alarmes falsos.

predadores online

Indivíduos que procuram atrair menores ou adolescentes para conversas com o propósito de envolvê-los em atividades sexuais ilegais. As redes sociais são o local ideal onde crianças vulneráveis podem ser facilmente caçadas e induzidas a praticar atividades sexuais, online ou face a face.

Programas compactados

Um arquivo em um formato de compactação. Muitos sistemas operacionais e aplicativos contêm comandos que permitem compactar um arquivo para que ele ocupe menos memória. Por exemplo, suponha

que você tenha um arquivo de texto contendo dez caracteres de espaço consecutivos. Normalmente, isso exigiria dez bytes de armazenamento.

No entanto, um programa que compacta arquivos substituiria os caracteres de espaço por um caractere de série de espaço especial seguido pelo número de espaços sendo substituídos. Nesse caso, os dez espaços exigiriam apenas dois bytes. Esta é apenas uma técnica de empacotamento - existem muitas outras.

Caminho

As direções exatas para um arquivo em um computador. Essas direções geralmente são descritas por meio do sistema de arquivamento hierárquico de cima para baixo.

A rota entre quaisquer dois pontos, como o canal de comunicação entre dois computadores.

Phishing

O ato de enviar um e-mail a um usuário que afirma falsamente ser uma empresa legítima estabelecida na tentativa de enganar o usuário para que entregue informações privadas que serão usadas para roubo de identidade. O e-mail direciona o usuário a visitar um site onde é solicitado que ele atualize as informações pessoais, como senhas e números de cartão de crédito, previdência social e contas bancárias, que a organização legítima já possui. O site, no entanto, é falso e criado apenas para roubar as informações do usuário.

Fóton

Photon é uma tecnologia inovadora não intrusiva da Bitdefender, concebida para minimizar o impacto da solução de segurança. Ao monitorizar a atividade do seu PC em segundo plano, ele cria padrões de utilização que ajudam a otimizar os processos de arranque e de análise.

Vírus polimórfico

Uma ameaça que muda a sua forma com cada ficheiro que infeta. Como não têm um padrão binário consistente, essas ameaças são difíceis de identificar.

Porta

Uma interface num computador, à qual se liga um aparelho. Os computadores pessoais tendo vários tipos de portas. Internamente, existem várias portas para ligar componentes de disco, ecrãs e teclados.

Externamente, os computadores pessoais portas para ligar modems, impressoras, ratos, e outros aparelhos periféricos.

Nas redes TCP/IP e UDP, um ponto de fim para uma ligação lógica. O número da porta identifica o tipo da porta. Por exemplo, a porta 80 é usada para o tráfego HTTP.

Ransomware

Ransomware é um programa malicioso que tenta lucrar com os utilizadores através do bloqueio dos seus sistemas vulneráveis. CryptoLocker, CryptoWall e TeslaWall são apenas algumas variantes que perseguem os sistemas pessoais dos utilizadores.

A infeção pode ser espalhada através do acesso a um e-mail de spam, transferência de anexos de e-mail ou da instalação de aplicações, sem que o utilizador saiba o que está a acontecer no seu sistema. Os utilizadores diários e as empresas são os alvos dos hackers ransomware.

Arquivo de relatório

Um ficheiro que lista acções que tiveram ocurrência. O BitDefender um ficheiro de reporte que lista o caminho examinado, as pastas, o número de arquivos e ficheiros examinados, e quantos ficheiros suspeitos e infectados foram encontrados.

Rootkit

Um rootkit é um pacote de ferramentas de software que proporcionam um nível de acesso de administrador a um sistema. O termo foi usado em primeiro lugar nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam aos intrusos direitos de administração, permitindo-lhes ocultar a sua presença de forma a não serem vistos pelos administradores do sistema.

O papel principal dos rootkits é ocultar processos, ficheiros, logins e registos. Eles também podem interceptar dados dos terminais, ligações de rede ou periféricos, se eles incorporarem o software para tal.

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam ficheiros críticos usando rootkits. No entanto, são principalmente utilizados para ocultar ameaças ou esconder a presença de um intruso no sistema. Quando combinados com ameaças, os rootkits são uma grande ameaça à integridade e à segurança de um sistema. Eles podem monitorizar tráfego, criar backdoors no sistema, alterar ficheiros e relatórios e evitarem ser detetados.

Script

Outro termo para macro ou ficheiro de porção, uma escrita é uma lista de comandos que podem ser executados sem a interação do utilizador.

Spam

Lixo de correio electrónico ou lixo de avisos de newsgroups. Geralmente atribuído a qualquer e-mail não solicitado.

Spyware

Qualquer software que encobertamente reune informação do utilizador através da ligação à Internet do utilizador sem o seu conhecimento, normalmente para propósitos de publicidade. As aplicações de spyware são tipicamente adicionadas como um elemento oculto de programas freeware ou shareware que podem ser download a partir da Internet; no entanto salientamos que a maioria das aplicações freeware ou shareware não possuem spyware. Uma vez instalado, o spyware monitoriza a actividade do utilizador na Internet e transmite essa informação em background para alguém. O spyware pode também ser capaz de obter endereços de e-mail e até mesmo palavras-passe e números de cartão de crédito.

O spyware é similar a uma ameaça Cavalo de Troia em que os utilizadores o instalam sem saberem, enquanto estão a instalar outra coisa qualquer. Uma forma comum de ser uma vítima de spyware é fazer download de determinado ficheiro peer-to-peer de produtos de swapping que se encontram actualmente disponíveis.

Para além destas questões de ética e privacidade, o spyware priva o utilizador de recursos de memória e também de largura de banda pois para enviar informação do utilizador para a fonte do spyware usa a ligação à Internet do utilizador. Por causa do spyware utilizar memória e recursos do sistema, as aplicações que estão a funcionar em background podem causar crashes no sistema ou uma grande instabilidade geral.

Itens de inicialização

Qualquer ficheiro colocado nesta pasta, irá abrir quando o computador iniciar. Por exemplo, um ecrã de arranque, um ficheiro de som a ser reproduzido quando o computador arranca, um calendário de lembretes ou aplicações podem ser itens de arranque. Normalmente, é colocado um pseudónimo deste ficheiro nesta pasta, em vez do ficheiro em si.

Inscrição

Acordo de compra que dá ao utilizador o direito de utilizar um produto ou serviço específico num número específico de dispositivos e durante um período de tempo determinado. Uma subscrição expirada pode ser automaticamente renovada utilizando as informações fornecidas pelo utilizador na primeira compra.

Bandeja do sistema

Introduzido com o Windows 95, o tabuleiro do sistema está localizado na barra de tarefas do Windows (normalmente em baixo, junto ao relógio) e contém ícones em miniatura para um acesso fácil às funções do sistema, tais como fax, impressora, modem, volume, etc. Faça duplo-clique ou clique com o botão direito sobre o ícone para ver e aceder aos detalhes e controlos.

TCP/IP

Transmission Control Protocol/Internet Protocol - Um conjunto de protocolos de uma rede de trabalho abrangentemente usados Internet que permite comunicações ao londo de redes de computadores interconectadas com várias arquitecturas de hardware e vários sistemas operaticos. O TCP/IP ínclui padrões de como os computadores comunicam e convenções para ligar redes e conduzir o tráfego.

Ameaça

Um programa ou um pedaço de código que é carregado no seu computador sem o seu conhecimento e executa-se contra a sua vontade. A maioria das ameaças também se pode replicar. Todas as ameaças de computador são criadas pelo homem. Uma simples ameaça pode copiar-se várias vezes e é relativamente fácil de produzir. Mesmo uma simples ameaça é perigosa porque pode rapidamente utilizar toda memória disponível e fazer o sistema parar. O tipo de ameaça mais perigoso é aquele que é capaz de se transmitir através de uma rede ou contornando sistemas de segurança.

Atualização de informações sobre ameaças

O padrão binário de uma ameaça é utilizado pela solução de segurança para detetá-la e eliminá-la.

Troiano

Um programa destrutivo que se mascara de aplicação benigna. Ao contrário de programas de software maliciosos e worms, os Trojans não se replicam, mas podem ser igualmente destrutivos. Um dos tipos mais

insidiosos de ameaças de cavalo de Troia é um programa que afirma remover as ameaças do seu computador, mas, em vez disso, introduz ameaças no seu computador.

O termo provém de uma história da Ilíada de Homero, na qual os Gregos deram um cavalo gigante de Madeira aos seus inimigos, os Troianos, como uma oferta majestosa. Mas após os Troianos levarem o cavalo para dentro das muralhas da sua cidade, os soldados Gregos saíram para fora do cavalo e abriram os portões da cidade, permitindo que os seus compatriotas entrassem e dominassem Tróia.

Atualizar

Uma nova versão de um produto de software ou hardware concebida para substituir uma versão antiga do mesmo produto. Em adição, a instalação de rotina da atualização verifica se a versão anterior já está instalada no seu computador; se não estiver, não poderá instalar a atualização.

O Bitdefender tem a sua própria funcionalidade de atualização que lhe permite verificar atualizações manualmente, ou permitir atualizar o produto automaticamente.

Rede Privada Virtual (VPN)

É uma tecnologia que ativa uma conexão direta temporária e criptografada para uma certa rede sobre uma rede menos segura. Dessa forma, enviar e receber dados é seguro e criptografado, difícil de virar alvo de espiões. Uma prova de segurança é a autenticação, que pode ser feita somente com o uso de um nome de usuário e senha.

Worm

Um programa que se propaga a si próprio ao longo de uma rede, reproduzindo-se à medida que avança. Não pode ligar-se sozinho a outros programas.