GEBRUIKSAANWIJZING

Bitdefender CONSUMER SOLUTIONS

VPN

Bitdefender VPN

Handleiding

Publication date 02/07/2024

Kennisgevingen

Bitdefender

Inhoudsopgave

OVER DEZE GIDS

Voor wie is deze handleiding bedoeld?

Deze gids is bedoeld voor alle Bitdefender gebruikers die Bitdefender VPN hebben gekozen als hun voorkeursservice die hen online anonimiteit verleent door al het inkomende en uitgaande verkeer op hun pc, Mac of mobiele apparaten te versleutelen.

U zult ontdekken hoe u Bitdefender VPN kunt configureren en gebruiken om uw online identiteit en activiteiten veilig te houden van hackers, internetproviders en snuffelaars. U leert hoe u het beste uit Bitdefender kunt halen.

We wensen u veel leesplezier met deze handleiding.

Hoe kunt u deze handleiding gebruiken?

De handleiding is ingedeeld aan de hand van enkele hoofdonderwerpen:

Wat is Bitdefender VPN (pagina 4)

Ga aan de slag met Bitdefender VPN door te leren wat het is en hoe het u kan helpen uzelf te beschermen door u echte online anonimiteit te verlenen.

Bitdefender VPN gebruiken (pagina 13)

Leer hoe u omgaat met Bitdefender VPN en zijn gebruikersinterface.

Bitdefender VPN Instellingen & Functies (pagina 17)

Meer informatie over de instellingen en functionaliteiten van Bitdefender VPN.

Hulp vragen (pagina 31)

Ontdek waar u hulp moet zoeken indien er zich onverwacht een probleem voordoet.

Conventies die in deze gids worden gebruikt

Typografische conventies

In deze gids worden verschillende tekststijlen gebruikt, zodat de tekst leesbaarder is. De weergave en betekenis worden in de onderstaande tabel voorgesteld.

Weergave	Beschrijving
voorbeeld-syntaxis	Voorbeelden van syntaxis worden weergegeven in een niet-proportioneel lettertype.
https://www.bitdefender.com	De URL-koppeling wijst naar een externe locatie op http- of ftp-servers.
documentation@bitdefender.com	E-mailadressen worden in de tekst ingevoegd voor contactgegevens.
Over deze gids (pagina 1)	Dit is een interne koppeling naar een locatie in het document.
bestandsnaam	Namen van bestanden en mappen worden weergegeven in een niet-proportioneel lettertype.
optie	Alle productopties worden **vet** weergegeven.
trefwoord	Sleutelwoorden en belangrijke zinsdelen worden **vet** weergegeven.

Waarschuwingen

De waarschuwingen zijn grafisch gemarkeerde opmerkingen in de tekst die extra informatie over de huidige paragraaf onder de aandacht brengen.

Opmerking

De opmerking is slechts een kort commentaar. Hoewel u opmerkingen kunt weglaten, kunnen ze toch waardevolle informatie bieden zoals over een specifieke functie of een koppeling naar een verwant onderwerp.

Belangrijk

Dit vereist uw aandacht en het wordt niet aanbevolen dit te negeren. Doorgaans betreft het niet-kritieke, maar belangrijke informatie.

Waarschuwing

Dit is kritische informatie die u aandachtig moet lezen. Er zullen geen ernstige problemen optreden als u de aanwijzingen volgt. U moet de informatie lezen en begrijpen omdat hier iets wordt beschreven dat hoge risico's inhoudt.

Verzoek om commentaar

We willen u uitnodigen ons te helpen dit boek te verbeteren. Wij hebben alle informatie zo goed mogelijk getest en gecontroleerd. Laat ons weten of u enige tekortkomingen hebt ontdekt in dit boek of als u ideeën hebt om dit te verbeteren, zodat wij u de best mogelijke documentatie kunnen bieden.

U kunt contact met ons opnemen door een e-mail te sturen naar documentation@bitdefender.com. Wij verzoeken u al uw e-mails met betrekking tot de documentatie in het Engels te schrijven, zodat we uw opmerkingen op een efficiënte manier kunnen verwerken.

1. WAT IS BITDEFENDER VPN

De VPN fungeert als een tunnel tussen uw apparaat en het netwerk waarmee u verbinding maakt om uw verbinding te beveiligen, de gegevens te coderen met behulp van codering op militair niveau en uw IP-adres te verbergen waar u ook bent. Uw verkeer wordt omgeleid via een aparte server; waardoor uw apparaat onmogelijk kan worden geïdentificeerd door uw ISP, via de talloze andere apparaten die onze services gebruiken. Bovendien hebt u, terwijl u via Bitdefender VPN verbonden bent met internet, toegang tot inhoud die normaal gesproken beperkt is in specifieke gebieden.

Opmerking

Bepaalde landen doen aan internetcensuur, waardoor het gebruik van VPN's op hun grondgebied bij wet verboden is. Om wettelijke gevolgen te vermijden, is het mogelijk dat er een waarschuwingsboodschap verschijnt wanneer u de functie van Bitdefender VPN voor het eerst probeert te gebruiken. Door deze functie te blijven gebruiken, bevestigt u dat u op de hoogte bent van de toepasselijke regels van dat land en van de risico's die u zou kunnen lopen.

1.1. Versleutelingsprotocollen

De standaard ciphersuite-sets ingeschakeld in Hydra-client en-server worden hieronder vermeld. Alle andere ciphersuites zijn uitgeschakeld.

Ciphersuites in Hydra-client:

- 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

Opmerking

Set aan server zijde is veel restrictiever, en zowel Hydra-client als -server zullen een modus andere dan GCM met AES weigeren. Hydra-server dwingt prioriteit aan server zijde af voor sterkere ciphersuites en zal TLS handshake weigeren als een zwakkere suite door een client wordt verzocht. Deze lijst kan ook worden geconfigureerd in runtime aan server zijde.

2. VPN-ABONNEMENTEN

Met Bitdefender VPN kunt u kiezen tussen twee soorten abonnementen:

- Het Basis-abonnement
- Het Premium-abonnement

2.1. Basis-abonnement

Bitdefender VPN biedt dagelijks 200 MB gratis verkeer per apparaat, om uw verbinding te beveiligen telkens u dat nodig hebt, en laat u verbinding maken met één locatie, die u niet kunt wijzigen.

Het Basis-abonnement is beschikbaar voor alle gebruikers die Bitdefender VPN dowloaden.

2.2. Premium-abonnement

Om onbeperkte toegang te krijgen tot alle voorzieningen inbegrepen in Bitdefender VPN, upgradet u naar de Premium-versie. Gebruikers met een actief Premium VPN-abonnement krijgen onbeperkt verkeer en kunnen verbinding maken met al onze servers, overal ter wereld.

Er zijn twee opties beschikbaar voor het Premium-abonnement: het Maandelijkse plan en het Jaarlijkse plan.

- Het Maandelijkse plan: met dit plan wordt u elke maand aangerekend voor de Premium VPN-diensten. U kunt zich altijd afmelden.
- Het Jaarlijkse plan: vereist een eenmalige betaling, en verleent u een gans jaar toegang tot onze Premium VPN-diensten.

2.3. Hoe upgraden naar Premium VPN

De meest eenvoudige manier om te upgraden naar de Premium-versie van Bitdefender VPN, is te klikken op de knop **Upgraden** in het onderste gedeelte van de hoofdinterface. Kies het gewenste abonnement en volg de instructies op het scherm.

Hebt u al een activeringscode, dan volgt u de onderstaande instructies:

- **Voor Windows-gebruikers**

1. Klik op het pictogram Mijn account aan de linkerkant van de VPN-interface.
2. Klik op **Hier toevoegen**.
3. Voer de code in die u via e-mail hebt ontvangen, en klik op de knop **Code activeren**.

- **Voor macOS-gebruikers**
  1. Klik op het tandwiel in de rechterbovenhoek van de VPN-interface en selecteer **Mijn account**.
  2. Klik **Voeg het hier toe**.
  3. Voer de code in die u via e-mail hebt ontvangen en klik vervolgens op de **activerings code** knop.
- **Voor Android-gebruikers**
  1. Tik op het tandwiel in de rechterbovenhoek van de VPN-interface en selecteer **Mijn account**.
  2. Tik op **Code toevoegen**.
  3. Voer de code in die u via e-mail hebt ontvangen en klik vervolgens op de **activerings code** knop.
- **Voor iOS-gebruikers**
  1. Tik op het tandwiel in de rechterbovenhoek van de VPN-interface en selecteer **Mijn rekening**.
  2. Kraan **Code toevoegen**.
  3. Voer de code in die u via e-mail hebt ontvangen en klik vervolgens op de **activerings code** knop.

3. INSTALLATIE

3.1. Voorbereiden voor installatie

Voordat u Bitdefender VPN installeert, moet u deze voorbereidingen voltooien om ervoor te zorgen dat de installatie vlot verloopt:

- Controleer of de apparaat waarop u Bitdefenderwilt installeren, voldoet aan de minimale systeemvereisten. Als de apparaat niet aan alle systeemvereisten voldoet, wordt het Bitdefender niet geïnstalleerd, of als het toch geïnstalleerd wordt, zal het niet goed werken en zal het systeem vertragen en instabiel worden.
  Raadpleeg Systeemvereisten (pagina 8) voor de complete lijst van alle systeemvereisten.
- Meld u aan bij de apparaat met een beheerdersaccount.
- Het wordt aanbevolen uw apparaat verbonden te laten met Internet tijdens de installatie, zelfs wanneer u vanaf een cd/dvd installeert. Indien er nieuwere versies van de toepassingsbestanden in het installatiepakket beschikbaar zijn, kan Bitdefender deze downloaden en installeren.

3.2. Systeemvereisten

- **Voor Windows-gebruikers**
  - **Besturingssysteem:** Windows 7 met Service Pack 1, Windows 8, Windows 8.1 Windows 10 en Windows 11
  - **Geheugen (RAM):** 1 GB
  - **Beschikbare vrije schijfruimte:** 500 MB vrije ruimte
  - **Net Framework:** min versie 4.5.2

    Belangrijk
    Systeemprestaties kunnen worden beïnvloed voor apparaten die CPU's van een oudere generatie hebben.
- **Voor macOS-gebruikers**
  - **Besturingssysteem:** macOS Sierra (10.12) of later

- **Beschikbare vrije schijfruimte:** 100 MB vrije ruimte

- **Voor Android-gebruikers**
  - **Besturingssysteem:** Android 5.0 of later
  - **Opslag:** 100MB
  - Een werkende internetverbinding

- **Voor iOS-gebruikers**
  - **Besturingssysteem:** iOS 12 of later
  - **Opslag op iPhone:** 50MB
  - **Opslag op iPad:** 100MB
  - Een actieve internetverbinding

3.3. Bitdefender VPN installeren

Om de installatie te starten, volgt u de instructies voor het besturingssysteem dat u gebruikt:

- **Voor Windows-gebruikers**

  1. Om de installatie van Bitdefender VPN op een Windows pc te starten, downloadt u eerst de installatiekit van https://www.bitdefender.com/solutions/vpn/download of uit de e-mail die u na een aankoop ontvangt.
  2. Dubbelklik op het gedownloade installatiebestand om het uit te voeren.
  3. Kies Ja als u de dialoog Gebruikersaccountbeheer ziet.
  4. Wacht totdat de download is voltooid.
  5. Selecteer de taal voor het product, aan de hand van het vervolgkeuzemenu in het installatiebestand.
  6. Vink “Ik bevestig dat ik de Abonnementsvoorwaarden en het Privacybeleid heb gelezen en aanvaard” aan en klik vervolgens op **INSTALLATIE STARTEN**.
  7. Wacht tot de installatie is voltooid.

8. **LOG IN** met uw Bitdefender Central-account. Als u geen Central-account hebt, maakt u er een aan via de knop **ACCOUNT MAKEN**.
9. Kies **Ik heb een activeringscode** als u een Premium VPN-abonnement hebt aangekocht.
   Anders kunt u **PROEFPERIODE STARTEN** kiezen, om het product 7 dagen lang gratis te testen, voordat u beslist om ervoor te betalen.
10. Voer de code in die u via e-mail hebt ontvangen, en klik op de knop **PREMIUM ACTIVEREN**.
11. Na een korte wachttijd is Bitdefender VPN geïnstalleerd en klaar voor gebruik op uw computer.

❍ **Voor macOS-gebruikers**

1. Om de installatie van Bitdefender VPN op macOS te starten, downloadt u eerst de installatiekit van https://www.bitdefender.com/solutions/vpn/download of uit de e-mail die u na een aankoop ontvangt.
2. Het installatiebestand wordt opgeslagen op uw Mac. In de map Downloads dubbelklikt u op het -pakketbestand.
3. Volg de instructies op het scherm en kies **Verdergaan**.
4. U wordt door de stappen geleid die nodig zijn om Bitdefender VPN op uw Mac te installeren. Klik tweemaal op de **Continue** knop.
5. Klik op **Akkoord** nadat u de voorwaarden van de softwarelicentie-overeenkomst hebt gelezen en deze aanvaardt.
6. Klik op **Installeren**.
7. Voer een beheerdersgebruikersnaam en -wachtwoord in en klik vervolgens op **Software installeren**.
8. U wordt op de hoogte gebracht dat een systeemextensie, getekend door Bitdefender, werd geblokkeerd. Dit is geen fout, enkel een beveiligingscontrole. Klik op **Beveiligingsvoorkeuren openen**.
9. Klik op het slotpictogram om te ontgrendelen.
   Voer een beheerdersnaam en -wachtwoord in en druk op **Ontgrendelen**.

10. Klik op **Toestaan** om de systeemextensie van BitdefenderBitdefender te laden. Daarna sluit u het venster Beveiliging en Privacy en het Bitdefender-installatiebestand.

11. Ga naar het schildpictogram in de menubalk en **Log in** met uw Bitdefender Central-account. Als u geen Central-account hebt, maakt u er een aan.

12. Kies Ik heb een **Activeringscode** als u een Premium VPN-abonnement hebt aangekocht.
    Anders kun je kiezen **START PROEF** om het product 7 dagen gratis uit te proberen voordat u ervoor gaat betalen.

13. Voer de code in die u via e-mail hebt ontvangen en klik vervolgens op de **activerings code** knop.

14. Na een korte wachttijd is Bitdefender VPN geïnstalleerd en klaar voor gebruik op uw Mac.

- **Voor Android-gebruikers**

1. Om Bitdefender VPN te installeren op Android, opent u eerst de app **Google Play Store** op uw smartphone of tablet.
2. Zoek Bitdefender VPN naar en selecteer deze app.
3. Tik op de knop **Installeren** en wacht totdat de download is voltooid.
4. Tik op **Openen** om de app uit te voeren.
5. Vink het vakje “Ik ga akkoord met de Abonnementsovereenkomst en het Privacybeleid" aan en tik op **Verdergaan**.
6. **Log in** met uw Bitdefender Central-account. Als u geen Central-account hebt, maakt u er een aan door te tikken op **Account maken**.
7. Kies **Ik heb een activeringscode** als u een Premium VPN-abonnement hebt aangekocht.
   Anders kunt u Proefperiode 7 dagen starten kiezen, om het product 7 dagen lang gratis te testen, voordat u beslist om ervoor te betalen.
8. Voer de code in die u via e-mail hebt ontvangen, en tik op **Code activeren**.

- **Voor iOS-gebruikers**

  1. Om Bitdefender VPN op iOS te installeren, opent u eerst **App Store** op uw iPhone of iPad.
  2. Zoeken Bitdefender VPN en selecteer deze app.
  3. Tik op het pictogram **Get** en wacht totdat de download is voltooid.
  4. Kraan **Open** om de app uit te voeren.
  5. Vink het vakje **Ik ga akkoord met de Abonnementsovereenkomst en het Privacybeleid** aan, en tik op **Verdergaan**.
  6. **Log in** met uw Bitdefender Central-account. Als u geen account hebt, maakt u er een aan door te tikken op **Account maken**.
  7. Tik op **Toestaan** als u Bitdefender VPN meldingen wilt ontvangen.
  8. Kiezen **Ik heb een activeringscode** als je een Premium VPN-abonnement hebt gekocht.
     Anders kunt u Start 7 days Trial kiezen om het product 7 dagen gratis uit te proberen voordat u ervoor gaat betalen.
  9. Voer de via e-mail ontvangen code in en tik vervolgens op **Activerings code**.

4. BITDEFENDER VPN GEBRUIKEN

4.1. Bitdefender VPN openen

- **Voor Windows**
  Om naar de **hoofdinterface van Bitdefender VPN** te gaan, volgt u een van de volgende methoden:
  - **Vanuit het systeemvak**
    Klik met de rechtermuisknop op het rode schildpictogram in het systeemvak, en selecteer dan **Weergeven** in het menu.
  - **Vanuit deBitdefender-interface**
    Als er al een Bitdefender-beveiligingsproduct zoals Bitdefender Total Security of Bitdefender Antivirus Plus, enz. op uw Windows-computer is geïnstalleerd, kunt u Bitdefender VPN van daaruit openen:
    1. Klik **Privacy** in de linkerzijbalk van de Bitdefender-interface.
    2. Klik op **VPN openen** in het VPN-deelvenster.
  - **Vanaf uw bureaublad**
    Dubbelklik op de Bitdefender VPN-snelkoppeling op uw bureaublad.
- **Voor macOS**
  U kunt de Bitdefender VPN-app openen door op het pictogram in de menubalk rechtsboven op het scherm te klikken.
  Als het Bitdefender-schild niet in de menubalk te vinden is, gebruik dan uw Mac Launchpad of Finder om het terug te halen:
  - **Vanuit Launchpad**
    1. Druk op **F4** op uw toetsenbord om naar de Launchpad op uw Mac te gaan.
    2. Blader door de pagina's met geïnstalleerde apps totdat u de Bitdefender VPN-app vindt. U kunt ook **Bitdefender VPN** in Launchpad typen om te beginnen met het filteren van uw resultaten.

3. Zodra u de Bitdefender VPN-app ziet, klikt u op het pictogram ervan om deze vast te zetten in de menubalk.

❍ **Vanuit Finder**

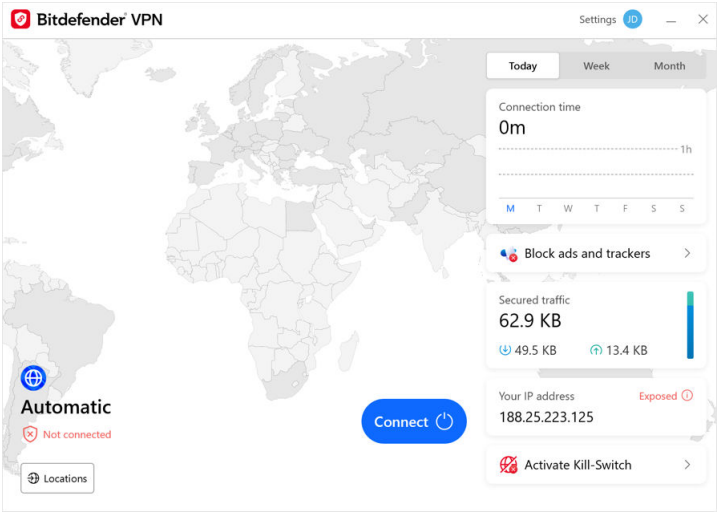
1. Klik op **Finder** linksonder in het Dock (Finder is het pictogram dat lijkt op een blauw vierkant met een smiley).
2. Klik vervolgens op **Ga** linksboven in het scherm, op de menubalk.
3. Kies **Programma's** uit het menu om de map Programma's op uw Mac te openen.
4. Ga naar de map Programma's, open de map **Bitdefender** en dubbelklik op de **Bitdefender** VPN-app.

Opmerking

Om toegang te krijgen tot Bitdefender VPN op uw mobiele Android- of iOS-apparaten, opent u gewoon de Bitdefender VPN-toepassing nadat u deze hebt geïnstalleerd.

4.2. Hoe verbinding maken met Bitdefender VPN

De VPN-interface geeft de status van de app weer: verbonden of niet verbonden. Voor gebruikers met de gratis versie stelt Bitdefender de serverlocatie automatisch in op de meest geschikte server. Premium-gebruikers hebben de mogelijkheid om de serverlocatie waarmee ze wensen te verbinden, te wijzigen, door de locatie te selecteren in de lijst Virtuele locaties. Om verbinding te maken of de verbinding te verbreken, klikt u gewoon op de aan/uit-knop van de VPN-interface.



- **Voor Windows:** Het systeemvakpictogram toont een groen vinkje wanneer het VPN is verbonden, en een zwart vinkje wanneer het VPN is verbroken. Tijdens de verbinding met een handmatig geselecteerde locatie wordt het IP-adres weergegeven op de hoofdinterface.
- **Voor macOS:** Het menubalkpictogram is zwart als het VPN is verbonden, en wit als het VPN is verbroken. Klik op de ronde knop in het midden van de interface en wacht tot de verbinding tot stand is gebracht.
- **Voor Android & iOS:** Om verbinding te maken met Bitdefender VPN voor Android, iOS en iPadOS:
  - **In de Bitdefender VPN-app:** Om verbinding te maken of de verbinding te verbreken, klikt u gewoon op de aan/uit-knop van de VPN-interface. De status van Bitdefender VPN wordt weergegeven.
  - **In de toepassing Bitdefender Mobiele Beveiliging:**
    1. Ga naar het VPN-pictogram op de onderste navigatiebalk van Bitdefender Mobiele Beveiliging.
    2. Tik op **VERBINDEN** wanneer u beschermd wilt blijven terwijl u verbonden bent met onbeveiligde draadloze netwerken. Tik

op **VERBINDING VERBREKEN** telkens als u de VPN-verbinding wilt uitschakelen.

4.3. Hoe verbinding maken met een andere server

Met een Premium abonnement kunt u MET Bitdefender VPN op elk moment verbinding maken met AL onze servers over de hele wereld. Hiervoor moet u:

1. De Bitdefender VPN app openen.
2. Tik op de knop **Virtuele Locatie** in het onderste gedeelte van de interface.
3. Selecteer een land.
4. Klik op de knop **Verbinden met [land]** in het onderste gedeelte van de interface.

- Het systeemvakpictogram geeft een groen vinkje weer wanneer de VPN is verbonden.
- Het IP-adres van de virtuele server wordt weergegeven op het startscherm terwijl u verbonden bent met Bitdefender VPN.
- Een samenvatting van uw verbindingstijd, de hoeveelheid beveiligd verkeer en de laatste 5 locaties waarmee u verbinding hebt gemaakt, worden ook weergegeven op het hoofddashboard.

5. BITDEFENDER VPN INSTELLINGEN & FUNCTIES

5.1. Naar Instellingen gaan

Om naar de instellingen van Bitdefender VPN te gaan, volgt u de onderstaande stappen:

- **In Windows**
  1. Open de app voor Bitdefender VPN op uw apparaat door in het systeemvak te dubbelklikken op het pictogram ervan of door er met de rechtermuisknop op te klikken en Tonen te selecteren.
  2. Klik op de knop **Instellingen** (voorgesteld door een tandwiel) aan de linkerkant van de interface.

- **In macOS**
  1. Open de app voor Bitdefender VPN op uw macOS-apparaat, door in de menubalk te klikken op het pictogram ervan.
  2. Klik in de rechterbovenhoek van de Bitdefender VPN-interface op het tandwiel en selecteer Instellingen.

- **Op Android**
  1. Open de Bitdefender VPN app op uw apparaat.
  2. Klik in de rechterbovenhoek van de Bitdefender VPN-interface op het tandwiel.

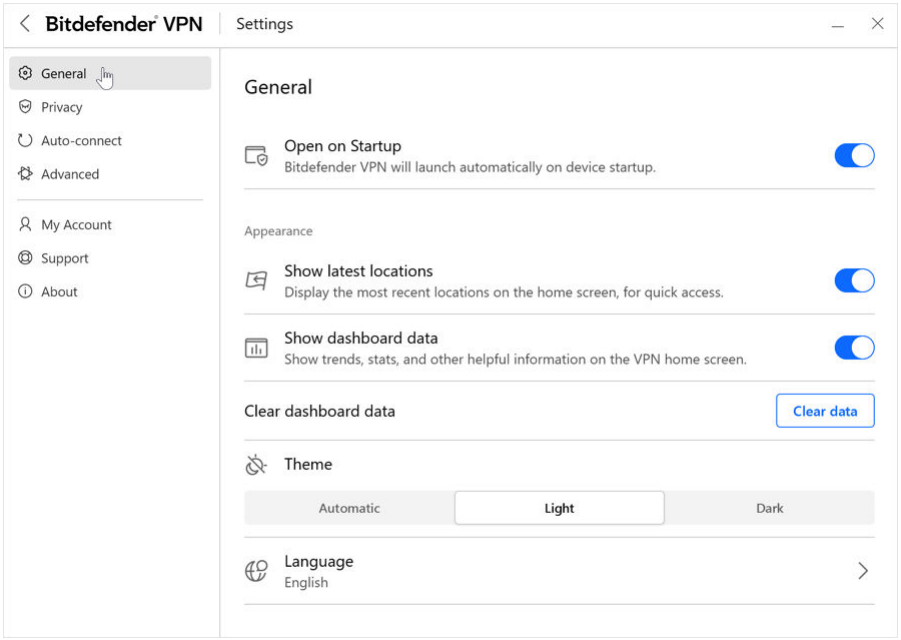
- **Op iOS**
  1. Open de Bitdefender VPN app op uw apparaat.
  2. Klik op de tandwielknop in de rechterbovenhoek van de Bitdefender VPN koppel.

5.2. Algemeen

Hier kunt u het volgende wijzigen:

- **Openen bij opstarten**– Bitdefender VPN wordt automatisch gestart bij het opstarten van het apparaat.

- **Toon nieuwste locaties**– Geef de meest recente locaties op het startscherm weer, voor snelle toegang.
- **Dashboardgegevens weergeven** – Toon trends, statistieken en andere nuttige informatie op het VPN-startscherm.
- **Duidelijke dashboardgegevens**– Al uw dashboardgegevens worden gewist en alle tellers worden gereset.
- **Thema**– Licht/donker thema
- **Taal**– Wijzig de taal van Bitdefender VPN.
- **Meldingen**– Beheer uw meldingsvoorkeuren.
- **Help Bitdefender VPN te verbeteren**– Dien anonieme productrapporten in om ons te helpen uw ervaring te verbeteren.
- **Reset alle instellingen**– Reset de VPN naar de oorspronkelijke instellingen zonder deze opnieuw te installeren.



5.3. Functies

5.3.1. Privacy

Internet-schakelaar

De Internet-schakelaar is een nieuwe voorziening in Bitdefender VPN. Wanneer ingeschakeld, heft deze voorziening al het internetverkeer tijdelijk op indien de VPN-verbinding wordt verbroken. Zodra u terug online bent, wordt de verbinding opnieuw tot stand gebracht.

Om de Internet-schakelaar te activeren, volgt u de onderstaande stappen:

- **Op Windows**
  1. Open de app voor Bitdefender VPN op uw apparaat door in het systeemvak te dubbelklikken op het pictogram ervan of door er met de rechtermuisknop op te klikken en **Weergeven** te selecteren.
  2. Klik op de **Instellingen** -knop (weergegeven door een tandwiel) aan de linkerkant van de interface.
  3. Selecteer **Geavanceerd**.
  4. Schakel de optie **Internet-schakelaar** in.

- **Op Android**
  1. Open de Bitdefender VPN app op uw apparaat.
  2. Klik op de tandwielknop in de rechterbovenhoek van de Bitdefender VPN koppel.
  3. Schakel onder **Instellingen** de optie **Kill-Switch** in.

- **Op iOS**
  1. Open de Bitdefender VPN app op uw apparaat.
  2. Klik op de tandwielknop in de rechterbovenhoek van de Bitdefender VPN koppel.
  3. Onder **Instellingen**, schakel de **Dodemansknop** keuze.

> **Opmerking**
> Deze functie is ook beschikbaar voor macOS-apparaten met besturingssysteem 10.15.4 of latere versies.

Advertentieblokker en anti-tracker

Deze functies zijn ontworpen om u te helpen privé te blijven en van het web te genieten zonder vervelende advertenties of bedrijven die bij u binnengluren. Ze helpen bij het blokkeren van advertenties en het stoppen van online trackers.

Advertentieblokker

De **advertentieblokker** wordt gebruikt om advertenties, popups, luide videoadvertenties of reclamebanners te blokkeren tijdens het surfen. Dit helpt websites sneller te laden, schoner te zijn en ook veiliger om mee te werken.

Om de Advertentieblokker in te schakelen:

1. Zoek de functie **Advertentieblokker en anti-tracker** in **Instellingen**.
2. Zet de schakelaar in de stand **AAN**.

Anti-tracker

De **Anti-tracker** wordt gebruikt om trackers te blokkeren die door adverteerders zijn ingesteld om u online te volgen en te profileren. Sommige websites kunnen storingen vertonen wanneer trackers worden geblokkeerd, maar door de URL aan de whitelist toe te voegen, kan dit worden verholpen.

Om de Anti-tracker in te schakelen:

1. Zoek de **Adblocker en Antitracker** functie in **Instellingen**.
2. Zet de schakelaar op de **OP** positie.

Witte lijst

Sommige websites worden mogelijk niet goed geladen als u hun trackercode en advertenties blokkeert. Door de URL's van deze specifieke domeinen aan de witte lijst toe te voegen, kunt u dit probleem oplossen, maar houd er wel rekening mee dat u tijdens het surfen op deze websites advertenties te zien krijgt en dat hun trackercode actief zal zijn.

Voeg websites toe die u wilt toelaten om advertenties te tonen en trackers te gebruiken door:

1. Zoek de **Adblocker en Antitracker** functie in **Instellingen**.

2. Klik op de koppeling **Beheren**. Ga vervolgens naar de Whitelist-sectie van het venster en klik op de bijbehorende koppeling **Beheren**.
3. Klik op **Website toevoegen** en voeg de gewenste URL in.

5.3.2. Automatisch verbinden

Als u onderweg bent, in een coffee shop gaat werken of in de luchthaven wacht, kan het de snelste oplossing zijn om een verbinding te maken met een openbaar draadloos netwerk om betalingen te doen, e-mails te lezen of sociale netwerkaccounts te raadplegen. Maar er kunnen nieuwsgierige ogen zijn, die uw persoonlijke gegevens proberen te stelen en kijken hoe de informatie door het netwerk heen druppelt.

Om u te beschermen tegen de gevaren van niet-beveiligde of niet-versleutelde openbare draadloze hotspots, omvat Bitdefender VPN de voorziening 'automatisch verbinden'. Dit betekent dat Bitdefender VPN in bepaalde omstandigheden automatisch kan worden geactiveerd, afhankelijk van uw voorkeuren en van het besturingssysteem dat u gebruikt.

- In **Windows en macOS** kan de voorziening automatisch verbinden voor de volgende omstandigheden worden ingeschakeld:
  - **Opstart:** Verbind het VPN bij het opstarten van Windows.
  - **Onbeveiligde wifi:** Gebruik het VPN wanneer u verbinding maakt met openbare of onbeveiligde wifi-netwerken.
  - **Peer-to-peer apps:** Maak verbinding met het VPN wanneer u een peer-to-peer app voor het delen van bestanden start.
  - **Apps en domeinen:** Gebruik het VPN altijd voor bepaalde apps en websites.

    Opmerking

    1. Klik op de koppeling **Beheren**.
    2. Blader naar de locatie van de app waarvoor u VPN wilt gebruiken, selecteer de naam van de app en klik vervolgens op **Toevoegen**.

  - **Websitecategorieën:** Maak verbinding met het VPN wanneer u specifieke websitecategorieën bezoekt. Bitdefender VPN kan automatisch verbinding maken voor de volgende websitecategorieën:

- Financiën
- Online betalingen
- Gezondheid
- File sharing
- Online dating
- Inhoud voor volwassenen

> **Opmerking**
> Voor elke categorie kunt u een andere server selecteren waarmee het VPN verbinding moet maken.

- In **macOS** kan de voorziening automatisch verbinden voor de volgende omstandigheden worden ingeschakeld:
  - **Opstart:** Verbind het VPN bij het opstarten van macOS.
  - **Onbeveiligde wifi:** Gebruik de VPN wanneer u verbinding maakt met openbare of onbeveiligde Wi-Fi-netwerken.
  - **Peer-to-peer-apps:** Maak verbinding met de VPN wanneer u een peer-to-peer-app voor het delen van bestanden start.
  - **Toepassingen:** Verbind het VPN altijd voor bepaalde apps.
- In **Android** en **iOS** kan Bitdefender VPN worden ingesteld om enkel automatisch verbinding te maken wanneer u een openbaar of niet-beveiligd wifinetwerk gebruikt.

5.3.3. Geavanceerd

Split-tunneling

Met de split tunneling van het Virtual Private Network (VPN) kunt u een deel van uw applicatie- of apparaatverkeer door een versleuteld VPN leiden, terwijl andere applicaties of apparaten rechtstreeks toegang hebben tot het internet. Dit is vooral nuttig als u wilt profiteren van diensten die het best presteren wanneer uw locatie bekend is, terwijl u ook veilige toegang hebt tot potentieel gevoelige communicatie en gegevens.

Door de functie **Split tunneling** in te schakelen, zullen geselecteerde apps en websites het VPN omzeilen en rechtstreeks toegang krijgen tot het internet.

Om de toepassingen en websites te beheren die het VPN omzeilen:

1. Klik op de koppeling **Beheren** zodra de functie is ingeschakeld.
2. Klik op de knop **Toevoegen**.
3. Blader naar de locatie van de betreffende app of voeg de URL van de gewenste website in en klik vervolgens op **Toevoegen**.

> **Opmerking**
> Door het toevoegen van een website wordt het hele domein, inclusief alle subdomeinen, omzeild.

> **Belangrijk**
> Op **macOS** apparaten is de functie Split tunneling alleen beschikbaar voor websites.

App Traffic Optimizer

Met de App Traffic Optimizer van Bitdefender VPN kunt u prioriteit geven aan verkeer naar de belangrijkste apps op uw apparaat zonder uw verbinding bloot te stellen aan privacyrisico's. VPN's leiden het internetverkeer om via een veilige tunnel en gebruiken robuuste versleutelingsalgoritmen om het te beschermen.

Deze combinatie van technieken kan echter enkele nadelen hebben, vooral wat de snelheid van de verbinding betreft. Verschillende factoren kunnen leiden tot vertragingen van de verbinding, de meest voorkomende zijn de afstand tot de server waarmee u verbinding maakt, netwerkcongestie en een hoog bandbreedtegebruik. Als u ooit het gevoel hebt gehad dat Bitdefender VPN uw verbinding soms onnodig belast en vertragingen u voortdurend in de weg zitten, is er misschien een beter antwoord dan de verbinding verbreken.

Hoe werkt App Traffic Optimizer?

Bepaalde apps en diensten zoals streamingplatforms, torrent clients en games vereisen meer bandbreedte. Het constante gebruik ervan kan de snelheid van uw internetverbinding beïnvloeden. Routering van uw verkeer door een VPN-tunnel onderwerpt uw verbinding al aan een

relatieve vertraging. Uw verbinding extra belasten kan uw online ervaring ernstig verslechteren.

De App Traffic Optimizer-functie van Bitdefender VPN kan u helpen vertragingen van de VPN-verbinding aan te pakken door voorrang te geven aan de app van uw keuze. De functie laat u beslissen welke apps het grootste deel van uw verkeer moeten ontvangen en wijst de middelen dienovereenkomstig toe. Als u bijvoorbeeld in een vergadering zit en merkt dat de kwaliteit van uw gesprek ondermaats is, kunt u met App Traffic Optimizer prioriteit geven aan de videoconferentie-app voor betere resultaten.

Meestal nemen VPN-gebruikers hun toevlucht tot het sluiten van alle storende processen op hun apparaat of schakelen ze zelfs hun VPN-verbinding uit om een snellere internetsnelheid te krijgen. App Traffic Optimizer laat u genieten van ononderbroken privacybescherming zonder afbreuk te doen aan uw verbindingssnelheid.

App Traffic Optimizer gebruiken

Momenteel is de functie alleen beschikbaar op Windows-apparaten en kunt u prioriteit geven aan maximaal 3 toepassingen.

Volg deze stappen om het met minimale inspanning in te schakelen en te configureren:

1. Start de Bitdefender VPN applicatie op uw Windows computer.
2. Klik op de knop in de zijbalk om de instellingen van het VPN te openen.
3. Ga naar het tabblad **Algemeen** en schakel de functie **App Traffic Optimizer** in. De kleur van de schakelaar zal veranderen van grijs naar blauw.

Om de toepassingen te beheren die van deze functie prioriteit krijgen:

1. Klik op de**Beheren**koppeling.
2. Blader naar de locatie van de app waarvoor u het verkeer wilt optimaliseren, selecteer de naam van de app en klik vervolgens op **Toevoegen**. De app verschijnt in de sectie **Met prioriteit**.

> **Opmerking**
> Als u de toepassing waaraan u prioriteit wilt geven onlangs hebt geopend, kunt u ook op de + knop drukken in het venster App Traffic Optimizer.

3. Verbreek de verbinding en maak opnieuw verbinding met Bitdefender VPN na het toevoegen of verwijderen van apps uit de lijst.

Om een app uit App Traffic Optimizer te verwijderen, klikt u gewoon op het pictogram naast de naam van de app.

> **Opmerking**
> De App Traffic Optimizer is niet beschikbaar op macOS.

Protocol

Hier kunt u het type protocol kiezen dat u voor de gegevensoverdracht wilt gebruiken. De volgende opties zijn beschikbaar:

- **Automatisch** - Bitdefender VPN selecteert het optimale protocol voor uw specifieke apparaat en netwerk.
- **Hydra-katapult** - Snel en veilig, ideaal voor streaming en gaming.
- **OpenVPN-UDP** - Geoptimaliseerd voor hoge snelheden. Dit protocol is echter niet zo betrouwbaar in termen van gegevensverlies als andere protocollen in de lijst.
- **OpenVPN-TCP** - Ontworpen voor betrouwbaarheid. Zorgt ervoor dat uw gegevens volledig worden geleverd, maar is niet zo snel als OpenVPN UDP.
- **Draadbeschermer** - Nieuwer protocol, dat krachtige beveiliging en een hoog prestatieniveau biedt.

Dubbele hop

Met deze functie kunt u de servers beheren waarlangs uw internetverkeer moet worden verzonden en dubbel gecodeerd. Uw gegevens gaan via twee VPN-servers in plaats van één, waardoor het moeilijker wordt om uw internetactiviteit te volgen.

Opmerking

Je kunt in totaal slechts 5 double-hop-locaties toevoegen. U kunt echter op elk gewenst moment de aangepaste dubbele hops in uw lijst verwijderen en andere maken.

Belangrijk

Het gebruik van servers op verschillende continenten in dezelfde double-hop kan uw verbindingssnelheid vertragen.

6. BITDEFENDER VPN WORDT GEDE-INSTALLEERD

De procedure om Bitdefender VPN te verwijderen, is vergelijkbaar met de procedure om andere programma's van uw computer te verwijderen:

- **Bitdefender VPN wordt gede-installeerd van Windows-apparaten**
  - In **Windows 7**:
    1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
    2. Zoek **Bitdefender VPN** en selecteer De-installeren.
       Wacht tot de de-installatieproces is voltooid.
  - In **Windows 8** en **Windows 8.1**:
    1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
    2. Klik op **Een programma de-installeren** of **Programma's en Functies**.
    3. Vinden **Bitdefender VPN** en selecteer **Verwijderen**.
       Wacht tot het verwijderingsproces is voltooid.
  - In **Windows 10** en **Windows 11**:
    1. Klik op **Start**, klik dan op **Instellingen**.
    2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
    3. Vinden **Bitdefender VPN** en selecteer **Verwijderen**.
    4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
       Wacht tot het verwijderingsproces is voltooid.
- **Wordt gede-installeerd van macOS-apparaten**
  1. Klik op **Ga** in de menubalk en selecteer **Toepassingen**.
  2. Dubbelklik op de map **Bitdefender**.
  3. **BitdefenderUninstaller** uitvoeren.

4. In het nieuwe venster vinkt u het vakje naast **Bitdefender VPN** aan en klikt u op **De-installeren**.
5. Voer een geldige beheerdersaccountnaam en -wachtwoord in en klik op **OK**.
6. Er wordt uiteindelijk gemeld dat Bitdefender VPN met succes werd gede-installeerd. Klik op **Sluiten**.

- **Wordt gede-installeerd van Android-apparaten**
  1. Open de app **Play Store**.
  2. Zoek naar **Bitdefender VPN**.
  3. Op de Bitdefender VPN app store pagina, selecteer **De-installeren**.
  4. Bevestig door op **OK** te tikken.
- **Wordt gede-installeerd van iOS-apparaten**
  1. Houd uw vinger op de Bitdefender VPN app.
  2. Kies **App verwijderen**.
  3. Tik op **Verwijderen**.

7. VEELGESTELDE VRAGEN

Wanneer moet ik Bitdefender VPN gebruiken?

U dient voorzichtig te zijn wanneer u inhoud van het internet bekijkt, downloadt of uploadt. Om ervoor te zorgen dat u beveiligd bent wanneer u surft op het internet, raden we aan dat u het VPN gebruikt wanneer u:

- wilt verbinden met publieke draadloze netwerken
- inhoud wilt bekijken die normaal afgeschermd wordt in specifieke gebieden, ongeacht of u thuis of in het buitenland bent
- uw persoonlijke gegevens privé wilt houden (gebruikersnamen, wachtwoorden, e-mailadressen, kredietkaartgegevens enz.)
- uw IP-adres wilt verbergen

Kan ik een stad kiezen met Bitdefender VPN?

Ja. Momenteel kunt u met Bitdefender VPN voor Windows, macOS, Android en iOS een specifieke stad selecteren. Hier is de lijst met de steden die op dit ogenblik beschikbaar zijn:

- **VSA:** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Angeles, Miami, New York, Newark, Phoenix, Portland, San Jose, Seattle, Washington
- **Canada:** Montreal, Toronto, Vancouver
- **VK:** Londen, Manchester

Kan Bitdefender VPN geïnstalleerd worden als alleenstaande toepassing?

De VPN-app wordt automatisch geïnstalleerd naast uw Bitdefender-beveiligingsoplossing. Ze kan ook worden geïnstalleerd als een op zichzelf staande app vanaf de productpagina, via Google Play Store & App Store.

Deelt Bitdefender mijn IP-adres en persoonlijke gegevens met derden?

Nee, met Bitdefender VPN is uw privacy 100% veilig. Niemand (reclamebureaus, internetproviders, verzekeringsmaatschappijen enz.) heeft toegang tot uw online logs.

Welk versleutelingsalgoritme gebruikt het?

Bitdefender VPN gebruikt het Hydra-protocol op alle platformen, 256-bit AES-encryptie of de hoogst beschikbare codering die zowel door de

client als de server wordt ondersteund, met Perfect Forward Secrecy. Dit betekent dat encryptiesleutels voor elke nieuwe VPN-sessie worden gegenereerd en uit het geheugen worden gewist wanneer de sessie voorbij is.

Heb ik toegang tot inhoud die op basis van geo-IP wordt afgeschermd?

Met Premium VPN hebt u toegang tot een uitgebreid netwerk virtuele locaties, overal ter wereld.

Zal het een negatieve invloed hebben op de levensduur van de batterij van mijn apparaat?

Bitdefender VPN is ontworpen om uw persoonlijke gegevens te beschermen, uw IP-adres te verbergen wanneer uw verbonden bent met onbeveiligde draadloze netwerken en om content te bekijken die in bepaalde landen afgeschermd wordt. Om onnodig verbruik van uw batterij te vermijden, raden we u aan VPN enkel te gebruiken indien nodig, en de verbinding te verbreken wanneer u offline bent.

Waarom vertraagt het VPN mijn internetverbinding?

Bitdefender VPN is ontworpen om een lichte ervaring te bieden tijdens het surfen op het web. Afhankelijk van de afstand tussen uw werkelijke locatie en de serverlocatie die u kiest om verbinding mee te maken, wordt enige snelheidsvermindering verwacht, maar deze is bijna altijd zo klein dat deze onopgemerkt blijft tijdens normale online activiteiten. Bovendien maken wij gebruik van een van de snelste VPN-infrastructuren ter wereld. Als het niet absoluut noodzakelijk is om vanaf uw locatie verbinding te maken met een ver weg gehoste server (bijv. van de VS naar Frankrijk), raden wij u aan het VPN toe te staan u automatisch te verbinden met de dichtstbijzijnde server of een server te vinden die dichter bij uw huidige locatie ligt.

8. HULP VRAGEN

8.1. Hulp vragen

Bitdefender biedt zijn klanten een ongeëvenaard niveau van snelle en nauwkeurige ondersteuning. Als u een probleem ondervindt of een vraag hebt over uw Bitdefender-product, kunt u verschillende online bronnen gebruiken om een oplossing of een antwoord te vinden. Tegelijkertijd kunt u contact opnemen met het klantenserviceteam van Bitdefender. Onze ondersteuningsmedewerkers zullen uw vragen tijdig beantwoorden en u de hulp bieden die u nodig hebt.

8.2. Online bronnen

Er zijn meerdere online informatiebronnen beschikbaar om u te helpen bij het oplossen van problemen en vragen met betrekking tot Bitdefender.

- Bitdefender Support Center:
  https://www.bitdefender.nl/consumer/support/
- De Community van Bitdefender-experts:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

U kunt ook uw favoriete zoekmachine gebruiken om meer informatie te zoeken over computerbeveiliging, de Bitdefender-producten en het bedrijf.

8.2.1. Bitdefender Support Center

Het Bitdefender Support Center is een online opslagplaats van informatie over Bitdefender-producten. Hier worden rapporten bijgehouden in een gemakkelijk toegankelijk formaat over de doorlopende technische ondersteuning en activiteiten voor foutoplossingen van de ondersteunings- en ontwikkelingsteams van Bitdefender. Daarnaast vindt u hier ook meer algemene artikels over dreigingspreventie, het beheer van Bitdefender-oplossingen met gedetailleerde uitleg en talrijke andere artikels.

De Bitdefender Support Center is toegankelijk voor het publiek en kan vrij worden doorzocht. De uitgebreide informatie die de database bevat is nog

een middel om BitDefender-klanten de technische kennis en het inzicht te bieden die ze nodig hebben. Alle geldige aanvragen voor informatie of foutrapporten die van BitDefender-klanten komen, vinden uiteindelijk hun weg naar de Bitdefender Support Center als rapporten over het oplossen van problemen, tips om een probleem te omzeilen of informatieve artikels om de helpbestanden van het product aan te vullen.

Het Bitdefender Support Center is te allen tijde beschikbaar op het volgende adres: https://www.bitdefender.nl/consumer/support/.

8.2.2. De Community van Bitdefender-experts

De Community van Experts is een omgeving waar gebruikers, enthousiastelingen en fans van Bitdefender aan kunnen deelnemen, waar ze ideeën kunnen uitwisselen, elkaar kunnen ondersteunen en hun kennis en oplossingen kunnen delen. Het is ook een plaats voor brainstorming en een bron van waardevolle feedback aan onze ontwikkelingsteams. De leden van de gemeenschap zijn ervaren Bitdefender-gebruikers die in hun eigen tijd graag anderen helpen. Met hun enorme bijdrage en oprechte vrijwillige inspanningen hebben we een kennisbank gecreëerd waar gebruikers antwoorden en begeleiding kunnen vinden, maar met dat menselijke tintje.

Hier vindt u zinvolle gesprekken met mensen die Bitdefender gebruiken op hun apparaten. De gemeenschap biedt een echte band met onze leden en laat uw stem horen. Het is een plek waar u wordt aangemoedigd om deel te nemen in de wetenschap dat uw mening en inbreng worden gerespecteerd en gekoesterd. Als gewaardeerde provider streven we ernaar een ongeëvenaard niveau van snelle, accurate ondersteuning te bieden en willen we onze gebruikers dichter bij ons brengen. Wij hebben onze gemeenschap met dit doel voor ogen ontworpen.

U vindt de website van onze Community van experts hier:

https://community.bitdefender.com/en/

8.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia heeft alle informatie die u nodig hebt over de nieuwste cyberdreigingen. Dit is de plaats waar Bitdefender-experts tips en trucs delen over hoe u beschermd kunt blijven tegen hackers, datalekken, identiteitsdiefstal en pogingen tot sociale imitatie.

De webpagina van Bitdefender Cyberpedia vindt u hier:

https://www.bitdefender.com/cyberpedia/.

8.3. Contactinformatie

Efficiënte communicatie is de sleutel tot succes. Sinds 2001 heeft BITDEFENDER een onberispelijke reputatie opgebouwd door voortdurend te streven naar een betere communicatie om de verwachtingen van onze klanten en partners telkens te overtreffen. Aarzel daarom niet om rechtstreeks contact met ons op te nemen als u iets wilt vragen, via onze Bitdefender Support Center.

https://www.bitdefender.nl/consumer/support/

8.3.1. Lokale verdelers

De lokale BitDefender-verdelers zijn altijd paraat om te reageren op aanvragen met betrekking tot hun bedrijfsgebied, zowel op commercieel als algemeen vlak.

Om een Bitdefender-verdeler te vinden in uw land:

1. Ga naar https://www.bitdefender.com/partners/partner-locator.html.
2. Kies uw land en stad met de overeenkomstige opties.

WOORDENLIJST

Activeringscode

Is een unieke sleutel die u in de handel kunt kopen en die gebruikt wordt om een specifiek product of een dienst te activeren. Met een activeringscode kan een geldig abonnement voor een bepaalde periode en een bepaald aantal toestellen geactiveerd worden en kunt u ook gebruiken om het abonnement te verlengen, op voorwaarde dat het voor hetzelfde product of dezelfde dienst is.

ActiveX

ActiveX is een model voor het schrijven van programma's zodat andere programma's en het besturingssysteem ze kunnen oproepen. De ActiveX-technologie wordt gebruikt bij Microsoft Internet Explorer om interactieve Webpagina's te maken die eruitzien en zich gedragen als computerprogramma's in plaats van statische pagina's. Met ActiveX kunnen gebruikers vragen stellen of beantwoorden, drukknoppen gebruiken en op andere manieren interactief omgaan met de Webpagina. ActiveX-besturingselementen zijn vaak geschreven met de hulp van Visual Basic. ActiveX is berucht door een compleet gebrek aan beveiligingscontroles; computerbeveiligingsexperts raden het gebruik ervan via het internet sterk af.

Advanced persistent threat

Geavanceerde aanhoudende dreiging (Advanced Persistent Threat - APT) maakt misbruik van kwetsbare plekken in systemen om belangrijke informatie te stelen en aan de bron te leveren. Grote groepen, zoals organisaties, bedrijven of overheden zijn doelgroepen voor deze bedreiging. Het doel van een advanced persistent threat is heel lang onopgemerkt te blijven en belangrijke informatie in te kijken en te verzamelen, zonder de toestellen te beschadigen. De methode die gebruikt wordt om de bedreiging in het netwerk te brengen verloopt via een pdf-bestand of een Office-document dat er onschuldig uitziet, zoadat elke gebruiker de bestanden kan openen.

Adware

Adware wordt vaak gecombineerd met een hosttoepassing die gratis wordt aangeboden op voorwaarde dat de gebruiker akkoord gaat met het uitvoeren van de adware. Omdat adware-toepassingen doorgaans

worden geïnstalleerd nadat de gebruiker een licentieovereenkomst die het doel van de toepassing vermeldt heeft geaccepteerd, wordt er geen inbreuk gepleegd. Pop-upadvertenties kunnen echter irritant worden en in sommige gevallen de systeemprestaties negatief beïnvloeden. De gegevens die door sommige van deze toepassingen worden verzameld, kunnen bovendien privacy-problemen veroorzaken voor gebruikers die niet volledig op de hoogte waren van de voorwaarden van de licentieovereenkomst.

Archive

Een schijf, tape, of map die bestanden bevat waarvan een back-up werd gemaakt.

Een bestand dat één of meer bestanden bevat in een gecomprimeerd formaat.

Backdoor

Een gat in de beveiliging van een systeem, dat opzettelijk werd achtergelaten door ontwikkelaars of beheerders. De motivatie voor dergelijke gaten is niet altijd boosaardig. Sommige besturingssystemen worden bijvoorbeeld geleverd met bevoegde accounts die bedoeld zijn voor gebruik door technici voor service ter plaatse of onderhoudsprogrammeurs van de leverancier.

Boot sector

Een sector aan het begin van elke schijf die de architectuur van de schijf identificeert (sectorgrootte, clustergrootte, enz.) Bij opstartschijven bevat de opstartsector ook een programma dat het besturingssysteem laadt.

Boot virus

Een bedreiging die de opstartsector van een vaste schijf of een diskette infecteert. Wanneer u probeert op te starten vanaf een diskette die geïnfecteerd is met een opstartsectorvirus, zal de bedreiging actief worden in het geheugen. Wanneer u vanaf dat ogenblik uw systeem opstart, zal de bedreigingen telkens in het geheugen geactiveerd zijn.

Botnet

Het woord "botnet" is samengesteld uit de woorden "robot" en "netwerk". Botnets zijn apparaten die met het internet verbonden zijn en met bedreigingen geïnfecteerd zijn en kunnen gebruikt worden om spammail te verzenden, data te stelen, kwetsbare apparaten van op afstand

te controleren of om spyware, ransomware en andere schadelijke bedreigingen te verspreiden. Het doel ervan is zoveel mogelijk apparaten te infecteren, bijvoorbeeld pc's, servers, mobiele of IoT-apparaten die eigendom zijn van grote bedrijven of sectoren.

Browser

De korte naam voor Webbrowser, een softwaretoepassing die wordt gebruikt op Webpagina's te zoeken en weer te geven. Populaire browsers omvatten Microsoft Internet Explorer, Mozilla Firefox en Google Chrome. Dit zijn grafische browsers. Dit betekent dat ze zowel grafische beelden als tekst kunnen weergeven. Bovendien kunnen de meeste moderne browsers ook multimedia-informatie voorstellen met geluid en video, hoewel voor sommige formaten plug-ins vereist zijn.

Brute Force-aanval

Aanval via raden van wachtwoord, gebruikt om in te breken in een computersysteem door mogelijke wachtwoordcombinaties in te geven, meestal te beginnen met het meest eenvoudig te raden wachtwoord.

Opdrachtregel

In een opdrachtregelinterface typt de gebruiker opdrachten in opdrachttaal rechtstreeks op het scherm in de ruimte die hiervoor wordt geboden.

Cookies

Binnen de Internetindustrie worden cookies beschreven als kleine programma's die informatie bevatten over individuele computers, die door adverteerders wordt geanalyseerd en gebruikt om uw on line interesse en smaak te volgen. De cookietechnologie wordt in dit kader nog steeds verder ontwikkeld met het doel reclameberichten rechtstreeks te richten op de interesses die u hebt meegedeeld. Dit is voor veel mensen een mes dat aan twee kanten snijdt. Aan de ene kant is het efficiënt en relevant aangezien u alleen reclames ontvangt voor zaken waarvoor u interesse hebt. Aan de andere kant betekent het ook dat elke plaats die u bezoekt en alles wat u aanklikt wordt "opgespoord" en "gevolgd". Het is dan ook te begrijpen dat er heel wat wordt gedebatteerd over privacy. Bovendien zijn veel mensen verontwaardigd omdat ze het gevoel hebben dat ze als een "SKU-nummer" worden beschouwd (u weet wel, de barcode op de verpakkingen die bij de kassa van het warenhuis wordt gescand). Hoewel dit standpunt misschien nogal extreem is, is het vaak een bijzonder nauwkeurige omschrijving.

Cyberpesten

Wanneer collega's of onbekenden met opzet onrechtmatige daden stellen tegenover kinderen, met de bedoeling om fysiek te kwetsen. Om emotionele schade te berokkenen, sturen de daders gemene berichten of onflatteuze foto's om hun slachtoffers af te zonderen van anderen of gefrustreerd te doen voelen.

Woordenboekaanval

Aanval via raden van wachtwoord, gebruikt om in te breken in een computersysteem door een combinatie van veel voorkomende woorden in te geven om zo mogelijke wachtwoorden te genereren. Dezelfde methode wordt gebruikt om decryptiesleutels van versleutelde berichten of documenten te raden. Woordenboekaanvallen slagen in hun opzet omdat veel mensen korte wachtwoorden gebruiken die uit slechts één woord bestaan en die makkelijk te raden zijn.

Schijfstation

Dit is een apparaat dat gegevens leest van en schrijft naar een schijf. Een harde-schijfstation leest en schrijft harde schijven. Een diskettestation opent diskettes. Schijfstations kunnen intern (binnen de behuizing van een computer) of extern zijn (in een afzonderlijke behuizing die op de computer wordt aangesloten).

Download

Om gegevens (meestal een volledig bestand) te kopiëren van een hoofdbron naar een randapparaat. De term wordt vaak gebruikt om het proces te beschrijven waarbij een bestand van een on line-service wordt gekopieerd naar de eigen computer. Downloaden kan ook verwijzen naar het kopiëren van een bestand van een netwerkbestandsserver naar een computer in het netwerk.

E-mail

Elektronische post. Een dienst die berichten naar computers verzendt via lokale of globale netwerken.

Gebeurtenissen

Een actie of gebeurtenis die door een programma wordt gedetecteerd. Gebeurtenissen kunnen gebruikersacties zijn, zoals het klikken met de muis of het indrukken van een toets, of systeemgebeurtenissen, zoals een tekort aan geheugen.

Exploits

Een manier om misbruik te maken van verschillende bugs of kwetsbaarheden in een computer (software of hardware). Zo kunnen hackers de controle over computers of over netwerken in handen krijgen.

Vals positief

Doet zich voor wanneer een scanner een bestand ten onrechte beschouwt als geïnfecteerd.

Bestandsextensie

Het gedeelte van een bestandsnaam achter de punt, waarmee het gegevenstype dat in het bestand is opgeslagen wordt aangeduid. Heel wat besturingssystemen, zoals Unix, VMS en MS-DOS, maken gebruik van bestandsextensies. Ze gebruiken doorgaans één tot drie letters (sommige betreurenswaardige oude besturingssystemen ondersteunen niet meer dan drie letters). Voorbeelden hiervan zijn "c" voor C-broncode, "ps" voor PostScript, "txt" voor tekst zonder opmaak.

Heuristisch

Een methode voor het identificeren van nieuwe bedreigingen op basis van regels. Deze scanmethode is niet gebaseerd op een specifieke informatie-database voor bedreigingen. Het voordeel van de heuristische scan is dat hij zich niet laat misleiden door een nieuwe variant van een bestaande bedreiging. Dit type kan echter af en toe een verdachte code rapporteren in normale programma's, zodat de zogenoemde "valse positieve" rapporten worden gegenereerd.

Honeypot

Een afleiding in uw computersysteem dat hackers aantrekt om te onderzoeken hoe ze te werk gaan en de afwijkende methodes die ze gebruiken om systeeminformatie te verzamelen, te identificeren. Bedrijven zijn steeds meer geïnteresseerd om honingpotten te implementeren en te gebruiken om hun algemene beveiligingsstatus te verbeteren.

IP

Internet Protocol - Een routeerbaar protocol in de TCP/OP-protocolreeks die verantwoordelijk is voor de IP-adressering, routing en de fragmentatie en defragmentatie van IP-pakketten.

Java applet

Een Java-programma dat is ontwikkeld om alleen op een webpagina te worden uitgevoerd. Om een applet op een webpagina te gebruiken, zou u de naam van het applet opgeven en de grootte (lengte en breedte in pixels) die het applet kan gebruiken. Wanneer de webpagina wordt geopend, downloadt de browser het applet van een server en voert hij het uit op de computer van de gebruiker (de client). Applets onderscheiden zich van toepassingen omdat ze worden beheerd door een streng beveiligingsprotocol.

Zelfs wanneer applets op de client worden uitgevoerd kunnen ze, bijvoorbeeld, geen gegevens lezen van of schrijven naar de computer van de client. Bovendien worden applets verder beperkt zodat ze alleen gegevens kunnen lezen van en schrijven naar hetzelfde domein waarvan ze worden bediend.

Keylogger

Een keylogger is een toepassing die alles wat u typt, logt. Keyloggers zijn in wezen niet kwaadaardig. Ze kunnen worden gebruikt voor rechtmatige doeleinden, zoals het bewaken van de activiteiten van werknemers of kinderen. Ze worden echter steeds meer gebruikt door cybercriminele voor boosaardige doeleinden (bijv. voor het verzamelen van persoonlijke gegevens, zoals aanmeldingsgegevens en nummer van de sociale zekerheid).

Macro virus

Een type computerbedreiging die is gecodeerd als een macro die in een document is ingesloten. Talrijke toepassingen, zoals Microsoft Word en Excel, ondersteunen krachtige macrotalen. Met deze toepassingen kan u een macro in een document insluiten, en die macro telkens laten uitvoeren wanneer het document wordt geopend.

Mail client

Een e-mailclient is een toepassing waarmee u e-mail kunt verzenden en ontvangen.

Geheugen

Interne opslaggebieden in de computer. De term geheugen staat voor gegevensopslag die in de vorm van chips wordt geleverd. Het woord opslag wordt gebruikt voor geheugen dat aanwezig is op tapes of schijven. Elke computer wordt geleverd met een bepaalde hoeveelheid fysiek geheugen, dat meestal het hoofdgeheugen of RAM wordt genoemd.

Niet-heuristisch

Deze scanmethode is gebaseerd op een specifieke informatie-database voor bedreigingen. Het voordeel van de niet-heuristische scan is dat deze zich niet laat misleiden door iets dat kan lijken op een bedreiging en geen vals alarm genereert.

Online predatoren

Personen die minderjarigen of adolescenten met opzet willen betrekken in gesprekken, om hen zo te betrekken in illegale seksuele activiteiten. Sociale netwerken zijn de ideale plaats waar kwetsbare kinderen gemakkelijk kunnen worden verleid om seksuele activiteiten uit te voeren, online of tijdens fysieke ontmoetingen.

Ingepakte programma's

Een bestand in een gecomprimeerd formaat. Talrijke besturingssystemen en toepassingen beschikken over opdrachten waarmee u bestanden kunt inpakken, zodat ze minder geheugen in beslag nemen. Veronderstel bijvoorbeeld dat u een tekstbestand hebt dat tien opeenvolgende spatietekens bevat. Normaal zou dit tien bytes opslagruimte vereisen.

Een programma dat bestanden inpakt kan echter de spatietekens vervangen door een speciaal spatiereeks-teken, gevolgd door het aantal spaties dat wordt vervangen. In dit geval hebben de tien spaties slechts twee bytes nodig. Dit is slechts één inpaktechniek, maar er zijn er veel meer.

Pad

De exacte weg naar een bestand op een computer. Deze weg wordt doorgaans beschreven door middel van het hiërarchische bestandssysteem van boven naar beneden.

De route tussen twee willekeurige punten, zoals het communicatiekanaal tussen twee computers.

Phishing

Het onder valse voorwendselen verzenden van een e-mail aan een gebruiker, waarbij de indruk wordt gewekt dat het bericht afkomstig is van een bestaande onderneming, in een poging de gebruiker persoonlijke gegevens te ontfutselen die zullen worden gebruikt voor identiteitsroof. In het e-mailbericht wordt de gebruiker doorverwezen naar een website waar persoonlijke gegevens kunnen worden bijgewerkt,

zoals wachtwoorden en creditcard-, sofi- en bankrekeningnummers, die reeds in het bezit zijn van de rechtmatige organisatie. De website is echter nep en alleen opgezet om de gebruikersgegevens te stelen.

Foton

Photon is een vernieuwende, niet opdringerige Bitdefender technologie, ontworpen om de invloed van uw beveiligingsoplossing op de prestaties te beperken. Door de activiteit van uw pc's op de achtergrond te bewaken, maakt het gebruikspatronen die helpen opstart- en scanprocessen te optimaliseren.

Polymorf virus

Een bedreiging die zijn vorm wijzigt bij elk bestand dat het infecteert. Aangezien ze geen consequent binair patroon hebben, zijn dergelijke bedreigingen moeilijk te identificeren.

Poort

Een interface op een computer waarop u een apparaat kan aansluiten. PC's hebben verschillende types poorten. Intern zijn er verschillende poorten voor het aansluiten van schijfstations, beeldschermen en toetsenborden. Extern beschikken PC's over poorten voor het aansluiten van modems, printers, muizen en andere randapparatuur.

Bij TCP/IP- en UDP-netwerken, zijn ze een eindpunt voor een logische verbinding. Het poortnummer duidt aan over welk type poort het gaat. Poort 80 wordt bijvoorbeeld gebruikt voor HTTP-verkeer.

Ransomware

Ransomware is kwaadaardige software waarmee criminelen proberen geld af te persen van gebruikers, door hun systemen ontoegankelijk te maken totdat er losgeld is betaald. Enkele van de vele varianten van ransomware voor persoonlijke computersystemen zijn CryptoLocker, CryptoWall en TeslaWall.

De infectie kan verspreid worden door spam-e-mail te openen, e-mailbijlagen te openen of toepassingen te installeren zonder dat de gebruiker weet wat er op zijn systeem gaande is. Dagelijkse gebruikers en bedrijven vormen een doelwit voor ransomwarehackers.

Rapportbestand

Een bestand dat de acties weergeeft die zich hebben voorgedaan. BitDefender houdt een rapportbestand bij met het gescande pad,

het aantal gescande mappen, archieven en bestanden, en het aantal gevonden geïnfecteerde en verdachte bestanden.

Rootkit

Een rootkit is een verzameling softwareprogramma's die op beheerdersniveau toegang biedt tot een systeem. Deze term werd voor het eerst gebruikt voor Unix-besturingssystemen en verwees naar opnieuw gecompileerde hulpprogramma's die beheerdersrechten gaven aan indringers, zodat ze hun aanwezigheid konden verbergen en onzichtbaar bleven voor de echte systeembeheerders.

De belangrijkste functie van rootkits is het verbergen van processen, bestanden, logins en logbestanden. Rootkits die de hiervoor benodigde software bevatten, kunnen ook gegevens onderscheppen van terminals, netwerkverbindingen of randapparaten.

Rootkits zijn in wezen niet kwaadaardig. Systemen en zelfs sommige toepassingen verbergen kritieke bestanden met de hulp van rootkits. Ze worden echter het vaakst gebruikt om bedreigingen of de aanwezigheid van een indringer op het systeem te verbergen. In combinatie met bedreigingen, vormen rootkits een ernstige bedreiging voor de integriteit en beveiliging van een systeem. Ze kunnen het verkeer controleren, achterpoortjes in het systeem maken, bestanden en logboeken wijzigen en detectie vermijden.

Script

Script, een andere term voor een macro of batchbestand, is een lijst opdrachten die kunnen worden uitgevoerd zonder tussenkomst van de gebruiker.

Spam

Elektronische junkmail of berichten van junknieuwsgroepen. Algemeen bekend als ongewenste e-mail.

Spyware

Elke software die heimelijk gebruikersgegevens verzamelt via de internetverbinding van de gebruikers zonder dat hij/zij zich hiervan bewust is, doorgaans voor reclamedoeleinden. Spywaretoepassingen worden doorgaans gebundeld als een verborgen onderdeel van freeware- of sharewareprogramma's die kunnen worden gedownload van het internet. We moeten echter wel vermelden dat de meeste shareware- en freewaretoepassingen geen spyware bevatten. Zodra de spyware is

geïnstalleerd, worden de activiteiten van de gebruiker op het internet gevolgd en wordt deze informatie op de achtergrond naar iemand anders doorgestuurd. Spyware kan ook informatie verzamelen over e-mailadressen en zelfs wachtwoorden en creditcardnummers.

Spyware is vergelijkbaar met een Trojaans paard omdat gebruikers ook in dat geval het product onbewust installeren wanneer ze een ander programma installeren. Een veel voorkomende manier waarbij men het slachtoffer wordt van spyware is bepaalde P2P-programma's voor bestandsuitwisseling te downloaden.

Naast het feit dat deze methode onethisch is en een inbreuk op de privacy van de gebruiker betekent, steelt spyware van de gebruiker door de geheugenbronnen van de computer te gebruiken en bandbreedte te verbruiken wanneer de informatie naar de thuisbasis van de spyware wordt verzonden via de internetverbinding van de gebruiker. Aangezien spyware geheugen- en systeemgeheugen gebruikt, kunnen de toepassingen die op de achtergrond worden uitgevoerd leiden tot systeemfouten of een algemene systeeminstabiliteit.

Startup items

Elk bestand in deze map wordt geopend wanneer de computer wordt gestart. Een opstartitem kan bijvoorbeeld een opstartscherm zijn, een geluidsbestand dat moet worden afgespeeld wanneer de computer voor de eerste maal opstart, een herinneringsagenda of apps. In normale omstandigheden wordt een alias van een bestand in deze map geplaatst, en niet het bestand zelf.

Abonnement

Koopovereenkomst die u het recht heeft om een specifiek(e) product of dienst op een specifiek aantal toestellen en voor een bepaalde tijd te gebruiken. Een vervallen abonnement kan automatisch worden verlengd met gebruik van de informatie van de gebruiker tijdens de eerste aankoop.

Systeemvak

Het systeemvak, dat met Windows 95 werd ingevoerd, bevindt zich in de taakbalk van Windows (doorgaans onderaan naast de klok) en bevat miniatuurpictogrammen die systeemfuncties zoals fax, printer, modem, volume en meer, gemakkelijk toegankelijk maken. Dubbelklik of klik met de rechtermuisknop op een pictogram om de details en de besturingselementen te bekijken en te openen.

TCP/IP

Transmission Control Protocol/Internet Protocol - Een reeks netwerkprotocollen, wijdverspreid gebruikt op het internet, die communicatie bieden tussen onderling verbonden computernetwerken met verschillende hardware-architecturen en diverse besturingssystemen. TCP/IP bevat standaarden voor de manier waarop computers communiceren en regels voor het aansluiten van netwerken en het routeren van het verkeer.

Dreiging

Een programma of een deel van een code die op uw computer wordt geladen zonder uw medeweten en tegen uw wil wordt uitgevoerd. De meeste bedreigingen kunnen zichzelf ook dupliceren. Alle computerbedreigingen zijn door de mens gemaakt. Een eenvoudige bedreiging die zichzelf steeds opnieuw kan dupliceren is relatief eenvoudig te maken. Zelfs een dergelijke eenvoudige bedreiging is gevaarlijk aangezien het snel al het beschikbare geheugen zal opgebruiken en het systeem zal blokkeren. Een nog gevaarlijker type is een bedreiging die in staat is zichzelf te verzenden via netwerken en beveiligingssystemen te omzeilen.

informatie-updates van dreigingen

Het binaire patroon van een bedreiging, gebruikt door de beveiligingsoplossing om de bedreiging te detecteren en te verwijderen.

Trojaans paard

Een destructief programma dat zich voordoet als een goedaardige toepassing. In tegenstelling tot kwaadaardige softwareprogramma's en wormen, vermenigvuldigen Trojaanse paarden zich niet, maar ze kunnen even vernietigend zijn. Een van de meest verraderlijke bedreigingstypes van de Trojaanse paarden is een programma dat beweert dat het uw computer kan bevrijden van bedreigingen, maar dat in werkelijkheid bedreigingen op uw computer installeert.

De naam komt uit een verhaal uit de Ilias van Homerus. De Grieken schonken hun vijanden, de Trojanen, een reusachtig houten paard, zogenaamd als vredesgebaar. Maar nadat de Trojanen het paard binnen de stadsmuren hadden gesleept, kwamen de Griekse soldaten uit de holle romp van het paard tevoorschijn en openden ze de poorten van de stad, zodat hun landgenoten Troje konden binnendringen en veroveren.

Update

Een nieuwe versie van een software- of hardwareproduct, dat werd ontwikkeld om een oudere versie van hetzelfde product te vervangen. Daarnaast zullen de installatieroutines voor updates vaak controleren of er reeds een oudere versie van het product op uw computer is geïnstalleerd. Is dat niet het geval, dan kunt u de update niet installeren.

Bitdefender heeft zijn eigen updatefunctie waarmee u handmatig kunt controleren op updates of die het product automatisch kan updaten.

Virtueel privénetwerk (VPN)

Dit is een technologie die een tijdelijke en versleutelde rechtstreekse verbinding met een zeker netwerk over een minder beveiligd netwerk mogelijk maakt. Op die manier is het verzenden en ontvangen van data veilig en versleuteld, zodat ze moeilijk te vangen is door spionnen. Een bewijs van veiligheid is de authentificatie, die enkel mogelijk is via een gebruikersnaam en wachtwoord.

Worm

Een programma dat zich verspreidt via een netwerk en zichzelf ondertussen reproduceert. Dit type kan zich niet vasthechten aan andere programma's.