

Bitdefender®

Bitdefender Technology Alliance Partner (TAP) Program Guide



Trusted. Always.

Bitdefender®



Bitdefender Technology Alliance Partner (TAP) Program Overview

Introduction

The Bitdefender TAP program was created to make cyber security better for our customers through validated interoperability. Cyber Security is an inherently promiscuous business where customers typically use dozens of vendors' solutions simultaneously and want them to interoperate. As a result, customers demand extensibility in the security products they buy.

Today, almost all vendors offer integration points in their products and platforms in the form of public and private APIs and customers are generally free to innovate and build on these integration points but rarely have enough time and resources. They expect complementary vendors to organize and deliver enhanced security and operational efficiency.

Program Goals

This program aims to make **building, testing, validating and documenting interoperability** between partner technologies and the Bitdefender platform as easy as possible and to make detailed information about the partner ecosystem and the catalogue of joint customer benefits easily accessible on a public facing website.

When considering new partnerships and integration use cases we ask if the work we do will **improve security efficacy, reduce time to detection and lower total cost of ownership**. Will it help our sellers win by removing friction and making our solutions a better fit? If the answer is yes for any of these questions, then let's partner!

This Guide

The purpose of this guide is to bootstrap our partnership and save you time looking for important documentation. We will update it as often as needed and your feedback is always appreciated.

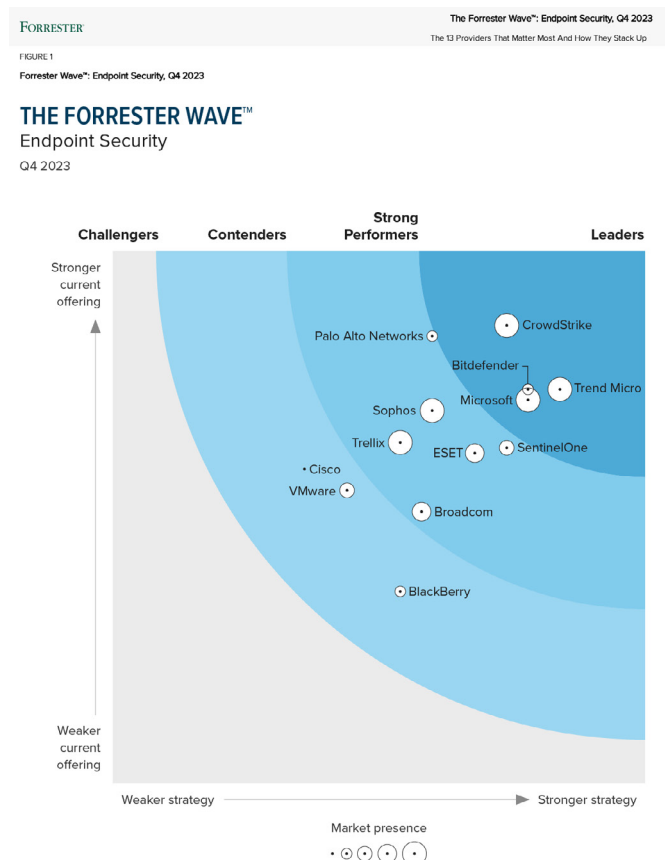
Bitdefender and the Platform

About the Company

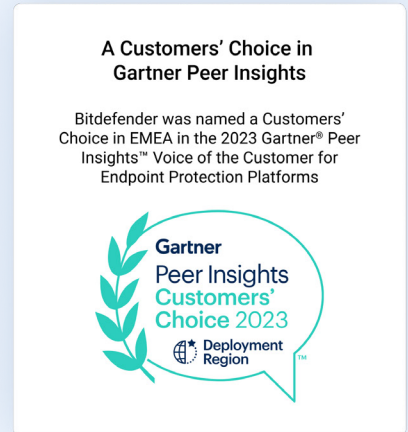
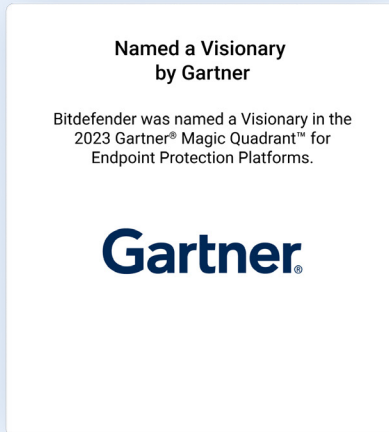
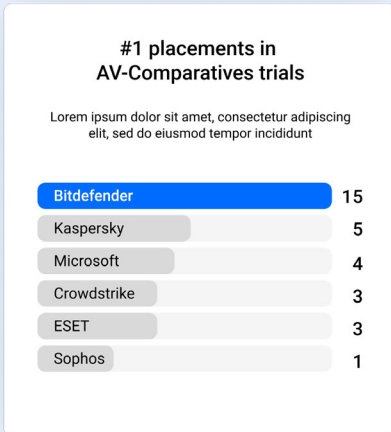
Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioural analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Bitdefender's Competitive Edge – Doesn't Everyone want the Best Detection?

- ↳ Unified prevention, protection, detection & response platform
- ↳ Unrivalled threat intelligence
- ↳ Unmatched attack protection
- ↳ Detection and response capabilities available to companies of all sizes
- ↳ Patented tamper-proof ransomware mitigation



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

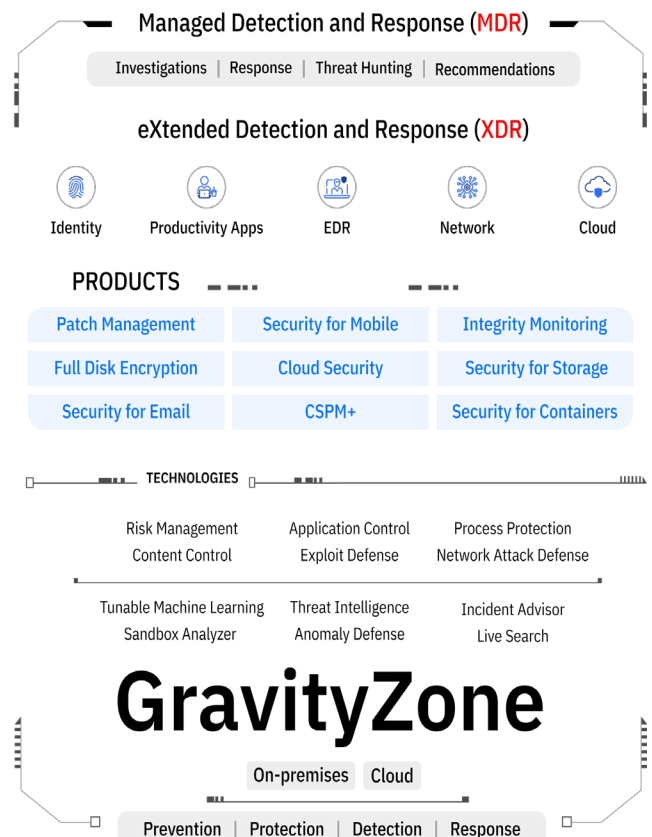


The GravityZone Platform

Bitdefender offers a flexible platform with multiple integration points across its security architecture. The various protocols, interfaces, and APIs available that enable technology partners to seamlessly integrate with Bitdefender are illustrated below. APIs are described in detail in a later section.

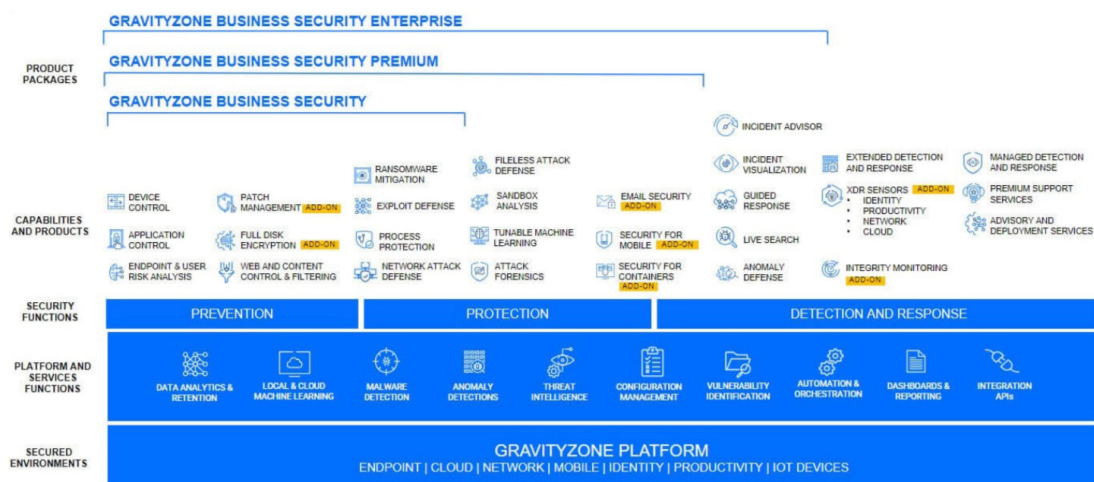
Unified Platform Securing the Entire Organization

- ↳ Maximize Operational Efficiency - Increase in administrative efficiency by up to 70%
- ↳ Stop Attacks More Effectively - Identify and mitigate risks faster, achieve 100% patch compliance, and reduce time to resolve attacks by up to 50%
- ↳ Optimize Security Investments - Optimize your security spend by consolidating vendors and solutions and cutting operational costs by up to 50% without sacrificing effectiveness



Security Layers of Gravity Zone

Bitdefender uses multiple layers of security measures to protect against a wide variety of threats, both anticipated and unexpected. Built on four key pillars - Prevention, Protection, Detection, and Response – the Bitdefender GravityZone security architecture provides a comprehensive set of security technologies with a single point of management. The consolidated approach works to decrease the risk profile of organizations by providing multiple layers of security, the result of which is a higher likelihood of defeating advanced attacks before they cause damage.



Partnering with Bitdefender

Program Features and Benefits

Every technology partnership is different and develops its own personality. Bitdefender's commitment to you as a partner is to consider and discuss all the possible ways to maximize the partnership's impact. Whether we formalize our partnership on the Bitdefender TAP agreement or by signing your partner agreement these are the main features of the Bitdefender program that we bring to the partnership.

Promoting the Partnership

- ↳ Dedicated URL for each partner on Bitdefender's TAP website
- ↳ Reciprocal branding and trademark usage to promote the partnership
- ↳ Access to NFR software and all essential API documentation



Joint Marketing and Selling Opportunities

- ↳ Participation in Field, Channel & Regional Sales Events
- ↳ Events and tradeshow co-sponsorships such as:
 - Lunch-and-learns and targeted user group events
 - Joint Webinars
 - Joint Selling

Collateral that we can Create (in addition to web content)

- ↳ Joint Solution Brief
- ↳ Integration Guide
- ↳ Customer Case Study
- ↳ Product Integration Video
- ↳ Joint White Paper

Go-to-Market Activities

When supported by a good business case there will be opportunities to engage with counterparts, common customers and prospects. We can also consider joint webinars hosted by Bitdefender or your company targeting field sales forces, sales engineers, or channel partners.

Bitdefender Training

At Bitdefender's discretion, Partners will receive access to our internal training system, Learning @ Bitdefender. On-demand training courses and materials are available to partners to enhance their understanding of Bitdefender GravityZone and various professional services. Additional training opportunities can be requested by partners and will be considered and approved case by case.

Brand Guidelines

Like all successful cyber security companies Bitdefender pays special attention to its brand and how it is used. Partners can access branding guidelines including official company logos and guidance on Bitdefender's [branding website](#).

APIs and Integration Points

Logging

Like most cyber technologies that offer detection and protection the Bitdefender portfolio generates high fidelity security alerts and informational logs, and this telemetry can be sent to almost any platform that collects this kind of data.

Bitdefender's GravityZone is the command-and-control platform that provides user interface for management of the endpoint agents and for analysis and incident response. The GravityZone platform and the Bitdefender Endpoint Security Tools (BEST) agent both generate and can send valuable data to SIEMs and other data analytic solutions.

GravityZone sends logs called 'Alerts' and depending on the security modules the customer has purchased and enabled the platform can produce and send any of these events/alerts [described here in detail](#). **GravityZone** has two methods for sending alerts. The data is sent via syslog and in a JSON 2.0 RPC format.

↳ Method 1 (Preferred): **Event Push Service** for SIEMs that have an HTTP Listener.

Helpful links below:

- <https://www.bitdefender.com/business/support/en/77211-135318-push.html>
- <https://www.bitdefender.com/business/support/en/77209-135319-setpusheventsettings.html>

↳ Method 2: **Event Push Service** for SIEMs that do NOT have an HTTP Listener for Gravity Zone Cloud implementations. This requires a connector to support https to Syslog. Helpful link here:

- <https://www.bitdefender.com/business/support/en/77211-463492-generic-integrations-for-siem-platforms-without-https-listeners.html>

Note: On-prem GravityZone deployments can send syslog natively directly from the platform without the need to run a connector on a separate machine or on the target SIEM platform.

Endpoint Agents can send a range of 'raw telemetry' events. These events are not security events but can be very useful when threat hunting or gathering more context around security events generated by GravityZone or other log sources. Configuring endpoints to send this telemetry is done through the GravityZone console and the steps are documented here:

- <https://www.bitdefender.com/business/support/en/77211-135318-push.html>

GravityZone Public API

The Bitdefender Public API is a RESTful API that supports automation and workflows. API calls are performed as HTTP requests with JSON-RPC messages as payload. HTTP POST method MUST be used for each API call. Also, it is required that each HTTP request have the Content-Type header set to application/JSON. Details can for developers be found [here](#).

Important information about dependencies:

- ↳ The **Maintenance** function requires enablement of the Patch Management module.
- ↳ The **Incidents** function requires the enablement of any of the EDR or XDR add-ons.
- ↳ The **Companies** and **Licensing** functions are only available to Resellers and MSPs servicing Bitdefender customers.

Sample Use Cases:

- ↳ **Remediation:** A third-party application can carry out changes on end point agents such as Respond to critical events with blocking actions.
- ↳ **Management:** Manage the GravityZone platform through another application.

GravityZone Cloud Security API – Available when using the CSPM+ module

Bitdefender's Cloud Security API is a RESTful API that allows developers to automate business workflows via the Cloud Security Posture Management product. The API calls are performed as HTTP requests with raw JSON messages as payload. There are both GET and POST endpoints requests available. There are multiple endpoints available, each one targeting distinct areas or functionalities in the product. Details can for developers be found [here](#).



RMM SDK Tools

The Bitdefender RMM SDK Tools is a CLI utility which can be used, together with the Gravity-Zone Public APIs, to instrument the agent integration actions with Bitdefender GravityZone. The Bitdefender RMM SDK Tools CLI allow you to carry actions including agent deployment, updating, or acquiring information including status on updates. Information on the SDK Tools can be found in this part of the Bitdefender online [documentation](#).

Use of the tools requires a significant commitment by both the partner and Bitdefender's Product Management and Engineering teams. Completion of the TAP partner agreement (see next section) agreement for these partnerships requires and approved Statement of Work (SOW).

Program Requirements and Rules

Partners are required to apply and receive acceptance to participate in the TAP Program. Bitdefender holds sole discretion over the participation. In general, the participants are required to sign a Technology Alliance Partner Agreement and show measurable progress towards a joint, marketable solution. Bitdefender reserves the right to modify any aspect of the TAP program at any time at its sole discretion.

Terms & Conditions

For detailed Terms and Conditions of the TAP program, please refer to the TAP Partner agreement.

GARTNER is a registered trademark and service mark of Gartner and Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. Gartner, Magic Quadrant for Endpoint Protection Platforms, Evgeny Mirolyubov, Franz Hinner, Deepak Mishra, Satarupa Patnaik, Chris Silva, September 23, 2024

Trusted. Always.

