Bitdefender

Stop Advanced Threats, Stay ahead of attackers with Adaptive, Layered Endpoint Security

Bitdefender's GravityZone Security for Endpoints defeats advanced and sophisticated threats by using an adaptive layered approach. Patented machine learning technologies combined with the ability to monitor behavior and detect attack techniques let GravityZone detect, prevent and block threats. It then automatically takes actions to keep businesses running normally, including rolling back malicious changes.

The GravityZone console centralizes security management for endpoint protection in physical, virtual and public Cloud environments. Administrators can customize the GravityZone Endpoint agent as needed for complete protection with minimum impact on performance

USE CASES

- Block Ransomware
- Advanced threat protection (protection against advanced targeted attacks)
- Exploit prevention - Zero-day vulnerability, unpatched vulnerability
- Clean up – automatic remediation
- Data Center security
- Security for Hybrid environment (public cloud, data center, physical, virtual)

BENEFITS

Identify and block never-before seen malware and ransomware
Bitdefender uses patented machine learning algorithms proven to accurately detect unknown malware, including ransomware new variants. These algorithms are trained and perfected using trillions of samples from a global network of 500 million sensors to predict the progression of threats and allow Bitdefender to adapt its technologies to outsmart attackers.

Block exploit-based attacks
Sophisticated attacks often start with exploits to gain control of the target endpoint.

Bitdefender advanced anti-exploit technology detects and blocks attacks exploiting zero-day and un-patched vulnerabilities with techniques such as return oriented programming (ROP).

Detect and disrupt advanced attacks with real-time monitoring
Operating on a zero-trust assumption, Bitdefender GravityZone endpoint protection continuously monitors all active processes and can stop malicious activity mid-stream and roll back changes. This lets GravityZone Security for Endpoint consistently detect zero-day malware and file-less attacks that hijack known, running processes.

Neutralize threats with automatic remediation
Bitdefender Security for Endpoint, equipped with the industry's best malware-removal tools, instantly neutralizes threats, including deep kernel-based malware, removes all malware, rolls back changes and offers information for remediation and forensics.

Fast performance - optimized for virtualization and cloud
The GravityZone Endpoint agent is modular and integrated. Administrators can customize it based on the functions and security policies needed for complete protection with a small footprint.

Visibility and manageability across entire environment
Bitdefender's GravityZone platform is designed from the ground up as a unified security management platform to protect physical, virtualized, cloud and mobile environments. Detailed reports and intelligent event correlation offer valuable insight into each attack, such as number of systems affected, and pinpoint the files or executables involved.

KEY FEATURES

Machine Learning techniques use well-trained machine models and algorithms to predict and block advanced attacks before execution. Bitdefender's machine learning models use 40,000 static and dynamic features and are continuously trained on billions of files gathered from over 500 million endpoints globally. This dramatically improves the accuracy of malware detection and minimizes false positives.

Advanced Anti-Exploit technology protects the memory and vulnerable applications such as browsers, document readers, media files and runtime (ie. Flash, Java). Advanced mechanisms watch memory access routines to detect and block exploit techniques such as API caller verification, Stack pivot, return-oriented-programming (ROP) and more.

Real-time process monitoring inspects all processes in the operating system using filters in user mode and kernel model. It hunts for suspicious signs or abnormal behavior and takes remediation actions, including process termination, and undoes any changes the process makes. It is highly effective in detecting unknown, advanced malware and file-less attacks.

Application Control/Whitelisting* takes a "snapshot" of each endpoint, allowing administrators to create a whitelist of applications. It supports both 'Default Deny' and 'Blacklist' mode and can run in either Audit or Enforcement mode.

Web Security filtering enables scanning of incoming emails and web traffic including SSL traffic in real time to prevent downloading of malware. Anti-phishing protection automatically blocks phishing web pages.

Smart Scanning Technology

Centralized scanning is now possible for both physical and virtual computers. Administrators can offload security functions such as anti-malware scanning to a centralized Security Appliance to preserve endpoint resources. For roaming devices, the environment-aware agent automatically finds the best scanning process and can decide whether to scan locally.

Endpoint Control

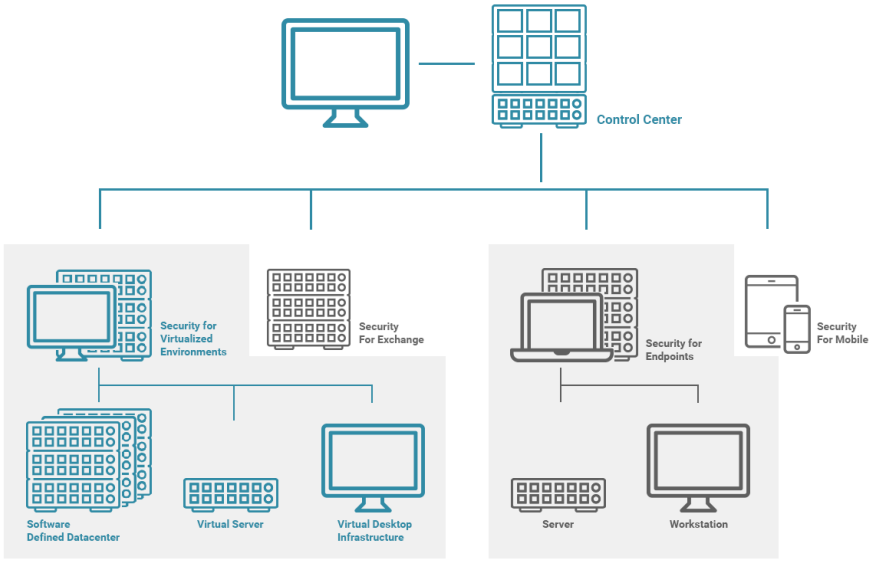
Policy-based endpoint controls include the firewall, device control with USB scanning, and web content control with URL categorization.

- *The Device Control module* prevents malware infection and data leaks by allowing administrators to manage permissions for external devices such as USB flash drives, Bluetooth devices, CD/DVD-players, etc.
- *Firewall* includes a two-way personal firewall and host-based intrusion detection and prevention control. This module controls applications' access to the network and the internet. It can also protect the system against port scans, restrict internet connection sharing and warn when new nodes join a Wi-Fi connection.
- *Web Content Control* dynamically manages access to websites based on their content and the Bitdefender tool bar informs users about the rating of web pages viewed. The Web Control policy can block users or applications from web access during specified times.

GRAVITYZONE ARCHITECTURE

Bitdefender GravityZone's scalable, resilient architecture features three key components:

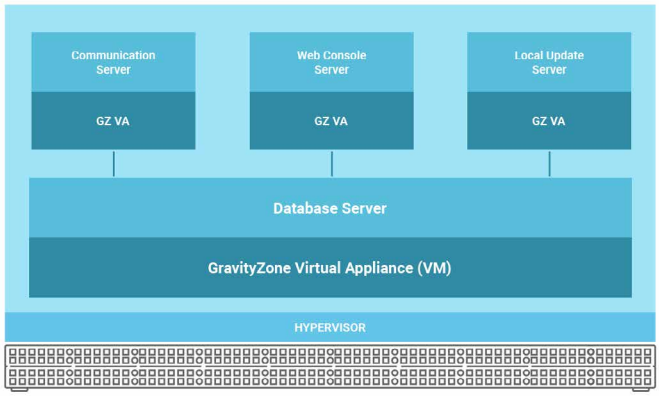
- GravityZone Control Center
- GravityZone Endpoint Agent
- Security Virtual Appliance (optional)



GravityZone Control Center

GravityZone Control Center is an integrated, centralized management console for GravityZone solutions including endpoint security, data center security, security for Exchange and mobile device security.

GravityZone Control Center can be hosted by Bitdefender** or deployed on premise. The Control Center incorporates the database server, communication server, update server and web console. The Control Center is delivered as one virtual appliance image that can be deployed on premise as quickly as in 30 minutes. For larger enterprises, GravityZone Control Center can be configured to use multiple virtual appliances with multiple instances of specific roles with a built-in load balancer for scalability and high availability.



GravityZone Endpoint Agent

The GravityZone Endpoint Agent consists of five modules: anti-malware, firewall, Web security/content control, device control and application control. The modular design lets administrators set security policies and services; and GravityZone automatically customizes the installation package and minimizes the agent footprint.

For distributed environments, administrators can leverage the Relay Role and designate computers to serve as communication proxy and update servers. Relay agents automatically discover unprotected computers on the network, and disseminate installation packages and updates to optimize network traffic.

Security Virtual Appliance

The Security Virtual Appliance is a purpose-built virtual appliance providing centralized scanning capabilities. Bitdefender Smart Scanning technology lets virtual and physical endpoints offload security tasks to the Security Virtual Appliance, freeing up computing resources.

* Not all features are available on all platforms. Application control and whitelisting is only available as part of Bitdefender GravityZone Enterprise Security.

** Also known as the GravityZone Cloud console, which is available in Business Security and Advanced Business Security bundles.

SYSTEM REQUIREMENTS AND SUPPORTED PLATFORMS

- GravityZone Security for Endpoint and the endpoint agent (Bitdefender Endpoint Security Tool) work on Windows, Mac and Linux operating systems.
- Bitdefender Security for Virtualized Environment supports a variety of Hypervisors including VMware ESXi, Citrix Xen, Microsoft Hyper-V, Nutanix, Red Hat KVM and Oracle VM.
- Security for Mobile Devices provides Android security and iOS device management
  For detailed system requirements, please refer to https://www.bitdefender.com/business/endpoint-security.html

LICENSING OPTIONS

Bitdefender Security for Endpoint is part of Bitdefender GravityZone Business Security, Advanced Business Security, and Enterprise Security. For more details and to compare packaging options, visit https://www.bitdefender.com/business/compare.html

Bitdefender®

PROTECTING OVER 500 MILLION USERS WORLDWIDE

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com/.

Bitdefender®

BD-NGZ-May 26 2017-Tk#crea1 287
Bitdefender 2017-NGZ-EndPointSecurity-DS-crea1287-AA-en_EN