GravityZone Endpoint Security for Linux and Mac

Stop Advanced Threats with Integrated Layered Next-Gen Security and Easy-to-Use EDR

Bitdefender's GravityZone Endpoint Security for Linux and Mac protects enterprises against the full spectrum of sophisticated cyber threats with speed, accuracy, low administrative overhead and minimal system impact. It enables incident response through fast alert triage, incident investigation, advanced data search and quick response actions. The integrated next-gen solution eliminates the need to run multiple endpoint security solutions on one machine, combining multi-stage next-gen detection techniques and easy-to-use EDR.

Benefits

Protection and Visibility

To keep enterprise digital assets safe, signature-less technologies, including advanced local and cloud machine learning and device hardening, work as a highly effective layered protection against sophisticated threats like fileless attacks, hacking tools, exploits, ransomware, cryptojacking and other types of malware obfuscation techniques. GravityZone extends endpoint security beyond prevention by providing pre- and post-compromise visibility, root cause analysis, investigation & remediation tools.

GravityZone Security leverages the largest security big-data platform (the Bitdefender Global Protective Network) collecting threat intelligence from over 500 million endpoints around the world. Specialized cloud machine learning algorithms process the data to uncover zero-day threats and identify global/regional patterns and indicators of attacks. Acting as a central source of threat intelligence, GPN anticipates emerging threats and delivers instant protection against both known and unknown attacks.

Automation and Ease of Use

Limited cybersecurity resources create management challenges and represent a critical vulnerability for enterprises. GravityZone Endpoint Security relies on automation technologies and ease of use to help organizations cope with the cybersecurity skill shortage with no compromise on the overall security posture. It accurately prevents cyber threats from running on the endpoint, sharply limiting the number of incidents that require manual analysis.

Use Cases

Advanced threat protection (protection against advanced targeted attacks)

Incident detection, investigation and response (EDR)

Data Center security

Security for Hybrid environment (public cloud, data center, physical, virtual)

Operational Simplicity

Running multiple agents on the endpoints not only increases the acquisition and operation costs but, due to limited compatibility, may also create security gaps. GravityZone Endpoint Security relies on a single lightweight agent, built from the ground up to integrate all security layers and to ensure cross-platform coverage: physical/virtual, Mac and Linux.

The GravityZone Console is designed for fast integration with pre-existing security operations tools and acts as a single pane of glass for complex heterogeneous environments, ensuring consistent management and protection across the entire enterprise infrastructure.

Some features are subject to the solution that is used.

Key features

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

Full Disk Encryption[1)]
GravityZone-managed full disk encryption uses Mac FileVault, taking advantage of the technology built into the operating systems.

HyperDetect[2)]
This new defense layer in the pre-execution phase features local machine learning models and advanced heuristics trained to spot hacking tools, exploits and malware obfuscation techniques to block sophisticated threats before execution.

HyperDetect lets security administrators adjust defense to best counter the specific risks the organization faces. With the "report only" option, security administrators can stage and monitor their new defense policy before rolling it out, eliminating business interruption. In a combination of high visibility and aggressive blocking unique to Bitdefender, users can set HyperDetect to block at normal or permissive level while continuing to report on aggressive level automatically, exposing early indicators of compromise.

Content Control [1)]
This module is designed to effectively protect endpoints against threats delivered via web traffic (spam, phishing) and to limit web browsing to business-approved content.

Device Control [1)]
The Device Control module prevents malware infection and data leaks by allowing administrators to manage permissions for unauthorized devices such as USB flash drives, Bluetooth devices, CD/DVD-players etc.

Response and containment
GravityZone offers the best clean-up technology on the market. It automatically blocks/contains threats and kills malicious processes.

Relay Function[3)]
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.

GravityZone Cloud Console
GravityZone Control Center is an integrated and centralized management console that provides a single pane of glass view for all security management components, including endpoint security and datacenter security. The GravityZone management center incorporates multiple roles and contains the database server, communication server, update server and web console. For larger enterprises, it can be configured to use multiple virtual appliances with multiple instances of specific roles with built-in load balancer for scalability and high availability.

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.

Integration with Microsoft Windows Defender Advanced Threat Protection

The GravityZone Console is integrated with Microsoft WDATP, enabling enterprises to protect their Linux and Mac endpoints while using the ATP console as a single pane of glass to oversee all security events throughout the entire IT environment (Windows, Mac and Linux endpoints)

Besides events related to threats already blocked by Bitdefender's next-gen security layers, security analysts and incident response teams will use the ATP console to investigate suspicious activities and apply quick response actions to block lateral spread and eliminate threats from Mac and Linux endpoints protected by Bitdefender.

Supported Endpoint Operating Systems

- macOS High Sierra (10.13.x) • macOS Sierra (10.12.x) • OS X El Capitan (10.11.x) • OS X Yosemite (10.10.5) OS X Mavericks (10.9.5) • macOS Mojave (10.14)
- Ubuntu 14.04 LTS or higher • Red Hat Enterprise Linux / CentOS 6.0 or higher • SUSE Linux Enterprise Server 11 SP4 or higher • OpenSUSE Leap 42.x • Fedora 25 or higher • Debian 8.0 or higher • Oracle Linux 6.3 or higher • Amazon Linux AMI 2016.09 or higher

Note: Specific kernel versions are supported. For details, please refer to the product documentation.

Best Protection 2017. Best Performance 2017

The combination of "Best Performance" and "Best Protection" is unique to Bitdefender, which scored best in these categories in all six tests performed by the prestigious AV-TEST throughout 2017.

[1)] Only Mac OS Endpoints
[2) 3)] Only Linux Endpoints

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

FOR MORE INFORMATION VISIT: bitdefender.com/business