Bitdefender

GravityZone Endpoint Security HD

The Layered Next Generation Endpoint Security Platform

Bitdefender Endpoint Security HD protects enterprises against the full spectrum of sophisticated cyber threats with speed, accuracy, low administrative overhead and minimal system impact. The next-gen solution eliminates the need to run multiple endpoint security solutions on one machine, combining preventive controls, multi-stage non-signature detection techniques, and automatic response in a single platform.

Endpoint Security HD prevents unknown threats and detects targeted attacks that evade other endpoint security solutions, using advanced machine learning, behavioral analysis and an array of other non-signature-based technologies. Once a threat is detected, Endpoint Security HD takes immediate actions, including rolling back malicious changes to keep your business running normally.

Highlights:

- **Ransomware protection**
- **Exploit prevention**
- **Detect and block file-less attacks**
- **Stop Script-based attacks**
- **Visibility into suspicious activities**

KEY BENEFITS

Detect and Prevent the full range of sophisticated threats and unknown malware
GravityZone Security HD defeats advanced threats and unknown malware, including ransomware, that evade traditional endpoint protection solutions. Advanced attacks such as PowerShell, script-based, file-less attacks and sophisticated malware can be detected and blocked before execution.

Blocks exploit based attacks
High-profile attacks often start with exploits to execute code on target systems. Bitdefender anti-exploit technology focuses on attack tools and techniques to detect and block advanced attacks that exploit zero-day and un-patched vulnerabilities, such as ROP (return oriented programming), Shellcode and virtual pointer. It also prevents browser exploits.

Enhance accuracy without false positives
In the adaptive layered architecture, anti-exploit, machine learning, behavioral analysis and Cloud-based Sandbox work together to achieve a higher detection rate with accuracy, eliminating disruption caused by false-positives.

Automatic and immediate action (Automate threat remediation and response)
Once a threat is detected, the endpoint security HD instantly neutralizes it through actions including process termination, quarantine, removal and roll-back of malicious changes. It shares threat information in real time with Global Protective Network, Bitdefender's cloud-based threat intelligence service, preventing similar attacks anywhere in the world.

Gain threat context and visibility
Bitdefender Endpoint Security HD's unique capability to identify and report on suspicious activities gives admins early warning of malicious behavior such as dubious operating system requests, evasive actions and connections to command and control centers.

Boost operational efficiency with single agent and integrated console
Bitdefender's single, integrated endpoint security agent eliminates agent fatigue. The modular design offers maximum flexibility and lets administrators set security policies. GravityZone automatically customizes the installation package and minimizes the agent footprint. Architected from the ground up post-virtualization and post-cloud security architectures, GravityZone provides a unified security management platform to protect physical, virtualized, and cloud environments.

HARDENING & CONTROL

- Application Control
- Content Control
- Anti-phishing
- Firewall
- Device Control
- Full Disk Encryption

MULTI-STAGE DETECTION

Pre-Execution

- Signature & cloud look-up
- Local & Cloud Machine Learning Models
- Hyper Detect

On Execution

- Sandbox Analyzer
- Anti-exploit
- Process Inspector

ACTION

- Block Access
- Quarantine
- Disinfect/ Remove
- Process Termination
- Roll Back

VISIBILITY & MANAGEMENT

- Reports
- Dashboard
- indicators of Compromise
- Suspicious Activities
- Threat Context
- Alerts & Notification

- Scalable
- Flexible Deployment

Bitdefender Layered Next generation endpoint protection platform uses adaptive layered architecture that includes endpoint controls, prevention, detection, remediation and visibility.

"GravityZone just works by itself. So we're free to divert our efforts to planning and helping the schools become more efficient."

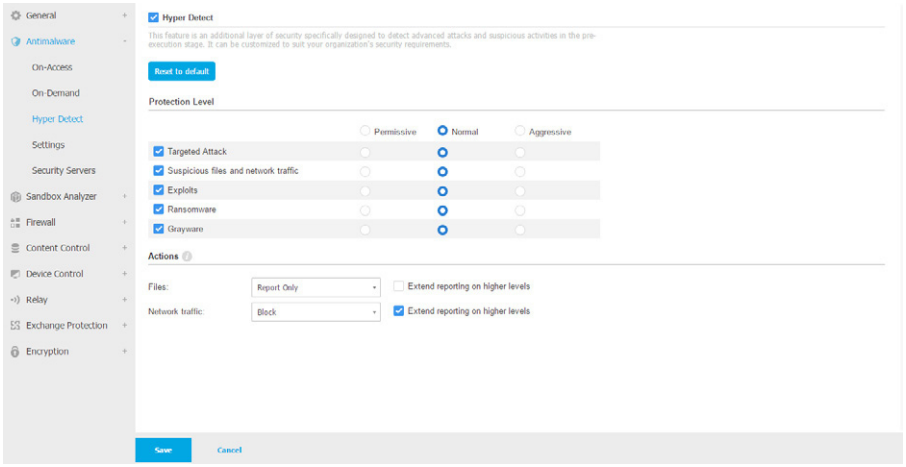
Rolland Kornblau, Director of IT, El Rancho, Unified School District

FEATURES

NEW HyperDetect

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. It also detects delivery techniques and sites that host exploit kits and blocks suspicious web traffic.

HyperDetect lets security administrators adjust defense to best counter the specific risks the organization likely 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.



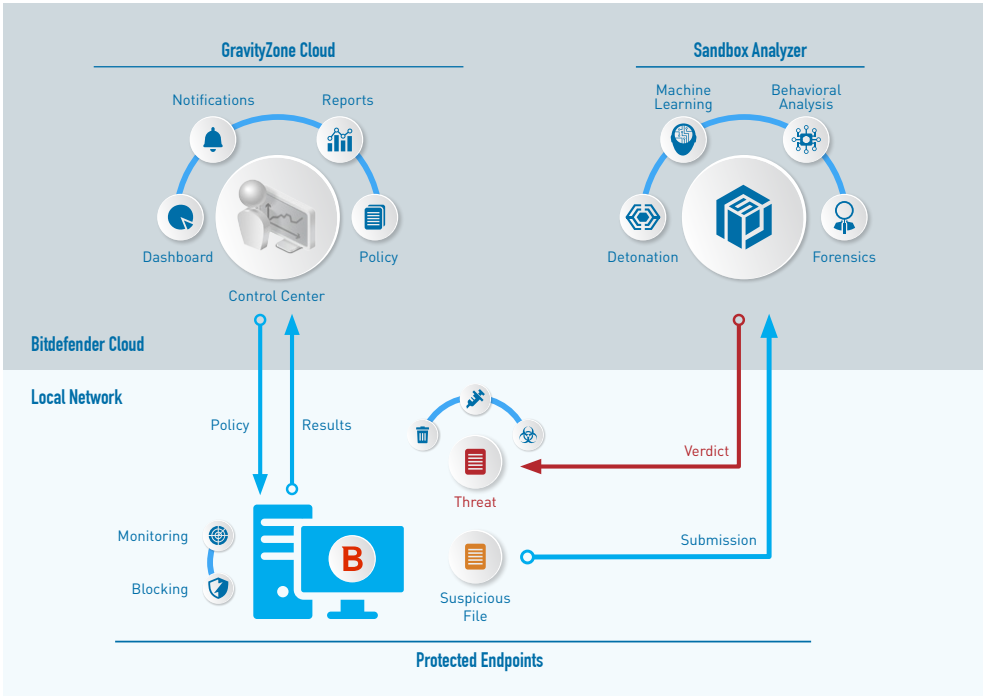
HyperDetect lets security administrators adjust aggressiveness of their defense and offer a unique combination of blocking and visibility of threats. For example, block at the "Normal" level and report at the "Aggressive" level.

NEW Endpoint Integrated Sandbox Analyzer

This powerful layer of protection against advanced threats analyzes suspicious files in depth, detonates payloads in a contained virtual environment hosted by Bitdefender, analyzes their behavior and reports malicious intent.

Integrated with GravityZone Endpoint agent, the Sandbox Analyzer automatically submits suspicious files for analysis. With a malicious verdict from the Sandbox Analyzer, the Endpoint Security HD automatically blocks the malicious file on all systems enterprise-wide immediately. The automatic submission function allows enterprise security administrators to choose monitor or block mode, which prevents access to a file until a verdict is received. Administrators can also manually submit files for analysis.

Sandbox Analyzer's rich forensic information gives administrators clear context on threats and helps them understand threat behavior.



Endpoint integrated Sandbox. The GravityZone endpoint agent automatically submits suspicious files to Sandbox Analyzer for further analysis.

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.

Advanced Anti-Exploit

Exploit prevention 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.

Process Inspector

Operating on a zero-trust mode, Process Inspector continuously monitors all processes running in the operating system. It hunts for suspicious activities or anomalous process behavior, such as attempts to disguise the type of process, execute code in another process's space (hijack process memory for privilege escalation), replicate, drop files, hide from process enumeration applications and more. It takes appropriate remediation actions, including process termination and undoing changes the process made. It is highly effective in detecting unknown, advanced malware and file-less attacks including ransomware.

Anti-phishing and web security filtering

Web Security filtering enables scanning of incoming web traffic, including SSL, http and https traffic, in real time to prevent the download of malware to the endpoint. Anti-phishing protection automatically blocks phishing and fraudulent web pages. Administrators can remotely restrict or block an end-user's access to certain applications or web pages for enhanced internet hygiene, acceptable web-usage and compliance.

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

Full Disk Encryption*:
GravityZone-managed full disk encryption using Windows BitLocker and Mac FileVault, taking advantage of the technology built into the operating systems.

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

SYSTEM REQUIREMENTS AND SUPPORTED PLATFORMS

For detailed system requirements, please refer to https://www.bitdefender.com/business/advanced-security.html
GravityZone Endpoint Security HD
- Workstation OS: Windows 10 RS2/RS1/TH2/TH1, Windows 8, 8.1, Windows 7 SP1

- Windows tablet and embedded OS: Windows Embedded 8 Standard, Windows Embedded 8.1 Industry, Windows Embedded Standard 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7

- Server operating systems: Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2, Windows Server 2016 Core

LICENSING OPTIONS

GravityZone Endpoint Security HD is included in the Bitdefender GravityZone Elite suite (Cloud-managed), and will be available as a standalone product.

GravityZone Elite suite also includes Security for Endpoint running on Windows, Mac and Linux
Security for Exchange
Security for Virtualized Environment (Datacenter security)

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/.

BD-NGZ-Jun.23.2017-TK#crea1.287
Bitdefender-2017-NGZ-EndPointHD-DS-crea1479-A4-en_EN