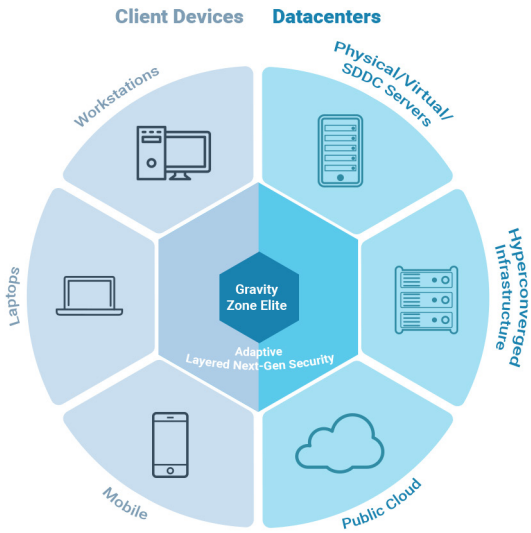
Bitdefender GravityZone Elite Suite

The Layered Next Generation Security Platform

Bitdefender GravityZone Elite suite is designed to protect enterprises against the full spectrum of sophisticated cyber threats with speed and accuracy. Elite combines Bitdefender's proven layered security approach with its next-generation tools and technologies to provide high-level performance and protection for all endpoints across the enterprise environment: desktops, laptops, mobiles, physical and virtual servers.

GravityZone Elite ensures a consistent level of security for the entire IT environment, limiting poorly protected endpoints that could serve as starting points for malicious actions against the organization. It relies on a simple, integrated architecture with centralized management for both endpoints and datacenter. Cloud and on-premise console options fit both cloud-ready and strictly regulated environments.



HIGHLIGHTS

- Detect and block file-less malware attacks
- Stop script-based attacks
- Unpack and analyze unknown malware at pre-execution
- Single agent, small footprint with low system impact
- Integrated management console for physical and virtual endpoints

Endpoint Protection

Bitdefender Endpoint Security HD – the endpoint security component of GravityZone Elite - 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.

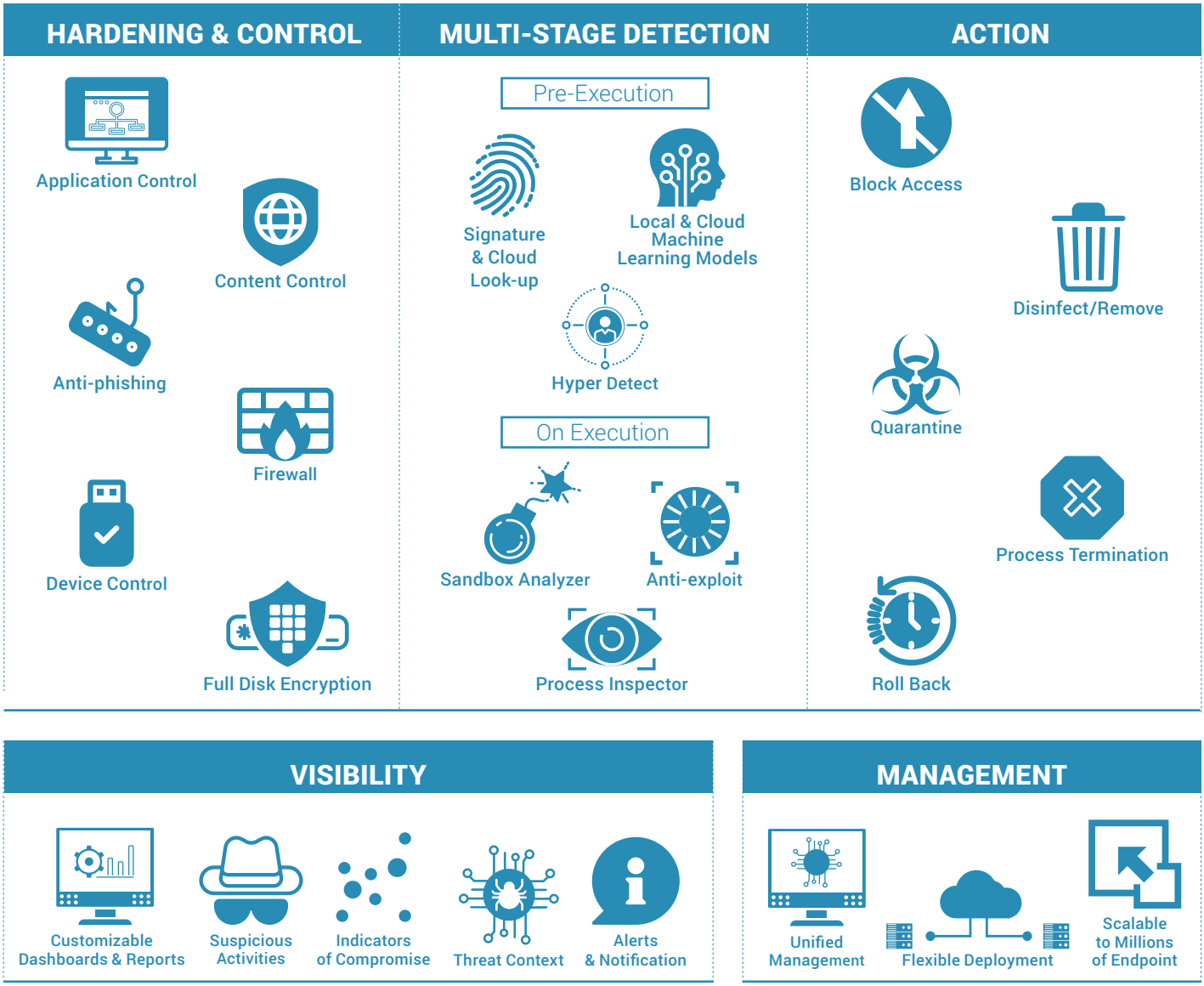
Key Benefits

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

Detect and Stop Fileless malware
Fileless malware attacks execute malicious code directly in memory. Since no file is present on the disk, most AV solutions designed for file analysis are blind to this type of attack. Bitdefender leverages Advanced Anti-Exploit, HyperDetect™ and Process Inspector to detect, block and interrupt fileless attacks.

Stop Macro and script-based attacks
In this case, attackers are trusted MS Office Macro that use Windows administration tools like PowerShell to run scripts and download malicious code to execute attacks. Since these are "trusted" Windows tools, most endpoint security products, including the so-called Next-gen AV providers, don't scrutinize scripts, like Powershell, WMI, Javascript interpretors etc. Bitdefender adds Command-line Analyzer techniques to intercept and securitize scripts, alerting admins and blocking the script from running, if it carries out malicious commands.

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 GPN, Bitdefender's cloud-based threat intelligence service, preventing similar attacks worldwide.

Gain threat context and visibility
Bitdefender Endpoint Security HD's unique capability to identify and report 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.

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.

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 threat blocking unique to Bitdefender, users can set HyperDetect to block at normal or permissive level but continue to report at the aggressive level exposing early indicators of compromise.

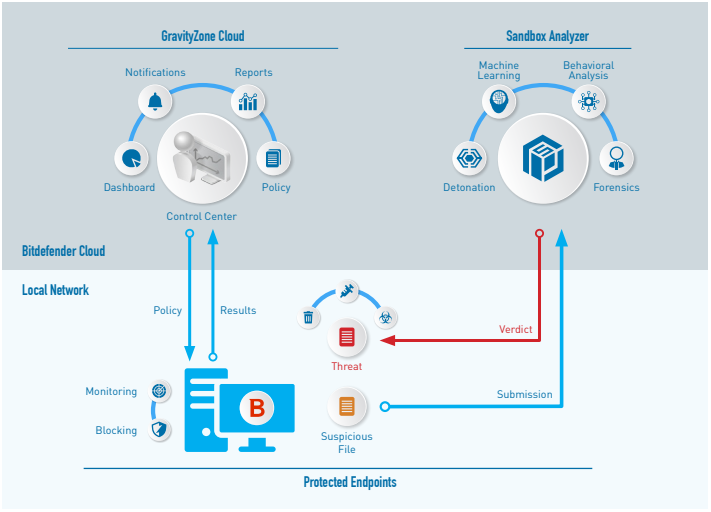
Endpoint Integrated Sandbox Analyzer
This powerful layer of protection against advanced threats analyzes suspicious files in depth, detonates payloads in a contained virtual

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 clear context on threats and helps them understand threat behavior.

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 others.

Process Inspector
Process Inspector operates in zero-trust mode, continuously monitoring 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 fileless 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.



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 firewall, device control with USB scanning, and web content control with URL categorization.

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.

Datacenter Protection

GravityZone Security for Virtualized Environments (SVE) leverages Bitdefender Endpoint Security HD's layered next-generation defenses to provide enterprises best-in-class security for server, VDI and cloud workloads, while maximizing infrastructure performance and operational efficiency. GravityZone SVE is designed as an enterprise solution that can support even the largest datacenters.

Key Benefits

Agility
SVE enables security automation across the datacenter lifecycle at rollout as well as during day-to-day security operations of a highly dynamic virtual environment. It integrates with VMware (vCenter, vShield, NSX), Citrix XenCenter and the Nutanix Enterprise Cloud Platform and enables fast automated provisioning.

Operational efficiency
The unified GravityZone Control Center management console simplifies security deployment, maintenance and upgrades, providing centralized visibility into all virtual and physical servers and workstations. It supports centralized creation and automatic administration of security policies to help streamline IT operations while improving compliance.

Improved infrastructure utilization
Centralized scanning and a small footprint agent greatly reduce the use of memory, disk space, CPU and I/O activity on host servers, increasing VM density and ROI on IT infrastructure.

Universal compatibility
Compatible with all virtualization platforms (such as VMware® ESXiTM, Microsoft® Hyper-VTM, Citrix® XenServer®, Red Hat® Enterprise Virtualization®, KVM, and Nutanix® Acropolis), Microsoft Active Directory, and both Windows® and Linux® guest operating systems, GravityZone simplifies deployment, endpoint discovery and policy administration.

Unlimited linear scalability
Multiple SVAs can be used to increase scanning capacity as the Datacenter grows and more VMs are created. As an existing SVA reaches a certain load threshold, new ones can be deployed to accommodate growth.

Layered next-gen defenses
GravityZone Security for Virtualized Environments incorporates all key security layers of Endpoint Security including HyperDetect, Sandbox Analyzer and fileless attack-detection methods to provide leading protection for enterprise digital assets stored or processed in the datacenter.

Security for iOS and Android Mobile Devices

This solution is designed to support controlled adoption of the bring-your-own-device (BYOD) concept by enforcing security policies consistently on all users' devices. As a result, mobile devices are controlled, and sensitive business information on them is protected. The administrative burden is reduced with the always-up-to-date status of compliant and non-compliant devices.

Security for Exchange Servers

It provides multiple layers of security for messaging: antispam, antiphishing, antivirus and antimalware with behavioral analysis and zero-day threat protection and e-mail traffic filtering, including attachment and content filtering. Antimalware scanning can be offloaded to centralized security servers from protected mail servers. Management and reporting are centralized, allowing unified policies for endpoints and messaging.

GravityZone Control Center

GravityZone Control Center is an integrated and centralized management console that provides a single pane of glass view for all the security management components including endpoint security, datacenter security, security for Exchange and mobile devices security. It can be cloud-hosted or deployed locally. 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.

GravityZone Elite Security protects desktops, servers (physical or virtual), mobile devices and e-mail boxes. Servers should account for less than 35% of all units.

For detailed system requirements, please refer to https://www.bitdefender.com/business/elite-security.html

BD-NGZ-Mar07.2018-TW#
Bitdefender-NGZ-Elite-Datasheet-creat-1973-A4-en_EN