

Bitdefender GravityZone Ultra Suite

UNCOVER AND STOP ELUSIVE THREATS WITH AGILITY AND PRECISION

GravityZone Ultra, featuring Endpoint Security XDR, excels where pure-play EDR products are too complex and noisy by smoothly preventing, detecting and responding to sophisticated attacks that evade traditional anti-malware. In a single, unified security suite, GravityZone Ultra provides:

- Attack surface reduction (via firewall, application control, content control and patch management)
- Data protection (via full disk encryption)
- Pre-execution detection and eradication of malware (via tunable machine learning, real-time process inspection and sandbox analysis)
- Automated detection, easy investigation and in-place remediation via the newly released endpoint event recorder and threat analytics in Endpoint Security XDR

The result is seamless threat prevention, accurate incident detection and smart response to minimize exposure to infection and stop breaches.

As an integrated endpoint protection suite, GravityZone Ultra ensures a consistent level of security for the entire IT environment, so attackers find no poorly protected endpoints to use as starting points for malicious action against the organization. GravityZone Ultra relies on a simple, integrated architecture with centralized management for both endpoints and datacenter. It lets companies deploy the endpoint protection solution quickly and requires less administration effort after implementation.

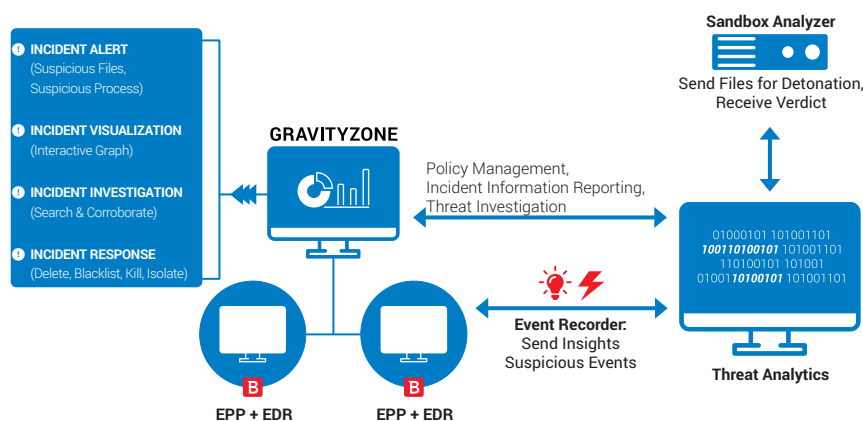


Figure 1. Bitdefender XDR: prevention, detection and response in one agent, managed by the GravityZone console

EDR made Easy

With clear visibility into indicators of compromise (IOCs) and one-click threat investigation and incident response workflows, GravityZone Ultra reduces resource and skill requirements for security teams. The new endpoint data recorder is a seamless addition to the existing threat-protection stack and performs a broad capture of system activities (file & process creation, program installation, module loading, registry modification, network connections etc.) to aid in an enterprise-wide visualization of the chain of events involved in the attack.

The threat analytics module operates in the cloud and continuously sifts through behavioral events in system activities and creates a prioritized list of incidents for additional investigation and response.

Key Benefits

Expanding beyond traditional EPP functionalities, Endpoint Security XDR provides security analysts and incident response teams with the tools they need to analyze suspicious activities and to investigate and adequately respond to advanced threats:

- Real-time endpoint visibility

- Expose suspicious activities
- One-click investigation
- Alert triage and incident analysis visualization
- Track live attacks and lateral movements
- Rapid response
- Reduce dwell time with fast resolution, containment and remediation

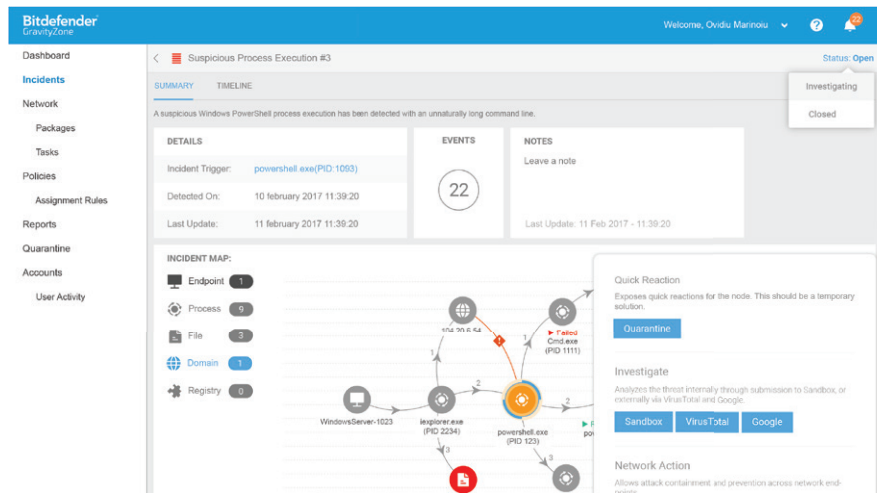


Figure 2. The Incident details page provides a clear overview of the “Blast radius” of the incidents. The practitioner can easily acquire supporting evidence and respond.

Enhance security optics. Avoid alert fatigue.

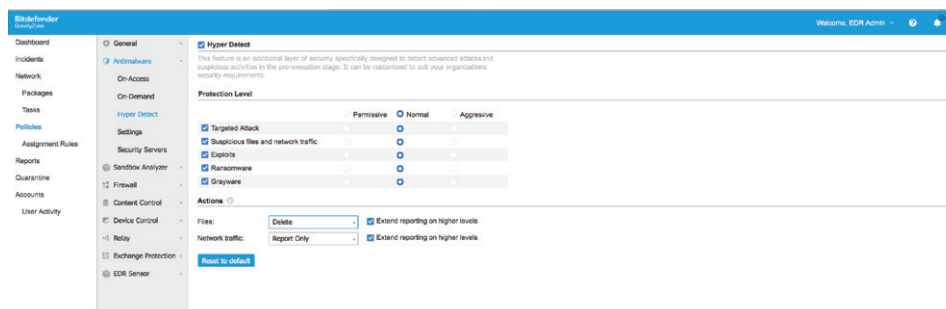
Only relevant, correlated and severity-rated events are presented for manual analysis and resolution. Noise and redundant information is kept at a minimum, as the vast majority of attacks and advanced attacks are blocked at the pre- or on-execution stages. Elusive threats, including fileless malware, exploits, ransomware and obfuscated malware are neutralized by the highly effective layered next-gen endpoint prevention technologies and on-execution behavior-based process inspector. Automatic response and repair eliminate the need for human intervention in blocked attacks.

High-fidelity detection lets security personnel focus only on real incidents and threats:

- Minimize noise and distraction from false alarms
- Reduce the volume of incidents with effective threat prevention
- Eliminate manual remediation of blocked attacks with automatic remediation and repair

Smart response means evolved prevention

Because GravityZone Ultra is an integrated prevent-detect-respond solution, it enables quick response and restoration of endpoints to a “better-than-before” stage. Leveraging threat intelligence gathered from the endpoints during the investigation process, a single interface provides the tools to immediately adjust policy and patch vulnerabilities to prevent future incidents, improving the security of your environment.



Comprehensive endpoint security platform in one agent and console

GravityZone Ultra inherits all the hardening and next-generation prevention controls included in Endpoint Security HD and the GravityZone Elite suite:

- Minimize exposure with strong prevention
- Machine-learning and behavior-based detection stops unknown threats at pre-execution and on-execution
- Detect and block script-based, fileless, obfuscated and custom malware with automatic remediation
- Memory protection to prevent exploits
- Reduce attack surface by enabling IT security controls
- Integrated client firewall, device control, web content filtering, app control, patch management and more.

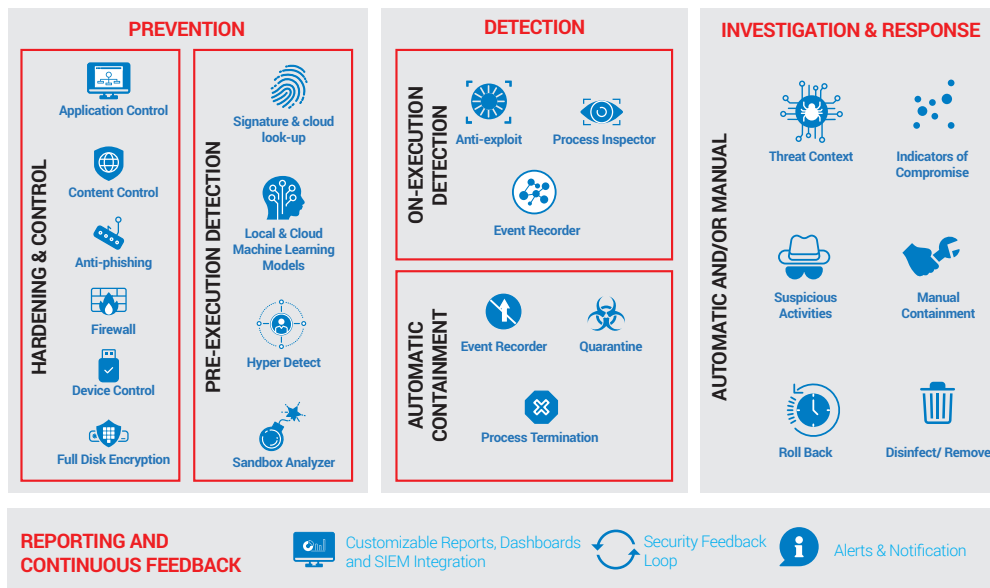
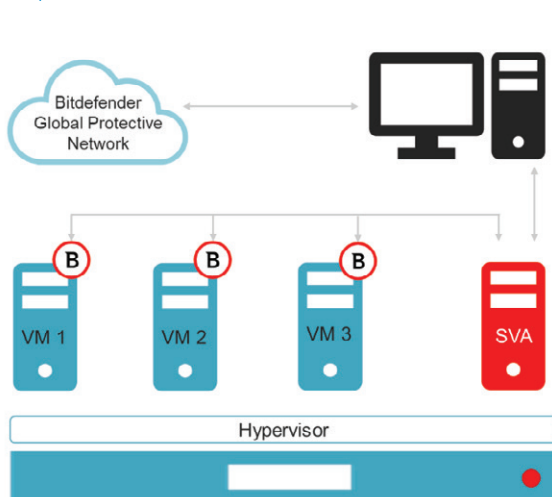


Figure 3. Bitdefender XDR: The Comprehensive Endpoint Security Platform

Protecting the Datacenter

Fully integrating with Bitdefender Endpoint Security XDR, the Datacenter Protection component of GravityZone Elite suite is the Security for Virtualized Environments (SVE). It is the most advanced virtualized datacenter security solution on the market in antimalware protection for virtual machines, optimizing not only consolidation ratios but also operating costs. GravityZone SVE is an enterprise solution that can support even the largest datacenters. Integration into a production environment is simple, and virtual environments of any size can benefit from this technology.

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 leading hypervisor platforms (VMware ESXi, Microsoft Hyper-V, Citrix Xen, Red Hat KVM, and Nutanix AHV) and both Windows and Linux as guest OSs.

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. An additional benefit of deploying multiple SVAs is improved resilience and load sharing: the load from a failed/overloaded SVA can be taken over by another active or less loaded SVA.

Layered Next-gen defenses

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

Features

- Engineered to enable datacenter transformation: SDDC, hyper-convergence and hybrid cloud
- Comprehensive integrations with VMware, Nutanix, Citrix, AWS, and Microsoft for investment protection, deployment automation and inventory and license management
- Support of multiple virtualization and cloud environments from a single deployment
- Single-pane-of-glass visibility and centralized manageability across the hybrid cloud
- Efficient, resilient and scalable SVA-based architecture supporting all hypervisors
- Maximized VM density, low boot latency and optimal application performance
- Advanced layered security with continuous coverage across the hybrid cloud

GravityZone Control Center

GravityZone Control Center is an integrated and centralized management console that provides a single-pane-of-glass view of all security management components, including endpoint security, datacenter security, security for Exchange and mobile device 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. The Control Center is delivered as one virtual appliance image and can be deployed in under 30 minutes. 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.

For detailed system requirements, please refer to www.bitdefender.com/business/ultra-security



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>.

All Rights Reserved. © 2017 Bitdefender. All trademarks, trade names, and products referenced herein are property of their respective owners.
FOR MORE INFORMATION VISIT: [bitdefender.com/business](http://www.bitdefender.com/business)

