Bitdefender GravityZone Ultra Suite

UNCOVER AND STOP ELUSIVE THREATS WITH AGILITY AND PRECISION

GravityZone Ultra is a complete Endpoint Security solution designed from the ground up as an integrated next-gen EPP and easy-to-use EDR. It offers prevention, threat detection, automatic response, pre and post compromise visibility, alert triage, investigation, advanced search and one-click resolution capabilities.

Relying on highly effective prevention, automated threat detection and response technologies, GravityZone Ultra sharply limits the number of incidents requiring manual analysis, reducing the operational effort required to run an EDR solution. Cloud-delivered and built from the ground up as a unified, single agent/single console solution, it's also easy to deploy and integrate in the existing security architecture.

GravityZone Ultra enables enterprise customers to accurately protect digital assets against even the most elusive cyber threats and effectively respond to all phases of an attack through:

- Attack surface reduction (via firewall, application control, content control and patch management)
- Data protection (via full disk encryption add-on module)
- Pre-execution detection and eradication of malware (via tunable machine learning, real-time process inspection and sandbox analysis)
- Real-time threat detection and automated remediation
- Pre and post compromise attack visibility (Root Cause Analysis)
- Fast incident triage, investigation and response
- Current and historic data search
- "Better-than-before" security posture (via patch management add-on module)

The result is seamless threat prevention, in-depth visibility, 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.
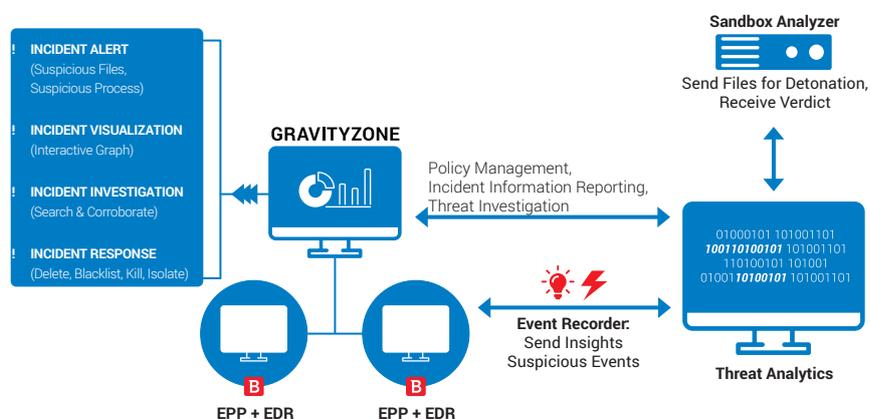

Figure 1. Bitdefender Ultra: prevention, detection and response in one agent, managed by the GravityZone console

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, program installation, module loads, registry modification, network connections, etc.) to aid in an enterprise-wide visualization of the chain of events involved in the attack.

Key Benefits

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

- Real-time detection and automatic remediation
- Fast incident triage, investigation and response
    - Suspicious activity detection
    - Suspicious activity validation and alert triage
    - One-click incident response

- Pre and post compromise forensics (Root Cause Analysis)
- Current and historic data search based on:
    - IOCs
    - MITRE tags
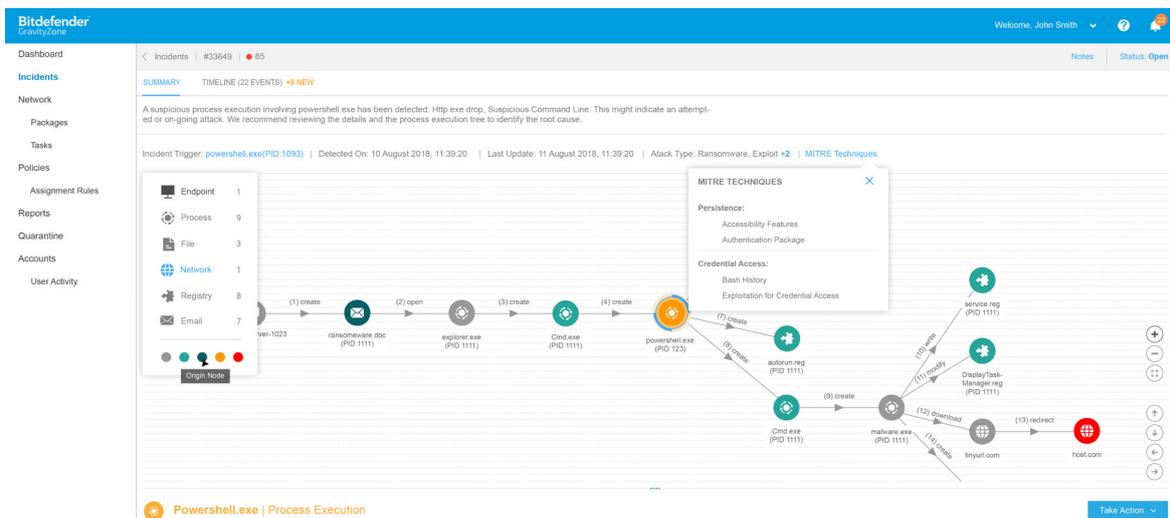   - Processes, Files, Registry entries or other parameters

Figure 2. The Incident details page provides a clear overview of the "blast radios" of the incidents. The practitioner can easily acquire supporting evidence and respond.

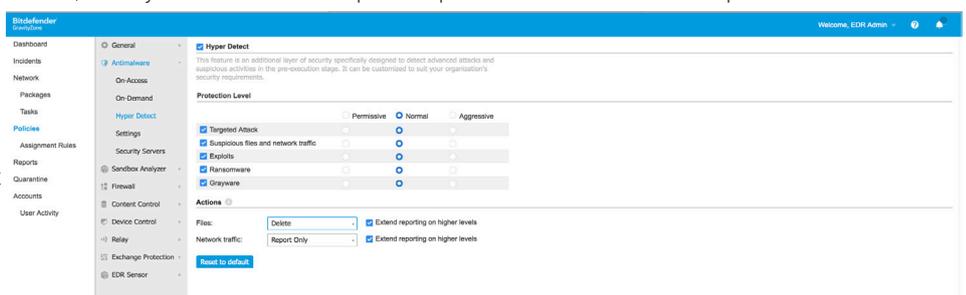# High-Fidelity detection means enhanced security optics and freedom from alert fatigue

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-execution 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

Easy incident investigation and smart response for evolved protection

As an integrated prevent-detect-respond-evolve solution, GravityZone Ultra enables quick response and restoration of endpoints to a "better-than-before" stage. Incident investigation tools like root cause analysis and sandbox report help security teams validate suspicious activities and respond adequately to cyber threats. Advanced search of current and historical data based on IOCs, MITRE tags and other relevant artifacts enables quick identification of threats that might hide in the endpoint infrastructure.

Leveraging intelligence gathered from the endpoints during the investigation, the single

management interface provides the tools to immediately adjust policy and/or patch identified 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 the GravityZone Elite suite:

- Minimize exposure with strong prevention
- Machine-learning and behavior-based detection stop unknown threats at pre-execution and on-execution
- Detect and block script-based, file-less, 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 and more
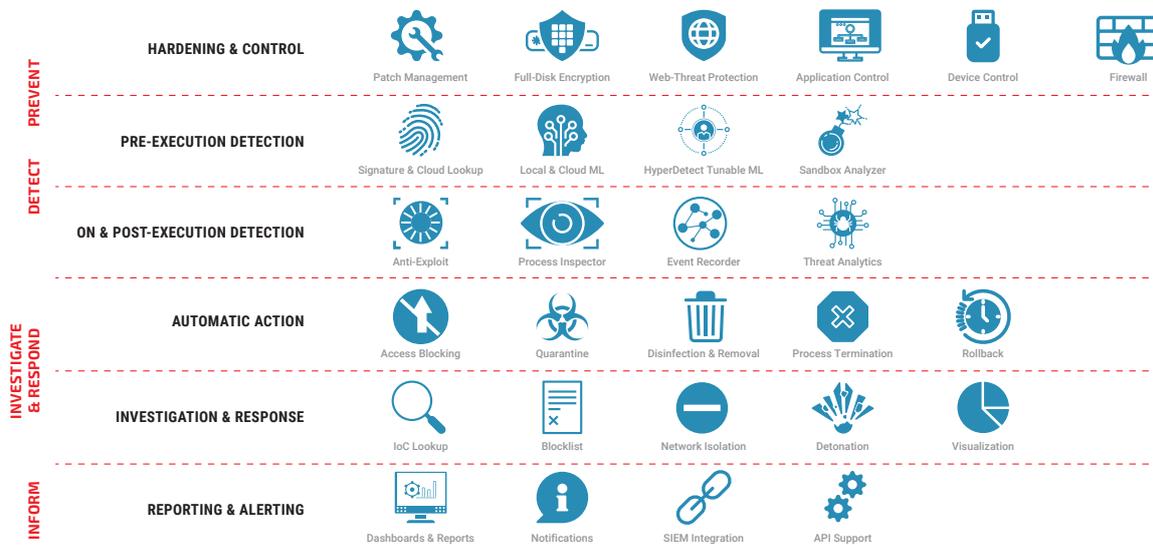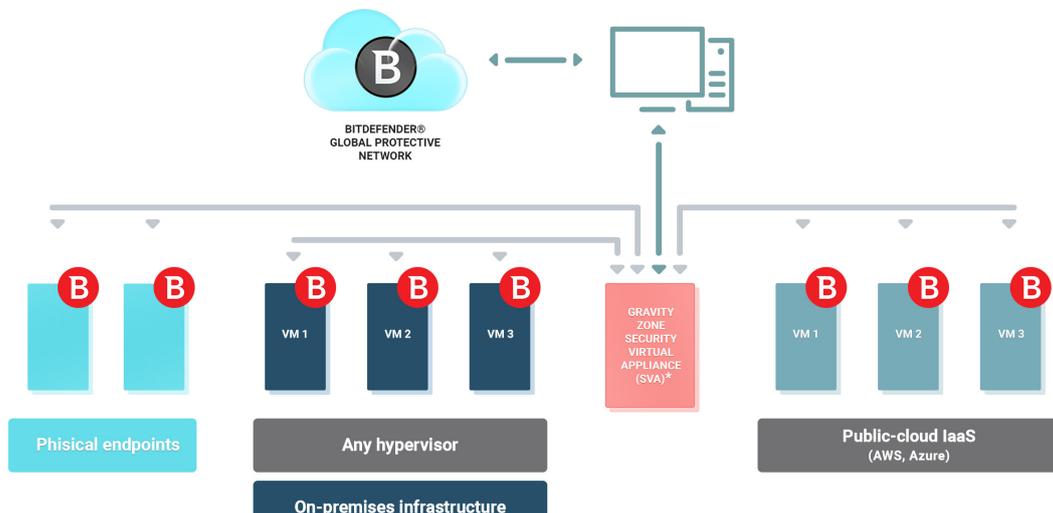- Add-on modules: Full Disk Encryption, Patch Management

Figure 3. Bitdefender GravityZone Ultra: The Comprehensive, EPP + EDR, Endpoint Security Platform

Protecting Datacenter and Cloud Infrastructure

An integral part of GravityZone Ultra, GravityZone Security for Virtualized Environments is its server- and VDI-workload security component engineered for agility, operational efficiency and infrastructure cost containment in software-defined, hyperconverged and hybrid-cloud environments.

* - Also, agentless deployments are supported with VMware® vShieldTM or NSXTM

Key Benefits

Higher Operational Efficiency and Agility
Compatible with multiple cloud platforms and all hypervisors (e.g., VMware® ESXiTM, Citrix® XenServer®, Microsoft® Hyper-V, Nutanix® AHV, KVM, RedHat® Enterprise Virtualization, or a combination thereof), GravityZone helps streamline IT and security operations while improving compliance. The GravityZone unified management console simplifies security deployment and administration, enabling automated security provisioning, centralized policy enforcement and single-pane-of-glass visibility across heterogeneous and distributed environments. Integration with virtualization-management tools (e.g., vCenter Server, XenServer, and Nutanix Prism) give GravityZone real-time awareness of the underlying infrastructure's operational context, including the global virtual machine (VM) inventory. Consequently, GravityZone can automatically apply VM-appropriate security policies that follow the workloads regardless of where in the hybrid cloud they reside, allowing customer IT operations teams to spin up thousands of secured VMs in a matter of hours.

Top Infrastructure Performance and Utilization
GravityZone's patented security algorithms and its efficient design—which eliminates the need to use resource-intensive agents inside each virtual machine—enable up to 35% higher virtualization density and 17% faster application response than the competition, promoting better infrastructure utilization and superior end-user experience.

Unlimited Linear Scalability
GravityZone's modular and resilient architecture provides the scalability to secure carrier-grade deployments. The platform can expand on demand in a linear and efficient fashion by adding Security Virtual Appliances or multiplying Control Center server roles, if required.

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.

GravityZone Control Center

GravityZone Ultra 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 and cloud security and security for Exchange. For GravityZone Ultra only cloud-hosted console is available. GravityZone management center incorporates multiple roles and contains the database server, communication server, update server and web console.

GravityZone Ultra is available with the cloud console. It protects desktops, servers and Exchange mailboxes. Servers should account for less than 35% of total units.

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