Bitdefender GravityZone Ultra

Unified Prevention, eXtended Detection, Response and Risk Analytics

GravityZone Ultra combines the world's most effective Protection with eXtended Endpoint Detection and Response (XEDR) capabilities to help you defend your endpoint infrastructure (workstations, servers or containers) throughout the threat lifecycle, with high efficacy and efficiency.The cross-endpoint event correlation[1] takes threat detection and visibility to a new level by combining the granularity and rich security context of EDR with the infrastructure-wide analytics of XDR (eXtended Detection and Response).By incorporating Risk Analytics (for endpoint and user generated risks) and hardening innovations natively, it minimizes the endpoint attack surface, making it more difficult for attackers to penetrate. With GravityZone Ultra, you will compress the time it takes to detect and respond to threats via an integrated security stack, while also reducing the need for multiple vendor solutions.

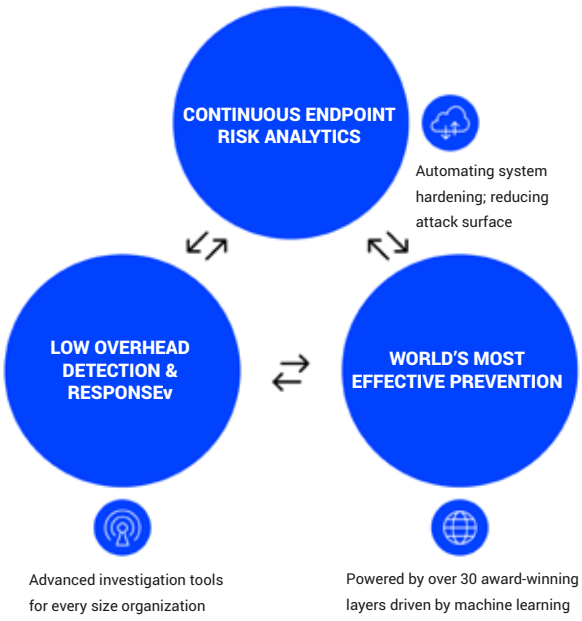


Figure 1. Bitdefender GravityZone Ultra: prevention, extended detection and response in one agent, managed by the GravityZone console

How does GravityZone Ultra help?

World's Most Effective Endpoint Protection

Unifying EDR, Risk Analytics and Hardening technologies in one, single agent-single console, GravityZone leverages 30 layers of advanced techniques to successfully stop breaches throughout the entire threat lifecycle, from first contact, exploit, persistence and malicious activity.

eXtended Endpoint Detection and Response (XEDR[2])

The new Endpoint Detection and Response capability from Bitdefender extends EDR analytics and event correlation capabilities beyond the boundaries of a single endpoint, to help you deal more effectively with complex cyber-attacks involving multiple endpoints. XEDR uniquely provides you with threat visualizations at the organizational level so you can focus investigations and respond more effectively.

Endpoint and Human Risk-Analytics driven Hardening

Bitdefender's risk analytics engine enables you to continuously assess, prioritize and harden endpoint security misconfigurations and settings with an easy-to-understand prioritized list. It also identifies user actions and behaviors that pose a security risk to your organization.

By simplifying and automating security operations and continually reducing the attack surface, you will achieve the highest levels of protection with the lowest cost of ownership.

The World's Most Effective Endpoint Protection

Most #1 rankings in from 2018 up to 2021 in AV comparatives tests.Over 30 protection technologies developed in 20 years by Bitdefender's world class researchers, mathematicians and data scientists result in superior protection that is currently licensed more than 150 leading technology companies.

Local and Cloud based Machine Learning: Bitdefender first launched machine learning in 2009, resulting in increased threat detection with low false positives that can stop unknown threats at pre-execution and on-execution.

Hyperdetect - Tunable machine learning: Enables IT teams to tune protection on sensitive business services with the highest risk.

Anomaly Defense: Advanced machine learning technology that baselines system services and monitors for stealthy attack techniques. Able to protect custom apps from malicious attack.

Cloud-Based Sandbox: provides pre-execution detection of advanced attacks by automatically sending files that require further analysis to cloud sandbox and taking remediation action based on the verdict.

Network Attack Defense: Detect and block new types of threats earlier in the attack chain, such as brute force attacks, password stealers, lateral movement.

1 cloud-deliver solutions only

2 eXtended EDR is available only on cloud-deliver solutions, standard EDR is available for on-premises solutions

Exploit Defense: Several exploit prevention engines protect memory and block attacks before they exploit systems, reducing triage efforts.
Fileless Attack Defense: Detect and block script-based, file-less, obfuscated and custom malware with automatic remediation.
Integrated client firewall, device control, web content filtering, app control and more

Extended incident investigation and smart response for evolved protection

GravityZone Ultra enables effective incident investigation and quick response to restore the endpoints to a “better-than-before” stage. Incident investigation tools like Extended Incident View provide organizational-level visibility on security incidents and 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.By using the 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.

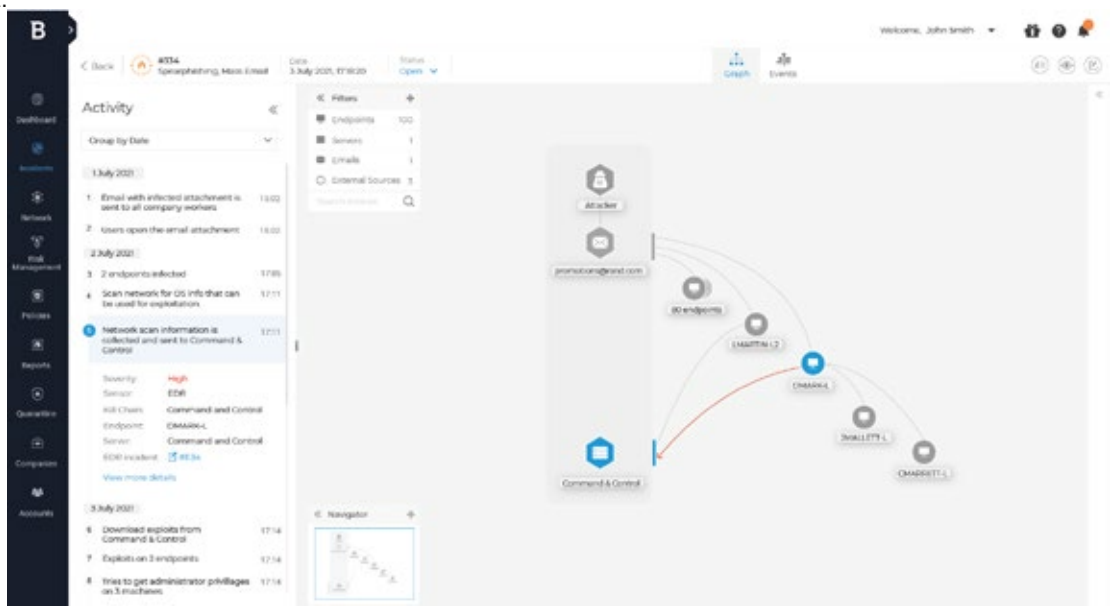
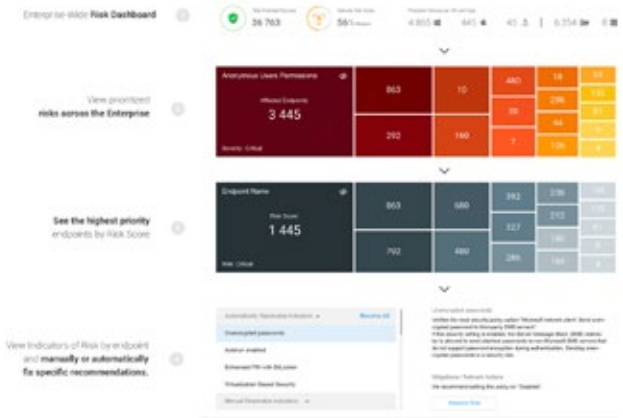


Figure 2. The Extended Incident View provides organizational-level visibility on the incident. The security analyst can easily acquire supporting evidence and respond effectively.Endpoint Risk Analytics for Continuous Attack Surface Management

Enables Active System Hardening Processes Across the EnterpriseBitdefender’s Endpoint Risk Analytics (ERA) engine enables organizations to continuously assess, prioritize, and harden endpoint security misconfigurations and setting with an easy-to-understand prioritized list. With unique risk analytics, there is continuous attack surface reduction.



Key Features

eXtended Endpoint Detection and Response (XEDR[3])

This cross-endpoint correlation technology, known as eXtended EDR, takes threat detection and visibility to a new level by applying XDR capabilities for detecting advanced attacks across multiple endpoints in hybrid infrastructures (workstations, servers or containers, running various OS).

Integrated Human and Endpoint Risk Analytics

Continuously analyze risk using hundreds of factors to uncover and prioritize configuration risks to all your endpoints, enabling automatic hardening actions. It identifies user actions and behaviors that pose a security risk to the organization such as using unencrypted web pages for logging into websites, poor password management, usage of compromised USBs, recurrent infections etc.

Layered Defense

Signature-less technologies, including advanced local and cloud machine learning, behavior analysis technologies, integrated sandbox and device hardening work as a highly effective layered protection against sophisticated threats.

Low Overhead Incident Investigation and Response

Fast alert triage and incident investigation, using attack timeline and sandbox output, enable incident response teams to react fast and stop ongoing attacks (one-click to respond).

Modern, Next-gen Prevention and Detection with Automatic Remediation

World's best prevention stack and on-execution behavior-based detection capabilities prevent and stop advanced threats from being executed on enterprise infrastructure. With advanced prevention capabilities such as PowerShell Defense, Exploit Defense and Anomaly Detection, GravityZone Ultra blocks modern day attacks earlier in the attack chain, at pre-execution, bullet-proofing your organization security posture. Once an active threat is detected, automatic response kicks-in for blocking further damage or lateral movements.

Network Attack Defense

Bitdefender Network Attack Defense, a new endpoint network security layer designed to detect and prevent attack attempts which are making use of network vulnerabilities blocks several networks stream based attacks such as Brute Force, Password Stealers or Lateral Movement before they can even execute. Network Attack Defense also generates EDR incidents and is an important source of information for EDR incidents correlations.

Cross platform Coverage and 3rd Party Integration API's

It covers all enterprise endpoints, running Windows, Linux or Mac, in physical, virtualized or cloud infrastructures, delivering consistent security across entire infrastructure. Supports integration with pre-existing security operations tools (including Splunk) and optimized for datacenter technologies including all major hypervisors.**eXtended EDR is available only on cloud-deliver solutions, standard EDR is available for on-premises solutions

3 eXtended EDR is available only on cloud-deliver solutions, standard EDR is available for on-premises solutions

Built for Cyber-Resilience

Bitdefender GravityZone Ultra relies on a single agent/single consoler architecture to provide the complete set of security capabilities, single-pane-of-glass visibility, and integrated management across the entire enterprise environment: workstations (physical and virtual), servers and cloud workloads. GravityZone is cloud-native but also supports on-premises deployments when regulations or business requirements are imposing so.

Figure 3. Bitdefender GravityZone Ultra: Unified Prevention, eXtended Detection, Response and Risk Analytics

Contact us

For more information about the Bitdefender technology solutions or to request an evaluation, please reach us at http://bitdefender.com/business

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is the industry's trusted expert* for eliminating threats, protecting privacy and data, and enabling cyber resiliency. With deep investments in research and development, Bitdefender Labs discovers 400 new threats each minute and validates 30 billion threat queries daily. The company has pioneered breakthrough innovations in anti-malware, IoT security, behavioral analytics, and artificial intelligence and its technology is licensed by more than 150 of the world's most recognized technology brands. Founded in 2001, Bitdefender has customers in 170 countries with offices around the world. For more information, visit https://www.bitdefender.com.

*Bitdefender has ranked #1 in 54% of all tests by AV-Comparatives 2018-2021 for real-world protection, performance, malware protection & advanced threat protection.

Bitdefender®

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne