Bitdefender GravityZone Business Security

Unified Prevention, Detection, Response and Risk Analytics

Increased adoption of cloud-based resources, increased employee mobility, newer developments in traditional and mobile operating systems, the rise of more capable adversaries, among others – have significantly impacted how organization's think about endpoint security. Organizations must protect against sophisticated, persistent threats - many which evade traditional protection. With limited resources, organizations need an integrated approach to endpoint security that can be leveraged across all workloads and infrastructure for prevention, detection and response.

Gravity Zone Business Security Enterprise is a complete Endpoint Security solution designed to provide prevention, threat detection, automated response, pre- and post-compromise visibility, alert triage, investigation, advance search and on-click resolution capabilities. By incorporating risk analytics, for both endpoint and user-generated risks, it minimizes the endpoint attack surface, making it difficult for attackers to penetrate.

GravityZone Business Security Enterprise enables organizations to accurately protect against even the most elusive cyber threats and effectively respond to all phases of an attack through:

- Attack surface reduction through firewall, application control and content control.
- Pre-execution detection and eradication of malware with tunable machine learning, real-time process inspection and sandbox analysis.
- Real-time threat detection and automated remediation.
- Pre- and post-compromise attack visibility with Root Cause Analysis.
- Fast incident triage, investigation and response.
- Current and historic data search.

With optional add-ons for:

- Data protection with full disk encryption
- Enhanced security posture with patch management.

WYCOM TECHNOLOGY

At-a-Glance

GravityZone Business Security Enterprise combines the world's most effective endpoint protection platform with Endpoint Detection and Response (EDR) capabilities to help you defend endpoint infrastructure (workstations, servers, and containers) throughout the threat lifecycle, with high efficacy and efficiency. It offers cross-endpoint prevention, threat detection, automatic response, pre and post compromise visibility, alert triage, investigation, advanced search and one-click resolution capabilities. Cloud-delivered and built from the ground up solution, it's also easy to deploy and integrate in existing security architecture.

Key Benefits

Industry-leading detection – Enhanced threat detection with comprehensive search capabilities for specific indicators of compromise (IoCs), MITRE ATT&CK techniques, and other artifacts to discover early-stage attacks.

Focused Investigation and Response – Organisational-level incident virtualisations enable you to respond efficiently, limit the lateral spread, and stop ongoing attacks

Maximum Efficiency – Our easy-to-deploy, low overhead agent ensures maximum efficiency and protection, with minimal effort. For a full managed solution, easily upgrade to Bitdefender Managed Detection and Response (MDR)

"GravityZone Business Security Enterprise is the next step in security protection. EDR makes detection more accurate and provides a solid background on what's happening at the endpoint. This helps us decide how to respond – Whether we quarantine, lock down, or delete files"

Lance Harris
Chief Information Security Officer
Esurance.

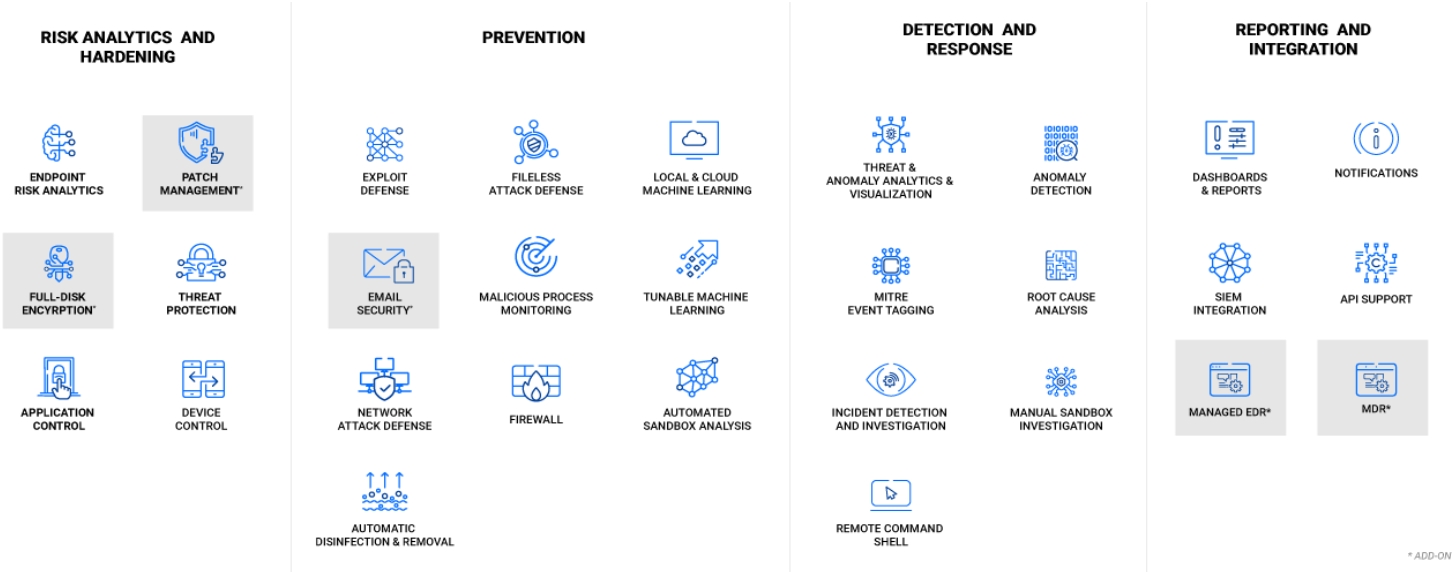
Expanding Beyond Traditional Endpoint Protection Platforms

GravityZone Business Security Enterprise provides security analysts and incident response teams with tools they need to analyse suspicious activities and investigate and adequately respond to advanced threats. With advanced prevention capabilities including anomaly detection and exploit defence, GravityZone Business Security Enterprise blocks sophisticated threats earlier in the attack chain. Pre-execution detection and EDR enhancements stop attackers from subverting your system and detect and block anomalous behaviour based on probability.

Organizations can quickly triage alerts and investigate incidents using GravityZone Business Security Enterprise attack timeline and sandbox output while enabling incident response teams to react swiftly to stop ongoing attacks with a single mouse click. In addition, MITRE attack techniques and indicators of compromise provide up-to-the-minute insight into named threats and other malware that may be involved.it continuously analyses risk using hundreds of factors to uncover, prioritize and automatically

The endpoint and human risk analytics provide an enterprise-wide Risk Dashboard for visibility and assessment of prioritized misconfigurations, applications, and user-generated vulnerabilities across the organisation's endpoint estate. Quickly review a risk snapshot for servers and end-user devices and find the endpoints and users exposed the most to zero in on misconfigurations, vulnerable applications, user behaviour risks, individual devices, and users to fix misconfigurations or patch vulnerabilities.

GravityZone Business Security Enterprise has an unmatched combination of defences at multiple levels, far exceeding competing security solutions:



Wycom is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Wycom Technology is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience.

With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioural analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands.

Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Microsoft Bitdefender Packages

FEATURES	BASIC CORE + ATS + EDR	STANDARD CORE + ATS + EDR + MDR	ADVANCED CORE + ATS + EDR + MDR + XDR
Core Features - Behaviour Monitoring - Cloud Intelligence and Machine Learning - Content Control - Device Control - Exploit Defense - Firewall - Network Attack Defense - Ransomeware Mitigation - Risk Analysis - Web Threat Protection	✓	✓	✓
ATS (Advanced Threat Security) **HyperDetect Tunable Machine Learning** (targeted attack protection, exploits, ransomeware, grayware)	✓	✓	✓
EDR (Endpoint Detection and Response) - Cross-endpoint correlation at the organizational level to effectively detect complex cyber-attacks involving multiple endpoints - Early Breach Detection - Streamlined investigation and Response options	✓	✓	✓
MDR (Managed Detection and Response) - 24x7 Monitoring - Threat inter-based hunts - Expert recommendations for containment and remediation - Recommendations and automated actions		✓	✓
XDR (Extended Detection and Response) - Enable fast, automated triage across organisation			✓

Wycom is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Wycom Technology is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience.

With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioural analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands.

Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.