Bitdefender®
Cybersecurity Built For Resilience

Integrated EDR
Cross-Endpoint Correlation
Focused Investigation and Response
XDR
Extended Incidents
Incident Advisor
GRAVITYZONE

WHY UPGRADE YOUR CYBERSECURITY WITH BITDEFENDER?

GRAVITYZONE ENTERPRISE

Industry leading Endpoint Protection and Risk Analytics that also includes:

Integrated Endpoint Detection and Response (EDR):
GravityZone Business Security Enterprise combines the world's most effective endpoint protection platform with Endpoint Detection and Response (EDR) capabilities. 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.

Cross-Endpoint Correlation:
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, and containers, running various OS).

Focused Investigation and Response:
Organizational-level incident visualizations enable you to respond efficiently, limit the lateral spread, and stop ongoing attacks.

Extended incidents/Incident advisor:
Security teams of any size and skillset are able to view threat detections, understand impact to operations and take recommended actions to contain or eliminate threats from a single view, greatly increasing efficiency. It displays all the complex incidents detected at global level in your environment, that may affect your entire network.

Extended Detection & Response (XDR):
Full XDR capabilities by purchasing Add-On XDR Sensors (Cloud, Identity, Network, Productivity)

MANAGED DETECTION AND RESPONSE

Achieve Superior Security Outcomes

Bitdefender MDR keeps your organization safe with 24x7 security monitoring, advanced attack prevention, detection and **remediation**, plus targeted and risk-based threat hunting by a certified team of security experts.

GRAVITYZONE ADD-ONS

Patch Management: Strengthen security and reduce the risk of potential vulnerabilities in software, operating systems and applications with automated patch management.

Full Disk Encryption: It provides centralized handling of the native device encryption mechanisms provided by Windows (BitLocker) and Mac (FileVault and the diskutil command-line utility) to ensure optimal compatibility and performance.

Security for Email: Multi-layered, cloud-based email security for all email service providers and supports hybrid environments using Exchange on-premises, Microsoft365, Exchange Online, or Gmail.

Security for Storage: delivers proven protection for ICAP-compatible file-sharing and network storage systems that is easy to manage

Mobile Threat Defense: insight into their mobile device footprint and associated risks to prevent and protect against attacks, detect and respond to compromised devices, and integrate mobile devices into overall security structures.

Container Security: Provides Antimalware / Anti-Exploit / EDR capabilities for Linux based Container workloads.

Integrity Monitoring: ensure you are meeting compliance and regulatory security standards by monitoring the integrity of entities such as files, registries, directories, installed applications, and   users for escalation of privilege throughout your organization.

GravityZone Data Retention (30/90/180 days): EDR Raw Data retention. Needed for compliance / historical search / threat hunting.

XDR Sensor Identity *(Local Active Directory / Azure AD / MS Intune):* Collects and processes user login information.

XDR Sensor Network: Providing insights and detections on the network.

XDR Sensor Productivity (*O365/Google Workspace*): collects and pre-processes data for email, user activity and other services.

XDR Sensor Cloud: (AWS/Azure): Collects and processes information about configuration changes and user activity.

GRAVITYZONE CSPM+

Going Beyond Cloud Security Posture Management

With GravityZone CSPM+, your overburdened teams, which are already stretched across multiple operations and security areas of expertise, can embrace cloud with confidence. CSPM+ provides visibility into your cloud footprint and automatically identifies configurations which are outside of compliance frameworks and best practices.

Going beyond standard Cloud Security Posture Management (CSPM), GravityZone CSPM+ also finds and maps over-privileged identities with Cloud Infrastructure Entitlement Management (CIEM). Finally, CSPM+ includes Threat Detection to alert your team to potential security issues to protect your cloud investment.

Cloud Risk Visibility
Inventory your cloud assets, find and prioritize misconfigurations and over privileged identities to lower risk.

Compliance Mapping
Eliminate high-effort manual efforts to quickly surface problematic configurations based on your compliance needs.

Threat Detection and Response
Detect threats and leverage actionable, human-readable outcomes in the graphical Incident Advisor.

- Visibility into your cloud platform
- Resolve misconfigurations
- Accelerate compliance
- Uncover risky identities

Leverage GravityZone CSPM+ So You Can Use Cloud With Confidence

ADVANCED THREAT INTELLIGENCE

Unique, Highly Curated and Enriched Intelligence

Bitdefender delivers accurate intelligence with value-added contextual insights focused on attack information.

The threat data is collected from its global network of hundreds of millions of sensors, as well as the technology licensing ecosystem, the Network Sandbox Analyser, cyber-security partners, plus global law enforcement agencies and turned into actionable insights — enabling customers to understand and respond to security threats even before they emerge.

Effective Alert Triage
Determine the severity of a cyber threat by prioritizing the stream of alerts and accurately differentiate between benign and dangerous situations.

Accelerated Incident Response
Enhance incident response and forensic capabilities to mitigate the latest sophisticated threats for your organization.

Proactively Uncover Attacks
Empower threat hunt missions with accurate, detailed sources of information on the threat actors most likely to penetrate your business environment.

- Unique insights into the latest threats
- Quality sourced for accurate intelligence
- Cyber-threat intelligence expertise
- Actionable threat intelligence at hand
- Robust integration ecosystem

Bitdefender Advanced Threat Intelligence Solution
delivers top-rated threat information

Learn more about CSPM+ and Threat Intelligence

bitdefender.com/business/products/gravityzone-cspm-plus.html | bitdefender.com/business/products/advanced-threat-intelligence.html