DATASHEET

Web Use Only

Bitdefender

Endpoint Detection and Response

Advanced Threat Detection, Focused Investigation And Effective Response

www.bitdefender.com

The advanced threat challenges you face today

Cyber-criminals are growing ever more sophisticated and today's advanced attacks are increasingly difficult to detect. Using techniques that individually look like routine behavior, an attacker may access your infrastructure and remain undetected for months, significantly increasing the risk of a costly data breach.

How does Bitdefender Endpoint Detection and Response (EDR) help?

When your existing endpoint security doesn't provide the advanced attack visibility and response required – adding easy-to-use Bitdefender Endpoint Detection and Response (EDR) quickly and effectively strengthens your security operations.

Advanced attack detection and response

Bitdefender EDR monitors your network to uncover suspicious activity early and provides the tools to enable you to fight-off cyber-attacks.

- EDR integrates Bitdefender's award-winning machine-learning, cloud-scanning and sandbox analyzer to detect activity that evades traditional endpoint prevention mechanisms.
- Full visibility on the techniques, tactics and procedures (TTPs) being used to attack your systems.
- Comprehensive search capabilities for specific indicators of compromise (IoCs), MITRE ATT&CK techniques and other artifacts to discover early stage attacks. In the April 2020 MITRE ATT&CK Evaluation, Bitdefender excelled at actionable detections & alerts across every step of the entire attack chain
- Take response actions to close vulnerabilities and eliminate the risk of recurrent attacks.

Bridging the cyber-security skills gap

- Easy-to-follow built-in response workflows enable your team to respond efficiently, limit lateral spread and stop ongoing attacks.
- Threat visualizations focus your investigations, help you understand complex detections, identify the root cause of attacks and maximize your ability to respond directly.
- Automated alert prioritization with one-click resolution capabilities.

Reducing organizational risk*

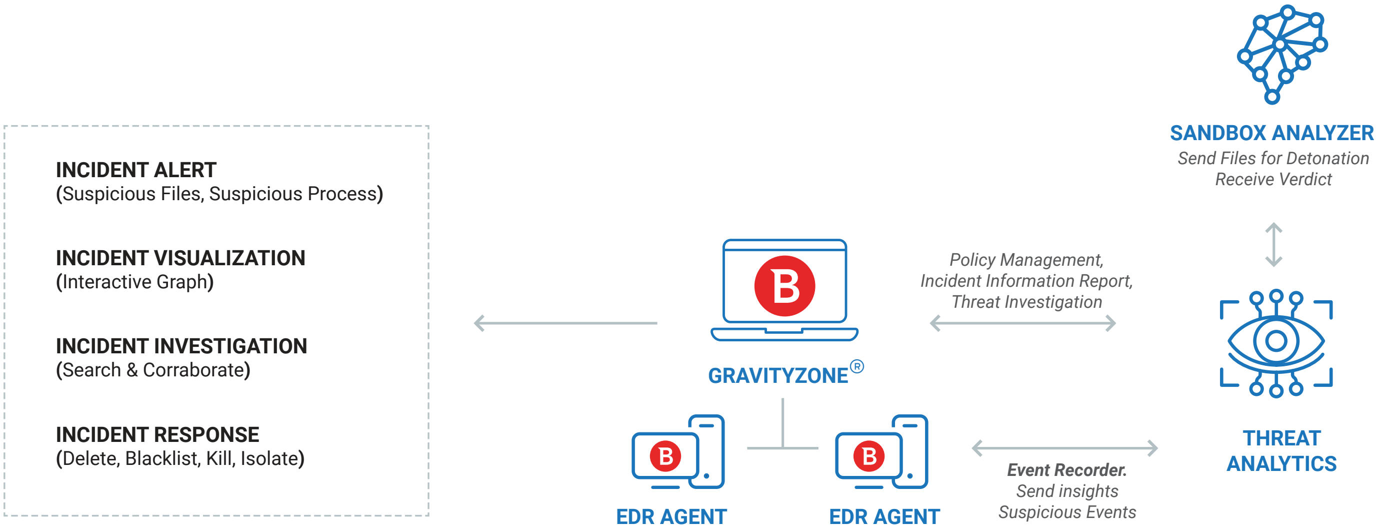
- EDR continuously analyses your organization using unique capabilities to identify risk across hundreds of factors. It provides clear guidance to assist you in mitigating your user, network and OS risks.

Minimizing operational burden

- EDR is available as a cloud and on-premises managed solution. Easy-to-deploy and integrate with your existing security architecture, it is fully compatible with your current endpoint antivirus solution.
- The lightweight agent has low disk space, memory, bandwidth and CPU resource overhead.
- Flexible, scalable and upgradeable to the full Bitdefender endpoint protection platform and to managed detection and response (MDR).

* cloud-delivered solution only

How it works



Above: Bitdefender Endpoint Detection and Response

Bitdefender EDR is a cloud or on-premises managed solution built on the Bitdefender GravityZone cloud platform. EDR agents are deployed on your organization's endpoints. Each EDR agent has an event recorder that continuously monitors the endpoint and securely sends insights and suspicious events to the GravityZone cloud.

In Gravity Zone, the Threat Analytics module collects and distils endpoint events into a prioritized list of incidents for additional investigation and response. It sends suspicious files for detonation in the Sandbox Analyzer then uses the sandbox verdict in EDR's incident reports. The EDR real-time dashboard can be accessed from any device to enable administrators to see alerts and visualizations, then investigate and respond effectively to threats.

Bitdefender Endpoint Detection and Response Features

Risk Analytics**

Human and Endpoint Risk Analytics

Continuously analyses your organizational risk using hundreds of factors to identify, prioritize and provide guidance on mitigating user, network and endpoint risks.

Detection

Industry-leading threat detection technology

Detects advanced threats including file-less attacks, ransomware and other zero-day threats in real-time. Complements your existing endpoint security solution to strengthen detection.

Threat Analytics

Cloud-based event collector continuously distils endpoint events into a prioritized list of incidents for additional investigation and response.

Event Recorder

Continuous endpoint event monitoring that feeds events to threat analytics to build threat visualizations of the events involved in an attack.

Sandbox Analyzer

Automatically executes suspicious payloads in contained virtual environment. The threat analytics module then uses this analysis to make decisions on suspicious files.

Investigate and Respond

IoC Lookup

Query the events database to uncover threats. Uncover MITRE ATT&CK techniques and indicators of compromise. Up to the minute insight into named threats and other malware that may be involved.

Visualization

Easy-to-understand visual guides, enriched with context and threat intelligence, highlight critical attack paths, easing burdens on IT staff. Helps identify gaps in protection and incident impact to support compliance.

Detonation

Operator-instigated sandbox investigation helps you make informed decisions on suspicious files

Blocklist

Stop the spread of suspicious files or processes detected by EDR to other machines

** cloud-delivered solution only

Process Termination

Instantly terminate suspicious processes to stop potential live breaches

Network Isolation

Block connections to and from endpoint to stop lateral movement and further breaches while investigating incidents

Remote shell

Execute remote commands on any workstation for immediate reaction to ongoing incidents

Reporting and Alerting

Dashboards and Reports

Configurable dashboards and comprehensive instant and scheduled reporting capabilities

Notifications

Configurable dashboard and email notifications

SIEM Integration and API Support

Supports further integration with 3rd party tools

Performance and Management

Optimized EDR agent

Low CPU, RAM, diskspace usage

Web console

Easy-to-use cloud-delivered management interface

About Bitdefender

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 antimalware, 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.