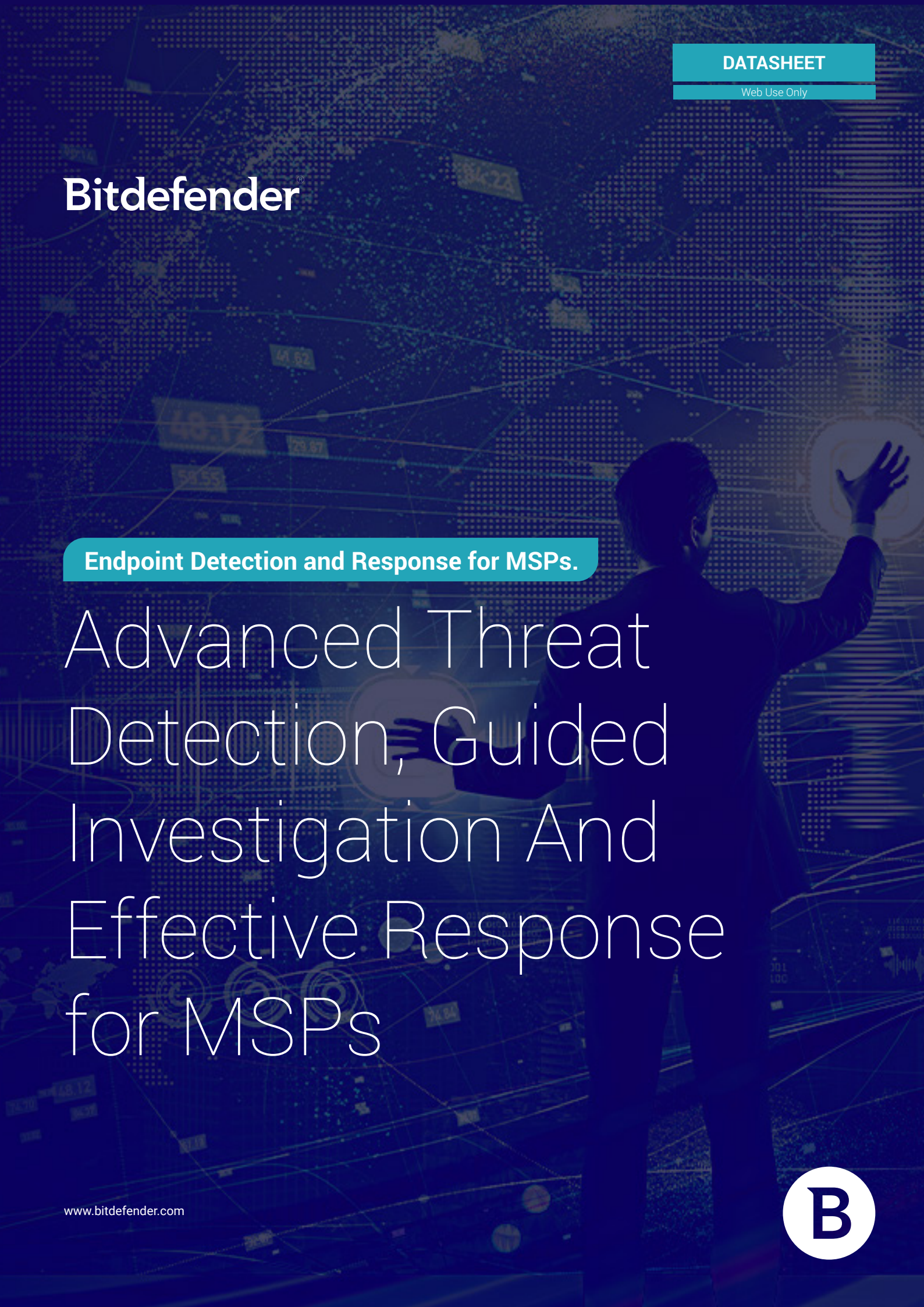
DATASHEET

Web Use Only

Bitdefender



Endpoint Detection and Response for MSPs.

Advanced Threat Detection, Guided Investigation And Effective Response for MSPs

www.bitdefender.com

Today's advanced attacks are increasingly difficult to detect. An attacker can use techniques that, individually, look like routine behavior to access your business infrastructures and remain undetected for months, significantly increasing the risk of a costly data breach.

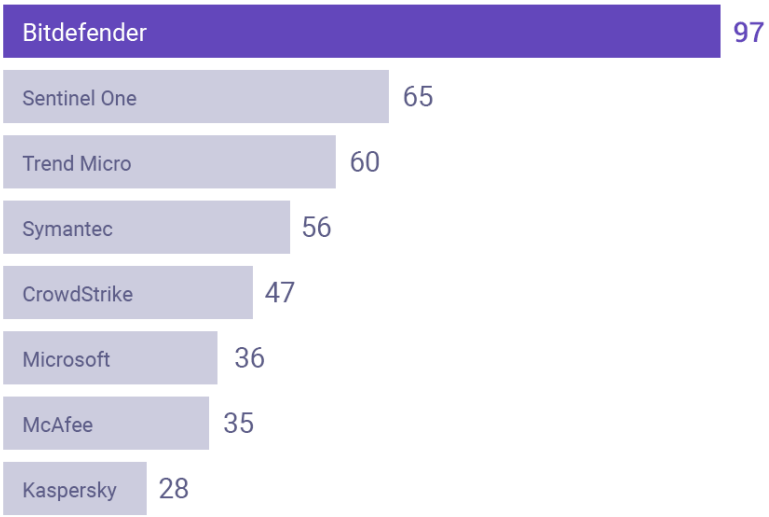
Bitdefender Endpoint Detection and Response continually monitors networks for suspicious activity and gives you the tools to fight off even the most evasive attacks. EDR's threat visualizations guide your investigations and reveal security gaps and incident impact, supporting compliance.

Integrating machine learning and behavioral technologies perfected since 2009, Bitdefender EDR delivers more actionable detections than any other vendor, as proven in MITRE 2020 tests. MSPs minimize their operational burden with more contextual information, extra technologies that filter out the noise, prioritized incidents, guided investigation and response steps.

Key benefits

- Top effectiveness in detecting advanced attacks, proven in MITRE testing
- Easy to use with prioritized incidents, guided investigations and rich context information
- Full attack chain visibility to identify security gaps and breach impact and support compliance
- Less alerts and overhead with unified Bitdefender hardening, prevention and EDR
- Enterprise-wide event correlation and analysis, detection of anomalous behavior, IOC search
- Rapid response with abilities to isolate endpoints or start remote shell connections

Top Contextual Attack Detections
For Midsized Organisations and MSPs



Sum of number of alerts for attack techniques, tactics and general detections compared to other security vendors.
Ideal for mid-sized organisations and MSPs, looking for actionable data. Bitdefender is also proven to provide alerts for every stage across the attack chain
MITRE ATT&CK 2020, APT29 evaluation roundhttps://attackevals.mitre.org/APT29/results/bitdefender/

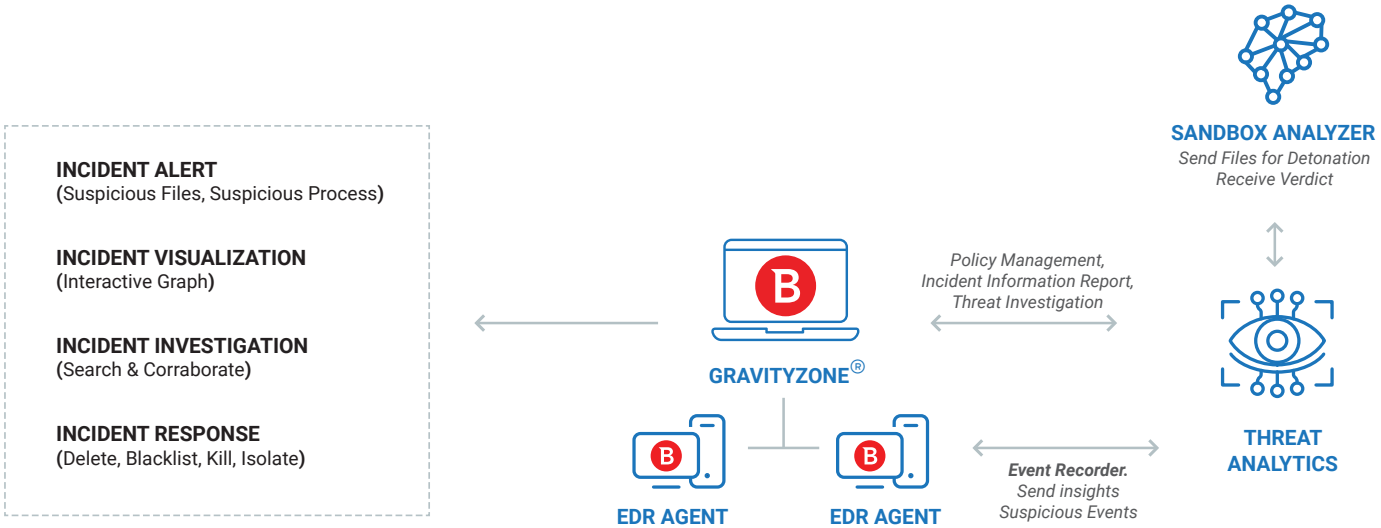
Use EDR as part of the unified MSP Security Suite or alongside 3rd party AV/EPP

For organizations whose existing endpoint security doesn't provide the advanced attack visibility and response required, adding Bitdefender EDR is a quick and effective way to strengthen security. Upgrading to EDR with Bitdefender hardening and next-gen AV is recommended to automatically stop most threats before execution, minimize data breach risks, and streamline security management.

How it works:

Bitdefender EDR is a cloud-delivered 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 data to the GravityZone cloud.

In GravityZone, 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 the EDR's incident reports. The EDR real-time dashboard can be accessed from any device to let administrators 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 fileless attacks, ransomware and zero-day threats in real time. Complements endpoint security 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 a 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.

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
Scheduled email notifications to stay informed.

SIEM Integration and API Support
Supports further integration with third-party tools.

Performance and Management

Optimized EDR agent
LowCPU, RAM, disk space usage.

Web console
Easy-to-use, cloud-delivered management.

WHY BITDEFENDER?

UNDISPUTED INNOVATION LEADER.
38% of all cybersecurity vendors worldwide integrated at least one Bitdefender technology. Present in 150 countries.

WORLD'S FIRST END-TO-END BREACH AVOIDANCE
The first security solution to unify hardening, prevention, detection and response across endpoint, network and cloud.

#1 RANKED SECURITY. AWARDED ACROSS THE BOARD.

AV comparatives CERTIFIED ATP Enterprise 2019

AV comparatives Product of the Year 2019

FORRESTER WAVE LEADER 2019 Cloud Workload Security

BITDEFENDER GravityZone Ultra v6.6.7.166 ADVANCED ENDPOINT PROTECTION NSS RECOMMENDED

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

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.

Bitdefender-EDR_MSP-DS-WebUseOnly-cresp4995-en_EN
1/1/0/20November 20, 2020 1:03 pm1/1/20/20