TECHNICAL SOLUTION BRIEF

Bitdefender®

Security

Why Security Teams Need EDR

www.bitdefender.com

Contents

Endpoint Protection, Essential but Limited

Prevention and Blocking are Not Enough

Today's **Endpoint Protection (EPP)** solutions from top security vendors as a whole have gotten really good. Compared with the past, modern EPP tools now stop more malware and more diverse threat types than ever before. Better vendors have incorporated artificial intelligence (AI), machine learning (ML) and adaptive heuristics that go far beyond the static and easily circumvented "virus definition files" of the past.

Pre-execution detection, on-execution blocking and even post-execution termination are now common capabilities of top EPP products. On balance there are fewer false-positive alerts, faster and more accurate detections and better explanations concerning what was detected and why. But EPP as a product category has fundamental limitations that every security leader should bear in mind. When everything is on the line for your business, you can't lose sight of what goes unseen by Endpoint Protection tools.

Where Endpoint Protection Comes Up Short

Breach prevention via detection and blocking at the very start of every attack would seem to be the ideal state that any InfoSec team would want to achieve, but history dating back to the first computer viruses in the mid-1980s proves that this is an elusive goal. Prevention has never been 100% and "perfect security" will realistically never be achieved. Fileless attacks and browser exploits offer no files to block and many advanced multi-stage, multi-vector attacks simply unfold in a way that makes them exceptionally difficult if not impossible to prevent. Many of these attacks can only be detected in-progress or after the fact. Specifically, EPP limitations include:

- **Too Little, Too Late:** EPP detection may occur but only after the malware has already achieved partial or total success and the target machine has been compromised with only one aspect of the attack blocked.
- **Missed Connections:** Many alerts may be generated by EPP with no obvious common threads to tie them together. Analysts can't see complete incidents or chains of related events.
- S**omething's Wrong, Now What?** Malware may have been blocked by EPP, but analysts don't know the extent of the breach, whether it exists on other machines or if anything else needs to be cleaned up.

Why You Need EDR in Your Defensive Stack

Close Key Security Gaps

Endpoint Protection is necessary for compliance and for deflecting routine malware and commodity threats, but it is far from sufficient to defend against advanced, sophisticated or targeted attacks. If you have significant intellectual property, PII/PHI, customer or financial data at risk, EDR is no longer a luxury—it is now a necessity.

Insufficient protection against advanced threats

On its own, Endpoint Protection generally offers insufficient protection against advanced threats. Sophisticated attacks often begin with benign or normal activity indicators—open a document, establish a remote connection, download a resource from the Internet, etc.—but then exhibit suspicious or malicious behavior only later on.

Lack of alert triage and response capabilities

Endpoint Protection generates many alerts, but it doesn't see every element of every attack. Although each alert represents a real threat that was blocked by EPP, there may be follow-up actions required to investigate and take corrective actions beyond deleting the identified malicious files across the enterprise. Where do you start?

Slow response to breaches once discovered

EPP provides few attack early warning signs and generates little distinction between “malicious” and “benign” assessments with few details about the threat assessment. A user may notice a misbehaving computer, or a network engineer may see unusual traffic patterns or data spikes, but no details are offered regarding causation.

Inability to identify root causes and prevent attack recurrence

OK, so your EPP solution blocked something. Don’t celebrate quite yet. Can you be certain that the entire attack was prevented or just a single aspect of it? Did the rest of the attack evade detection and succeed? What was the entry point? Where did it come from? How do we close off that path so the attack doesn’t happen again?

No visibility on TTPs / IOCs being used across the organization

Was this a one-time event or is it systemic across many victim machines within the enterprise? Has the same or similar attack occurred multiple times already? Is the attack still taking place on other machines within the organization? Can you take a single indicator of attack or compromise and search for it systemwide?

No advice on proactively improving security posture

How can you improve on your security posture and harden your defenses against future intrusions? Can you identify operating system misconfigurations, application vulnerabilities and human behavioral factors that add risk to your organization? Once identified, can you measure and track progress against improvement metrics?

EDR Business Drivers

Here are the primary business drivers that necessitate adding EDR to your defensive arsenal:

- You cannot ensure 100% protection against advanced attacks that allow intruders to remain on your systems
- You cannot terminate suspicious activity or isolate infected machines once you notice potential breach indicators
- You lack actionable intelligence to act upon or step-by-step advice to follow for how to deal with an identified breach
- You lack a centralized database of threat data for coordinated attack analysis and remediation across systems
- You are unaware of the systemic risks facing your infrastructure or how to improve your security posture proactively

The Case for Standalone EDR

Endpoint Detection and Response delivers separate value and stands on its own merits, separate and complementary to Endpoint Protection. Consider the two solutions as tandem “belt and suspenders” protection against the toughest attacks built to evade frontline defenses. You can even keep your current EPP and still add essential EDR protection.

How Do You Rate Your EPP Tools?

All EPP solutions have pros and cons and involve tradeoffs. Which statement best describes your EPP situation?

- I’m *happy* with my EPP solution but I recognize its limitations in terms of investigation and remediation
- I’m *unhappy* with current my EPP solution, but I still have time remaining on my existing contract
- I’m *indifferent* toward my current EPP solution, but it’s too disruptive to “forklift” in another tool

Regardless of how you rate your EPP solution, read on to see how a standalone EDR solution could prove to be the easiest and most significant upgrade to your security stack. It's simpler and more cost-effective than you might think.

When Standalone EDR Makes Sense

Security leaders might consider Standalone EDR to be a valuable addition to EPP under these circumstances:

- Security analysts lack visibility into suspicious and malicious activity on endpoints and on the network
- The existing EPP solution lacks easy, attractive options to add cloud delivered EDR, EDR+EPP or MDR
- Need for an incident detection and reporting capability that is compatible with existing EPP solution
- Seeking a cloud incident response platform with a thin and light agent that is easy to deploy and manage
- Desire for simplified step-by-step operational workflows for threat forensics and endpoint remediation

Bitdefender Endpoint Detection and Response

Bitdefender Endpoint Detection and Response offers/provides a combination of detective, investigative and compensative security controls which allow our customers to see beyond the typical alerts from our preventative framework. It utilizes the latest and current technologies to provide higher visibility and collect and correlate threat information, while employing analytics and automation to help detect suspicious events.

Adversary TTP Visibility

Bitdefender Endpoint Detection and Response delivers advanced attack detection and response capabilities that security teams don't get with their conventional Endpoint Security tools. Traditional products lack the visibility on the tactics, techniques and procedures being used to attack their systems. They also don't advise analysts on specific remediation steps to take or provide the tools required to directly respond to those attacks.

MITRE ATT&CK Techniques

Mapping against a global security industry standard to see the detected events and individual alerts for every phase of the attack including: Execution, Persistence, Privilege Escalation, Defense Evasion, Credentialed Access Discovery, Lateral Movement, Collection, Command & Control, and Exfiltration. When combined with other tools that also map to MITRE ATT&CK techniques, a complete picture of the attack becomes evident, along with any remaining visibility or coverage "gaps" that may still need to be addressed.

IOC / IOA Search & Correlation

What telltale signs can you look for to see if a machine has been attacked or infected? InfoSec teams can query for individual Indicators of Attack (IOAs) and Indicators of Compromise (IOCs) across the organization to look for compromised machines that may not be generating any outward evidence of being breached to either their users or security administrators.

Complete Attack Visualization with Root-Cause Analysis

Step-by-step sequences of events from initial email attack vector to first-client infection, to privilege escalation, to discovery, to lateral movement, to data collection, to exfiltration.

Prevent Attack Recurrence

Examine the paths that successful (and partially successful) attacks took and highlight ways to close these ingress and access points for recurring attacks of the same or similar nature in the future.

Alert Triage and Prioritization with One-Click Resolution

EDR helps InfoSec teams to quickly identify and prioritize incidents for focused attention and remediation, often with one-click resolution to kill suspicious processes, quarantine malicious files, blacklist attacker domains, etc.

Ease the Operational Burden

Bitdefender EDR eases the operational burden for our customers by providing capabilities that are fast and easy to deploy, do not require specialized skills to maintain, and consume minimal system resources. The product is flexible, scalable and upgradable to the full endpoint protection platform and easily supports managed security services as Bitdefender MDR.

Close the Cybersecurity Skills Gap

It helps midsize organizations to bridge the cybersecurity skills gap, through easy-to-follow built-in workflows that enable efficient security response to stop ongoing attacks and clean up any damage that has been done. Threat visualizations focus investigations to understand complex detections, identify root causes of attacks and maximize the customer's ability to respond.

Manage and Reduce Organizational Risk

Bitdefender EDR technology also helps customers assess and minimize their overall organizational risk—specifically in the areas of System Misconfigurations, Application Vulnerabilities and Human Risks—showing InfoSec teams exactly where risks arise and prioritizing the tasks necessary to quickly mitigate these risks.

EDR vs. SIEM Tools

EDR Optimized for Security Generalists

EDR occupies the "middle ground" between Endpoint Protection and a fully realized Security Information and Event Management (SIEM) system. SIEM tools are powerful and perform a valuable role in larger enterprises, but they are also expensive—initially to acquire and on an ongoing basis to staff, operate and maintain—hurdles that typically place them out of reach of small and midsize enterprises and make a poor fit for SMB customers.

SIEMs typically focus on specific alerts, discrete events or indicators—they're not designed to support complete incidents, attacks or campaigns, or the causal links, progressions or relationships between events—leaving it up to the skilled analysts to draw their own conclusions as to what exactly the data contains. Data visualizations that suggest incident relationships have to be built by hand, leading to wide variability in results across teams.

SIEMs are not actionable. They aggregate the results of one-way data feeds with no path back to the originating systems. No updates can be made, and no direct actions can be taken from within the SIEM tool to perform remediation. New events simply get posted on top of old ones. This provides a wealth of raw information for skilled analysts to search, correlate and draw their own conclusions—depending on their skill and experience.

EDR is purpose-built for detecting and responding to incidents. It automatically up-levels individual alerts into comprehensive incidents, showing chains of causation across all stages of the attack—and then makes investigation and remediation immediately actionable right from the console. Furthermore, EDR is "for everyone" in that it makes detection and response easy to follow for mid-sized, mid-skilled InfoSec teams.

Endpoint Detection and Response	Security Information & Event Management
Purpose-built to display endpoint security incidents	Aggregates generic security events and logs
Bidirectional data flows back to originating system	One-way data flows from originating system only
Pre-built security response dashboards	Analysts must build their own dashboards
Clear causal-link attack chain visualizations	No built-in attack chain visualizations
Automated incident triage and prioritization	Event severity is subject to analyst interpretation
Security response workflows and recommendations	Analyst determines response steps and sequence
Directly actionable by security responders	Not actionable by security responders
Optimized for security generalists on smaller teams	Best suited for security specialists on larger teams

Table 1: EDR and SIEM Tools Compared

Why EDR is the Better Choice

EDR is the clear choice for actionable detection and response by security generalists on mid-sized InfoSec teams at SMBs up through mid-sized enterprises, while SIEM maintains the edge for pure "big data" investigation and alert correlation across multiple input sources for large teams of highly trained security specialists.

- EDR is designed around incidents instead of alerts, up-leveling related events into comprehensive views
- EDR contains ready-built, actionable security-focused dashboards facilitating quick incident response
- Incident responders can take straightforward remediation actions directly from within the EDR console
- Analysts can perform relevant queries and correlations among IOCs and IOAs across the enterprise
- Security teams can perform root-cause analyses using clear attack-chain visualizations
- Admins can measure and reduce systemic risks across endpoint OS, applications and human elements
- Incident responders can quickly triage and prioritize alerts, then follow clear remediation instructions

Beyond EDR

Endpoint Protection is necessary for compliance certification and for deflecting the low-hanging fruit of traditional attacks but has built-in limitations. Endpoint Detection and Response is much better suited to handle sophisticated multi-stage, multi-vector attacks that are specifically designed to evade frontline defenses.

For business leaders focused on security outcomes rather than tools, **Managed Detection and Response (MDR)** ensures that you get the most out of your security stack with optimal analysis and response performed by trained security experts operating around-the-clock from a dedicated **Security Operations Center (SOC)**.

What Comes Next?

Network Detection and Response (NDR) takes EDR to the next level, leveraging network traffic analytics generated by traditional endpoints as well as IoT devices to create a comprehensive picture of the current threat environment. Further still, Extended Detection and Response (XDR) automatically collects and correlates data across multiple enterprise security controls—email, endpoint, server, cloud workloads and network—so that threats can be detected faster, and security analysts can shorten investigations and speed response times across all security controls. This unified security approach delivers complete visibility into data patterns and events across networks, clouds, endpoints and applications while applying analytics and automation to detect, analyze, hunt and remediate advanced threats across the enterprise. This is where Bitdefender's portfolio is going next.

About Bitdefender

The Most Awarded Endpoint Security Vendor

Bitdefender is consistently ranked tops in independent third-party tests and evaluations:

- "Best Hosted Endpoint Protection and Security Software for 2020" – Ranked #1 and PC Editors' Choice
- "The biggest EDR vendor you haven't considered but should have" – Forrester WAVE for EDR 2020
- MITRE ATT&CK Evaluation 2020 – Bitdefender a Stellar EDR Vendor for Midsized Organizations and MSPs
- 100% detection vs. real world threats – GravityZone Ultra EDR on AV-Test evaluations for Jan-Oct 2020

See Bitdefender EDR in Action

- Watch the EDR videos: Part 1: Advanced Threats and Use Cases; Part 2: Technical Overview and Product Demo
- Get a free 1-month trial of Bitdefender Endpoint Detection and Response with our unique, limited time offer
- Service providers, get a free 45-day full-featured trial of multi-tenant Bitdefender GravityZone Cloud MSP Security

Contact Us for More Information and a Demo

Please contact us to schedule an in-depth product demonstration and discussion of Bitdefender Endpoint Detection and Response or GravityZone Ultra EPP+EDR to learn how these solutions work to prevent and mitigate ransomware attacks.

RECOGNIZED BY LEADING ANALYSTS AND INDEPENDENT TESTING ORGANIZATIONS

TECHNOLOGY ALLIANCES

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.