Bitdefender Global Leader In Cybersecurity

Consolidate Endpoint Security to Reduce Cost

A practical guide to empowering Lean IT Teams with Unified Prevention, Detection, and Proactive Attack Surface Reduction

SOLUTION GUIDE

Organizations face a fragmented security landscape, often combining endpoint protection (EPP) with separate Endpoint Detection and Response (EDR) solutions. This siloed approach introduces unnecessary complexity, duplicated costs, and create gaps in visibility and control.

Leading organizations are consolidating their security stack by unifying prevention, protection, detection, and response in a single platform. At the same time, they are moving toward proactive hardening to reduce risk before attacks occur.

A unified approach reduces alert noise, streamlines operations, and stops threats earlier. Organizations can lower total cost of ownership, often by up to 50%, while enabling teams to do more with existing resources.

At the same time, attackers are faster, more automated, and increasingly rely on Living-off-the-Land techniques (LOTL) to evade traditional controls. This complex, tool-heavy environment, combined with the cybersecurity skills shortage, is not sustainable.

Organizations using Bitdefender GravityZone Endpoint Protection (EPP) already have one of the most trusted and proven endpoint protection capabilities in place. This means many attacks are stopped automatically.

The next step is to build on it, further consolidating security and improving resilience against modern threats.

The question for IT leaders is no longer whether detection and response capabilities exist, but whether their current approach is delivering the outcomes the business requires.

Reduce Complexity. Lower Risk. Stop Attacks Earlier.

Now is the time to move beyond fragmented tools and reactive workflows toward a unified, prevention-first security architecture that seamlessly integrates advanced detection with proactive attack surface reduction to simplify operations and improve security outcomes.

The Current State: Complexity, Cost, and Gaps

For many organizations, endpoint security has organically evolved into a fragmented, multi-vendor environment that creates more challenges than it solves. Tool sprawl is driving unsustainable complexity. According to IBM research, organizations now manage an average of **83 separate security solutions**[1].

Deploying endpoint protection (EPP) alongside separate, third-party EDR tools further compounds the problem. Limited integration creates visibility gaps and forces IT teams to switch between consoles, manage multiple agents, and investigate alerts without full context.

The impact can be significant: organizations spend an **average of 32 days**[2] fixing perimeter device flaws, leaving a massive window of exposure for attackers to exploit. Standalone tools are struggling to keep up, with ransomware now appearing in **44%** of breaches; representing a 37% year-over-year rise[2].

The Reality: Attackers Are Outpacing Traditional Defenses

The nature of cyberattacks has fundamentally changed. Today's threat actors do not just "hack in", they "sign in". They are faster, increasingly AI-enabled, and heavily utilize Living-off-the-Land (LOTL) techniques. These techniques involve attackers abusing legitimate, trusted binaries such as PowerShell or Windows Management Instrumentation Command-line (WMIC) to evade detection, like an intruder using a valid badge instead of breaking a window.

A recent analysis revealed that 84% of cyberattacks now abuse legitimate tools to evade detection. Because these actions appear trusted, conventional security tools and reactive EDR systems often fail to flag them until the attacker has already established a foothold.

Relying on detection alone is simply no longer sufficient. Without proactive controls to dynamically reduce the attack surface, security teams are forced into a reactive cycle of monitoring and responding after the fact, which extends the time required to contain threats.

At the same time, the operational model supporting security has not kept pace. Managing multiple disconnected tools requires specialized SecOps expertise that are difficult to recruit and retain. Most critically, each tool adds to the attack surface and increases the chance of misconfigurations that attackers can exploit.

Your Biggest Cyber Risk Could Be What You Already Trust: a fresh, standard Windows 11 installation includes 133 native Living-off-the-Land binaries (LOLBins) that attackers can weaponize. Furthermore, up to 9**5% of user access to these risky administrative tools is completely unnecessary** for their day-to-day work. As a prime example of this unnecessary risk, **99% of companies have** Bitsadmin **enabled**, despite not actually using it.

What's the Risk of Keeping the Current EDR Approach?

Maintaining the status quo carries clear operational and financial risk. Organizations that fail to modernize their approach face:

↳ Higher risk of breaches: Gaps between EPP and standalone EDR solutions increase the likelihood and impact of ransomware, data loss, supply chain risk, and business disruption.

↳ Operational burnout: Constant alert monitoring across disconnected tools is unsustainable; 49% of security professionals report burnout[3].

↳ Growing skills gap pressure: Complex environments require scarce expertise, with 57% of executives reporting the cybersecurity skills shortage has worsened over the last 12 months[3].

↳ Rising costs: Duplicated tools, manual investigations, and incident downtime significantly inflate the total cost of endpoint security.

The Mid-Market Disadvantage: Lean teams are disproportionately affected by tool sprawl and visibility gaps. Organizations with fewer than 1,000 employees are **almost 20% more likely to see a security incident escalate into a full data breach** compared to larger enterprises with vast security budgets[2].

The Desired Security Outcomes: Future State

The future state of endpoint security is built on consolidation and proactive defense. Organizations require a mature EDR platform that delivers advanced investigation workflows, customizable detections, and response automation to help lean IT and security teams operate more efficiently and respond faster to threats.

Rather than layering multiple vendor solutions, organizations can unify prevention, protection, detection, and response within a single platform managed through a single agent and console.

These layers are further strengthened by Dynamic Attack Surface Reduction (DASR) dynamic attack surface hardening that continuously reduces exposure by limiting risky user behavior, controlling excessive privileges, and preventing the misuse of legitimate tools commonly leveraged in modern attacks.

In this future state, security teams no longer wait for alerts to trigger a response. With prevention, detection, and automated response working together, organizations can proactively prevent the conditions that allow attacks to succeed while simultaneously reducing operational burden on security teams.

Consolidation of tools and optimized operations reduces reliance on large teams of costly security professionals. One Bitdefender customer estimated they reduced incident response times by 50%[4].

Your Next Step in Security Maturity: Bitdefender EDR + PHASR

Bitdefender addresses the complexities of modern cybersecurity by consolidating critical capabilities into the GravityZone Platform. Its core differentiation lies in a prevention-first architecture: a multi-layered, defense-in-depth framework where independent controls overlap, meaning multiple layers would have to be bypassed simultaneously for an attacker to succeed.

For organizations running standalone EDRs, Bitdefender offers a powerful consolidation path: Bitdefender Business Security Enterprise (EPP + EDR) augmented with PHASR (Proactive Hardening and Attack Surface Reduction).

Security Stage	Current State (Bitdefender EPP + 3rd party EDR)	Added value from the upgrade (+ Bitdefender EDR + PHASR)
Prevention	Baseline risk reduction: existing EPP capabilities, such as risk management, device control, provide visibility into vulnerabilities and baseline policies, but rely on static rules. This lack of dynamic control creates a blind spot around excessive user permissions and the misuse of legitimate native tools.	Dynamic attack surface reduction: PHASR continuously learns user behavior and dynamically restricts up to 95% of unnecessary tools and privileges before they can be exploited.
Protection	Blocks malware execution: pre-execution defenses automatically prevent known and unknown malware.	Stops stealthy attacks: by removing the legitimate tools attackers need to move silently (living-off-the-land techniques), PHASR halts stealthy attacks early and significantly cuts investigation workloads.
Detection	Isolated alerting: the standalone 3rd-party EDR surfaces suspicious activity, but lacks context from the EPP layer, often resulting in alert fatigue.	Mature, automated cross-endpoint correlation: Gravityzone EDR automatically correlates signals across endpoints and security layers, transforming fragmented alerts into a unified, actionable incident view.
Response	Disjointed containment: teams must manually pivot between separate EPP and EDR consoles to investigate and contain incidents.	Accelerated resolution: A single console provides real-time attack visualization and single-click response capabilities, accelerating incident response times by up to 50%.

The result is a unified, highly efficient security operating model:

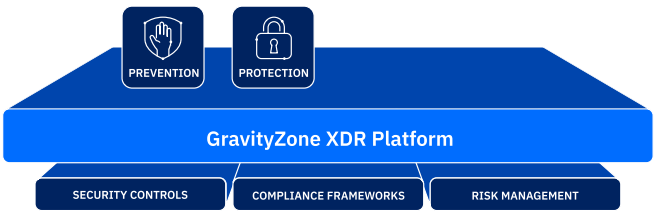
↳ A single agent & console eliminates the complexity, blind spots, and duplicated costs of managing multiple vendors.

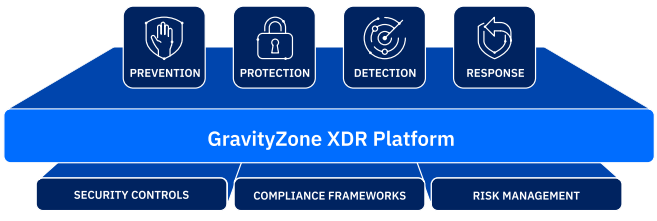
↳ PHASR proactively reduces what attackers can do, cutting cyber risk and eliminating unnecessary alert noise.

↳ Bitdefender EDR ensures that when threats do bypass preventative controls, your team has the automated context required to respond instantly and accurately.

The value of this consolidation is straightforward: lower total cost of ownership, fewer tools to manage, a drastically reduced attack surface, and faster, more accurate incident resolution.

Independent tests confirm GravityZone's high efficacy and accuracy with minimal false positives. One of Bitdefender's customers even reported an 80 to 90% drop in the volume of endpoint-related security incidents.





Bitdefender Labs

How It Works

GravityZone is built on a preemptive security architecture, where the primary objective is to stop attacks before they reach the execution phase. The platform's detection and response capabilities are engineered as backstops for a primary, prevention-centric strategy. We have built a series of coordinated, overlapping layers designed to neutralize threats at the earliest possible stage of the kill chain.

Bitdefender GravityZone Endpoint Detection & Response (EDR)

GravityZone EDR provides automatic correlation of attacks across endpoints. By automatically consolidating individual incidents into a unified, larger incident view, it accelerates response and streamlines workflows.

↳ **More Actionable Detections:** GravityZone EDR correlates a wide array of events to identify threats that bypassed other layers and consistently demonstrates a high percentage of actionable detections with minimum noise in MITRE ® ATT&CK Evaluations.

↳ **Real-Time Attack Visualization:** It provides a graphical representation of the attack chain, allowing analysts to instantly understand where an incident originated, how it propagated, and its impact.

↳ **Powerful Threat Hunting and Response:** Analysts can leverage intuitive and powerful capabilities built into GravityZone EDR such as Historical Search and Live Search to look for Indicators of Compromise (IOCs) and identify events and endpoint configurations to support regulatory compliance.

↳ **Accelerated Response:** It accelerates incident response by 50% with actionable incident insights and one-click response recommendations, empowering teams of any size and experience level.

> *"We spend 70 percent less time on incident response, which gives us more time for other strategic and complex projects."*
>
> **Macmillan Cancer Support**
> Tim O'Neill, Head of Information Security

Bitdefender GravityZone PHASR: Proactive Hardening and Attack Surface Reduction

GravityZone PHASR is a groundbreaking, dynamic attack surface reduction technology. Conventional security relies on static rules that negatively impact employee productivity. PHASR, conversely, uses AI algorithms to build risk profiles for each user endpoint combination, identifying unnecessary tools and tailoring hardening dynamically.

↳ **Dynamic Attack Surface Reduction:** It continuously learns and adapts autonomously to changing behaviors, identifying unnecessary tools, and tailoring hardening dynamically.

↳ **Precise Control:** It allows granular restriction of risky behaviors within allowed tools. For example, it can allow standard PowerShell usage for IT staff while blocking encrypted or malicious commands.

↳ **Remarkable Efficacy:** PHASR restricts up to 95% of the legitimate actions that attackers abuse, enabling organizations to cut cyber risk by 30% or more in just 30 days without adding IT burden.

↳ **Simplified Deployment and Management:** Seamlessly integrated within the GravityZone Platform. Existing customers can activate and start identifying risks in minutes.

> *"We achieved close to a 70% reduction in attack surface by locking down living-off-the land binaries and remote tools. We moved from discovery to blocking LOLBins in weeks, without investigation or disruption."*
>
> **Greenman-Pedersen, INC**
> JASON KRAAI, Systems Administrator

Multi-Layered Prevention and Protection

Underpinning EDR and PHASR are Bitdefender's robust prevention layers, including Patch Management, Risk Management to identify misconfigurations, Full Disk Encryption, and Network Attack Defense. Advanced Threat Control (ATC) applies a zero-trust model to active processes, instantly terminating sequences that attempt unauthorized code execution, thereby neutralizing supply chain compromises.

AV-Comparatives 2025 EPR Test: Bitdefender achieved top breach prevention and the lowest TCO and was the only vendor to block 100% of attacks during the first stage.

The Transformation at a Glance: Fragmented vs. Unified Security

Commercial Outcomes

Bitdefender EPP + 3rd Party EDR	Bitdefender EPP + EDR + PHASR
High total cost of endpoint security Fragmented tools increase the total cost of ownership of endpoint security through multiple vendors, licenses, and management overhead.	**Lower cost of endpoint security** A cost-efficient upgrade adds Bitdefender EDR to your existing EPP, avoiding the need for a separate solution. Consolidated licensing and simplified management eliminate the cost of acquiring, deploying, and operating an additional vendor.
Increased risk due to security gaps Siloed tools create gaps in visibility and coverage, increasing risk across the attack lifecycle, while modern attacks are faster, more AI-enabled and they abuse legitimate tools, which makes it harder for teams to detect and respond before a breach occurs.	**Reduced risk across the attack lifecycle** A single platform consolidates critical security capabilities to deliver unified management, visibility, and reporting across your entire security program. With PHASR continuously hardening your environment and stopping attacks before they escalate, you reduce risk across the entire cyberattack lifecycle.
Reactive security with no control over risky behavior Without dynamic attack surface reduction, teams must manually monitor and respond to risky user actions and tool misuse, increasing workload and reliance on skilled specialists.	**Increased efficiency for lean IT teams** Proactive control of risky behaviour with PHASR reduces investigation and response workloads, enabling teams to operate more efficiently. “Customers have reduced their attack surface by up to 95%”.
Higher financial exposure to cyberattacks Gaps between EPP and EDR increase the likelihood and impact of ransomware, data loss, and business disruption. Modern attacks exploit trusted tools.	**Reduced financial exposure to cyberattacks** A unified platform minimises financial risk through innovative, automated hardening with PHASR that stops threats before they begin, combined with rapid detection and response.

Technical/Capability benefits

Bitdefender EPP + 3rd Party EDR	Bitdefender EDR + PHASR
Limited visibility into in-progress attacks Trusted, innovative protection blocks known and unknown threats as they attempt to execute on endpoints, but attackers can abuse excessive privileges. Even with EDR, compromised users may have more permissions than they need, giving attackers room to move laterally, escalate privileges or increase impact.	**Stop attacks before they escalate** Bitdefender combines prevention, protection, detection, and response, with PHASR that dynamically reduces unnecessary user privileges and risky actions, limiting what attackers can do even if an account or endpoint is compromised.
Tool sprawl increase complexity Multiple tools with separate consoles and workflows increase operational complexity.	**Reduce time to value** A single platform and agent simplify deployment, and PHASR continuously adapt to changing behaviors, minimizing IT overhead.
Alerts lack context across security layers Alerts are investigated without context from prevention and protection controls, slowing investigations and delaying response.	**Demonstrable reduction in business impact of incidents** Integrated attack surface reduction, automated protection and accurate, rapid detection with single click response to easily contain an attack before breach.

Key Outcomes

By upgrading from a fragmented EPP + 3rd-party EDR setup to Bitdefender EDR + PHASR, organizations achieve measurable, high-impact outcomes:

Commercial Outcomes:

↳ **Lower Total Cost of Endpoint Security:** Eliminating redundant third-party EDR tools, consolidating licenses, and removing the hidden costs of managing multiple vendors, can lower total cost of ownership by up to 50%.

↳ **Reduced Financial Exposure:** Automated hardening via PHASR stops threats before they begin, minimizing the likelihood of business disruption, ransomware payouts, and data loss.

↳ **Increased Efficiency for Lean Teams:** Reducing alert noise and automating investigation workloads allows existing staff to operate more efficiently, mitigating the need to hire scarce security experts.

Technical Outcomes:

↳ **Stop Attacks Before Escalation:** Eliminating redundant third-party EDR tools, consolidating licenses, and removing the hidden costs of managing multiple vendors, can lower total cost of ownership by up to 50%.

↳ **Reduced Time to Value:** Automated hardening via PHASR stops threats before they begin, minimizing the likelihood of business disruption, ransomware payouts, and data loss.

↳ **Demonstrable Incident Reduction:** Reducing alert noise and automating investigation workloads allows existing staff to operate more efficiently, mitigating the need to hire scarce security experts.

Stop Stealthy Ransomware Attacks
Faster, stealthier, AI-automated attacks and increased attack surfaces have made chasing EDR/XDR alerts unsustainable, especially for lean teams. PHASR disrupts ransomware attacks by proactively restricting up to 95% of the legitimate actions that attacks abuse.

Achieve Stronger Endpoint Security Without Added Complexity

The era of combating modern, AI-enabled threats with a patchwork of fragmented security tools is over. Relying on isolated EPP and third-party EDR solutions inflates costs, creates risky visibility gaps, and overwhelms lean IT teams with unmanageable alert fatigue.

By consolidating EPP, EDR, and PHASR's dynamic attack surface reduction within the Bitdefender GravityZone platform, organizations can fundamentally transform their security posture.

Rather than simply reacting to incidents after they occur, security teams can reduce unnecessary risk exposure, proactively restrict risky behaviors, lower total cost of ownership, and shrink their attack surface by up to 95%.

Security Self-Assessment: Is Your Current Stack Working for You?

Before deciding on your next endpoint security renewal, ask yourself and your team these critical questions to uncover the hidden operational and financial friction in your environment:

→ Are you currently relying on a third-party EDR solution running alongside your existing Bitdefender endpoint protection?

→ How much time is your lean IT team spending managing alerts, correlating data, and constantly switching between separate EPP and EDR consoles?

→ Have you evaluated the true total cost of ownership (TCO) of running, licensing, and managing multiple endpoint security vendors?

→ You already have strong endpoint protection in place, but how effectively and rapidly are you able to detect, investigate, and contain advanced threats that manage to slip through?

→ How are you actively handling the risk of legitimate, native tools (like PowerShell or WMIC) being weaponized and used maliciously within your environment?

If you struggled to answer these confidently, maintaining your fragmented setup may cost you more while leaving you exposed to modern attacks.

Start Your Upgrade Journey

Why pay twice for endpoint security when you can consolidate EPP and EDR into one unified platform?
We are offering a proof of concept of Bitdefender EDR, allowing you to deploy GravityZone side-by-side with your existing environment. Validate the value, experience the reduction in alert noise, and see how PHASR stops modern attacks before they escalate; with zero disruption to your business.

→ Schedule your proof of concept today

References:

1. IBM Institute for Business Value: Capturing the cybersecurity dividend
2. Verizon 2025 Data Breach Investigations Report
3. Bitdefender, 2025 Cybersecurity Assessment
4. Bitdefender Named a Customers' Choice in the 2026 Gartner® Peer Insights™ Voice of the Customer for Endpoint Protection Platforms Report
5. Bitdefender Case Study: Cora Systems Expands Cybersecurity Visibility

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071

T: +40 21 4412452

US HQ
111 W. Houston Street,
Suite 2105, Frost
Tower Building,
San Antonio, Texas
78205, USA