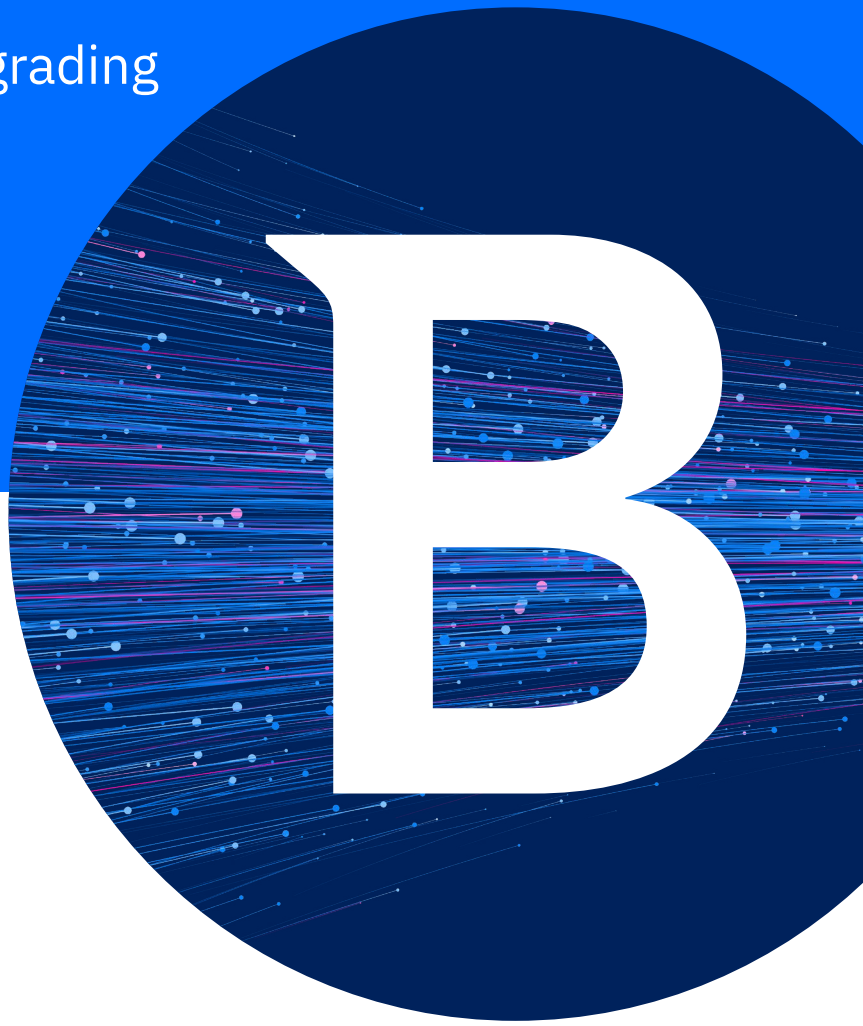
Bitdefender®

GravityZone

SOLUTION GUIDE

Addressing Modern Attacks with Proactive, Managed Security.

The Business Case for Upgrading



All Rights Reserved. © 2026 Bitdefender. All trademarks, trade names, and products referenced herein are the property of their respective owners. The information contained in this document is confidential and only for the use of the intended recipient.

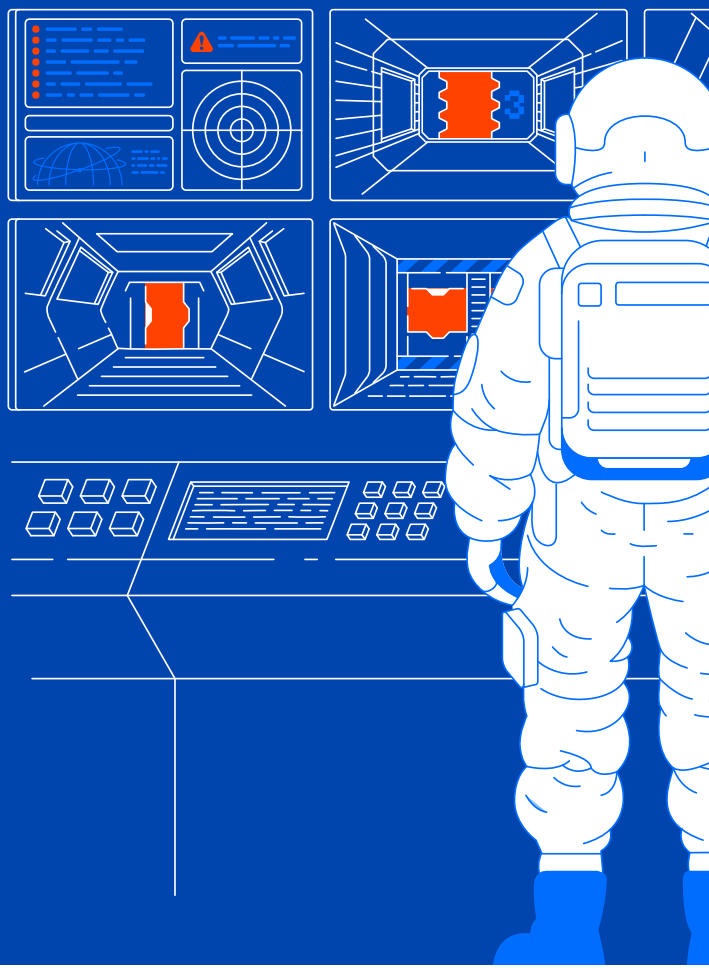
You may not publish or redistribute this document without advance permission from Bitdefender.

Your organization has already made a security investment with Bitdefender GravityZone Business Security Enterprise (BSE). You have one of the most trusted and proven endpoint protection and Endpoint Detection and Response (EDR) capabilities in place. This means many attacks are stopped automatically, and you have visibility to investigate stealthy threats that bypass other security layers and may be hiding within your network.

Despite leading and ever-improving investigation and response automation capabilities in your GravityZone product, such as recommended and automated responses, IT and security teams are resource and skills constrained. Alerts need to be reviewed. Incidents need to be investigated. Response decisions need to be made quickly. And attacks increasingly happen outside normal working hours, when the people who understand the environment are not always available.

At the same time, attackers are changing how they operate. They are moving faster, using more automation and AI, and abusing hundreds of legitimate tools that already exist on endpoints. Restricting trusted OS utilities and stopping Living off The Land (LOTL) attacks is difficult as conventional solutions such as application whitelisting create significant manual overhead and end up being too permissive to avoid impacting productivity.

For IT and security leaders, this creates a practical question.



How do you address modern threats and reduce cyber risk without adding complexity?

The answer is to extend the value of your existing GravityZone Business Security Enterprise environment with two additional capabilities:

- **Bitdefender GravityZone Proactive Hardening and Attack Surface Reduction (PHASR)**, which dynamically and autonomously reduces the attack surface by limiting risky tools, actions, and privileges based on what users actually need.

- **Bitdefender Managed Detection and Response (MDR)**, which adds 24/7/365 expert monitoring, threat hunting, investigation, and response.

Together, PHASR and MDR help your organization move from endpoint detection to proactive, managed security. PHASR reduces the opportunities attackers can exploit. MDR ensures experts are watching, investigating, and responding when action is needed, 24x7x365.

This is the next step in making your investment in GravityZone work even harder.

The issue is not visibility. It is the ability to act fast enough.

Endpoint protection and EDR remain essential. They help block attacks, detect suspicious behavior, and give your team the data needed to investigate incidents.

But EDR does not operate itself. Your team still needs to monitor alerts, understand which ones matter, investigate the scope of an incident, contain affected systems, and identify what needs to change so the same issue does not happen again. In a lean IT environment, that is difficult to sustain.

The operational pressure usually appears in four places.

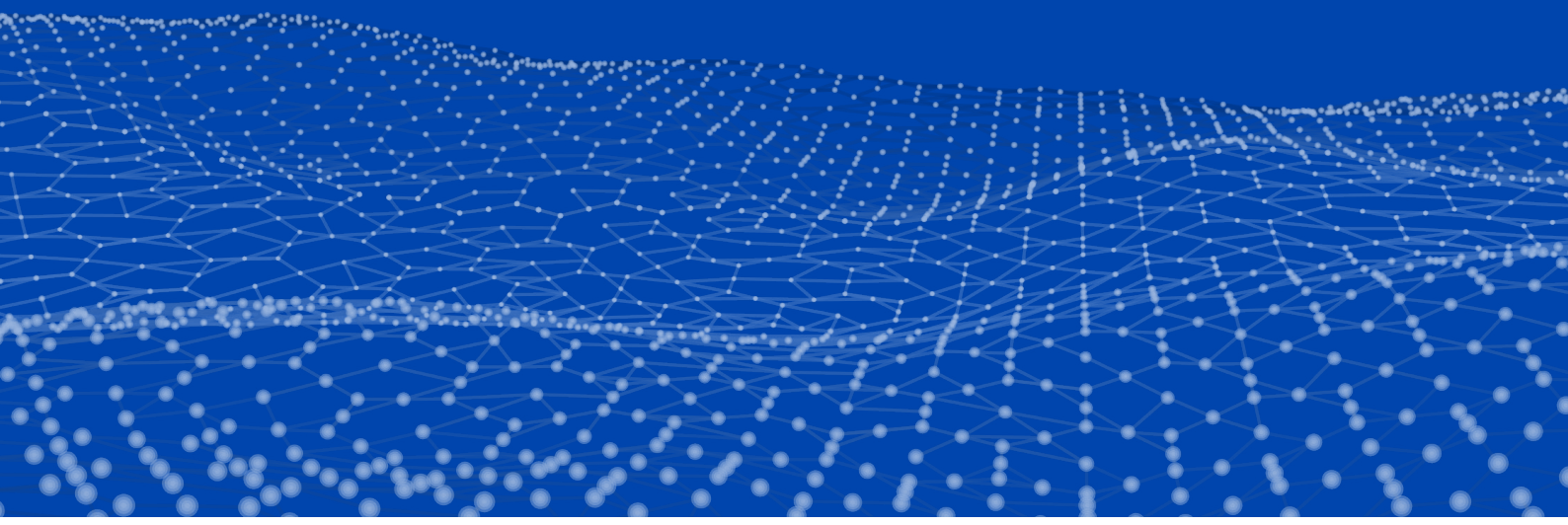
1. Security work competes with business-critical IT work
Your team is responsible for more than security. They support users, manage infrastructure, maintain systems, deliver transformation projects, and keep the business running. Using conventional tools such as application control to reduce potential abuse of legitimate tools is inefficient. Teams need to review best practices, apply hardening rules, apply and maintain exceptions, review and update regularly. Relying on detection and response to stop stealthy attacks after they execute quickly become unsustainable and it pulls people away from work that improves productivity, modernizes IT, or supports growth.

2. Response depends on availability
Attackers often operate outside business hours. When key staff are unavailable overnight or during weekends, response slows and adversaries gain valuable time inside the environment. The longer a threat advances unchecked, the greater the likelihood that an incident escalates into a widespread breach, ransomware event, or major business disruption. This is why having staff ready to investigate and stop attacks as they happen, 24/7, has become essential.

3. Legitimate tools are difficult to control
Many modern attacks abuse tools that already exist in the environment, including command-line utilities, scripts, remote administration tools, and other applications that may also be used legitimately. Blocking them broadly can disrupt users. Leaving them broadly available gives attackers more room to operate.

4. EDR value depends on specialist skills
EDR provides visibility and investigation capability, but the value depends on having skilled personnel. Many organizations have the technology but lack the time, depth of expertise, or coverage needed to get the full benefit from it.

This is why the next step for many GravityZone Business Security Enterprise customers is not another standalone tool. It is a more operational security model built around proactive hardening, continuous 24/7 monitoring, and expert-driven threat detection and response.



Why the threat model has changed

Traditional endpoint security was built around identifying and blocking malicious files, suspicious processes, and known attack behaviors. That is still necessary, but attackers increasingly try to avoid obvious malicious activity.

Instead, they use legitimate tools already present on endpoints. This is often referred to as Living Off The Land (LOTL). The tools themselves may not be malicious. The issue is how they are used.

For example, an attacker who compromises an account or endpoint may try to use native utilities or remote administration tools to discover systems, move laterally, escalate privileges, disable controls, or prepare for ransomware deployment. To security tools and administrators, some of these actions can look similar to legitimate administrative work until enough context is available.

Bitdefender research has found that **attackers abuse legitimate tools in 84% of incidents**. That matters because it changes the prevention strategy. You cannot rely only on identifying malware. You also need to limit what an attacker can do after compromising a user or endpoint.

That is the role of proactive hardening, often referred to as Dynamic Attack Surface Reduction (DASR).

Your next step in security maturity: **Extend your EDR to stay ahead of modern threats**

GravityZone Business Security Enterprise (BSE) provides a strong foundation: endpoint protection and endpoint detection and response.

Adding PHASR and MDR strengthens that foundation across the full attack lifecycle.

Security stage	Current value from BSE	Added value from PHASR and MDR
PREVENTION	Risk Management, Device Control, Content Control and other capabilities reduce risk exposure	PHASR proactively limits risky tools, actions, and privileges before attackers can abuse them, while risk-based threat hunting uncovers vulnerabilities and dormant threats early.
PROTECTION	Prevents attacks from executing and gaining a foothold	Reduced attack surface lowers the number of tools attackers can stealthily abuse, disrupting attacks.
DETECTION	Surfaces suspicious endpoint activity for investigation	MDR analysts monitor and investigate activity around the clock
RESPONSE	Gives teams tools to contain and investigate incidents	MDR experts can contain attacks by executing pre-approved actions and guide remediation

The result is a more complete security operating model:

- **BSE** provides the endpoint security foundation.
- **PHASR** reduces what attackers can do.
- **MDR** ensures expert response when something requires action.

The value is straightforward: better risk reduction, faster response, less operational pressure, and stronger evidence that security is being actively managed.

PHASR: automatically closes the paths attackers rely on

Most hardening programs are difficult to maintain. They rely on static policies, manual rules, and exceptions. Over time, those policies either become too restrictive and disrupt users, or too permissive and leave risky tools available to people who do not need them.

PHASR takes a more practical approach.

It uses individualized AI algorithms and dynamically hardens endpoints by learning how users and applications normally behave, then restricting risky tools and actions that are not needed for legitimate work. This allows security teams to reduce attacker opportunity without creating a heavy policy-management burden.
PHASR is especially relevant for living-off-the-land attacks. Instead of asking your team to manually decide which tools should be available to every user, PHASR helps tailor controls automatically to actual user needs and changing behavior.

WHAT PHASR CHANGES

It reduces unnecessary access.
Users often have access to tools, scripts, or administrative capabilities they do not need for their roles. PHASR helps identify and restrict unnecessary access so a compromised user or endpoint gives an attacker fewer options.

It limits risky actions inside legitimate tools.
The goal is not simply to block tools outright. PHASR can restrict risky behaviors while preserving legitimate use cases, helping avoid disruption to normal work.

It adapts as users and threats change.
Static hardening requires constant upkeep. PHASR is designed to adapt to changes in user behavior and attacker techniques, reducing the manual work required from IT.

It makes risk reduction measurable.
Attack surface reduction should not be invisible. PHASR helps quantify the impact of hardening activity so IT leaders can show how risk is changing over time.

It reduces the burden on response teams.
When attackers have fewer viable actions available, fewer incidents should reach the point where they require full investigation and containment.

PHASR has demonstrated the ability to reduce the attack surface and improve security efficiency without disrupting users' activity. Greenman-Pedersen achieved close to a **70% reduction in attack surface** by locking down Living-Off-The-Land binaries and remote tools while UK-based MSP, BDR Group, reported 7 ransomware attacks stopped and approximately 80% attack surface reduction in 90 days.

For organizations already using BSE, PHASR is a logical next step because it strengthens prevention before an alert becomes an incident.

MDR: add expert response without building a security operations center (SOC)

EDR creates visibility. MDR turns that visibility into a managed outcome.
For many organizations, building a full internal SOC is not realistic. It requires hiring analysts, covering nights and weekends, building processes, maintaining detections, training staff, and managing retention in a competitive labor market.

Bitdefender MDR gives your team access to expert security operations without having to build that capability from scratch.

MDR provides 24/7/365 monitoring, proactive threat hunting, investigation, response, root cause analysis, and recommendations. It is designed to work as an extension of your team, not as another source of alerts for your team to interpret on its own.

WHAT MDR CHANGES

It closes the coverage gap.
Bitdefender experts monitor continuously, including nights, weekends, and holidays. Security events do not wait until your team is online.

It improves response speed.
MDR analysts investigate suspicious activity and can act through pre-approved response actions when containment is required.

It reduces alert fatigue.
The value of MDR is not simply more notifications. The value is analysis, prioritization, and action. Bitdefender MDR focuses on high-fidelity, actionable reporting so your team can focus on what matters.

It improves security maturity over time.
Incident root cause analysis, expert recommendations, and threat hunting help your organization learn from activity in your environment and improve preventive controls.

It gives your team room to focus.
When monitoring, triage, and response are performed by experts, internal staff can spend more time on infrastructure, modernization, user support, and other high-value IT work.

MDR is particularly valuable for BSE customers because Bitdefender analysts are experts who fully understand the GravityZone platform and can help operationalize the detection and response capabilities already available in the environment.

WHY PHASR AND MDR WORK BETTER TOGETHER

PHASR and MDR address different sides of the same risk problem.

PHASR reduces the likelihood that an attacker can progress by limiting the tools and actions available after compromise. It also cuts the alert noise and improves the context for SOC teams, enabling them to act faster and be more efficient. MDR reduces the impact of incidents that still require investigation or containment.

Commercial outcomes that you can expect

WITH BSE ONLY	BSE + PHASR + MDR
Risk exposure increases as attacks evolve EDR provides visibility, but modern attacks move faster, are increasingly automated and AI-enabled, and often abuse legitimate endpoint tools. Lean teams may struggle to investigate and respond quickly enough, especially after hours.	**Lower risk with faster time to value** PHASR proactively reduces the attack surface commonly abused in attacks, while Bitdefender MDR adds 24x7x365 expert monitoring, investigation, threat hunting, and response.
Security operations can slow business transformation Lean IT and security teams spend too much time reacting to alerts, investigating incidents, and maintaining controls. This pulls focus away from strategic technology projects that improve business competitiveness.	**More focus on strategic business priorities** Bitdefender experts extend your team, while PHASR helps prevent more threats before they become incidents. Internal teams regain time to support transformation, modernization, and growth initiatives.
EDR investment is underutilized Many organizations buy EDR but lack the time, staff, or SecOps expertise to fully investigate, prioritize, and respond to threats. The result is unused capability and a weaker return on security spend.	**Greater return from the existing GravityZone investment** Adding PHASR and MDR helps customers operationalize more of their existing platform, reduce risk more effectively, and simplify day-to-day security operations without adding headcount.
Customer onboarding and partner assurance can be harder Organizations may struggle to demonstrate sufficient security coverage to customers, partners, insurers, or auditors. This can delay onboarding, complicate procurement reviews, or weaken business confidence.	**Stronger security assurance that supports revenue** 24x7x365 MDR, defined response processes, SLAs, and warranty coverage help demonstrate a more mature security program to customers, partners, auditors, and insurers.
Manual hardening creates cost, complexity, and user friction Static hardening rules require maintenance, can disrupt legitimate work, and often fail to keep pace with changing user behavior and attacker techniques.	**Adaptive, automated risk reduction** PHASR uses dynamic hardening that adapts to user behavior and evolving threats, reducing risky access without relying on constant manual tuning or broad restrictions.

Technology and capability benefits compared

WITH BSE ONLY	BSE + PHASR + MDR
Teams remain overloaded by alerts and response work EDR surfaces alerts and provides investigation tools, but internal teams still need to monitor, triage, investigate, and respond. High alert volumes can delay action.	**Smarter prevention with less disruption** PHASR restricts risky behaviors based on what each user actually needs for their role, reducing attacker opportunity while preserving legitimate work.
Compromised users may have too much access Even with EDR, attackers can abuse excessive permissions, unnecessary tools, and risky user actions to move laterally, escalate privileges, or increase impact.	**Proactive risk reduction before attacks progress** PHASR continuously hardens users and applications, while MDR threat hunting helps uncover hidden threats and reduce exploitable pathways before incidents escalate.
Living-off-the-land attacks are difficult to stop Attackers can abuse trusted tools, scripts, and administrative utilities in ways that may not look malicious until the attack is already underway.	**AI-enabled SOC benefits without the operational burden** Bitdefender MDR uses advanced generative AI capabilities to help experts investigate faster, respond more efficiently, and stop attacks with less effort from the customer's team.
Security remains too reactive EDR helps detect and investigate suspicious activity, but many risks are addressed only after compromise indicators appear.	
AI-driven security is hard to operationalize AI promises faster security operations, but building, integrating, and maintaining these capabilities internally can become a complex project with uncertain results.	

How to evaluate whether you are ready

- Are you using GravityZone EDR to its full potential to maximize your investment?
- Can your team monitor and respond to security alerts 24/7?
- How quickly can your team contain a confirmed threat?
- Are security incidents delaying other IT projects?
- Does your team have the time to investigate alerts in depth?
- Can you proactively hunt for hidden threats?
- Do you know which legitimate tools attackers could abuse in your environment?
- Can you restrict risky actions without disrupting users?
- Are your hardening policies updated as users, roles, and threats change?
- Can you quantify and demonstrate to leadership where risk was reduced over time?
- Can you demonstrate 24/7 monitoring and response readiness?
- Can you show auditors or insurers that controls are being actively managed?

If several of these answers are “no” or “not consistently,” adding PHASR and MDR is a practical next step.

Conclusion

GravityZone Business Security Enterprise gives your organization a strong endpoint security foundation. Adding PHASR and MDR up-levels your security to address the velocity and stealth of modern attacks as well as the constraints on your lean IT and security team.

PHASR reduces attacker opportunity by dynamically limiting risky tools, actions, and privileges without adding overhead or slowing business. MDR adds expert monitoring, threat hunting, investigation, and response around the clock. Together they enable a more practical security operating model: fewer viable attack paths, faster expert response, better use of existing GravityZone capabilities, and less pressure on the internal team.

See how PHASR and MDR can help your team reduce attacker opportunity, accelerate response, and strengthen security without adding complexity.

↳ Visit the MDR and PHASR product pages to learn more.

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, enterprise, and government environments, Bitdefender is one of the industry’s most trusted experts for eliminating threats, protecting privacy, digital identity and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers hundreds of new threats each minute and validates billions of 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 200 of the world’s most recognized technology brands. Founded in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Release Date: May 2026

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