Bitdefender®

GravityZone

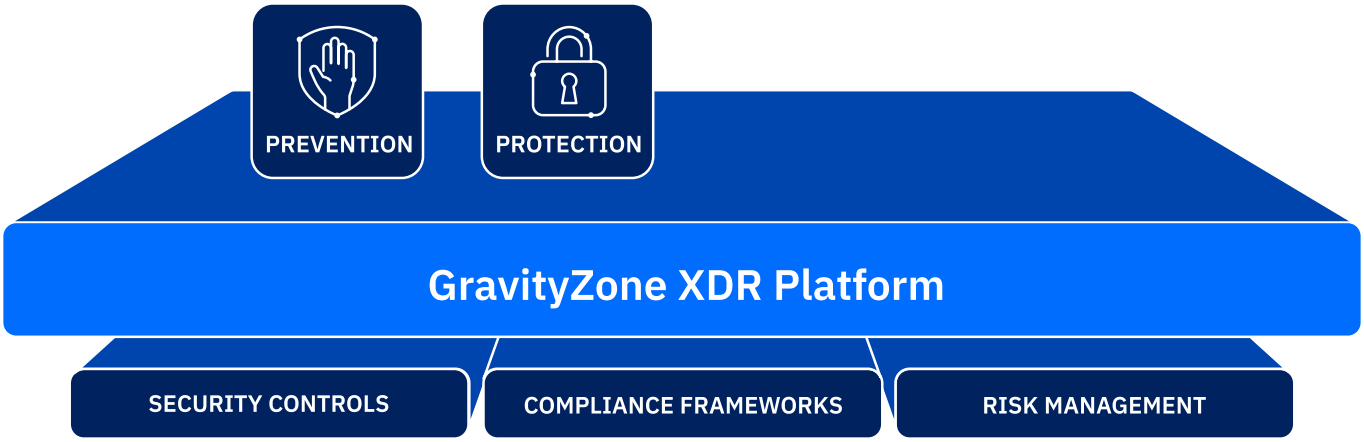
SOLUTION GUIDE

From Endpoint Protection to Managed Detection & Response

The Business Case for Upgrading

Endpoint Detection & Response is a Foundational Component of a Security Program

Your organization has already made a security investment with Bitdefender GravityZone Business Security or Business Security Premium. You have one of the most trusted and proven endpoint protection platforms (EPP) in place. This means many attacks are blocked automatically, pre-execution. However, to protect against today's threats you need a detection and response capability.



New Bitdefender research reveals that 97% of respondents use endpoint detection & response (EDR)[1]. This might appear high, especially for mid-market organizations, but even if we consider those who misunderstood the question or sampling bias, it is clear the vast majority of businesses today have already upgraded their endpoint protection.

Organizations that have not yet deployed EDR typically fall into one of two categories.

1. They don't know that EDR is now considered "table stakes" for endpoint security and is needed to achieve the security levels mandated by many regulations, cyber insurers and organizations when onboarding business partners and suppliers.

2. They know they need EDR. However, they also recognize that to obtain value from it they need resources with cybersecurity skills that they do not have today. They therefore see little point in upgrading from endpoint protection.

Whichever of these reflects your situation, there is a solution. This guide outlines the impact of not deploying EDR and the solution.

Commercial Success Can Rely on Your Security Program

Cyber attacks threaten every business, and everyone knows this. Where once breaches were reported by IT media, today they receive extensive coverage in the mass media. The result is awareness at every level of every business, from the IT security and support staff, who maintain security tools, to the CXO who is responsible for compliance, brand reputation and the company's stock price.

In a world of heightened cybersecurity awareness, proving your security infrastructure meets foundational standards is essential for commercial success. Consider three key related reasons for upgrading to EDR.

1. Supply chain attacks drive strict business partner onboarding
You have successfully won a new contract. The quicker you can onboard with this new business partner, the shorter your time to revenue. However, onboarding today is far more complex than simply negotiating a contract.

Supply chain attacks have become one of the most significant cybersecurity threats facing organizations and have driven strict vendor onboarding and third-party risk management requirements. Examples range from software suppliers, such as the SolarWinds attack that impacted thousands of organizations reliant on their software, to the more recent Jaguar Landrover attack, which caused major disruption for its complete upstream and downstream partner eco-system.

An awareness of such attacks has forced organizations to adopt more rigorous onboarding processes. These include enhanced security assessments, continuous monitoring, incident response validation, compliance verification, and stricter contractual security obligations to reduce the risk introduced through third-party vendors.

2. Compliance mandates security controls
Many broad operational, financial, privacy, and industry regulations indirectly require organizations to implement advanced security technologies and controls. Regulations governing data protection, financial reporting, operational resilience, privacy and supply chain governance increasingly depend on organizations being able to securely manage, monitor, and protect critical systems and sensitive information.

Frameworks such as GDPR, SOX and DORA reporting obligations require incident management. To support this requirement, organizations deploy detection and response technologies.

3. Cyber insurance providers mandate EDR
Cyber insurance providers are increasingly mandating the deployment of EDR solutions as a prerequisite for coverage, with many insurers requiring continuous endpoint monitoring, incident response capabilities and evidence of active threat detection before issuing or renewing cyber policies.

There is a direct link between vendor onboarding and cyber insurance coverage, as it is often a prerequisite of the process. Regardless, because of the strict mandates required to obtain coverage, it serves as a mechanism to prove security maturity.

Why Endpoint Protection is No Longer Enough

Endpoint protection stops threats at the point of entry, before they execute. It includes anti-malware, signature-based detection, exploit prevention, firewall, device control, and basic behavioral analysis.

Today, attackers try and avoid obvious malicious activity. Novel, highly-evasive threats can penetrate defenses, often by exploiting a vulnerability, and lay dormant, waiting for an attacker to activate them. Stolen credentials allow an attacker direct access to user accounts where they can go hands-on and silently progress their attack, moving laterally, elevating privileges until they locate information to steal or encrypt and hold for ransom. Once inside, there is little that endpoint protection can do; you need a security tool that can detect these behaviors.

EDR focuses on detection, investigation, and response after suspicious activity occurs. It continuously monitors and correlates behaviors across multiple endpoints, collects telemetry, identifies advanced threats and anomalous activity, and enables security teams to investigate and respond to incidents. EDR solutions typically provide capabilities such as threat hunting, forensic visibility, attack timeline reconstruction, automated containment and isolation of infected devices.

The challenges associated with EDR

EDR is “table stakes” for endpoint security, but there are a number of challenges associated with it.

EDR value depends on specialist skills
EDR provides visibility and an investigation capability, but to obtain best value from it you need personnel with security skills and the time to manage it. Bitdefender GravityZone EDR was built from the ground up to reduce the complexity associated with EDR, and many customers with lean IT and security teams obtain significant value from it, but it does require security skills and time.

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. Managing your security posture and investigating incidents pulls people away from work that improves productivity, modernizes IT, or supports growth.

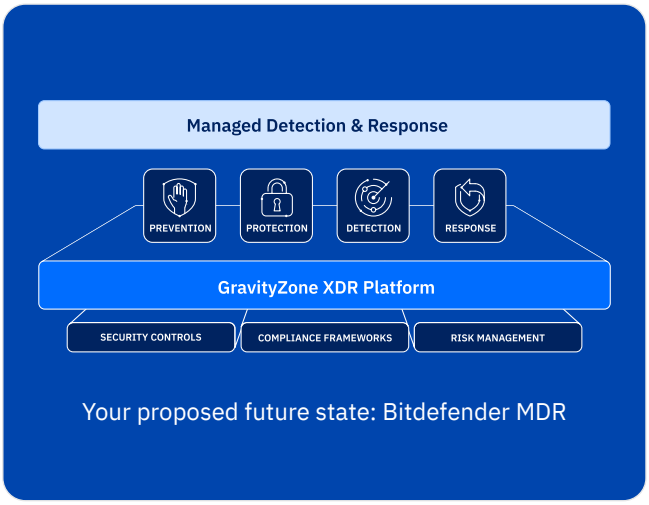
Attackers do not work business hours
If an alert appears at night, during a weekend, or when key staff are unavailable, response can slow down. That delay matters. The longer an attacker can operate, the greater the potential impact.

To address modern threats and reduce cyber risk, without adding complexity and people, you should extend the value of your existing GravityZone Business Security or Business Security Premium by upgrading to Bitdefender GravityZone Managed Detection and Response (MDR).

Your next step in cybersecurity maturity: Bitdefender MDR

The Bitdefender GravityZone platform with EDR capabilities simplifies security operations and reduces risk across the complete cyber threat lifecycle. However, to maximize its value, it does require security-savvy personnel and for many organizations, building a security team is unrealistic. It requires hiring analysts, covering nights and weekends, building processes, maintaining detections, training staff, and managing retention in a competitive labor market.

By upgrading to Bitdefender MDR, you realize all the benefits of GravityZone EDR, managed by an expert team.



The value is straightforward: better risk reduction, rapid response, no increase in operational pressure, and most importantly, stronger evidence that security is being actively managed. MDR turns the visibility provided by EDR into a managed business outcome.

MDR brings 24x7x365 monitoring, proactive threat hunting, investigation, response, root cause analysis, and recommendations. The Bitdefender MDR security experts work as an extension of your team.

WHAT Bitdefender MDR BRINGS

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

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

It doesn't create work for your team
The value of MDR 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.

THE Bitdefender MDR ADVANTAGE

Once you decide that MDR is the right solution, you have numerous options of providers. Expanding your existing relationship with Bitdefender is the natural choice.

Bitdefender analysts are experts who fully understand the GravityZone platform and can help operationalize the detection and response capabilities already available in the environment. Because telemetry, detection logic, and response controls are platform-native, analysts operate with first-party visibility and tuning authority, enabling faster root-cause analysis and continuous detection refinement.

Key benefits and outcomes: current state V future state

Commercial outcomes

CURRENT STATE BUSINESS SECURITY (PREMIUM)	FUTURE STATE MDR
Accepting significant risk Low cost of acquisition and ongoing management at the expense of accepting significant risk.	**Significantly reduced risk** Significantly reduced risk at an incremental cost, from a trusted, already approved and onboarded supplier, enabling rapid time to protection and value realization.
May realize you are accepting risk but are resource constrained The path to risk reduction requires, at least, an upgrade to EDR, which is considered "table stakes" cybersecurity. For EDR to be effective, even with the least complex platforms like GravityZone, to effectively respond to incidents you need staff with cybersecurity skills. This will likely necessitate increased expensive headcount.	**The problem is outsourced to experts** 24x7x365 security cover from GravityZone SecOps experts removes the cost and burden of recruiting, training and retaining highly sought after individuals. Bitdefender's security operations centers (SOC) support 1000s of customers, creating economies of scale and cost savings that are passed on as a cost-effective MDR service.
Not achieving regulatory compliance You are likely not achieving the security coverage to comply with various regulations, many of which mandate continuous monitoring and incident detection and response.	**Demonstrable compliance achievement** Goes beyond ticking the EDR box, with professional incident response, backed by SLAs, remediation recommendations and risk-based threat hunting. Demonstrable compliance through summary reports that highlight the measures you are taking.
Unable to acquire cost-effective cyber insurance EDR is typically mandated by cyber insurance providers, so you are likely paying extremely high premiums or have zero cover.	**Easy to acquire cyber insurance at a lower cost** Insurers often provide favorable premiums and lower barriers to onboarding for organizations with enhanced security provided by MDR.
Potentially losing business/slow onboarding You might have difficulty demonstrating adequate security coverage to business partners and customers, which could prolong onboarding or contribute to lost business. This is especially true if you are unable to demonstrate that you have cyber insurance cover.	**Easy to acquire cyber insurance at a lower cost** Satisfies supply chain partner requirements by demonstrating 24x7x365 security from a well-known, trusted, global MDR provider with SLAs and warranty cover for residual risk should the service not deliver.

Technology/capability benefits

CURRENT STATE BUSINESS SECURITY (PREMIUM)	FUTURE STATE MDR
At risk of a breach Novel, highly-evasive threats can penetrate defenses, often by exploiting a vulnerability, and lay dormant, waiting for an attacker to activate them, steal information or encrypt it and hold it for ransom.	**Demonstrable increased security posture** Regular and risk-based threat hunting, performed by Bitdefender SecOps experts, discovers vulnerabilities and dormant threats that have already penetrated defenses, then provides recommendations to enable remediation.
No means to detect in-progress attacks Trusted, innovative protection blocks known and unknown threats as they attempt to execute on endpoints, but highly sophisticated, novel and offensive AI attacks can evade this protection layer, often by exploiting a vulnerability.	**Rapid detection of in-progress attacks** An AI-enabled SOC executes rapid, cross-endpoint event correlation and anomaly detection of highly sophisticated, novel attacks that have evaded defenses and are in progress.
High risk of successful ransomware attack and/or data breach Highly sophisticated, novel attacks that have evaded the protection layer can progress to steal data, encrypt it and hold it for ransom.	**Attacks are rapidly contained before damage is done** Bitdefender GravityZone SecOps experts, supported by an AI-enabled SOC, rapidly respond and contain an attacker, before they achieve their objectives, by executing pre-approved actions.
Expensive manual recovery Post incident recovery is an expensive manual process, involving clean-up, re-imaging of infected endpoints and restoration of off-line backups, if they exist and are not infected.	**Low risk of a successful attack** Pre-approved actions triggered by GravityZone SecOps experts, acting as a human-in-the-loop to avoid false positives, significantly reduce the risk of an incident progressing to a breach.
Risk of the threat reoccurring Post incident manual investigation is necessary to understand the incident, remediate and deploy measures to ensure it doesn't recur. There remains a possibility that the threat might not be eradicated and digital forensics incident investigation specialists may be required to ensure your environment is clean.	**Help and recommendations aid rapid recovery** Self-service reports for all investigations highlight affected assets, response actions and full visibility of the end-to-end attack. Detailed recommendations enable remediation and prioritization of additional security controls. Reactive threat hunting is triggered following an incident to ensure any residual threat is remediated.

Conclusion

GravityZone Business Security and Business Security Premium give your organization a strong endpoint security foundation. Today, EDR is “table stakes”, and to get the best from it, MDR up-levels your security to address the security program expectations of your business partners, regulators and cyber insurers.

MDR adds expert monitoring, threat hunting, investigation, and response around the clock, enabling you to prove security program maturity.

↳ **Visit the GravityZone MDR product page to learn more.**

Endnotes
1 Research to inform the Bitdefender Cybersecurity Assessment Report 2026

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