

Bitdefender®

GravityZone

SOLUTION GUIDE

Operationalizing AI Across Prevention, Protection, Detection and Response



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.

According to research by IBM, on average, organizations use 83 separate security solutions. It is hardly surprising that 52% of security professionals identify complexity as the biggest impediment to effective operations¹. For an IT or security leader in a mid-market organization, who knows they have gaps in security coverage, this might seem like a nice problem to have.

Most mid-market businesses have the fundamentals in place, such as Endpoint Protection Platforms (EPP), email filtering, and patch management. However, many aren't fully realizing the capabilities of these existing tools. This creates some security gaps, but when combined with a lack of preventative exposure management controls, their visibility across attack surfaces is severely impaired.



AI-Enabled Threats: Everyone's New Security Problem

For some time, the technology and mainstream media have reported the rise of offensive AI, AI-powered or AI-enabled cyber-attacks. Many have treated these reports with a degree of cynicism. However, the Bitdefender Cybersecurity Assessment 2026, a survey of 1200 IT and cybersecurity professionals across Europe, North America and South-East Asia found that only 18% of security professionals now believe that AI attacks are "mostly industry hype".

- ▶ 59% say their organization has experienced social engineering attacks they believe involve AI.
- ▶ 56% say their organization has experienced malware-based attacks that involve AI.
- ▶ 70% say they are seeing more sophisticated phishing attacks powered by AI.

The consensus among security practitioners, industry analysts and solution providers is that AI has reduced the barriers to entry for building cyber-attacks, including the cost and skills required. While the tactics, techniques and procedures associated with AI attacks are not new, what has changed is their speed. AI-based automation at machine speed can rapidly:

- ▶ Generate new malware and modify it.
- ▶ Generate highly targeted phishing emails.
- ▶ Automate attacks.
- ▶ Adapt attacks based on the target's response.
- ▶ Automate and execute vulnerability scans at scale.

AI-enabled threats are growing in number.
Tactics, techniques and procedures (TTPs) are not radically different.

The Expanding Attack Surface: Exacerbating the Problem

Organizations' attack surfaces are constantly expanding. They include not only their technologies, but their people and their business partners' technologies and people.

It has been widely reported that frontier AI models have accelerated discovery of new vulnerabilities and reduced the time to exploitation. As modern attacks become increasingly automated and happen at machine speed, the weaknesses they can exploit to get in or move across the environment grow larger: soaring and insecure AI adoption within organizations and over-privileged access to legitimate endpoint tools have emerged as two critical attack surfaces that modern attacks will exploit.

Breadth of Security Coverage: The Mid-Market Challenge

According to a report by the IBM Institute for Business Value: Capturing the cybersecurity dividend, on average, organizations use 83 separate security solutions. It is hardly surprising that 52% of security professionals identify complexity as the biggest impediment to effective operations. For an IT or security leader in a mid-market organization, who knows they have gaps in security coverage, this might seem like a nice problem to have.

Most mid-market businesses have the fundamentals in place, such as Endpoint Protection Platforms (EPP), email filtering, and patch management. However, many aren't fully realizing the capabilities of these existing tools. This creates some security gaps, but when combined with a lack of preventative exposure management controls, their visibility across attack surfaces is severely impaired.

It's an understandable challenge. For many mid-market organizations, the time, expertise, and resources needed to fully operationalize security tools can feel overwhelming. As a result, desirable capabilities enjoyed by larger enterprises can seem out of reach. The key is finding ways to broaden security coverage and strengthen protection without overextending your team.

The challenge faced by mid-market organizations:
How to fill gaps in security coverage, without adding complexity and cost



Enter AI: The Solution or Additional Complexity?

AI, of course, brings significant benefits for security teams, but it can also bring complexity. The question leaders of lean IT and security teams must ask themselves is: “Where can it benefit us most and provide the best ROI?” There are four key considerations and questions to ask yourself.

1 Benefits for your overall security program	→ Will it help improve my security posture or just detection and response times? → Does it offer help and guidance or fully autonomous response?
2. Direct benefits for your team	→ Will it improve workflows, integrate with existing playbooks and save time? → Will it proactively interrupt my team when they need help or do they have to understand when and exactly how to prompt it? → Will we be required to make wholesale changes to our working practices?
3. Trust and proof of AI capabilities	→ Is it accurate, consistent, and transparent? → Does it hallucinate? → Are appropriate safeguards in place for the AI models themselves?
4. Cost and ROI	→ How is it priced? → Are the direct costs predictable? → What are the indirect costs?

Maximize Your ROI: Operationalize AI Across Your Security Platform

Most mid-market organizations already have powerful Endpoint Detection and Response (EDR) in place, as a component of their EPP, but are unable to use it to its full potential. Setup can be complex, and high alert volumes result in overloaded teams and unresolved incidents. This is because many EDR platforms have their roots in the enterprise, with bloated functionality that requires security operations (SecOps) experts to manage.

To help them, enterprise security vendors have added AI capabilities such as chatbots, automated triage, incident investigation, autonomous response, threat hunting, and more. Clearly, accommodating this AI disruption will result in

significant changes to security teams, who must retrain and acquire new skillsets.

How will this impact mid-market organizations with lean IT and security teams who already lack deep cybersecurity skills? A belief that AI can help might not be realized; instead, the complexity levels associated with their security tooling choices may be amplified.

If your EDR platform includes under-utilized capabilities, adding AI alone is unlikely to help. You will continue to realize little return on your investment and possibly leave your organization vulnerable. The solution is to replace it with a security platform that makes AI accessible within existing workflows – one designed specifically to enable any IT professional to rapidly respond to and contain an incident before it progresses to a breach.

Action 1: Deploy a security platform that empowers your team to easily operationalize AI to maximize their effectiveness and your ROI

Add Context: Extended Detection & Response

EDR is helpful on its own, but it primarily focuses on endpoint signals. Incorporating these insights with identity, cloud, network, and email controls makes detection and response far more effective. This broader approach is known as Extended Detection and Response (XDR). It correlates signals from across your environment to provide IT and security teams with rich context so they can prioritize investigation of the most potentially dangerous threats.

However, for mid-market organizations with lean teams, deploying and managing tens of discreet integrations to provide these signals adds significant complexity. The solution is native XDR with built in AI-driven automation. With this approach, the XDR vendor provides agents, installed across your high-priority assets, to gather only the crucial signals that can add helpful context to the insights gleaned from your EDR. This creates high-fidelity detections and reduces the false positives that slow down response.

Action 2: Add native XDR to maximize your detection fidelity and IT and security team effectiveness

Stop AI Attacks: Shift to Preventative-first

The mantra of “breach is inevitable” has existed for many years in cybersecurity and drove proliferation of detection and response technologies. Often, this was at the expense of preventative security which when done right, can significantly reduce the burden of response. If you do not stop machine-speed, AI-enabled attacks early in the cyber kill chain, your detection and response layers will be overwhelmed.

Effective security programs incorporate prevention and protection from the start, hiding and blocking the entry points that attackers rely on. Prioritizing prevention means you will stop the deluge of AI-enabled attacks before they escalate into incidents that require investigation. This approach reduces the workload on your IT and security team, allowing them to focus on more urgent, high-priority tasks.

To realize prevention-first, enterprises add new point solutions which add to the tool sprawl discussed earlier. Many leaders in mid-market organizations recognize the benefits of preventative security but assume it is beyond their reach due to complexity and cost. However, there are security platforms available that have combined the most critical capabilities of enterprise tools, such as Threat Exposure Management (TEM) and Attack Surface Management (ASM).

Easily operationalized AI capabilities further remove the barrier for mid-market organizations shifting to a prevention-first security strategy by taking the guesswork out of where to prioritize and focus efforts. AI clearly brings significant benefits to detection and response, but for lean teams, getting guidance that can stop attacks before they develop into incidents removes a significant burden on them.

“Without preemptive cybersecurity, no organization is safe. The increasing speed, sophistication and scope of AI-enabled threats is destroying the reliability of existing stand-alone detection and response (DR) cybersecurity methods.”

Gartner, Tech FutureSight:
Preemptive Cybersecurity Is the Only Way to Secure
Emerging AI Attack Surfaces, Carl Manion et al., 9 May 2025

GARTNER is a trademark of Gartner, Inc. and its affiliates.

Action 3: Operationalize AI to help prioritize and guide deployment of proactive security measures that reduces the burden of response on lean IT and security teams

The Platform Advantage: AI-enabled Security Across Prevention, Protection, Detection and Response

Today’s security platforms evolved from EPP/EDR to XDR and most recently, to also incorporate prevention capabilities designed to harden systems and stop machine-speed, AI-enabled attacks from gaining a foothold. These capabilities reduce the need for resource-intensive detection and response.

Context-aware AI increases the value of this integrated approach by drawing on signals and insights from across the platform to help teams understand risk, prioritize what matters, and take appropriate action within existing workflows, while keeping people in control.

Native integrations and ready-to-use workflows simplify daily operations, eliminating the need for specialized development of integrations or custom tuning of detection rules. And the preventative capabilities provided by many platforms extend this simplicity to risk management and compliance. The result is more comprehensive security and enhanced prevention and protection, without the enterprise-level burden.

To learn more about the pros and cons of platformization, read [The Security Platform Is Dead. Long Live the Security Platform.](#)

Action 4: Operationalize AI-enabled security across prevention, protection, detection and response.

Augment Your Team: The AI-enabled MDR SOC

A unified platform that has operationalized AI across the attack lifecycle provides strong security coverage. If you are considering extending this, building out a larger team with your own 24x7x365 SOC, you might consider whether now, when AI is disrupting every aspect of security, is the right time.

The alternative is to consider Managed Detection and Response (MDR). Providers offer 24x7x365 monitoring of your platform. This augments and supports your team by helping them identify and investigate suspicious activity before it has a chance to escalate. When incidents do occur, MDR analysts take swift, decisive action to contain threats, guide remediation, and accelerate recovery.

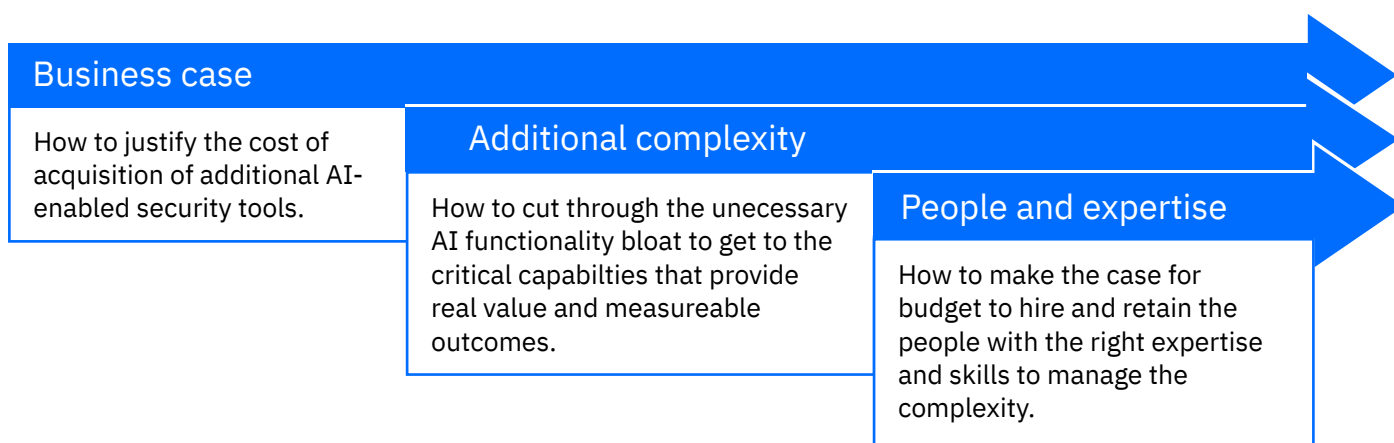
By opting for MDR you are placing significant trust in your provider, so you must ensure that they have built and deployed an AI-enabled SOC and have the skills and expertise to adapt to the disruption caused by AI.

Action 5: Consider MDR to empower your team and strengthen your overall security program.

Achieve Outcomes: Attainable, Improved, Demonstrable

For many mid-market organizations, this breadth of AI-enabled security capabilities can feel unachievable. This perception is the result of a continuum of challenges, where one leads to the next.

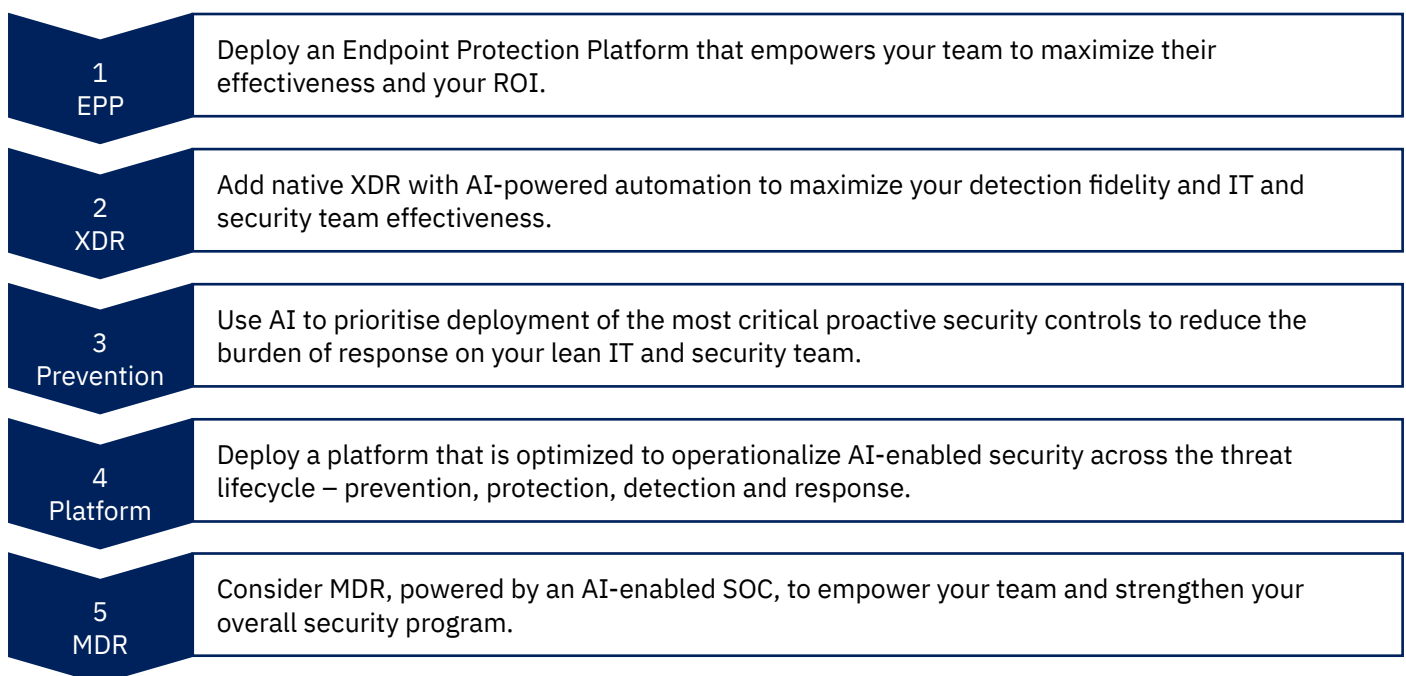
The Challenge Facing Mid-Market Organizations



As machine-speed AI-enabled threats become the norm, comprehensive visibility and defense is essential. Strengthening security coverage requires a strategic approach and intelligence, rather than simply adding headcount to manage more point solutions.

Your 5-Point Action Plan to Operationalize AI Across the Threat Lifecycle

How to achieve AI-enabled prevention, protection, detection and response within the constraints of a mid-market organization with a lean IT and security team.



Learn how real organizations obtain an ROI from their security platform: [GravityZone Platform and MDR Financial Impact Assessment](#).

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: September 2026

For more information, visit <https://www.bitdefender.com>.

Romania HQ

Orhideea Towers
15A Orhideeor 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