Bitdefender®

GravityZone

SOLUTION GUIDE

How to Secure Your Mid-Market Business Across the Complete Threat Lifecycle

Breadth of Security Coverage: **The Mid-Market Challenge**

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 operationsi. 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 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**

Maximize Your ROI: **Exploit Underused Tools**

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 challenge around the complexity associated with EDR has its roots in its history. It was originally designed to complement EPP and enable security analysts to detect and respond to in-progress cyber attacks. It was a discreet tool built for enterprises with expert security operations (SecOps) teams, so complexity was not considered an issue.

Today, EDR is a component of all leading endpoint security products. In the last decade, EPP vendors added EDR and EDR vendors added functionality to become a full EPP. The result is that many endpoint security deployments have their roots in the enterprise, with bloated functionality that requires SecOps experts to manage.

If your EPP includes under-utilized capabilities that your IT and security team cannot maximize the value of, you are not obtaining a return on your investment and possibly leaving your organization vulnerable. The solution is to replace it with one that includes EDR designed specifically to enable any IT professional to rapidly respond to and contain an incident before it progresses to a breach.

Action 1: **Deploy an Endpoint Protection Platform that empowers your team 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 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 and divert your IT and security team from other activities.

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

Be Proactive: **Preventative Security Measures**

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.

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 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.

Enterprises enhance their prevention and protection capabilities by adding new point solutions which adds to the tool sprawl discussed earlier. Many IT 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).

Action 3: **Deploy the most critical proactive security controls to reduce the burden of response on lean IT and security teams**

The Platform Advantage: **Breadth With Reduced Complexity**

The cybersecurity industry is attempting to address the complexity of tool sprawl by consolidating capabilities onto a single platform.

> *"By 2029, 30% of midsize organizations will converge workspace, data security, and identity security capabilities into a workspace security platform, enabling holistic protection and centralized policy management."*
>
> **Gartner, 2025 Strategic Roadmap for Workspace Security**
> Peter Firstbrook, Evgeny Mirolyubov, Franz Hinner, 21 April 2025.
>
> GARTNER is a trademark of Gartner, Inc. and its affiliates.

Today's security platforms evolved from EPP/EDR to XDR and most recently, to also incorporate prevention features designed to harden systems and stop attackers from gaining a foothold. They also have protection mechanisms to block threats pre-execution. These capabilities reduce the need for resource-intensive detection and response capabilities later in the security lifecycle.

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: **Deploy a platform that is optimized to provide security across the threat lifecycle – prevention, protection, detection and response**

Augment Your Team with MDR

A unified platform provides strong coverage. You can extend this security further with Managed Detection and Response (MDR) to ensure 24/7 monitoring of the platform. MDR 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.

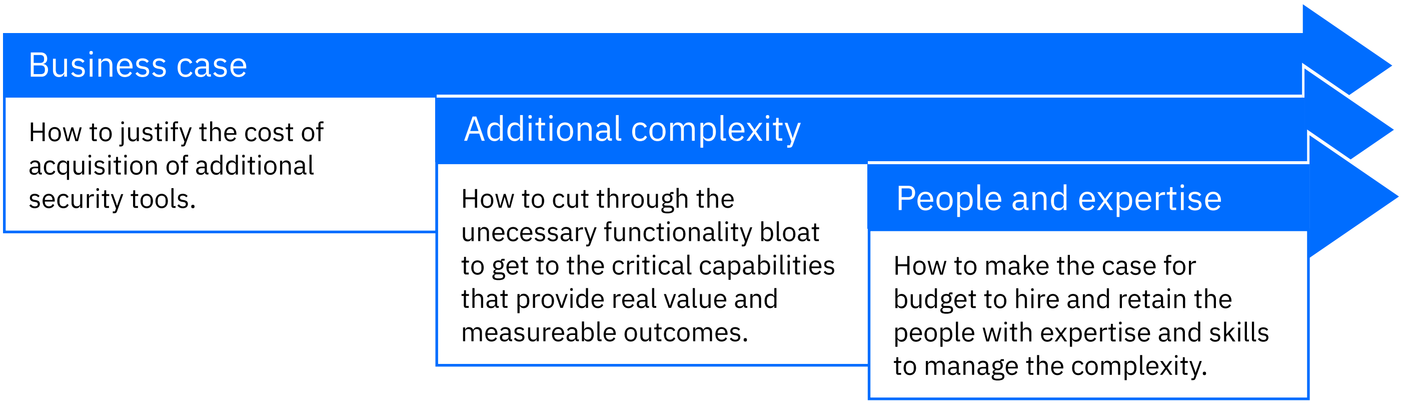
Many services extend your platform's preventative capabilities by offering expert insights and recommendations that enable you to improve your security posture. This empowers and upskills your team on the job, strengthening your overall security program without the need to build a large in-house security function.

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

Attainable, Improved, Demonstrable Outcomes

For many mid-market organizations, this breadth of 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



Business case

How to justify the cost of acquisition of additional security tools.

Additional complexity

How to cut through the unecessary functionality bloat to get to the critical capabilities that provide real value and measureable outcomes.

People and expertise

How to make the case for budget to hire and retain the people with expertise and skills to manage the complexity.

As threats become more difficult to defeat across dynamic environments, 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 Obtain Security Across the Threat Lifecycle

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

1 EPP	Deploy an Endpoint Protection Platform that empowers your team to maximize their effectiveness and your ROI
2 XDR	Add native XDR to maximize your detection fidelity and IT and security team effectiveness
3 Prevention	Deploy the most critical proactive security controls to reduce the burden of response on your lean IT and security teams
4 Platform	Deploy a platform that is optimized to provide security across the threat lifecycle - prevention, protection, detection and response.
5 MDR	Consider MDR to empower your team and strengthen your overall security program

To understand how to action this plan, read the Buyer's Guide for Mid-market Businesses: Choosing the Right Security Platform.

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: November 2025

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

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