Bitdefender®

GravityZone

Buyer’s Guide for Mid-market Businesses

Choosing the Right Security Platform

BUYER’S GUIDE

Is a security platform right for you?

Mid-market businesses with lean IT and security teams suffer similar cybersecurity challenges to their larger peers and competitors with extensive budgets and an army of security and risk management professionals. Your attack surface might not be as extensive as theirs, but it has likely expanded significantly over the last few years, providing a larger target for ransomware and other threat actors.

However, your business challenges might run deeper. The 2025 Verizon Data Breach Investigations Report stated that 30% of reported breaches involved a 3rd party[1]. This level of supply chain attacks has resulted in organizations stringently vetting their business partners, who must demonstrate they have adequate security measures in place. If you cannot do so you could lose business to competitors or, at best, delay your time to revenue due to a prolonged onboarding process while your security posture is audited.

How do you remain competitive and not lose business to your better financed and resourced competitors?

A security platform might be the answer to not only securing your business but enabling you to demonstrate that you are doing so. This will accelerate your time to revenue and if you are in a regulated industry, reduce the effort required for compliance auditing.

This buyer's guide outlines six key steps to help you understand whether a security platform is right for you.

1 What is the status of my security program?

2 Is a security platform the correct approach?

3 How do I choose the right platform?

4 How do I choose the right platform vendor?

5 How do I get the best from my chosen platform?

6 Validate my choice

When you complete these six steps and confirm that a platform is the correct approach for you and your business, the final section of the guide provides the questions you should ask the vendors on your short list to ensure you make the correct choice to meet your requirements.

Understand your security posture

Before embarking on this journey and making any changes to your security program, you should first understand if and why you might need to do so.

Gaining visibility of your attack surface is key for understanding your security posture. There are many technical solutions that can help. You are likely to have a patch management solution and a configuration management database. However, enterprise-class tools, such as a cyber threat exposure management platform (CTEM), are probably not attainable with your budget constraints. Even if they were, they would add complexity to your security program and place a significant burden on your lean IT and security team.

Important terms defined

Security posture is your overall state of information security readiness, including visibility of the state of all hardware, software, services and information.

Attack surface is the sum of everything that a bad actor can exploit to achieve their goals.

Simplified security frameworks can help

There are many organizations that publish security frameworks and guidance to help inform your understanding of your current status and your most critical gaps. These include the International Standards Organization (ISO), European Union Agency for Cybersecurity (ENISA) and North American Institute for Standards and Technology (NIST). Some create simplified frameworks for smaller and mid-market organizations.

Priority action: **Understand your current security technologies**

Whether you align with a framework or not, your first task, before considering changing or adding security technologies, is to understand what you already have in place to protect your major assets and points of initial access that might be exploited by a threat actor.

Consider your security coverage across:

- ↳ **Endpoints:** managed and unmanaged
- ↳ **Identities:** human and non-human
- ↳ **Cloud:** infrastructure and SaaS
- ↳ **Email:** gateway and platform
- ↳ **Network:** perimeter and intern

Good coverage	Gaps in coverage
If you have coverage across all, you are in good shape. Now you need to determine how effective these controls are and if they are point solutions, whether consolidating them onto a security platform will be beneficial.	If you have gaps, you should prioritize securing them based on the risk they pose. Consider the likelihood of them being compromised and the impact of an incident if they were. You must then decide whether to deploy point security solutions or if a platform meets your needs.

Confirm a security platform is the correct approach for you

Consolidating security tools onto a platform is not new. Back in 2023, eSecurity Planet reported that a Gartner survey found 75% of security buyers were pursuing vendor consolidation, and this was driving vendors to merge point products onto platforms[2]. This consolidation was driven, first and foremost, by reducing complexity, rather than direct costs.

By reducing the numbers of point security tools, you reduce your attack surface and often, because a platform typically offers tight integration and alert correlation, you can reduce your time to respond and contain an attack.

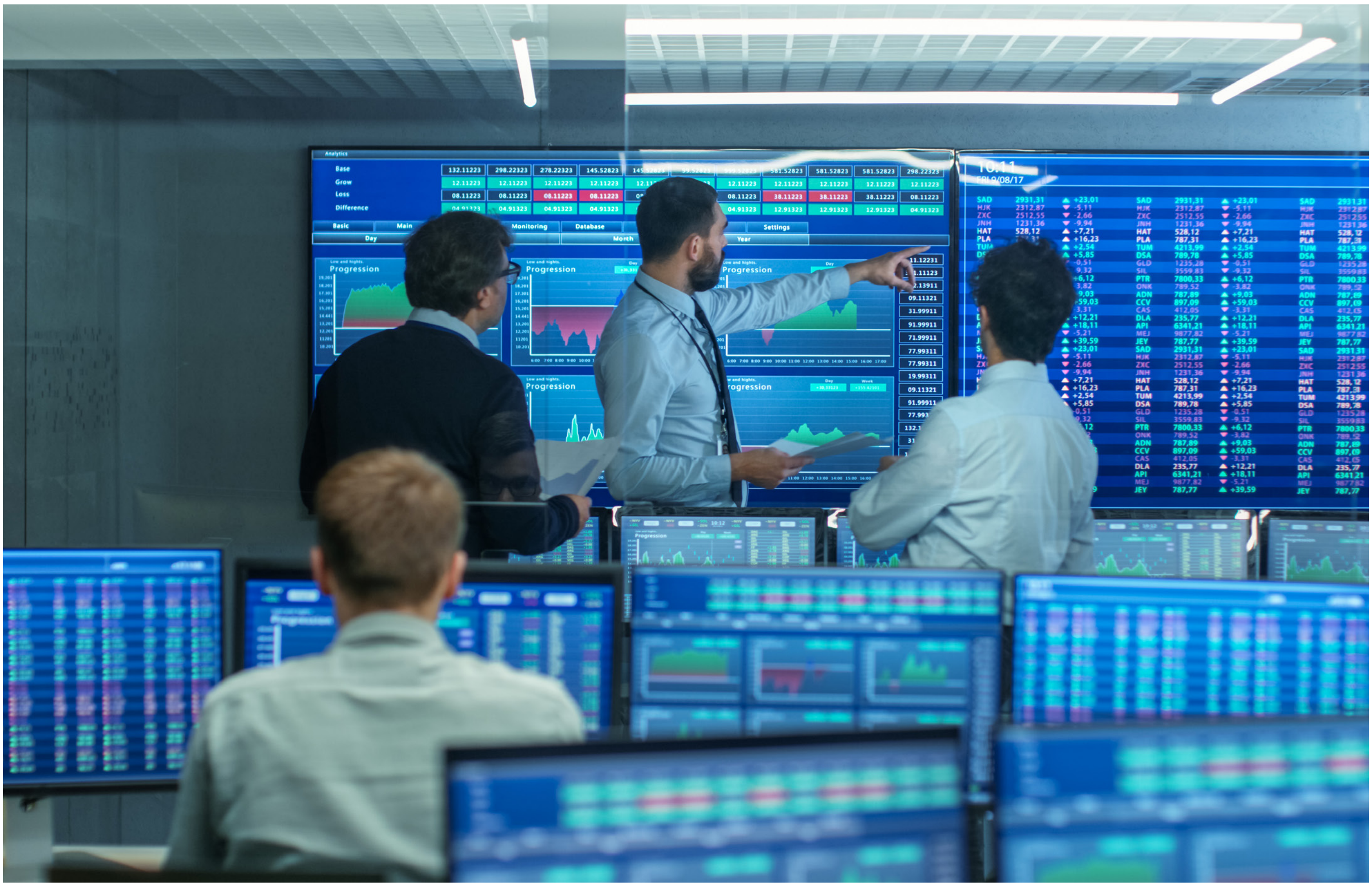
However, whether platform adoption has become a broad reality is disputed, especially for large organizations with large security budgets and teams.

For a mid-market organization with a lean IT and security team, reducing complexity is imperative, but you must avoid doing so to the detriment of your security posture. Armed with visibility of your current state and an understanding of your desired state, you should weigh up the pros and cons of point solutions over a security platform approach.

Download: *Bitdefender Solutions guide: How to build a robust security program with a lean team.*

Security Platform Benefits	
Reduced fragmentation.	Unified prevention, protection, detection and response reduces risk across the entire cyber attack lifecycle and all your digital and non-digital assets.
Reduced complexity.	Fewer tools reduce the attack surface, the likelihood of a misconfiguration and potential vulnerabilities.
Increased efficiencies and productivity.	A single UI simplifies management and operations, reduces console fatigue and enables tasks to be performed easily and quickly.
Improved incident response.	Tight integration across multiple tools increases threat visibility and alert correlation to reduce false positives and time to contain and respond to an attack.
Simplified compliance.	Consistent reporting from a single source reduces audit overhead.
Reduces the total cost of ownership.	Lowers cost of acquisition, ongoing maintenance, support and training to achieve operational efficiencies.

Security Platform Disadvantages	
Potential single point of failure.	Reliance on a single vendor concentrates risk. The vendor could experience an outage or commercial event that could lead to a change in service levels.
Vendor lock-in and dependency.	If the platform fails to meet your future needs, it could be difficult to switch to another vendor.
Functionality gaps.	No single platform can meet all your security needs and specific functionality might not be as appropriate for your needs as a comparable point product.
Initial deployment and migration.	Migrating to a new platform can entail a high implementation cost and time to realize value.



Determine which platform approach is best for your needs

There are many security platforms on the market for you to choose from. Below are some of the key questions to ask yourself.

Was the platform built for large enterprise SOCs?	These are likely built around SIEM and/or SOAR platforms and often NDR. They offer excellent functionality for organizations with complex environments. However, you will need a team of security and risk management professionals to get the best value from them.
Does the platform add unnecessary complexity?	Functionality you don't need or use adds complexity and increases your attack surface. You could be increasing, not reducing, risk.
Is the platform costly due to the breadth of functionality?	Understand your priority requirements. Vendors continuously add new functionality to demonstrate they are adding value. Don't pay for functionality that you will not use.
Does the platform offer flexible licensing?	You will likely not want to go all-in on day one and license everything a platform offers, but you need assurances that you can add integrated functionality as your security program matures.
Does the platform include significant (AI-based) automation?	Lean IT and security teams need as much guidance and help as they can get. Automation is key, not only for rapid response, but to help guide you through incident investigation and recovery.
Does the platform offer coverage across your priority assets?	The platform must secure endpoints, networks, cloud, identities and email.
Does the vendor offer MDR?	MDR service wrappers are essential to ensure that, when you do need to augment your team, you are using SecOps personnel who are experts on the platform.

Choose a platform founded on EDR

For a mid-market organization, with a lean IT and security team, an XDR security platform founded on EDR provides the best balance between security and complexity. Other platforms you might consider are those that have evolved from NDR and general SOC tools, such as SIEM and SOAR. The high-level, relative strengths and weaknesses of each are outlined below.

	XDR founded on EDR	XDR founded on NDR	SIEM & SOAR
Deployment	Easily deployed as part of your endpoint security. Most offer a choice of cloud or on-premises console.	A hardware or virtual appliance is installed on the network, connected in-line or using a SPAN port. Most offer a choice of cloud or on-premises console.	Most offer a choice of cloud or on-premises console.
Integration and coverage	Agents, connectors and APIs provide additional signals across networks, identities, cloud and email. Strong coverage across the vendor's ecosystem and high priority signals that provide most value. E.g. identities. Data ingestion from 3rd party tools is dependent on the vendor.	As EDR, plus additional probes for network segments.	Complex integration to ingest log data into a SIEM from all assets and security enforcement points, including endpoints, network, identities, cloud and email. The numbers of SOAR playbooks that need to be created is dependent on the complexity of your environment.
Time to value	Quick initial endpoint deployment and a short period of passive learning to baseline behaviours.	Dependent on the network architecture and the number of probes required. As EDR, it will require a period of learning.	Dependent on the complexity of the environment, the numbers of logs being ingested from the assets being monitored, the required tuning and the numbers of playbooks.
Attack visibility	Good visibility of attacks at the endpoint. Most attackers will attempt to compromise an endpoint to reach sensitive information. Lateral movement is detected as an attacker attempts to compromise an endpoint. Attempts to compromise unmanaged devices and lateral movement to/from them is detected by network agents. Visibility across other assets is dependent on the agents, connectors and APIs in use.	Good visibility of attacks on unmanaged endpoints, such as sabotage of operational technology. Good visibility of lateral movement attempts from compromised unmanaged devices, before the attack reaches a managed device. Visibility across other assets is dependent on the agents, connectors and APIs in use.	Dependent on the depth of data sources from the tools and assets across your environment. When optimally configured, SIEMs provide alert correlation and deep insights across your entire environment to allow good early visibility of initial access, lateral movement and compromised assets.
Protection	Endpoint protection to block attacks pre-execution is included with all leading EDRs. Relies on other security measures to block attacks over email, web, etc.	NDR can disrupt attacks, depending on deployment. Relies on 3rd party EPP and other security measures to block attacks at the endpoint and over email, web, etc.	Relies on 3rd party EPP and other security measures to block attacks at the endpoint and over email, web, etc.

	XDR founded on EDR	XDR founded on NDR	SIEM & SOAR
Detection	Primary detection is on the endpoint using out of the box, deep EDR capabilities, including AI-powered behavioral analysis. This is augmented by corelating signals from other agents, connectors and APIs.	Primary detection is on the network using deep packet inspection and AI-powered behavior analysis. This is augmented by corelating signals from other agents, connectors and APIs.	Highly customizable, powerful correlation rules require manual configuration, tuning and ongoing maintenance.
Detection efficacy/ fidelity	Excellent efficacy and low false positives, especially when additional signals are used to add context.	Often high levels of false positives and alerts. Requires significant tuning to ensure alert fidelity.	Dependent on the data ingested. Requires significant tuning to ensure alert fidelity.
Response	Automated and guided attack containment with minimal user disruption through easy actions, ranging from endpoint isolation to killing a process.	Disruption is dependent on deployment. Minimal options for endpoint response; dependent on the agent and any integration with EPP.	SOAR provides strong orchestration/automation but requires playbook building and integration with the SIEM and other external tools.
Ease of use	Varies significantly depending upon the vendor. Should include dashboards, workflows and guidance as well as query tools for deeper incident investigation where required.	Similar to EDR. In addition, NDRs are notoriously noisy and will require expertise for incident analysis and response.	SIEM and SOAR require the expertise to build and maintain integrations with the assets and security enforcement points across your environment. SIEM requires query knowledge. SOAR requires playbook building to automate response.
Total cost of ownership	EDR is included with the market leading endpoint protection products. Some additional costs for connectors, agents and API connection. Most offer cloud-based consoles to remove the need for costly infrastructure. Low management overhead and many include human readable reports and the capabilities for rapid incident response without requiring expensive SecOps personnel.	Hardware or virtual appliances must be installed and maintained on-premises. Most offer cloud-based consoles to remove the need for costly infrastructure and deployment. NDRs require expensive SecOps personnel for incident analysis and response.	Requires infrastructure, storage, tuning, dedicated SecOps personnel and ongoing maintenance. Deep integration with an existing complex environment will help you realize an ROI on existing security tools.

Obtain maximum value through key differentiating functionality

The information above validates that, for a mid-market organization with a lean IT and security team, a security platform founded on EDR is the best choice. Now build your vendor short list by considering not only the best detection and response, but the important value-add that the best XDR platforms bring to elevate them beyond just XDR.

Independent tests prove detection fidelity

MITRE | ATT&CK®

Validate the platform's detection efficacy and fidelity

The table above suggests some NDR platforms are noisy. This is also true of EDR, so one of your key considerations should be, not just how good it is at detecting a threat, but how good it is at recognizing anomalous behaviors that are not a threat. If your lean IT and security team is burdened with hundreds of alerts to manually corelate and prioritize, an incident is highly likely to turn into a breach before they can contain it.

Consider platforms that are proven to offer high-fidelity detection. I.e. they are highly accurate with low numbers of false positives.

Consider securing every point of the attack lifecycle

Some XDR vendors are 100% focused on the premise that an incident is inevitable and you should focus heavily on detection and response. However, this is of little help to an organization with a lean IT and security team and no SOC. Your goal is to prevent as many threats as possible turning into an incident and placing the burden of response on your team.

Independent tests prove efficacy

AV comparatives

AV-TEST The Independent IT-Security Institute Magdeburg Germany

Block as many threats as possible pre-execution

Your easiest first step is to obtain the best possible protection – block as many threats as possible pre-execution. Consider a vendor that performs consistently well in independent evaluations of their efficacy.

Focus on prevention first

Prevention technologies to help you understand and manage your attack surface, security posture and vulnerabilities, were once beyond the reach of mid-market organizations. Today, some XDR vendors differentiate by integrating some of these critical capabilities onto their platform. Those focused on enterprises expect their customers to already have these point solutions so consider XDR platforms that are optimized for mid-market organizations.

These bring significant tangible and demonstrable benefits to your security program:

- Proactively reduce the risk of a successful attack.
- Quantify the results of your ongoing risk reduction activities.
- Easily demonstrate security posture changes to your leadership.
- Reduce the likelihood of an incident and the resulting burden of response on IT and security staff.
- Demonstrably lower the cost and effort of achieving and maintaining regulatory compliance.
- Lower the cost and effort of acquiring cyber insurance.

Consider a platform that doesn't just bundle, but integrates compliance, attack surface, vulnerability and patch management alongside risk analytics and attack surface reduction with tools like endpoint hardening.

Integration is key to maximize value from these tools. Beware of vendors that have acquired technology and simply reskinned their UI.

Ensure differentiating functionality doesn't introduce unnecessary complexity

Your goal throughout this process is to ensure your chosen solution simplifies your security operations and reduces risk. During evaluation of your short list, you must consider this and keep in mind that additional functionality could detract from the goal. But do also keep in mind that value-add does not necessarily mean complexity, and you should strike a balance between the two. When doing so, consider platforms that optimize any additional functionality for organizations like yours.

Ensure your chosen vendor can augment and support your team and security program

MDR is an important add-on to augment lean IT and security teams and reduce risk by strengthening your entire security program. Your first decision is whether you need MDR or not. Consider the following benefits:

- ↳ Maximize the return on your XDR platform investment by leveraging the expertise available in your chosen vendor's SOC.
- ↳ Overcome headcount limitations and eliminate recruitment and retention challenges.
- ↳ Empower your lean IT and security team with the support they need and focus their efforts on activities that provide best ROI.
- ↳ Demonstrably lower the cost and effort of achieving and maintaining regulatory compliance and acquiring cyber insurance.

Consider the differentiating service offers

Consider XDR platform vendors with the flexibility to allow you to add MDR later. Beware, not all service wrappers are equal, so even if you are not subscribing immediately, you should evaluate your chosen XDR vendor's MDR. The differentiating services to look for are:

- ↳ Expert recommendations to help you improve your preventative security controls and reduce your attack surface.
- ↳ Direct access to an expert cyber threat intelligence team to perform personalized, dedicated research.
- ↳ Regular threat hunting to proactively detect emerging threats in your environment and bad actors that have evaded your defenses and are silently progressing their attack.
- ↳ Not act only as an alert aggregator but respond on your behalf with pre-approved actions to rapidly contain an attack with minimal business disruption.
- ↳ Incident root cause analysis to enable rapid recovery and return to business as usual.

Choose a security platform that is optimized for lean IT and security teams

Even enterprises with large teams of security professionals are demanding consolidation to remove complexity. The result is that enterprise focused vendors are marketing what are often a set of loosely integrated point products, bloated with functionality that mid-market organizations do not have the time, people or skills to extract value from.

There are platforms available that are more suited to mid-market organizations but choose wisely and consider:

- Does it provide security across the complete threat lifecycle – prevention, protection, detection and response?
- Does it simplify security operations to support your consolidation strategy and reduce operational risk?
- Does it provide the flexibility to help you migrate today but add functionality as your security program matures to support your business needs?
- Does the platform vendor provide the support services required to help your lean team mature with your security program?

Validate your choice with 3rd-party reviews

This is your final task.

Focus on references and reviews from organizations like yours. Positive reviews from large enterprises with completely different environments and security programs do not carry as much weight as those from similar organizations. Gartner Peer Insights is a good source of independent reviews and they create customer choice awards for vendors that excel in each category they cover.

Also consider industry analyst reports, like Gartner's market guides and magic quadrants. Do exercise caution when considering rankings, as these are often based on enterprise-class functionality, not mid-market. Inclusion, though, does highlight that your chosen vendor is important, as they are covered by analysts.

Questions to ask security platform vendors

General	↳ Does it help me reduce risk across the complete attack lifecycle with critical prevention, protection, detection and responsetools? ↳ Does it protect all my assets – endpoint, identities, cloud, network and email? ↳ How easy is it for my team to deploy and manage? ↳ How does it reduce my TCO? ↳ How flexible is the licensing model?
Prevention	↳ Does it report on and demonstrate how I am reducing risk and achieving compliance with regulations we must adhere to? ↳ Does it help me identify non-compliance and provide actionable insights to resolve gaps? ↳ Does it include the critical prevention capabilities from the following tools: ↘ Cyber Asset Attack Surface Management (CAASM) ↘ Continuous Threat Exposure Management (CTEM) ↘ Cloud Security Posture Management (CSPM) ↘ External Attack Surface Management (EASM) ↳ Does it provide actionable insights, recommendations and guided remedial actions that are prioritized based on severity and potential impact? ↳ What attack surface reduction capabilities does it include? E.g. patch management and endpoint hardening.
Protection	↳ How does it perform in independent technical tests to measure efficacy and accuracy? ↳ What credentials does the vendor's threat researchers have? ↳ What assets does the protection cover?

Detection & response	↳ From which assets across my infrastructure does it ingest alerts? ↳ Does it provide visibility of the assets in my organization that an attacker might target? ↳ What automation is included to help correlate and triage alerts? ↳ How does it perform in independent tests that measure efficacy, accuracy and alert volumes? ↳ What actions can I take to respond to an incident but minimize business disruption? ↳ What root cause analysis tools does it provide? ↳ Does it include human-readable reports and deep query capabilities?
MDR	↳ How detailed are the vendor's recommendations to help me improve my security posture? ↳ Do I have direct access to the vendor's threat researchers? ↳ How often does the vendor perform threat hunting in my environment? ↳ Does the vendor respond on my behalf and how granular are the actions they take to ensure minimal business disruption? ↳ Does the vendor perform root cause analysis? ↳ Does the vendor provide a cybersecurity warranty?

Endnotes

1 Verizon 2025 Data Breach Investigations Report

2 Security Buyers Are Consolidating Vendors: Gartner Security Summit

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 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