White paper

Upgrading from EDR to XDR: knowing when to advance

kaspersky bring on the future

Upgrading from EDR to XDR: knowing when to advance

Organizations no longer need to be high-profile to be high-risk. This reflects a significant turning point in cybersecurity. Traditionally, only large organizations were considered worthwhile targets for more advanced cyberattacks – which warranted robust security solutions being catered to larger enterprises. However, recent years have shown that mid-market organizations have become lucrative and strategic targets for similar types of sophisticated attacks.

This shift is forcing many Chief Information Officers (CIOs) and IT security specialists to rethink their cybersecurity strategies. Additionally, many existing solutions, especially those used by smaller security teams or broader IT departments, are proving inadequate in managing the increasing threat volume and the complexity of modern threats.

Why are mid-market companies becoming top targets for cybercriminals?

Businesses with smaller cybersecurity teams have become top targets for more advanced cyberattacks. We found that SMBs experience an average of 16 attacks per year, with larger organizations experiencing up to 18, depending on the industry.[1] But why the interest in smaller companies that, at face value, shouldn't need enterprise-grade protection?

Stepping stones to larger organizations

Many smaller organizations serve as critical links to larger corporations. Cybercriminals often consider the larger network and exploit the easiest entry point. By doing so, they can disrupt the greater supply chain and cause cascading damage. In 2025 alone, 54% of large organizations cite supply chain interdependencies as the leading factor in the increasing complexity of cybersecurity.[2] But while larger organizations have recorded an increase in cyber-resilience over 2024, smaller organizations remain at a disadvantage, with 35% stating insufficient cyber-resilience.[2]

A lack of qualified personnel

Most smaller cybersecurity teams want to improve their threat detection and incident response capabilities, but lack the resources or budget to do so. In fact, recent studies show that 41% of InfoSec professionals say their organization's cybersecurity teams are "somewhat" or "significantly" understaffed.[3] In many cases, this means that SMBs largely rely on general IT personnel to handle cybersecurity tasks. This not only stretches smaller teams beyond their means, but also exposes businesses to increased cyberthreats due to a lack of specialized training. Unfortunately, cybercriminals are aware of this vulnerability and exploit it with ease.

Easy targets for sophisticated tools

Medium-sized organizations have proven to be easy targets, with many lacking the necessary cybersecurity to adequately protect them from complex threats. However, it should be noted that being an "easy target" isn't solely a reflection of the IT team, but also of the fact that sophisticated threats are easier to deploy than ever. Smaller companies generally use simpler IT security solutions such as network security, EPP and CWPP – all growing more ineffective as cybercriminals leverage sophisticated tools to bypass basic cybersecurity with ease.

SMBs experience an average of 16 attacks per year.[1]

How modern tools and factors make life easier for attackers

To best understand the rapid increase in complex attacks, we need to view cybercrime as more than just a technical threat – but rather a thriving global enterprise. Cybercriminals have developed scalable business models that enable them to streamline operations, diversify their revenue streams and innovate with speed and precision. Accelerating the rise in sophisticated attacks is the advent of force multipliers, with advanced tools now equipping even low-skilled cybercriminals to launch those attacks.

Cybercriminals are constantly evolving their tactics, leveraging new technologies and systemic weaknesses to carry out attacks more efficiently.

Below are key tools and factors that enable attackers to exploit victims with greater ease.

Social engineering

Social engineering attacks, like phishing, use manipulation techniques that exploit your team to gain private information – and AI technologies have made it easier to deploy than ever before. For example, a cybercrime-orientated AI chatbot can help attackers create polished emails and fraudulent DocuSign requests. With minimal effort, attackers can avoid traditional phishing red flags, personalize fraudulent emails and use manipulation tactics to create a sense of urgency and authenticity. Other social engineering attacks follow a multi-stage approach. The attack starts by sending mass email spam that eventually forces employees to create legitimate help-desk tickets. Attackers then pose as IT support staff, contacting employees via Microsoft Teams and tricking them into receiving malicious QR codes designed to deliver remote monitoring tools that can be exploited for network access.

Spyware as a Service

Spyware developers also rent or sell access to their tools, often via dark web forums or nefarious channels. Customers (typically hackers, nation-states or stalkers) pay for access to keyloggers, microphone/camera access tools, mobile surveillance kits, remote access tools (RATs), browser and email interception tools or GPS trackers.

These tools can be used to collect and transmit information from a victim device without the user's knowledge or consent.

Ransomware as a Service (RaaS)

RaaS kits are essentially "plug and play" tools that allow cybercriminals to launch sophisticated cyberattacks with little hands-on work. They deploy malicious malware that can effortlessly adapt its code to avoid detection by security systems (like antivirus or firewalls). Many cybersecurity frameworks are therefore inadequate in providing sufficient protection to fight RaaS, exposing businesses, governments and individuals to high-risk situations.[4]

Similar to Software as a Service (SaaS) models, RaaS kits allow affiliates to access ransomware tools, 24/7 tech support, payment processing portals and more for as little as USD 40 per month. And for some perspective, the average ransomware breach costs its victim USD 4.91 million (including downtime, lost customers, fines, etc.).[5]

Outdated software

Many businesses struggle to stay on top of patching and updates, which can leave their software vulnerable. Ransomware groups in particular are leveraging zero-day vulnerabilities knowing they can beat the speed at which organizations patch. In fact, 85% of critical vulnerabilities aren't remediated at 30 days after discovery, 47% are still out there at 60 days, and 20% continue to linger after half a year.[6]

In 2024, 41.6% of incidents were related to ransomware, compared to 33.3% in 2023. Ransomware looks likely to remain the primary threat to organizations around the globe for the foreseeable future.[7]

The need for advanced protection

Disrupted processes:

- Communications — 41%
- Customer support — 36%
- Marketing automation — 34%
- Logistics — 32%
- Product development/production — 31%
- CRM, sales — 27%
- Purchasing and payment — 26%
- Payroll — 17%

Security breaches cost SMBs 1.5x their allocated cybersecurity spend.[1]

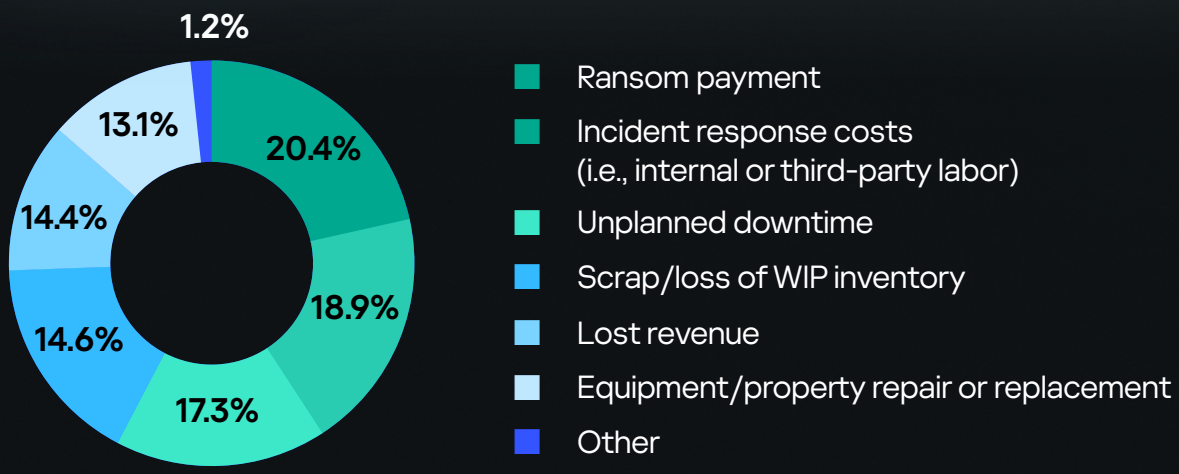
Along with increased complex cyberattacks, recent studies highlight that the costs from lost business and post-breach response rose nearly 11% over the previous year.[6] This hike is largely due to sophisticated attacks causing longer breach lifecycles.

Cyberattacks are now inevitable – but how quickly you detect and respond to them determines whether an incident becomes a minor event or a catastrophic breach. For example, in 2024, the three breach types by initial vector that took the longest to contain were phishing, malicious insiders and stolen/compromised credentials. These were also three of the four costliest breach types by initial vector, highlighting the link between dwell time and damage caused.[5]

The longer attackers operate undetected, the more damage they inflict. This is where your Mean Time to Detect (MTTD) becomes a main key performance indicator in incident management – and speaks to your team's ability to detect or discover an incident. Consequently, your Mean Time to Respond (MTTR) speaks to the average time it takes to neutralize the threat. Security operations automation plays a significant role in improving those metrics. In fact, those engaged in security process automation report benefits such as a 46% improvement in their MTTR.[8]

The difference between a contained incident and a full-blown disaster often comes down to speed of response. MTTD is meaningless without MTTR – finding a threat quickly means nothing if you can't stop it fast. Time equals money, and every second counts. Organizations that respond to breaches swiftly can save millions, easily meet regulatory requirements and protect their reputation.

Average cybersecurity breach costs for food and beverage[9]



When EDR isn't sufficient anymore

For many years, endpoint detection and response (EDR) tools have been the baseline of any cybersecurity strategy – and rightfully so. EDR provides cybersecurity teams with valuable data and visualization tools to ascertain the root cause of the threat and whether any additional response actions are needed – far surpassing traditional antivirus tools in both capability and effectiveness.

But the threat landscape has grown significantly, and so has the importance of incident response and threat investigation – pushing high-risk organizations towards more complex needs that only XDR functionalities can fulfill.

However, investing in a full-fledged XDR solution often proves unfeasible for smaller organizations lacking the hardware, budget or qualified personnel to handle and analyze telemetry effectively.

This leaves small and medium businesses in a tricky middle ground where current solutions no longer suffice, but enterprise-level XDR is too advanced, expensive and unpractical to resolve their current issues. All the while, the attack surface is expanding and your team is overwhelmed with the sheer number of alerts that need to be analyzed.

So, how do you know that it's time to step up?

Alert fatigue is overwhelming your team

If your organization uses a variety of cybersecurity tools that generate numerous alerts, your IT security team can be quickly overwhelmed. This is especially true if your team lacks sufficient context to prioritize and investigate these alerts effectively. The process can be tedious, and your team will become increasingly likely to miss an incoming threat if working manually. Your team may even suffer burnout, causing them to look for opportunities elsewhere.

> "When a cybersecurity professional is doing their job well, nothing happens and their day-to-day work is largely mundane – checking logs and rules, reviewing accounts, ensuring policy compliance. These aren't complex steps, but they are critical. Doing them manually quickly leads to burnout."
>
> Head of Unified Platform at Kaspersky, Ilya Markelov

While EDR platforms do a good job of flagging endpoint-level anomalies, they often lack the broader context needed to understand the full scope of an attack. As a result, analysts are forced into detective work. It is therefore crucial to find a way to triage alerts effectively and gain clear visibility.

The attack surface is increasing, but your resources stay the same

System hardening is a crucial component in helping small and mid-market organizations reduce the attack surface. In essence, system hardening involves identifying and fixing cybersecurity weaknesses to minimize potential attack vectors and eliminate unnecessary services or features that attackers could easily exploit.

However, keeping systems hardened requires ongoing monitoring and patching to address new vulnerabilities – not to mention the burden of maintaining compliance with quick-to-change cybersecurity regulations. Needless to say, effective system hardening often proves challenging for a smaller team with limited resources.

Your employees are struggling to withstand phishing and social engineering attempts

Despite investing in EDR, you might still see your employees falling victim to phishing and social engineering attacks. This isn't a failure of EDR but a sign that the threat landscape has evolved. EDR is good at identifying known malware, monitoring system behavior and flagging anomalies, but it isn't designed to prevent human error, which plays a hand in 22% of breaches.[5]

Phishing attacks don't need to exploit a vulnerability in software – they exploit a vulnerability in human behavior. A well-crafted email or spoofed login page can bypass even robust EDR platforms by getting an employee to hand over credentials or download malicious files.

If your employees are struggling to recognize these types of attacks, it's a clear indicator that your cybersecurity strategy needs to go beyond EDR. Proactive defense means building a security culture supported by continuous training and tools that facilitate identity protection. Stepping up from EDR means addressing the full spectrum of risks, especially those that originate from social engineering.

Attacks are being caught too late

When attackers gain access through legitimate channels, your EDR may detect the intrusion too late, after access has already been granted. IBM found that in 2024, organizations took an average of 194 days to identify a breach, and an additional 64 days to contain it.[5] This isn't a minor delay. It's numerous months of potential exfiltration, lateral movement and persistence.

Every day an incident goes undetected increases the risk of sensitive data being stolen, systems being compromised or ransomware being deployed.

Manual response is slowing you down

Companies with strong and regularly tested incident response plans see an average of 58% cost savings compared to those without one.[10] But what makes an incident response plan "strong"? In short, it's all about speed. Modern attack frames are rapidly shortening; for instance, ransomware can lock critical systems in just minutes and in today's fast-evolving threat landscape, manual incident response cannot keep up.

Unlike automated systems, manual response is slower to respond to cybersecurity incidents and even the slightest delay could lead to a greater compromise and risk.

The importance of automation in incident response cannot be overestimated. By leveraging automation, teams can identify and counteract threats in real time, significantly reducing the window of exposure. Moreover, it allows your team to focus on other critical tasks that might require their expertise – saving you time, money and resources.

To extend or not to extend?

Full-fledged XDR solutions – although crucial for protecting against advanced threats – have yet to meet the specific needs of smaller IT and cybersecurity teams.

> The same challenges that make mid-market companies vulnerable to complex cyberattacks (limited budget, lack of resources) are the same reasons they struggle to implement advanced protection effectively.

These specialized solutions are notoriously complex to implement and navigate and often require too steep of a learning curve for smaller IT teams. But the need for at least some XDR functionality is becoming increasingly important – and it's not just enterprises who have the need for them. Our MDR Analyst Report states: "In 2024, the mean time to investigate and report cyberincidents surged by 48% compared to 2023, reflecting a significant increase in attack complexity. This is supported by the analysis of triggered detection rules and Indicators of Attack (IoAs) – the vast majority of which were from specialized XDR tools. This marks a shift from previous years, where detection by OS logs played a significant role. In these conditions, specialized tools, like XDR, are essential for successful detection and investigation of modern threats."[7]

How Kaspersky can help

Enterprise-grade protection optimized for smaller teams

Kaspersky NEXT XDR Optimum is designed for small IT and cybersecurity teams. The solution strengthens incident response and builds expertise without the added burden of time-consuming routine tasks.

With multiple processes automated, you can focus on what matters most.

Unleash outstanding endpoint protection

Leverage automated protection to avoid business disruption. With industry-proven ML-based anti-ransomware and anti-malware tools, you can effortlessly prevent infections from both known and unknown threats.

Fix vulnerabilities through system hardening and training

Reduce your attack surface with system hardening based on user behavior. Save time with centralized vulnerability, patch and encryption management and provide all the training your team needs to make the most of your new cybersecurity capabilities.

Extend your detection and response capabilities

Gain insights into threats and how they move within and beyond endpoints. Use automation and guided response to counter attacks, and essential investigation tools to trace their activity.

Train your entire team to play an active role in security

Equip your IT staff and non-technical employees with the knowledge and skills to stay secure. Strengthen your IT security team while building a strong, security-conscious culture across your workforce.

Control shadow IT with cloud security you can rely on

Reduce your vulnerability and safeguard your data and employees by controlling shadow IT. See which cloud services are in use, block unauthorized access and identify what sensitive data is stored in Microsoft 365 apps.

Minimize alert fatigue

The alert aggregation feature of Next XDR Optimum, combined with having effective and proven endpoint protection, reduces the number of alerts that teams need to analyze. This increases efficiency and alleviates alert fatigue and frees up your team to focus on other critical tasks.

Bibliography:

[1] Kaspersky, B2B IT security risk tracker report, (Kaspersky, 2024)
[2] Tuteja, Akhilesh, 5 risk factors from supply chain interdependencies in a complex cybersecurity landscape, (World Economic Forum, 2025)
[3] Kaspersky, A portrait of a modern Infosec professional, (Kaspersky, 2024)
[4] Willie, Alan, The Evolution of Ransomware-as-a-Service (RaaS): AI's Role in Cybercrime and Countermeasures, (Stanford University, 2025)
[5] IBM, Cost of a Data Breach Report 2024, (IBM, 2024)
[6] Verizon, 2024 Data Breach Investigations Report, (Verizon, 2024)
[7] Kaspersky, Fortress under fire: cyber threat chronicles 2024, (Kaspersky MDR Analyst Report, 2024)
[8] Verizon, 2024 Data Breach Investigations Report, (Verizon, 2024)
[9] Kaspersky and VDC Extended Survey Findings, (Securing OT environments, 2024)
[10] IBM, Cost of a Data Breach Report 2022, (IBM, 2022)

www.kaspersky.com

#kaspersky
#bringonthefuture