Cybersecurity megatrends and their implications for cyber protection

Rethinking EPP, EDR and XDR for today, tomorrow and the future

kaspersky

Executive summary

Each year, leading analysts, commentators, trade associations and more highlight the 'megatrends' they expect to shape their industry in the near-term.

Cybersecurity is no different. And vital as these insights are in helping C-level executives anticipate major trends and plan their organizations' futures, when it comes to Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), IT security and IT teams, what's just as important is how their implications can be accommodated and operationalized in practical terms.

To assist you in this process, this e-book summarizes some of the most challenging security trends impacting the IT industry today. And, in particular, the implications of these for organizations' use of solutions ranging from endpoint protection platforms (EPP) through endpoint detection and response (EDR) to extended detection and response (XDR).

Contents

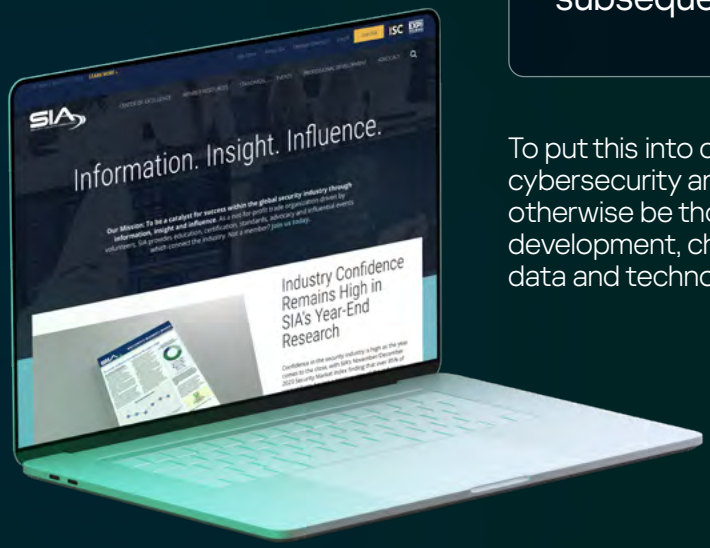
- Executive summary page 2
- You say megatrend. I say expanded attack surface page 3
- What about more IT-specific trends? page 4
- How the latest megatrends are influencing the threat landscape page 6
- How did we get from EPP to EDR to XDR? page 7
- Who needs which kind of security? page 8
- How to assess your evolving security requirements – EPP, EDR and MDR page 9
- How to assess your evolving security requirements – XDR page 15
- Specific capabilities and benefits you should expect from an XDR platform page 17
- How to justify the investment in XDR page 21
- Addressing the broader threat landscape page 23
- How Kaspersky can help page 25

You say megatrend. I say expanded attack surface

Even for people working in the IT industry, it can sometimes be difficult to fully appreciate the vital importance of cybersecurity within its broader market context.

The Security Industry Association (SIA), for example, is the leading trade association for global security solution providers, with over 1,400 members. In the introduction to the 2023 edition of its vision for the industry, the SIA notes that 'It's not surprising in the least to see the cybersecurity of physical security reign again in our list of 2023 Security Megatrends'.

> 'AI and cybersecurity continue to jostle for the top trends impacting the security industry, but the data was clear: cybersecurity is top of mind for security industry leaders.' And, 'AI and cybersecurity were orders of magnitude higher rated than the subsequent trends.'



To put this into context, security industry professionals consider cybersecurity and AI to be far more critical than megatrends that might otherwise be thought to dominate the industry, such as workforce development, changing economic conditions, and ethical/safe use of data and technology.

What about more IT-specific trends?

Review similar reports by leading analysts such as Gartner, IDC and Frost & Sullivan, and you'll find references to everything from the increased dynamism of network environments making vulnerabilities harder to defend, to the accelerating volume and sophistication of cyberattacks exploiting these vulnerabilities.

In Cybersecurity Megatrends 2022, for example, IDC highlights '7 Trends of the Cybersecurity Reality' including:

- Digital transformation, hybrid work and death of the perimeter
- Scarcity of information security professionals
- Sophistication of cyber miscreants growing rapidly
- Proliferation of security tool sets and platformization
- Continued growth of compliance regulations
- New buyers and old buyers with new priorities
- Trust

Gartner's Top Trends in Cybersecurity 2023, meanwhile, states that 'This year's Gartner Top Trends in Cybersecurity show increased recognition of the importance of employee engagement in the security program to address cybersecurity risks and sustain an effective cybersecurity function. The increasingly distributed nature of work amplifies the adoption of cloud. In turn, this increases dependency on end-to-end visibility of expanding digital ecosystems and having resilient supply chains. In addition, CIOs are changing their IT operating models to foster enhanced business agility. The regulatory environment continues to evolve, forcing boards to take a more active role in managing cybersecurity risks. While ransomware payments are falling, large-scale ransomware attacks and attacks on identity systems continue.

These global trends are seeing leading security and risk management (SRM) leaders focus their efforts by:

1. Driving focus on the essential role of people for security program success and sustainability.
2. Implementing technical security capabilities that provide far greater visibility and responsiveness across the organization's entire digital ecosystem.
3. Restructuring the way the security function operates to enable agility without compromising security.'

To address these issues, Gartner recommends 'security and risk management (SRM) leaders should:

- Adopt an attacker's mindset to prioritize cyber-risk mitigation efforts by taking an end-to-end view of the attack surface and consolidate vendor portfolios, where appropriate.
- Optimize the alignment of cybersecurity capabilities to new, distributed ways of working by adopting new security operating models and architectural approaches that foster agility and embed security by design.
- Prioritize and optimize investments in employee behavior improvement to enhance and sustain the efficacy of enterprise security.'

All these recommendations are clearly sound advice. So how can you go about operationalizing them inside your organization?

To answer that we need to start by looking in more detail at the evolving threat landscape, and what this means in the context of your existing IT security infrastructure, tools and controls.

'Zero-day vulnerabilities are rarely the primary cause of a breach. In other words, breaches could be prevented if organizations fix their exposure to a threat before an attacker exploits it. However, fixing every known vulnerability has always been operationally infeasible.'

Gartner: Top Trends in Cybersecurity 2023

How the latest megatrends are influencing the threat landscape

Compared to just a few years ago, the threat landscape is evolving faster than ever before. It's now rare, for example, for even a week to go by without a report of the latest high-profile ransomware attack, scam or data breach – and not only are cyberattacks increasing in number, they're also more sophisticated, more targeted and more difficult to detect.

Many of the individuals involved in launching cyberattacks are career criminals, and with experience comes success. The popular misconception of hackers as lone keyboard warriors also no longer applies.

To take ransomware as an example, the groups involved are increasingly behaving like decentralized corporations, with complex networks of affiliates responsible for individual steps in the process – from reconnaissance, access, malware creation, distribution and data exfiltration, to ransom negotiation, publishing stolen data online and laundering ransomware payments.

A majority of ransomware attacks now have dwell times measured in hours rather than days. Groups also offer ransomware-as-a-service, and conduct attacks that are more like advanced persistent threats (APTs) in terms of their scale. And hacktivists and nation states may use ransomware and other techniques (such as wipers) for destructive or geopolitical rather than purely commercial purposes.

On top of this, the tactics, techniques and procedures (TTPs) used by cybercriminals are becoming increasingly sophisticated. Examples include the use of self-spreading and self-propagation features; exploiting public-facing applications, compromised accounts and malicious emails; and making use of tools such as PowerShell that are extensively used in normal IT operations, thereby making these attacks much harder to spot.

As a result, establishing the optimum level of protection for your organization – whether you're using EPP, EDR and/or XDR – has never been more important.

How did we get from EPP to EDR to XDR?

Traditionally, alongside defending their perimeters with firewalls and email protection, organizations have focused their efforts on endpoints – PCs, laptops, servers (physical and virtual) and workstations – as their primary defense against cyberthreats, to the extent that endpoint protection platforms (EPP) have become a fundamental step in combating complex attacks.

More recently, organizations have added to this by deploying more advanced tools to defend against attacks. These can be used to identify and respond to anomalous behavior either on endpoints - through endpoint detection and response (EDR) - or the network, through network detection and response (NDR).

But as we've just seen, cybercriminals are continually refining their tactics, and developing more sophisticated ways to target businesses. Today's attackers are increasingly taking a multi-vector approach to staging their attacks, often involving multiple entry points into the infrastructure, and a variety of different tactics and techniques.

Malicious actors leverage advanced techniques such as social engineering (including phishing and business email compromise), compromised accounts, public-facing app and zero-day exploits to breach organizational defenses – making protecting businesses from these evolving threats a considerable challenge.

APTs, for example, bypass traditional endpoint detection and can stay active for weeks or months – moving laterally through the network, gaining permissions, exfiltrating data, and gathering information from the different layers of the IT infrastructure in preparation for a large-scale attack or data breach.

The sheer volume and complexity of these attacks make it difficult for organizations to stay one step ahead. And their ever-expanding attack surface – including mobile devices, cloud environments and remote work, as well as servers etc. - further compounds the difficulties.

51% of organizations struggle to detect and investigate advanced threats with current tools.

ESG Research Report, SOC Modernization and the Role of XDR, June 2022

On top of this, organizations have to contend with insider threats, supply chain vulnerabilities, compliance and regulatory requirements, while at the same time addressing the ongoing shortage of skilled cybersecurity professionals. And the potential damage to corporate systems, operations and reputations resulting from data breaches, ransomware, distributed denial of service (DDoS) attacks, APTs, cyber espionage etc. can be enormous.

Achieving effective security against these threats therefore requires a comprehensive and proactive approach combining advanced technologies, robust policies, vigilant monitoring, ongoing training and more - which is exactly the 360° view of the threat landscape that XDR sets out to deliver.

By breaking down the silos between layer-specific point solutions, XDR gives security operations centers (SOCs) and IT security teams the end-to-end visibility and integration they need to identify threats faster, respond to them more quickly, resolve them more effectively and minimize the damage they cause.

Who needs which kind of security?

The ideal solution is one that supplements endpoint protection with EDR-class security which significantly lightens the EDR workload – as the more threats that are prevented, the less noise is created for security teams to investigate.

For years, small-to-medium businesses (SMBs) and low-end enterprises have been able to rely on EPP to defend themselves against an extensive range of commodity threats. But as we've briefly discussed, today's attackers are focusing on organizations of all sizes, industries and levels of preparedness – with SMBs and smaller enterprises increasingly at risk from the more advanced evasive threats previously only directed at much larger organizations.

In response, IT security teams have been supplementing EPP with EDR and/or managed detection and response (MDR) services that enable them to detect and investigate security incidents, contain the threat at the endpoint, and receive an automated response and/or guidance for remediation.

The ideal solution is one that supplements endpoint protection with EDR-class security which significantly lightens the EDR workload – as the more threats that are prevented, the less noise is created for security teams to investigate. This in turn enables IT teams to optimize key resources and focus on the business of IT, rather than chasing false positives and overwhelming volumes of alerts.

Moving up a level from EDR and MDR, the 'extended' in extended detection and response reflects the fact that in XDR, an EDR solution is supplemented by and closely integrated with a variety of other security tools that may not necessarily be designed to work together. Rather than utilizing various security tools as siloed point solutions, XDR lets organizations create a comprehensive, flexible and scalable security ecosystem that maximizes the benefits of their existing tools, can be tailored to the needs of their organization, reduces risk and makes them safer.

So to answer the question 'Who needs which kind of security?', the key points to bear in mind are that:

- All organizations need a solid foundation of modern endpoint security.
- The additional level(s) of security required on top of this will largely depend on a combination of the types of cyberattack to which the organization is potentially exposed, and the IT security skills of the IT team tasked with implementing and using the tools required to prevent these.

We'll now look at five key steps that will help you assess and operationalize your security requirements in relation to these considerations.

How to assess your evolving security requirements – EPP, EDR and MDR

Step 1:

Review your existing endpoint protection

With so many advanced cybersecurity solutions available on the market, it's easy to forget the vital role played by endpoint protection. Why are endpoints so important? Not only are they the most common entry points into an organization's infrastructure – and cybercriminals' primary target - they're also key sources of the data needed for effective investigation of complex incidents.

As a result, every organization should choose an EPP solution delivering automated protection against the large numbers of possible incidents caused by commodity threats – including fileless threats and ransomware.

Because this type of setup requires relatively limited specialist security knowledge or personnel, it meets the endpoint security needs of SMBs or smaller enterprises without a dedicated security team, or organizations with very low levels of cybersecurity expertise.

It's also a crucial foundation stage for midsize and larger enterprises where, by dealing automatically with large numbers of minor threats, the solution clears the way for security teams to focus on more advanced defenses where needed.

Key considerations

When reviewing EPP to assess if it's delivering the capabilities you need or should expect, consider:

- How effective is it?
- How many false positives are you receiving?
- Does it offer effective attack surface reduction capabilities like file, web and mail antivirus, network protection, Antimalware Scan Interface (AMSI), exploit prevention, remediation, behavior detection and host intrusion prevention (HIPS)?
- Does it help to automate routine tasks?
- Is it easy to operate, and does it help to minimize costs and overheads on your IT team?
- Does it assist with critical tasks such as vulnerability assessment, software/ hardware inventory, firewall, web, device and application controls, and cloud discovery?

Step 2:

Identify any critical gaps in your endpoint defenses

Why modern EPP requires EDR capabilities

As we've discussed in this e-book, the evolving threat landscape means that over time, increasingly sophisticated threats that previously affected only large organizations are cascading down to impact SMBs and smaller enterprises that do not possess the in-house resources needed to deal with them effectively.

In particular, the advent of evasive threats - which use legitimate tools in attacks, include readymade scenarios to bypass EPP, are low cost and readily available on the dark web – has significantly increased cybersecurity risks for organizations using traditional EPP solutions.

These issues are further compounded by the lack of transparency provided by traditional EPP. Effectively these solutions offer only a red light / green light representation that an attack either is or is not taking place. Whereas, what an IT team with even basic security skills requires is visibility into what's happening on individual endpoints, so that this can be analyzed in more detail to increase understanding of the threat.

Modern EPP solutions incorporating simple EDR capabilities therefore provide an important steppingstone between traditional EPP and more advanced, fully featured EDR solutions.

While EPP will protect against an extensive range of commodity threats, you also need to consider your defense against new, unknown and evasive threats that are bypassing your EPP.

Preparing an attack is becoming cheaper for cybercriminals, putting more organizations at risk. And as well as occurring more frequently, these kinds of attacks have become much more effective due to criminals combining, testing and using varied techniques in order to effectively bypass endpoint security.

The urgent need to deal with these threats has also become increasingly critical due to changes such as dissolving corporate perimeters resulting from the surge in remote working. Together, these trends are creating a need for EPP whose capabilities extend beyond those provided by traditional EPP solutions, and in particular include basic EDR capabilities such as simple root cause analysis.

Key considerations

Telltale signs that it's time to expand your defenses beyond traditional EPP include:

- Your EPP is failing to stop an increasing number of new, unknown and evasive threats.
- You have limited visibility into what's happening on your endpoints. This includes being unable to undertake root cause analysis, investigation and real-time threat response - or having to do this manually, with standard operating system (OS) tools on a case-by-case basis, which is slow, complex and error-prone.
- You don't have the specialist IT security skills or capacity needed to deal with increasingly sophisticated threats.
- You're concerned about potential fines, or the threat to your business's reputation resulting from a major security incident.

To implement an effective solution to defend against these threats, you'll also need to consider aspects of your organization including its size, corporate profile, security preparedness, existing resources and expertise – and in particular the security skills of your IT or IT security team.

Step 3:

Be clear about what you want to achieve

Many organizations have limited time and resources (or a small IT security department and no plans to expand it), but need to understand what's happening to their infrastructure and be able to respond to evasive threats before damage can occur.

Adding appropriate EDR capabilities to modern EPP can provide highly effective defense against more advanced evasive threats. This should enable automated and/or fast, accurate 'single-click' responses like quarantining files, host isolation, stopping a process, deleting an object etc. And, if you have IT security specialists, it should give them the information, insights and tools they need for effective investigation, such as root cause analysis, creating custom Indicators of Compromise (IoCs), importing IoCs, and scanning for these across all endpoints.

You'll also want a solution that makes the best use of all the functions you actually need, rather than paying for large numbers of functions you don't really want, and then trying to recruit IT security experts with the skills needed to work with these.

5 common misconceptions about EDR

1 Our endpoint protection's fine - we don't need EDR

Misconception: Cybercriminals aren't interested in businesses like ours – we're under the radar for the kinds of attacks that EDR defends against.

Reality: While it's easy to think that cybercriminals tend not to target smaller businesses, the reality is that SMBs face many of the same threats as larger enterprises. Although the vast majority of cyberattacks are commodity threats, a large part of the remainder are new, unknown and evasive attacks that bypass traditional EPP. These threats are hard to detect due to the range of evasion techniques being adopted - particularly the use of legitimate and system-native tools. By staying undetected for longer, they also have the time needed to explore and entrench themselves in a business's infrastructure and do a greater amount of damage – be it a data breach, ransomware or spyware attack, or directly overriding operations.

2 We need EDR to make up for weak EPP

Misconception: Our EPP isn't effective enough so we need EDR to strengthen it.

Reality: Trying to strengthen your endpoint security by investing in an EDR solution without addressing issues with your EPP is like building a tower block on quicksand. A weak EPP can actually undermine EDR so that it fails to deliver the required results. Plus, if the EDR solution is over-specified for your actual needs, it may also be overly costly and difficult for your team to understand and use.

3 To use EDR you need an expert IT security team

Misconception: SMBs and low-end enterprises don't have enough security specialists with the skills to understand and operate the tools needed to detect, investigate and respond to evasive threats.

Reality: When EDR was first introduced, the systems were complicated and difficult to use. But with modern solutions, each time you receive an alert, EDR will help you understand where the threat came from, how it developed, what its root cause is, whether it's touched any other hosts, and therefore what its scale is. It should also guide you through a simple incident handling process including steps such as identification, containment, eradication, recovery, and analyzing lessons learnt to help prepare for future attacks.

4 You can't combine EDR and MDR

Misconception: If you want EDR-class security, you either have to invest in EDR for use by your in-house team, or offload managed detection and response (MDR) to a specialist provider.

Reality: EDR-class security isn't an either/or decision. EDR and MDR each bring their own benefits, and the best option is often to combine the two. So, for example, an SMB or low-end enterprise could use MDR to instantly raise their IT security capability and protect against evasive threats, without the need to invest in additional staff or resources; while a larger enterprise could use it to offload incident triage and investigation processes 24/7, and better focus in-house IT security resources by using EDR for detailed investigation and response.

5 EDR increases alert fatigue and isn't worth the hassle

Misconception: EDR is notorious for generating large numbers of alerts and false positives that IT teams have neither the time nor resources to action or resolve.

Reality: Modern EDR solutions not only automate many tasks - EDR and/or MDR has the power to take you from a situation where you're under significant risk of an evasive attack, to one where you have renewed confidence in your endpoint security. Rather than being unsure about what's happening in your environment, you'll have visibility and control over all your endpoints. And, instead of being reluctant to upgrade security because of complexity, you'll have a simplified and consolidated solution that helps optimize your resources.

Try our interactive ransomware simulation game to discover how to better protect your IT infrastructure:
https://www.kaspersky.com/response-game/en/

Step 4:

Think about your use cases

Before you can identify the protection that best fits your needs, you need to set clear requirements for it. This means considering critical aspects of the solution's performance and regular use, such as the use cases you need it to fulfil and the results you expect it to deliver.

For example, when you receive a security alert, EDR and/or MDR should enable you to answer key questions such as:

- What's the context of the alert?
- What actions have been performed on the alert already?
- Is the detected threat still active?
- Are other hosts under attack?
- What path did the attack take?
- What's the root cause of the threat?

It should also help you understand the full scope of the threat. For example:

- If you're at risk of a global threat, your management team will likely want to be reassured you're not currently under attack, for which you'll need the ability to find an Indicator of Compromise (IoC) online, run a scan and answer their concerns correctly.
- If a regulatory authority asks you to run a scan for a specific IoC, you should be able to import IoCs from trusted sources and run periodic scans for signs of an attack.
- If you've thoroughly investigated an alert, and generated an IoC based on the discovered threat, rather than running scans throughout the entire network to find if other hosts have been affected, this should be done for you automatically.

Similarly, you should be able to quickly respond to prolific, fast-moving threats by:

- Containing the threat by isolating the host, quarantining the file or preventing files being executed during the investigation.
- Using automated cross-endpoint response based on IoC scans – enabling you to respond to evasive threats as soon as they're discovered – or guided and remote response scenarios if you're using MDR.

Among the key results you should therefore expect from your solution include:

- Protecting against more frequent and more disruptive evasive threats.
- Saving time and resources with a simple, automated tool.
- Assessing the scope of an attack by scanning for IoCs across all endpoints.
- Understanding the root cause of each threat and how it actually occurred.
- Avoiding further damage with rapid automated response.

5 common misconceptions about MDR

1 MDR is just another managed security service

Misconception: MDR is just like any other managed security service (MSS) involving vendor-side management of your IT infrastructure.

Reality: MSSs typically cover a range of general cybersecurity services such as regulatory compliance assessment, technologies like VPNs and firewalls, penetration testing, offering recommendations etc. Whereas, MDR focuses on advanced detection and rapid response to new, unknown and evasive threats bypassing automated EPP, through a combination of TTP-based threat hunting, detection and analysis.

2 MDR is only for big companies

Misconception: Because MDR deals with complex sounding capabilities like threat hunting and Indicators of Attack (IoAs), it's only suited to the needs of major enterprises.

Reality: MDR isn't a one-size-fits-all solution. It provides different capabilities for different kinds of organization. An SMB or low-end enterprise could use MDR to instantly improve their IT security and protect against evasive threats, while a larger enterprise could use it to offload incident triage and investigation, and better focus their in-house IT security resources.

3 AI-based MDR doesn't need human experts

Misconception: Artificial intelligence (AI) and machine learning (ML) have advanced to the point where the use of human experts in MDR will soon be a thing of the past.

Reality: AI, ML and proprietary IoAs enable automatic processing of large numbers of alerts - automating initial incident triage, minimizing mean time to detect (MTTD) and respond (MTTR) by significantly increasing MDR analyst throughput, and ensuring continuous protection against even the most innovative non-malware threats. But for previously unknown or human-driven TTPs that do not result in automatic detection, managed threat hunting still relies on the painstaking, proactive, hands-on efforts of experienced threat hunters.

4 MDR is difficult to implement

Misconception: MDR is often marketed as providing the capabilities of a 24/7 SOC, so it must be complicated to use.

Reality: As highlighted above, MDR can be used for everything from preventing threats bypassing existing cyber-defenses to providing a second opinion or freeing up in-house experts to focus on more important tasks. It can do this as an easily implemented turnkey service delivering dramatic improvements in MTTD and MTTR - and the faster MTTD and MTTR, the less disruption caused by incidents and the lower the resulting costs.

5 Even with MDR your team still have a lot to do

Misconception: MDR services grind to a halt after incident investigation, leaving clients with technical reports and recommendations to apply to their systems, and adding even more pressure on IT security resources.

Reality: While this was certainly the case in the past, with modern MDR services you can opt to authorize the provider to respond for you automatically, initiate recommended response actions yourself (such as isolating the host, moving files to quarantine, removing files, terminating processes, requesting files from or running a program on the host, IoC scanning etc.), or leverage managed remediation scenarios which you can pre-approve or manually approve for each alert.

Kaspersky's Security Operations Center (SOC) and Global Emergency Response Team (GERT) have analyzed a year's worth of security incidents spanning every sector to develop an unrivalled snapshot of the threat landscape.

Get access to the reports:
https://go.kaspersky.com/mdr-and-ir-reports-2022.html

Step 5:

Choose the protection that best fits your needs

Many organizations may not employ anyone dedicated specifically to IT security. Some may just be beginning to build their IT security department. And others may already have fully formed and skilled-up IT security teams.

Many organizations may not employ anyone dedicated specifically to IT security. Some may just be beginning to build their IT security department. And others may already have fully formed and skilled-up IT security teams. The quality of these organizations' available expertise in relation to threat defenses will therefore vary widely - as can the amount of time they can dedicate to this task.

To deal with these differing circumstances, organizations without dedicated IT security personnel, or those whose IT security staff are overloaded with routine tasks, will need to make strategic use of automation to counter the latest evasive threats.

This means supplementing their EPP with additional EDR tools which, while protecting against these threats, also incorporate appropriate levels of automation (full or partial).

Alternatively, rather than investing in an overly complex EDR solution for which they may not have the necessary time or skills, MDR lets organizations access capabilities such as 24/7 security monitoring by industry experts, automated and managed threat hunting, and guided and remote response scenarios - either from a vendor, managed service provider (MSP) or managed security service provider (MSSP).

A third option is to combine EDR and MDR. Many organizations do not have the expertise required for threat hunting, so outsourcing this while implementing detection and response capabilities in-house is often an ideal solution. And this can be particularly beneficial for businesses that want to develop their own cybersecurity team, but lack the resources, personnel and/or skills to support specialist detection and response.

What if you only have limited in-house resources?

Let's assume you have limited internal IT security resources, or a small team of one or two security specialists. Let's also assume you're trying to decide whether to supplement your EPP with EDR and/or MDR. What kinds of benefits can you expect and which would be right for you?

If you prefer a more hands-on approach (and your IT team has sufficient IT security skills), EDR can help prevent business disruption and damage by eliminating the risks posed by new, unknown and evasive threats, and giving your security personnel the visibility needed for threat investigation, root cause analysis and response.

This can drive cost efficiencies by enabling your security team to work more effectively without having to juggle multiple tools and consoles, and maximize capacity by automating an extensive array of processes. It also gives you peace of mind by making it easy to monitor and detect threats, and respond to and prevent attacks.

If you're looking to expand your internal IT security capacity by offloading key detection and response tasks, MDR can offer advanced, round-the-clock protection from threats that can otherwise bypass automated security barriers. This can help to empower your business by solving the cybersecurity talent crisis, and supplying all the major benefits of a 24/7 SOC.

MDR can also drive cost efficiencies by focusing in-house resources on those critical tasks that really demand your IT or IT security team's involvement, and maximize capacity by leveraging advanced ML models to significantly increase analyst throughput and minimize MTTR. Plus it can deliver continuous security monitoring by industry experts, along with automated and managed threat hunting. This includes analysis of complex non-malware threats, and dangerous, hard to detect threats using legitimate OS tools in attacks.

Combining EDR and MDR, meanwhile, lets you tailor their respective EDR-class capabilities to your particular needs, for example by outsourcing threat hunting (for which you may not have the required expertise) while implementing endpoint detection and response capabilities in-house.

How to assess your evolving security requirements – XDR

40% of organizations will have deployed an XDR platform by 2027, up from 5% in 2021

According to IBM's Cyber Resilient Organization Study 2021, 32% of organizations reported using 21 to 30 individual security tools in response to each threat, and 13% reported using 31 or more tools.

As a result of the number of tools involved, advanced threats take too long to identify and contain.

IBM's Cost of a Data Breach 2022 report found the average data breach took 277 days to detect and resolve, so a breach occurring on 1 January wouldn't be contained until 4 October.

XDR in a nutshell

If yours is a mid-size or major enterprise, and your SOC or IT security team haven't already been pestering you about XDR, it's only a matter of time before they do.

As noted by CRN (15.2.23), 'When it comes to threat detection and response, just looking at the endpoint or the network are no longer enough. The approach that many of the world's biggest cybersecurity companies have been moving toward in this sphere is XDR, or extended detection and response. One of the fastest-growing categories in cybersecurity today, XDR aims to provide enhanced security by correlating data from across an organization's environments and devices, and then prioritizing the most serious threats for a response.

'Regardless of exactly how they define themselves, XDR platforms all share a focus on giving a boost to shorthanded security teams, with the aim of improving the quality of threat detection while also reducing the overload in alerts.'

With XDR, security solutions that aren't necessarily designed to work together can interoperate seamlessly on threat prevention, detection, investigation and response. And, by eliminating visibility gaps between cybersecurity tools and layers, XDR enables overburdened security teams to detect and resolve threats faster and more efficiently; and capture more complete, contextual data to help them make better security decisions and prevent future attacks.

So what exactly does XDR do, what are the benefits, and why is it potentially one of the most significant security investments your organization will ever make?

EDR vs MDR vs XDR

EDR
Endpoint detection and response

- Identifies new, unknown and evasive threats bypassing endpoint protection, and automates routine security tasks

MDR
Managed detection and response

- Offloads threat detection, threat hunting and incident investigation, or supplements existing measures by delivering 24/7 advanced threat protection

XDR
Extended detection and response

- Proactively detects complex threats across multiple infrastructure levels, and automatically responds to and counters these threats

How it works

- Enhances threat visibility and visualization
- Provides advanced detection mechanisms (e.g. IoC, IoA)
- Simplifies root cause analysis and supports threat hunting
- Delivers quick, automated response

- Delivers continuous expert protection against even the most complex and innovative non-malware threats

- Integrates with multiple security tools, applications and existing cybersecurity infrastructure
- Monitors data across multiple sources to detect and eliminate complex threats

Business value

- Enables IT security teams to work more effectively without having to juggle multiple tools and consoles
- Automates a vast array of processes to avoid reliance on traditional remediation processes that might result in downtime
- Makes it easy to monitor and detect threats, centrally aggregate forensics data, and respond to and prevent attacks

- Focuses expensive in-house resources on those critical tasks that really demand an IT security team's involvement
- Leverages proprietary machine learning models to significantly increase analyst throughput and reduce MTTD and MTTR
- Solves the cybersecurity talent crisis
- Supplies all the major benefits of a 24/7 SOC

- Ecosystem approach maximizes efficiency of the cybersecurity tools involved, saves resources and reduces risk
- Simplifies the work of IT security specialists and gives them the additional context needed to investigate multi-vector attacks
- Minimizes MTTD and MTTR - crucial in combating complex threats and targeted attacks
- Provides holistic protection against the evolving threat landscape

Who's it best for?

- Tech-conservative, risk-averse businesses wanting to add visibility to automatic protection
- Mainstream IT users wanting to develop incident response processes
- Organizations using IT as a competitive advantage and needing to enable experts to find and neutralize complex threats

- Companies seeking to expand internal IT security capacity by offloading key detection and response tasks
- Organizations that might not have the budget or specialist staff available to build their own internal SOC

Organizations with significant security resources wanting a single platform delivering:

- A coherent picture of what's happening throughout their infrastructure
- Built-in threat hunting and threat intelligence
- Superior incident prioritization and fewer false positive alerts

Specific capabilities and benefits you should expect from an XDR platform

Single platform integrates multiple security tools

With XDR, security solutions that aren't necessarily designed to work together can interoperate seamlessly on threat prevention, detection, investigation and response.

- These could, for example, include solutions designed to protect mail, web, the network, cloud infrastructure, applications, identity etc., enabling additional kinds of attack scenarios to be detected and investigated, and strengthening the process of combating complex threats.
- XDR can also integrate threat intelligence tools – such as threat data feeds and the platform used to manage this data – to give SOC teams the additional context which is so important when investigating complex cyber incidents.
- Plus, depending on an organization's industry and requirements, XDR can integrate operational technology (OT) and Internet of Things (IoT) security tools, and so extend a comprehensive security umbrella across IT/OT environments.

Unites multiple telemetry types

By enabling real-time behavioral and telemetry analysis across multiple security layers including endpoint, network and cloud, security analysts can better visualize cyberthreats, and target and eliminate threats based on the severity with which they can impact the organization's IT infrastructure.

Delivers end-to-end threat visibility

By breaking down the silos between layer-specific point solutions, XDR gives SOC and IT security teams the end-to-end visibility and integration they need to identify threats faster, respond to them more quickly, resolve them more effectively and minimize the damage they cause.

Because XDR can link each step throughout an entire kill chain and present this as a single alert detailing the full context of the attack, this reduces alert volumes, increases alert quality, and enables end-to-end orchestration and response.

Streamlines and centralizes data collection, and increases efficiency

A single data lake delivers comprehensive log collection, management and storage, by providing a centralized platform to collect, index and analyze logs from diverse sources including security solutions (EPP, FW, NGFW, IAM, SIEM, SOAR etc.), operational systems, business applications (HR systems, office tools), physical security (automated access control systems) and other devices.

This enables SOC and IT security teams to gain valuable insights, detect anomalies, and identify potential security incidents by leveraging rich log data covering both past and present (real-time) events. Integration with other security tools and platforms also enhances operational efficiency by centralizing security management and providing a unified view of security events and incidents.

Accelerates threat detection, investigation and response

By eliminating visibility gaps between cybersecurity tools and layers, XDR enables overburdened security teams to detect and resolve threats faster and more efficiently, and capture more complete, contextual data to help them make better security decisions and prevent future attacks.

By automating routine tasks such as threat triage, containment and remediation, organizations can optimize their security resources and focus on more strategic activities.

Reduces MTTD and MTTR

XDR helps minimize mean time to detect (MTTD) and mean time to respond (MTTR) - crucial for combating complex threats and targeted attacks, where quick actions taken by IT security experts reduce dwell time and the attackers' chances of achieving their goal of inflicting financial or reputational damage on the organization.

Improves threat hunting

By leveraging the latest threat intelligence, XDR enhances threat hunting and discovery, while the automation of routine tasks, guided investigation processes and customizable detections all promote speedy incident resolution. Advanced threats are detected and neutralized faster and more accurately - crucial in dealing with complex and APT-like attacks.

Helps address the global shortage of IT security experts

Amid a global shortage of IT security experts, XDR provides holistic protection for an expanding, changing IT infrastructure against a rapidly evolving cyberthreat landscape. XDR simplifies the jobs of valuable, scarce resources such as IT security specialists, reduces their need to get involved in routine tasks, and frees them to engage in the process of working with complex incidents.

Supports regulatory compliance and risk management

By providing comprehensive visibility, threat intelligence and reporting capabilities, organizations can demonstrate compliance with industry regulations and frameworks such as GDPR, PCI DSS, HIPAA and others. This helps mitigate legal and financial risks associated with non-compliance.

Log management also plays a crucial role in ensuring compliance with industry or regional standards and regulations, by facilitating the storage and retention of data and logs for the prescribed duration(s), and enabling organizations to easily retrieve and analyze logs when needed.

Delivers user friendly management via a single console

User-friendly XDR solutions provide comprehensive insights into ongoing threats and suspicious activities via a single console. This enables proactive threat hunting and faster incident response, and delivers a holistic view that helps SOC teams identify suspicious activities and potential security incidents more efficiently.

Open and Native platform options

Open XDR supports third-party integrations to collect specific forms of telemetry to enable threat detection, hunting and investigation across different data sources and execute response actions. This avoids vendor lock-in, and lets organizations leverage their already deployed third-party security tools and choose the most suitable products from different vendors.

Native XDR is a solution built by a single vendor and designed to work with that vendor's products.

Cloud and/or on-premises deployment

While the vast majority of XDR platforms are Open and cloud-based, on-premises deployment is ideal for organizations wanting to enable full data sovereignty, and ensure they meet their regulatory and compliance requirements.

Integration with Zero Trust

When used together, XDR and Zero Trust provide powerful defense against cyberthreats. Zero Trust helps prevent unauthorized access to resources and applications or revoke access already granted if conditions have changed, while XDR helps detect and respond to potential threats that manage to bypass those initial access controls.

XDR vs SIEM vs SOAR

XDR
Extended detection and response

- Proactively detects complex threats across multiple infrastructure levels, and automatically responds to and counters these threats

SIEM
Security information and event management

- Collects, aggregates, analyzes and stores log data from across the IT infrastructure for use cases including governance and compliance, and rule-based correlation matching for suspicious activity

SOAR
Security orchestration and automated response

- Ingests data from a variety of sources across the infrastructure, including management systems and threat intelligence platforms, and provides priority analysis
- Enables security teams to configure multi-stage, cross-solution automated responses to incoming threats

How it works

- Integrates multiple tools and security applications
- Monitors data on endpoints, networks, clouds, web servers, mail servers etc. to detect and eliminate complex threats

- Looks for any patterns or events that might indicate suspicious behavior, and generates an alert for the SOC or IT security team

- Uses playbooks to automate a wide range of workflows such as vulnerability scanning, log analysis, user access management, threat triage and more
- Orchestrates multiple disparate tools and processes into a larger workflow, collating all relevant data into a single platform for consolidated, actionable information

So what are the differences?

- Ecosystem approach maximizes efficiency of the cybersecurity tools involved, saves resources and reduces risk
- Simplifies the work of IT security specialists and gives them the additional context needed to investigate multi-vector attacks
- Minimizes MTTD and MTTR - crucial in combating complex threats and targeted attacks
- Provides holistic protection against the evolving threat landscape

- Huge dataset provided by SIEM can result in too many alerts that have to be manually filtered, processed and analyzed
- Doesn't provide the context needed to deal with new, complex or sophisticated attacks
- Passive solution doesn't include blocking, quarantining or response capabilities
- Best used in tandem with proactive investigation and response solutions like XDR or SOAR

- Maintaining a well-configured SOAR platform which integrates with partner tools requires the ongoing effort of a highly skilled, mature SOC
- Without such skilled, vigilant maintenance, SOAR analysts can end up with too many low-priority alerts, false positives, and a generally incoherent dataset as a result of all the various siloed tools feeding into the platform - exactly what they were trying to avoid

How to justify the investment in XDR

Alongside the technical benefits, there are sound business reasons for investing in XDR, such as those related to attack mitigation, detecting insider threats, cloud and compliance, incident investigation and response and more.

Attack mitigation

If an organization has fallen victim to a ransomware attack which resulted in critical data being encrypted and operations halted, XDR's proactive threat detection capabilities would have helped to identify and prevent this kind of attack before it could wreak havoc, through the ability to detect suspicious behaviors, isolate infected endpoints and provide real-time incident response - significantly reducing the impact of the attack and quickly restoring business continuity.

Insider threat detection

Insider threats are a top concern for most organizations - intentional or otherwise. But because XDR delivers comprehensive visibility across endpoints, networks, applications and the cloud, it can detect telltale signs of insider threats such as anomalous user behavior, attempts at data exfiltration and unauthorized access. And, by correlating and analyzing data from multiple sources, XDR can help identify and mitigate insider threats, protect sensitive information and maintain data integrity.

Cloud and compliance

As more organizations embrace cloud technologies, ensuring robust security and compliance is becoming ever more important. By providing unified visibility and threat detection across hybrid and multi-cloud environments, XDR enables organizations to monitor cloud workloads, detect misconfigurations and identify suspicious activities - and so maintain a secure and compliant cloud infrastructure while mitigating the risks associated with cloud-based attacks.

Incident response and investigation

Swift responses and thorough investigations are critical in minimizing damage and preventing future incidents. XDR streamlines incident response processes by automating threat detection, alert triage and investigation workflows, and providing security teams with a comprehensive view of incidents enabling them to respond quickly and effectively. The savings in time and resources resulting from XDR's automated response capabilities make it a game-changer in incident management.

Complements EPP, EDR, SIEM and more

Preventing the kinds of threats outlined above more than justifies the investment in XDR, while for users of EPP, EDR, SIEM and more, XDR strengthens the performance of all of these solutions.

- For EPP, XDR enhances endpoint protection capabilities by providing advanced threat detection, response automation, and improved visibility across network and cloud environments – making it the next logical step in security roadmaps, and enabling organizations to achieve a higher level of protection against evolving threats.
- For EDR, XDR (which is often built on EDR) extends the solution's capabilities beyond endpoint-focused detection and response, by providing holistic visibility and threat detection across the protected infrastructure - including network, virtual machines, applications and cloud environments - and enabling more efficient incident response and enhanced threat hunting capabilities.
- For SIEM, XDR complements the solution by providing real-time threat detection, advanced response capabilities, and enhanced visibility and correlation of security events across endpoints, networks and the cloud, enabling faster incident response and reduced investigation times.

For those likely to invest in XDR technology in the near future, ease of use is, by far, the most important perceived benefit to their organization, whether planning to integrate the technology with their existing security tools or establishing a single-vendor, XDR-ready infrastructure. Respondents also indicated other near-term investments in solutions for unifying detection and response and improving visibility across security products/services were most likely to be endpoint detection and response (EDR), network detection and response (NDR), security information and event management (SIEM), and threat intelligence.

CRA Business Intelligence, XDR Poised to Become a Force Multiplier for Threat Detection, March 2022

Addressing the broader threat landscape

In many organizations, security analysts spend more than half their time sorting out false positives instead of proactive threat hunting and response, leading to significant increases in detection times

Threat intelligence

For many organizations, and especially those that are vulnerable to targeted attacks and APTs, threat intelligence (TI) is a vital tool in enabling proactive threat defense. But while the uses and benefits of TI are many and varied, so are its sources, meaning that identifying what will work best for a particular organization can be a challenge in itself.

In many organizations, security analysts spend more than half their time sorting out false positives instead of proactive threat hunting and response, leading to significant increases in detection times. Feeding security operations with irrelevant or inaccurate TI will drive the number of false alerts even higher, with serious negative impacts on both response capabilities and overall security. So how can this be avoided?

While there are no universally agreed criteria for evaluating commercial TI offerings, aspects to take account of when doing so include:

- With an extensive range of providers to choose from, organizations should look for TI that transforms understanding of their specific threat landscape - for example through detailed analysis of historical and emerging threats targeting their particular industry, region or individual enterprise - to improve the performance of functions such as vulnerability management, threat hunting, incident response and more.
- To effectively combine TI with the security tools, controls and processes an organization already uses and knows, it should look for delivery methods, integration mechanisms and formats that support smooth integration of TI into its existing security operations.
- It's also important to identify TI with global reach. As attacks have no borders, does the vendor source information globally and collate seemingly disjoined activities into cohesive campaigns, as this kind of intelligence will help take more appropriate actions?
- Organizations looking for more strategic content to inform their long-term security planning should look for a TI provider with a proven track record of continuously uncovering and investigating complex threats in their region and/or industry.
- The provider's ability to tailor its research capabilities to the specifics of the organization is also critical.

Threat intelligence (TI) is a constantly evolving resource. And to be effective, so must be the internal TI programs that utilize it. Benchmark your current performance with our interactive TI assessment tool and get customized recommendations for improvement based on your responses: https://go.kaspersky.com/ti_tool_2023.html

In addition, utilizing Kaspersky Threat Intelligence Portal helps an organization aggregate, manage and operationalize TI – vital when security tools are utilizing TI from multiple sources. Specifically, Kaspersky Threat Intelligence Portal should enable the organization to:

- Respond to threats more effectively by checking any threat indicator considered to be suspicious, whether it's a file, file hash, IP address or web address.
- Analyze files to detect advanced commodity, evasive and APT-like threats.
- Submit IP addresses, file hashes, domains or web addresses considered to be suspicious, to quickly validate and prioritize alerts and incidents using risk levels and supporting contextual information to determine which are real threats.
- Receive regular reports on the behavior of specific files or web addresses.
- Automate security workflows by connecting relevant applications with Kaspersky Threat Intelligence Portal.

Security awareness

More than 80% of all cyber-incidents are caused by human error

More than 80% of all cyber-incidents are caused by human error, not least because, as cybersecurity solutions are rapidly developing and adapting to complex threats, this is making life more difficult for cybercriminals who are turning to the most vulnerable element of cybersecurity - the human factor. Examples of the impacts of this are that:

- 52% of C-level executives say employees are the biggest threat to operational security.
- 43% of small businesses have suffered a security incident due to violation of IT security policies by employees.
- 60% of employees have confidential data on their corporate device (financial data, email database etc.).
- 30% of employees admit that they share their work PC's login and password details with colleagues.

A culture of cybersafe behavior, together with fundamental cybersecurity skills and awareness throughout an organization, are therefore key to reducing its attack surface and the number of incidents its IT team has to deal with.

How Kaspersky can help

Kaspersky Next EDR Foundations

Kaspersky Next EDR Foundations' powerful ML-based endpoint protection, flexible security controls and EDR root cause analysis equip organizations with the most straightforward way to build a strong core for their cybersecurity. A simple console, cloud or on-premises deployment, and a variety of quality-of-working-life promoting features reduce complexity and boost efficiency.

Kaspersky Next EDR Optimum

Kaspersky Next EDR Optimum provides strong endpoint protection, improved controls, training, patch management and more – all enhanced by essential EDR functionality. Threat visibility, investigation and response are simple, quick and guided, to help IT and IT security teams deflect attacks rapidly and with minimal resources.

Kaspersky Next XDR Expert

Kaspersky Next XDR Expert integrates seamlessly with an organization's existing security infrastructure, providing real-time visibility and deep insights into evolving cyberthreats to deliver advanced threat detection and automated response, and the essential XDR capabilities outlined in this e-book.

Kaspersky Managed Detection and Response

Kaspersky MDR delivers advanced, round-the-clock protection from the growing volume of threats circumventing automated security barriers, and provides relief to organizations struggling to find specialized staff or with limited in-house resources. Its superior detection and response capabilities are supported by one of the most successful and experienced threat hunting teams in the industry. Unlike similar offerings, Kaspersky MDR leverages patented ML models, unique ongoing threat intelligence (TI) and a proven track record of effective targeted attack research. It automatically strengthens corporate resilience to cyberthreats while optimizing existing resources and future IT security investments.

Kaspersky Threat Intelligence

Kaspersky's TI portfolio covers a full range of security scenarios including prevention, detection, investigation, response and strategic reporting, all of which can be tailored to the needs of individual organizations. Our Global Research and Analysis Team (GReAT) are an elite group of experts who, by infiltrating closed communities and dark forums worldwide, have discovered and dissected more than 50 of the world's most sophisticated targeted attacks. And our knowledge, experience and deep intelligence on every aspect of cybersecurity have made us a trusted partner of premier law enforcement and government agencies including INTERPOL and leading CERTs.

Examples of our innovative TI solutions and services include more than 20 types of threat data feeds; extensive range of TI reports; in-house developed sandbox for detecting sophisticated and evasive threats; open threat intelligence portal; and services such as customer-specific threat landscape analysis, and Kaspersky Digital Footprint Intelligence, which analyzes digital footprint data to identify potential threats and vulnerabilities.

Kaspersky Security Awareness

Kaspersky Security Awareness offers a range of highly engaging and effective training solutions that boost the cybersecurity awareness of employees at all levels and help them play their part in overall cyber safety. Because sustainable changes in behavior take time, our approach involves building a continuous learning cycle with multiple components including interactive protection simulations covering a range of industry scenarios; gamified assessment tools; an automated security awareness platform delivering simulated phishing campaigns; C-level executive training and more.

Kaspersky Professional Services

Kaspersky's Professional Services portfolio of assessment, implementation, maintenance and optimization services helps organizations meet their unique needs, minimize their security risks, maximize return on investment, minimize the strain on their resources, respond fast to new security threats, and extract maximum benefit from their Kaspersky solutions.

Trust

Proven. Transparent. Independent.

In 2017 Kaspersky launched our Global Transparency Initiative. This means that – unlike any comparable vendor – if you're worried about our products you're free to review our source code, software updates and threat detection rules, as well as our secure development lifecycle processes, and software and supply chain risk mitigation strategies. To support this initiative we've opened more than 10 Transparency Centers around the world, which have hosted visits by regulators, critical infrastructure providers, customers, partners, the media and more. And, for customers requiring them, we're SOC2 audited and ISO/IEC 27001 certified.

Kaspersky Next EDR Foundations — Learn more

Kaspersky Next EDR Optimum — Learn more

Kaspersky Next XDR Expert — Learn more

Cyber Threats News: securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

kaspersky.com

Learn more about Kaspersky Next at: https://go.kaspersky.com/next

Choose the tier that suits you best by taking a short survey in our interactive tool: https://go.kaspersky.com/Kaspersky_Next_Tool