Buyer's Guide

A Buyer's Guide to Extended Detection and Response

What is XDR and how can it strengthen your security?

Rene Holt

Digital Security
Progress. Protected.

August 2023

Digital Security
Progress. Protected.

Table of Contents

Introduction

If you are responsible for IT security at your company, then this guide on extended detection and response (XDR) serves two purposes.

- **First, to gain insight into how an XDR solution can enhance your company's security.**
- **Second, to point out the features of an XDR solution that are well worth considering in your purchase decision.**

The prerequisite question before even thinking of buying XDR is: Do you need it? Multiple pain points could trigger such a need ranging from the rise of ransomware, the risk of supply-chain attacks, the continued abuse of IT admin tools by attackers, to regulatory and insurance requirements.

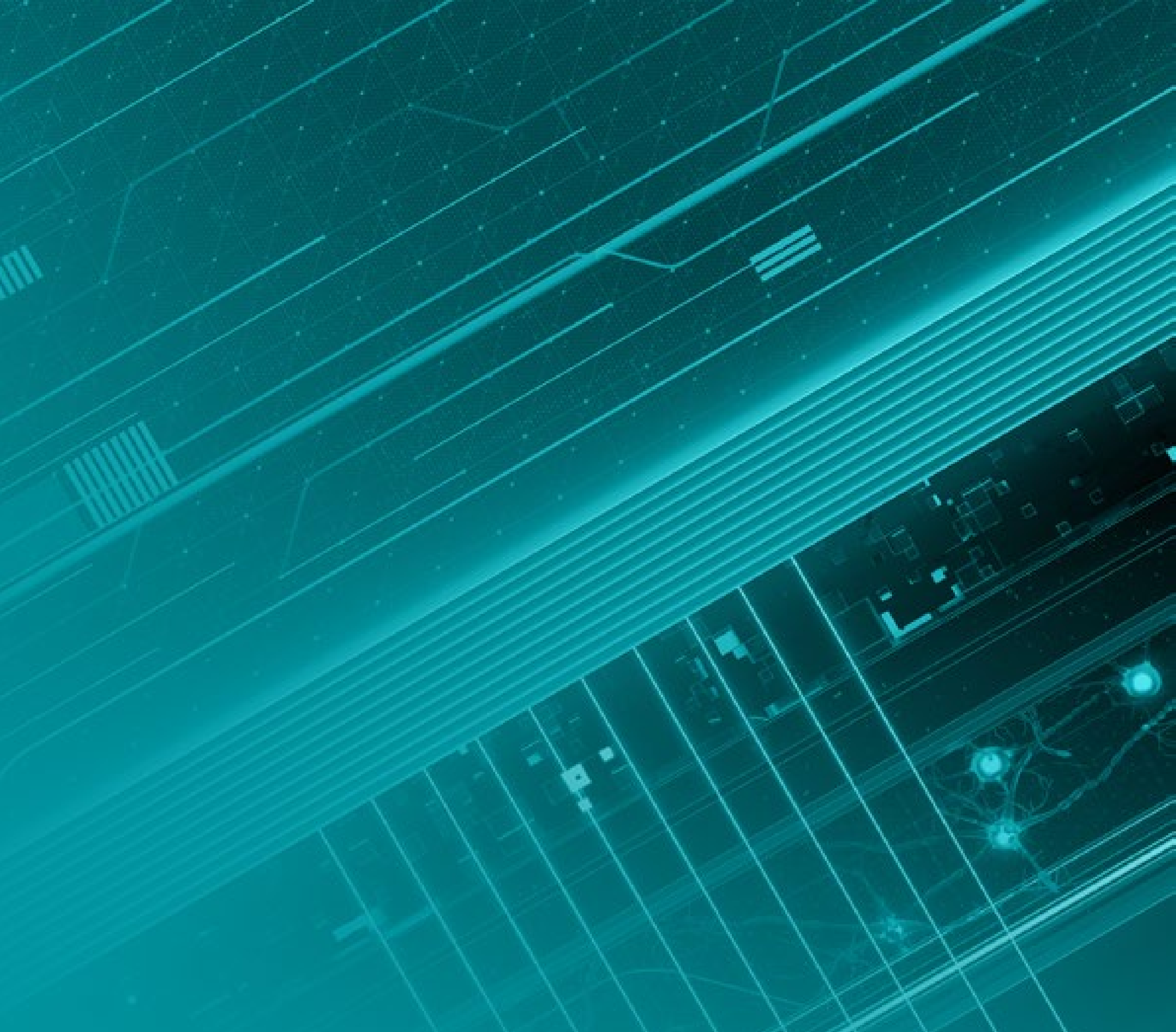
But apart from addressing threats and meeting requirements, a melting pot of marketing messages has muddled the very meaning of XDR. Under one definition, a solution may be considered as XDR, yet under another it is only "XDR-like".

Is it too bold to say that vendors are defining XDR according to the particular strengths of their solutions? Or should it be said that vendors are designing their XDR solutions according to philosophies that are as disparate from each other as they are from their practical experience with security?

Discerning between XDR solutions is not a question of whose philosophy is right or wrong, but of what philosophy makes the most sense for the company you are charged with securing, using the resources given.

Vendors have the duty of clearly articulating their philosophies so that you can make a decision based on an accurate vision of each vendor's XDR. By the end of this guide, we hope to impress upon you at least one lasting message: our XDR-enabling solution, ESET Inspect, returns the decision-making power over the detections and responses to be made back into the hands of an organization's defenders.

ESET Inspect equips IT admins with a tool powerful enough to gather the information needed to make decisions with confidence. The positive cumulative effects for your defenses include improved risk assessment; lowered security expenses in the long-term; simplification of security processes; and shortened times to detect, investigate, and respond to threats.



Discerning between XDR solutions is not a question of whose philosophy is right or wrong, but of what philosophy makes the most sense for the company you are charged with securing, using the resources given.

Chapter 1: Current threats

The cyberwar waged between defenders and adversaries is an endless struggle. From 2021 to 2022, ESET telemetry[1] recorded a 13% increase in the total number of threat detections.

Although endpoint security has been an indispensable aid in this fight, certain threats seem to defy even this protection, especially when systems have been left exposed with gaping security holes.

To better understand how XDR can help address such dangerous threats, let's run through the following four: ransomware and wipers, abuse of IT admin tools, leaked corporate secrets, and supply-chain attacks. While these are not the only threats that XDR helps to address, they represent challenges that can be particularly difficult to handle without it.

THE FALL OF RANSOMWARE AND THE RISE OF WIPERS

In 2022, ESET telemetry registered a decline in ransomware and a rise in wipers, particularly in Ukraine. Is this decline due to fewer ransomware attacks? Or have would-be ransomware attacks been detected earlier on, preventing attackers from having the opportunity to deploy ransomware?

Whatever the answer, ransomware and wipers are a critical concern because of the catastrophic damage they could impose. Should the malware operators exfiltrate any data, they can even attempt double exploitation of the victim, promising not to leak the data if the demands are met. Even if the chances were low, the potential damage is significant enough to warrant intense scrutiny of your defenses against such destructive malware.

A stealthy enough attack could exploit a gap or weakness in your defenses and then attempt to deploy ransomware or a wiper, while evading detection. XDR can give defenders visibility into the earlier (and later) stages of an attack, helping defenders to detect the attack in the early stages before any attempted deployment of destructive malware.
In other words, by leveraging XDR for

[1] See more in the ESET Threat Report T3 2022.

threat hunting you can significantly reduce adversary dwell time in your network.

ABUSE OF IT ADMIN TOOLS

Attackers are just as well versed in the use of IT admin tools as defenders, meaning that the abuse of these tools can provide a false cover of legitimacy. Some tools we have seen employed by attackers are PowerShell, certutil, PsExec, and SDelete.

For example, LookingFrog – an adversarial group known for targeting diplomatic missions, charitable organizations, and industrial manufacturing companies – used certutil to deliver a web shell. Agrius – known for targeting HR firms, IT consulting companies, diamond wholesalers, and jewelers – used PsExec to execute the Fantasy wiper via a Windows batch file. NikoWiper, based on the SDelete tool for securely deleting files, was detected at a company in the Ukrainian energy sector.

The tools used by IT admins have functionalities that, in the wrong hands, can be abused to download malware, reconfigure systems, disable security settings, perform reconnaissance, and even destroy data. Since these tools are legitimate, endpoint security software is limited in its ability to differentiate between fair use and abuse.

However, with XDR you can monitor how IT admin tools are being used and alert defenders to actions that are not typical for admins or potentially dangerous.

LEAKED CORPORATE SECRETS

In a surprise discovery by ESET researchers, a number of core routers sourced from the secondary market contained sensitive information from their former employment in corporate networks. This was surprising because you would think that large organizations have the processes and staff to ensure that devices are securely wiped before being offered for resale.

Considering that such devices are cheap for attackers to purchase, any sensitive data left behind could provide a boost to plans for breaching those networks.

In the face of such a leak, at least two steps can be taken. First, rotate out any cryptographic keys that may have been stored on resold devices so that they cannot be used to gain unauthorized access to your network. Second, equip yourself with XDR to hunt down attackers leveraging corporate secrets about your network.

SUPPLY-CHAIN ATTACKS AND THIRD-PARTY RISKS

Naturally, companies place trust in their software suppliers that updates are not trojanized. Attackers that compromise software developers can abuse that trust for initial access into customers' environments.

In an Agrius campaign, for example, the update servers of an Israeli software developer in the diamond industry were compromised and used to send a malicious update containing the Fantasy wiper to customers.

Interestingly, in the case of a Tick campaign, the attackers compromised the update servers of a data-loss prevention company to move laterally on the network, rather than to perform a supply-chain attack against external customers.

In a further twist in this Tick campaign, trojanized installers for Q-Dir – a multipane file explorer for Windows – were transferred via remote support tools to customers of the compromised company, probably during technical support sessions.

XDR is relevant for threats such as these because it can alert defenders to malicious activity following the exploitation of a trusted relationship with a software supplier or another third party.

Ransomware and wipers are a critical concern because of the catastrophic damage they could impose. Should the malware operators exfiltrate any data, they can even attempt double exploitation of the victim, promising not to leak the data if the demands are met.

Chapter 2: What is XDR?

Having considered some of the threats facing organizations and XDR's role in detecting them, let's take a quick look at the XDR market.

MARKET PREDICTIONS

According to Gartner®, "by year-end 2028, XDR will be deployed in 30% of end-user organizations to reduce the number of security vendors they have in place, up from less than 5% today."[2] That is incredible growth in the adoption of XDR! Another analyst firm, IDC, predicted similarly incredible growth but in revenue. A November 2022 IDC report forecasted the worldwide revenue for cloud-native XDR to see a compound annual growth rate of 66.1% from 2021 to 2026.

As organizations seek to up their game against adversaries, XDR has clearly stirred up momentum as a go-to solution.

DEFINING TERMS

As alluded to in the introduction, XDR, and related terms like endpoint detection and response (EDR) and managed detection and response (MDR), are defined variously by vendors. Even the borderline between endpoint security and EDR sometimes appears blurred in marketing materials. Because of the muddy understanding of these terms, it is not uncommon for critiques based on different definitions, expectations, and experiences to be voiced.

A probable source of this confusion is that many vendors are approaching XDR from different areas of expertise. For ESET, the journey started over thirty years ago with conducting malware research and developing endpoint security software, later leading to EDR, and now XDR. Other vendors may be approaching XDR with experience in security analytics or threat intelligence platforms on their résumés instead.

Here, we will go over a quick and basic explanation of how ESET understands these terms.

EDR VS. ENDPOINT SECURITY

To protect devices, endpoint security uses multiple layers of technology, each tuned to detect and block threats automatically. For the IT admin, the experience with endpoint security is largely passive and automated. In one

[2] Gartner, Market Guide for Extended Detection and Response, August 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

sense, this is beneficial because the IT admin is not burdened with security issues that are dealt with right away.

On the other hand, the IT admin is typically provided little information as to why certain threats are detected, that is, if there isn't a deeper underlying cause of the detected symptoms. An EDR solution gives the IT admin visibility into the events happening on endpoints, thus allowing a diagnosis of the symptoms to be made.

An EDR solution can detect specific events, or sequences of events, that are suspicious or worthy of monitoring. These detections are triggered by an engine that analyzes these events and alerts the admin when a behavioral match occurs. In addition, EDR makes response actions available to admins, such as killing a process, isolating a computer from the network, blocking an executable, and so on.

In short, EDR requires a hands-on and active approach to security because it empowers defenders to monitor and investigate low-level events for the possible use of attack techniques. Other proactive measures such as adversary simulation and threat hunting become easier to do with EDR as well.

XDR VS. EDR

If an EDR solution can ingest data from additional devices and sources, such as network devices and cloud services, then it is XDR. In other words, "extended" refers to data beyond endpoints. Evolving EDR into XDR requires increased integration with security solutions from the vendor and perhaps third parties as well.

One challenge spurring the growth of XDR is the fatigue caused by a multiplicity of tools each of which give only a piecemeal view of an organization's security. If more types of data can be fed into one detection engine and provided to the defender in a cogent and easy-to-understand way, then the defender gains a broader view of the organization's security. In turn, this can lead to more efficient incident response and increased automation.

What is EDR?

Endpoint detection and response (EDR) analyzes system, process, and user activity to detect security threats. It provides remedial guidance for threats that bypass prevention controls and enables endpoint threat investigations. EDR capabilities are often included in endpoint protection platforms and delivered as software agents connected to centralized cloud-based security analytics and management software.

Source: *Hype Cycle™ for Endpoint Security, 2023, Franz Hinner, et. al., August 2023.*

What is XDR?

Extended detection and response (XDR) delivers security incident detection and automated response capabilities for security infrastructure. XDR integrates threat intelligence and telemetry data from multiple sources with security analytics to provide contextualization and correlation of security alerts. XDR must include native sensors, and can be delivered on-premises or as a SaaS offering. Typically, it is deployed by organizations with smaller security teams.

Source: *Gartner: Market Guide for Extended Detection and Response. Thomas Lintemuth. [17 August 2023] ID: G00761828.*

However, gaining this bird's-eye view may not always benefit threat hunting if the data is sourced externally. Because the vendor's data sources are typically richer and better normalized than third-party data, increased integration with a vendor's solutions (also referred to as native XDR) usually offers greater help in hunting and responding to attacks.

MDR VS. XDR

Since XDR is most effective with highly skilled staff who have time dedicated to operating it, outsourcing the management of XDR may be a desired option. As the name suggests, MDR is a managed security service combining XDR with cybersecurity experts and additional services offered by the vendor or a third party. Some even use the term MxDR to differentiate from the "old" meaning of MDR that referred to EDR.

MDR can help organizations overcome certain challenges to make the jump to XDR that would otherwise not be possible. Such challenges include alert fatigue, the difficulty of finding and hiring talented or experienced security staff, the costs of running an in-house security operations center, and the demand on time to keep up with quickly evolving threats.

Possible issues related to XDR capability

Complexity of the tool

Alert fatigue of the tool

Lack of qualified IT resources

Limited time for threat monitoring in XDR

Chapter 3: How can XDR help you?

While monitoring low-level events on endpoints might sound interesting for security analysts, let's step back and consider the benefits to your company's security. Can the detection of suspicious events actually improve your defenses?

KEY BENEFITS

Organizations using XDR for the first time may be surprised by all the events that trigger detections. It can be a watershed moment revealing a host of poorly configured systems, vulnerabilities, or threats. The initial deployment of XDR can thus lead quickly to a couple of benefits: uncovering poor cyber-hygiene practices in your organization and discovering threats lurking in your network.

In Chapter 1, we considered a number of threats that organizations may be hard-pressed to defend against without XDR, meaning that with XDR you gain the following benefits: increased confidence to detect ransomware, wipers, and supply-chain attacks, and to discover attackers abusing IT admin tools or leveraging corporate secrets, perhaps purloined off decommissioned devices.

Because of the visibility granted into low-level events, another benefit of XDR is that defenders can test their coverage of adversarial tactics and techniques as described in the MITRE ATT&CK® knowledge base. Of course, there are often multiple ways to perform a technique, not all of which are recorded in ATT&CK. Yet the recorded techniques do serve as faithful signposts along the way to discovering weaknesses and gaps in your defenses. To assist in adversary emulation, XDR solutions reference detections to ATT&CK techniques.

Another benefit of XDR is threat hunting. The security news cycle often reveals ongoing attacks, sometimes happening on a mass scale. With defenders careening to their consoles to test the newly reported attacks and tune defenses accordingly, XDR provides the benefit of being able to write threat hunting rules that can search your database of events, looking for potential signs of compromise.

Once a threat is discovered, XDR provides incident responders with various remediation options. To decrease the mean time to respond to threats, XDR can trigger response actions automatically.

Incident responders are also interested in tracing attacks back to initial access. Since XDR keeps track of process trees and can correlate events, responders are better positioned to discover the initial attack vector. This capability is especially crucial to mitigate against attacks beginning with the exploitation of a zero-day or still unpatched vulnerability, supply-chain attacks, and insider threats.

XDR also facilitates cooperation between incident responders, incorporating collaboration features inspired by incident response platforms.

Demonstrating XDR's value

In 2023 and beyond, IDC anticipates vendors will shift from promoting their XDR readiness to demonstrating tangible proof of XDR's multifaceted value. Included in this value demonstration is the following: sharpening organizations' understanding of cyber-risk and the pathways to structurally reduce that risk, improving performance metrics (e.g., mean time to detect, investigate, and respond), and curbing the impact of cybersecurity's technology sprawl on organizations' overall security expenditures and collective complexity.

Source: IDC, *Worldwide Modern Endpoint Security Market Shares, July 2021–June 2022: Currency Exchange Rates Slightly Trimmed Accelerating Growth, Doc # US49982022*, *January 2023*

Chapter 4: What to look for in XDR

This chapter walks potential XDR buyers through the nine criteria they should consider before purchasing.

DETECTION

To detect attacks, XDR monitors events. Some events can, depending on the circumstances, indicate malicious intent or merely be benign activity. This dual-purpose nature leads to a greater chance for false positives. Thus, an XDR solution should come with a detection engine that has been well tested in its default configuration to minimize false positives for as many types of organizations as possible.

The strategy that XDR takes to minimize false positives involves a delicate balance. Sometimes it's better for a particular environment not to have an XDR rule enabled for events that are frequently generated and observed in attacks, but instead rely on detecting the attack with another event. The attack is still detected, even though you may not have been alerted to each step. This means that not every XDR solution is necessarily monitoring the same events to detect the same attack.

A further complication is that the frequency of an event is affected by the use of particular systems, apps, or tools at an organization. What is commonplace for one organization may not be for another. The same applies to job roles within a company.

Another consideration is that too many false positive detections cause admin fatigue, requiring the optimization of the XDR solution after initial deployment. If your organization is not able to do the initial optimization, look for an XDR vendor that offers this service.

Any detection should offer context, such as the possible malicious and benign causes, an estimate of the severity, and information about the events that triggered it. After all, XDR is designed to assist the investigative work of threat hunters.

Finally, look at the detection sources – this critically affects an XDR solution's capability to detect threats. Does the telemetry data include detections from API monitoring, memory scanning, scripts exposed by the Windows Antimalware Scan Interface (AMSI), or even network traffic content analysis?

XDR monitors low-level events, including:

- HTTP requests
- TCP/IP connections
- Code injection
- Registry values set
- Registry keys deleted
- File operations
- Windows API calls
- WMI events
- Scripts
- DLL loading
- Driver loading
- Kernel module loading
- Executables dropped
- Named pipe creation
- User account events
- Endpoint security detections

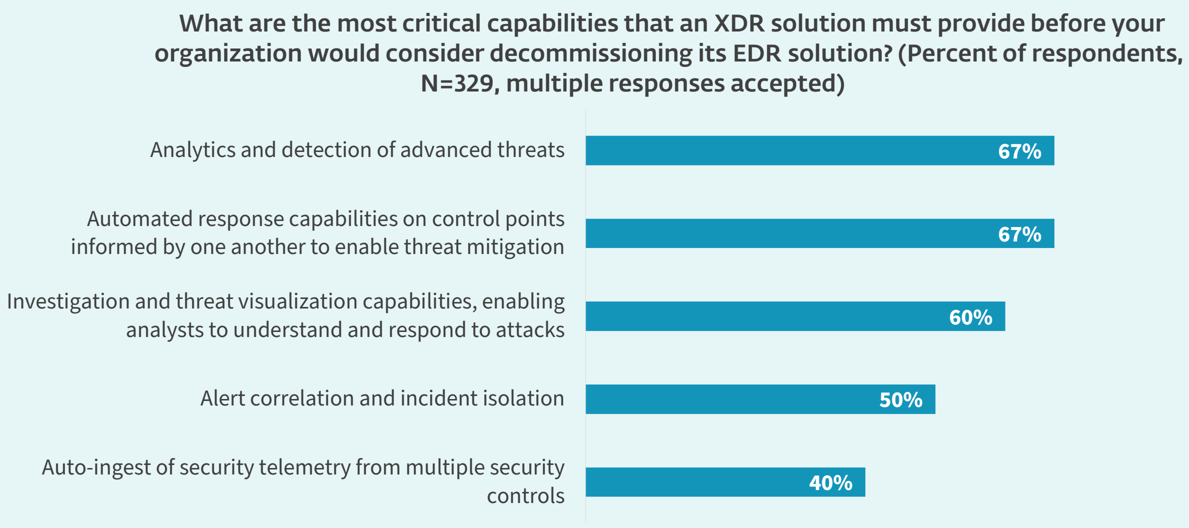
There should be overlaps in the detection sources for robustness.

RESPONSE

XDR should offer recommended investigation steps, remediation actions, and automated response. Such actions could include blocking the running of executables and loading of code libraries (DLLs), shutting down or rebooting the computer, forcing a logout, isolating the computer, killing processes, and cleaning files.

Potential buyers should be wary of automated responses that are too aggressive and thus break the functioning of systems in their environment. Part of the false positive testing for a new rule should include assessment of how severe the threat associated with the detection is and how probable the cause is malicious before attaching automated responses that block execution or kill a process.

In a 2022 survey of medium and large enterprises in North America, cybersecurity professionals identified detection and response as the most critical XDR capabilities. (See the graph on the next page.)



Source: *ESG Brief: The Demise of EDR?, April 2022, p. 2.*

BALANCE

Although increased visibility into events may allow you to detect more steps of an attack, this can be a double-edged sword. You need to see enough to stop an attack, but not so much that you are overwhelmed with detections triggered by normal behavior in your organization.

The role of a balanced XDR solution is not to alert defenders to every single procedure carried out during an attack, but rather to alert them that an attack is ongoing and to assist them in investigating it.

TRANSPARENCY

Some XDR vendors close the engine to customers so that IT admins have little to no visibility into what the solution is monitoring. Although not usable by every organization, an open rule set empowers the security analyst to view, audit, and analyze the events the XDR solution monitors.

CUSTOMIZATION

One of the challenges for detection is false positives. But if the XDR rule set is transparent, IT admins can customize the solution for their environment, thus decreasing the number of false positives.

Customization is at the heart of optimizing an XDR solution initially and afterward. Consider an XDR solution that allows you to set up custom exclusions, modify the automated responses with different actions, and write your own rules. This enables the most powerful use of an XDR solution, tuned according to what's "normal" for your environment.

Ultimately, it's the organization's defenders who are in the best position to know the configuration of the XDR engine that achieves the desired balance between risk and noise.

INTEGRATION

A solution that integrates with the vendor's security solutions and those from third parties is a crucial capability for XDR. Integration includes exporting and importing data into the XDR tool, for example, via an application programming interface (API). Check whether you can export detections for use in a security information and event management (SIEM) system and import hashes from threat data feeds.

Regarding native integrations, many vendors typically offer both endpoint security and cloud-based reputation and detection systems that, together, provide a comprehensive prevention, detection, and response capability.

XDR builds on the protection offered by endpoint security and other solutions – it's not an isolated technology. Therefore, keep in mind that the quality of endpoint telemetry generated by different vendors' solutions vary. Threats blocked by your endpoint security software could be a trigger to dive deeper into the possible causes with XDR and look for ways to improve defenses.

MULTIPLATFORM

On the client side, XDR should support endpoints running major operating systems, such as Windows, macOS, and Linux. With multiplatform coverage, defenders can more easily track lateral movement by attackers.

On the server side, purchasing and maintaining the necessary hardware and software to run the XDR server and database are potentially prohibitive costs associated with XDR. The hardware needs to handle the typical number of events generated by all the endpoints in your organization. Furthermore, if you desire increased visibility, this may increase the hardware cost because storing many events (especially frequently generated ones) can quickly become a resource hog.

If on-premises deployment is not an option for you, look for cloud-based XDR in which you hand off the server-side hardware responsibility to the vendor.

SERVICES

Investing in XDR should encompass more than the product: it should include services. Determine whether the vendor provides the following:

- Deployment and optimization services
- Managed detection and response services, including threat hunting
- Security health checks
- A partner or local office in your region
- Technical support in local languages

VENDOR

The lifetime value of your XDR investment strongly depends on the stability and reputation of the vendor. Consider the vendor's demonstrated security expertise and track record. This includes the vendor's entire product and services portfolio, proven competence in preventing threats, threat intelligence capability, and published malware research.

In addition, look at third-party assessments, such as AV-Comparatives' Endpoint Prevention & Response (EPR) Test. This test evaluates an XDR solution's response to multiple attack scenarios across three phases: initial foothold, propagation, and asset breach.

Another third-party resource is the MITRE Engenuity ATT&CK® Evaluations that pit XDR solutions against known adversarial techniques. These evaluations reveal the level of visibility into malicious techniques and the depth of context provided by each detection. It should be stressed that these evaluations do not have winners, nor do they test false positives or the impact on performance.

With an XDR solution, you can gain the following benefits: increased confidence to detect ransomware, wipers, and supply-chain attacks, discovering attackers abusing IT admin tools or leveraging corporate secrets, perhaps purloined off decommissioned devices.

Chapter 5: How can ESET help with XDR?

Using behavioral analytics across the endpoint, network, cloud, email, and other layers is a defining framework for ESET's approach and methodology.

It enables spotting suspicious activity and stopping attackers before they can make an impact. To make this possible, ESET leverages its industry-leading technology solutions such as XDR.

ESET Inspect, our **XDR-enabling solution**, provides risk managers and incident responders with outstanding visibility into threats. It allows them to perform fast and in-depth root cause analysis and immediately respond to incidents. Paired with the time-tested preventive power of ESET's endpoint protection products, ESET Inspect is a **cloud-delivered**, XDR-enabling solution that can:

- Detect advanced persistent threats
- Stop fileless attacks
- Block zero-day threats
- Protect against ransomware
- Prevent company policy violations

THE ESET DIFFERENCE

COMPLETE PREVENTION, DETECTION, AND RESPONSE

ESET Inspect enables quick analysis and remediation of any security issue in your network. ESET's underlying multilayered security, in which every single layer sends data to ESET Inspect, analyzes vast amounts of data in real time to detect threats.

SOLUTION FROM A SECURITY-FIRST VENDOR

ESET has been fighting cyberthreats for more than 35 years. As a science-based company, it has long been at the leading edge of developments like machine learning, cloud technology, and now XDR.

PREVENTION IS BETTER THAN CURE

ESET's approach to XDR is tightly connected to its multi-award-winning prevention products. Thanks to our commitment to developing high-quality detection technology, ESET prevention technology is world leading.

DETAILED NETWORK VISIBILITY

With transparent detection rules (ESET Inspect has 1250+ and counting), advanced indicators of compromise (IoC), and search capability, an in-depth review of your network will allow you to identify suspicious behavior.

READY TO START WORKING NOW

ESET's solution works out of the box and is powerful enough to allow granular modification by experienced threat hunters.

FLEXIBILITY OF DEPLOYMENT

We let you decide how to deploy your security solution: ESET Inspect can run on your own server or in the cloud, allowing you to tune your setup according to your TCO targets and hardware capacity.

MITRE ATT&CK®

ESET Inspect references its detections to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, which – with just one click – provides you with comprehensive information about even the most complex threats. ESET is a top independent cybersecurity software company and in the top 10 out of more than 350 contributors to ATT&CK.

REPUTATION SYSTEM

Extensive filtering enables security engineers to identify every known good application, using ESET's robust reputation system. The ESET system contains a database of hundreds of millions of benign files to ensure security teams spend their time on unknown – and potentially malicious – files, not on false positives.

AUTOMATION AND CUSTOMIZATION

Easily tune ESET Inspect to the level of detail and automation you need. Choose your level of desired interaction, and the type and amount of data to be stored, during the initial setup and with the help of preset user profiles, and then let Learning Mode map your organization's environment and suggest exclusions to false positives where needed.

BENEFITS OF ESET'S XDR SOLUTION

Organizations now require greater visibility into endpoints, devices, and networks to protect their profits and reputation from emerging threats, employee risks, and unwanted applications. **ESET Inspect** – part of ESET PROTECT – is a **cloud-based, XDR-enabling solution** that delivers unique behavior and reputation-based detection, providing real-time feedback to security teams using global threat intelligence from ESET LiveGrid®. Organizations can benefit from this solution thanks to:

EXPERTISE

Detection and response from a trusted, research-based, security-first vendor with over 35 years of experience on the cutting edge of digital security.

QUALITY

Tight integration with ESET's multilayered prevention products, built on award-winning technology with industry-wide recognition.

FLEXIBILITY

Works out of the box and is powerful enough for experienced threat hunters, offering granular controls for optimal tailoring to each user's environment.

TRANSPARENCY

Transparent detection rules ensure detailed visibility across multiple layers, including email, networks, and servers.

ESET's approach and methodology enable spotting suspicious activity and stopping attackers before they can make an impact. To make this possible, ESET leverages its industry-leading technology solutions such as XDR.

Deploying XDR: A real-life scenario

The Customer

The Raicam Group is an automotive company specializing in the design, development and production of brakes, clutches and actuators. Raicam places a heavy emphasis on the high quality and safety of the products and services in its portfolio. Many of the world's best known vehicle manufacturers have chosen to work with Raicam based on the quality of its products.

The Challenge

With several international offices, Raicam required a cybersecurity solution that could provide complete coverage on a global level—a system that was easy to manage but that guaranteed a high level of digital risk protection. Another factor that led Raicam to consider a new solution was the need for an endpoint protection product with **XDR technology**, one that was easy to integrate and light on resources. The goal: centralized control from a single console, where all security controls could be managed without added work for internal teams.

The Solution

Raicam entrusted **ESET** with the IT safety of its various production sites in Italy and abroad. It adopted the ESET PROTECT Platform, which incorporates various solutions under a single management console, including ESET Inspect, the **XDR-enabling solution**.

Under this comprehensive cybersecurity framework, Raicam's endpoints and servers are protected against ransomware attacks, zero-day threats, data breaches and more—ensuring business continuity and safeguarding business-critical data. All with extensive customer support, available 24/7. The adoption of such robust technology has also helped Raicam satisfy regulatory standards.

> "ESET's multilayered approach to security allows us to answer positively to the safety audits requested by our customers."

Antonella Bertola, IS Manager of Raicam

What is MDR?

It is a type of **managed security service** that combines tools, technologies, and cybersecurity experts to provide organizations with powerful detection and response capabilities.

MDR is effectively an outsourced version of extended detection and response (XDR), sometimes combined with other tools.

> “MDR service providers still offer more mature detection and response outcomes than XDR products and can help augment security teams struggling to find or retain talent.”
>
> Source: *Forrester: Planning Guide 2024: Security and Risk.* Merritt Maxim and Team, August 1 2023.

What is **ESET PROTECT MDR**?

It supports cyber risk management by providing visibility into your IT environment, managed from a single pane of glass console that can be installed on premises or in the cloud, depending on your requirements.

The ESET MDR service is a holistic solution that can be purchased as part of the ESET PROTECT MDR offering.

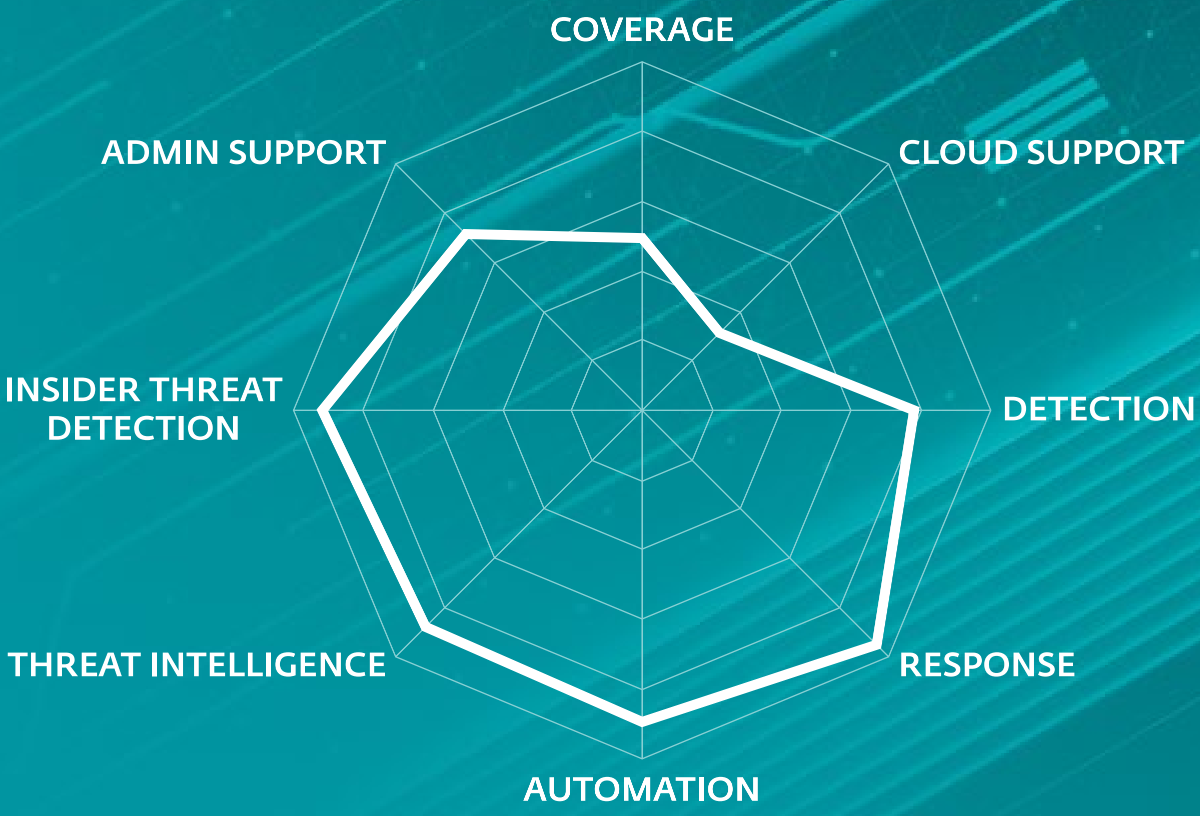
It is a more comprehensive option combining products and services covering prevention, detection, and response.

ESET AS A 2023 MDR LEADER

KuppingerCole offers a comprehensive comparison of MDR providers based on standardized criteria in the categories of Product, Innovation, and Market position.

The report highlights the Overall leaders among MDR providers, and **ESET** is proud to be recognized as both a **market leader** and an **overall leader** in the 2023 MDR Leadership Compass thanks to ESET PROTECT MDR.

ESET



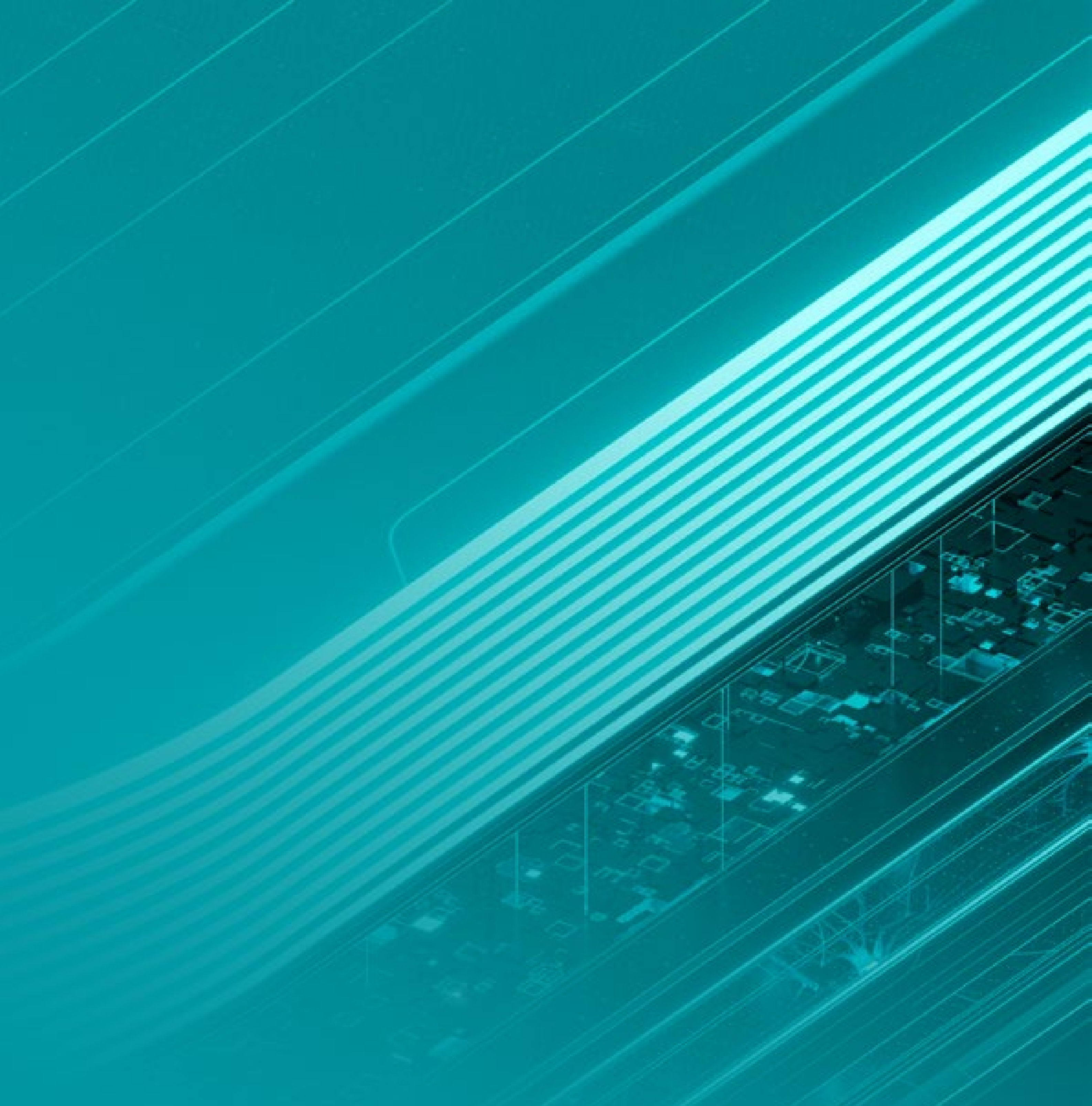
Source: *KuppingerCole Leadership Compass 2023: Managed Detection & Response (MDR)*, *July 2023, p. 39.*

Conclusion

XDR does not stand in isolation from the rest of an organization’s defenses. Rather, XDR plays its best role within a proactive security ecosystem that includes modern endpoint protection, cloud sandboxing, machine learning, threat intelligence, and dedicated security staff.

This multilayered approach to security is crucial because, while it’s important to have increased visibility into an attack happening on your network, it’s more important to be able to sift through a myriad of events to spot an attack. Then you can move more quickly to remediation steps, thwarting the attack from further progress.

Of course, the best case is to block an attack right away at the initial access attempt, or at least soon after – a capability you can build if you take the time to test your defenses thoroughly against adversarial techniques with XDR at your side.



We advocate that the only viable approach to effectively protect your organization's data is to have multiple layers of protection in place.

About ESET

When technology enables **progress**, ESET is here to **protect it**.

For more than 30 years, ESET® has been developing industry-leading IT security software and services to deliver comprehensive, multilayered protection against cybersecurity threats for businesses and consumers worldwide.

ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

Canon

protected by ESET since 2016
more than 32,000 endpoints

ISP security partner since 2008
2 milion customer base

Allianz
Suisse

protected by ESET since 2016
more than 4,000 mailboxes

MITSUBISHI
MOTORS
Drive your Ambition

protected by ESET since 2017
more than 9,000 endpoints

30+
years of expertise

1bn+
internet users protected

400k+
business customers

195
countries & territories

13
global R&D centers

Find out what makes ESET's **XDR solution** a perfect fit for your needs.

LEARN MORE

30+ years of continuous innovation

Leading European Union vendor

Always focused on technology

Growing YoY since its inception