Mastering Cybersecurity with MDR:

The Ultimate Guide to Managed Detection & Response

Book a demo

ESET Cybersecurity
Progress. Protected.

Introduction: A Multilayered Preventive Approach

The world is changing faster than many network defenders can handle. They face an agile and determined adversary, armed to the teeth with the latest technology. As the corporate attack surface expands with each new digital investment, the chances and costs of a serious security breach increase. The average cost of a data breach globally now stands at nearly $4.9m.

In order to **manage these escalating risks**, organizations should consider taking a **proactive**, **prevention-first approach** designed to minimize the attack surface, reduce cost and complexity, and enhance cyber-hygiene.

More than half of breached organizations are facing high levels of security staffing shortages. This issue represents a

26.2%

between 2023 and 2024.

Source: *IBM: Cost of a Data Breach Report 2024*.

Threat actors need only to succeed once to cause significant damage. This is why the most mature approach to corporate cybersecurity combines multi-layered prevention with detection and response. However, the challenge many organizations face is that:

SKILLS GAPS AND KNOWLEDGE SHORTAGES impact their ability to run 24/7/365 security operations (SecOps).

THE COMPLEXITY of detection and response tools means some businesses might not have anyone in house to operate them.

CYBER-THREATS ARE BECOMING MORE SOPHISTICATED and impactful, enabling threat actors to achieve their goals more rapidly.

BUDGETS ARE LIMITED, especially for large on-off purchases of detection and response infrastructure and human operators.

COMPLIANCE PRESSURES are building, amplifying the negative impact of attacks in case of non-compliance.

That's why many organizations are turning to **managed detection and response** (**MDR**). By doing so, they can gain access to the combined power of an expert third-party SecOps team using sophisticated AI tooling for rapid response and threat containment. The best MDR services will automate tracking and reporting for improved compliance and continuous enhancements to cyber-resilience. This will free up in-house teams to focus on higher value strategic tasks for the business.

$4.88 million

was the global average cost of a data breach in 2024, which is the biggest jump since the pandemic.
Source: *Cost of a Data Breach Report 2024*.

Chapter 1: Why Your Business Needs MDR

Today's organizations continue to build out cloud infrastructure and applications, support remote working, and expand their digital and traditional supply chains. That provides more opportunities for highly motivated threat actors, who are increasingly leveraging AI and automated tooling, "as-a-service" offerings and more to upskill, professionalize, and amplify attacks. In this context, **MDR is becoming a necessity for businesses of all sizes**.

FROM PREVENTION TO MDR

In-house security teams are struggling to manage the volume, variety, speed, and—in some cases—sophistication of threats facing their organization. Ransomware is among the most serious. Ransomware-as-a-service (RaaS) is a highly competitive underground "industry" where gangs innovate continuously to bypass security controls and grow their profits. According to British government security experts, the threat is expected to surge as more adversaries get hold of AI tools.

The frequency of ransomware attacks on governments, businesses, consumers, and devices is expected to rise to

every 2 seconds by 2031

Source: *Cybercrime Magazine: Top 10 Cybersecurity Predictions and Statistics For 2024*.

"AI services lower barriers to entry, increasing the number of cyber criminals, and will boost their capability by improving the scale, speed, and effectiveness of existing attack methods."

James Babbage, Director General for Threats at the National Crime Agency.

Threat actors are using such tools to shorten the time it takes from initial access to data theft or ransomware deployment. This is a challenge not just in the context of ransomware but the full range of threats facing organizations—from crypto mining malware and botnets to banking trojans and spyware.

The cumulative impact of these trends should focus IT security leaders on an inescapable truth. Bad actors' motivation to succeed is often greater than companies' preparedness via preventive measures. They go to great lengths to get into the corporate environment unseen. That's why organizations should **balance prevention with detection and response**. This is what ESET's prevention-first approach focuses on, **by blending multiple layers of security technology**. It aims to protect by blocking malicious code or actors from entering or damaging a user's system.

Phishing was the most costly and frequent attack vector in 2024, with a cost of

€4.88 million

and a

15% share

of all attacks.

Source: *IBM: Cost of a Data Breach Report 2024*.

However, if these measures are bypassed by sophisticated actors, there is fast and reliable detection and response to mitigate advanced threats that manage to compromize a system. Think of it as locking and bolting all your doors and windows, but then installing motion detection alarms to catch suspicious activity if anyone does make it inside the house.

XDR is a key asset here. It enables security operations (SecOps) teams to gain **unparalleled visibility** into their IT environment from a single pane of glass, and spot anomalies indicating threats via high-fidelity alerts. XDR is an evolution of EDR, which optimizes threat detection, investigation, response and hunting in real time.

XDR unifies security-relevant endpoint detections with telemetry from security and business tools such as network analysis and visibility (NAV), email security, identity and access management, cloud security, and more. It is a cloud-native platform built on big data infrastructure to provide security teams with flexibility, scalability, and opportunities for automation.

XDR ENABLES YOU TO ANSWER SEVERAL KEY QUESTIONS ABOUT A CYBERATTACK:

How did it start?
Where did it start?
When did it start?
Which endpoints are infected?
Is it contained?
How do we prevent it in the future?

Most importantly, it can help you take rapid remedial action to resolve incidents before they severely impact the organization.

However, even with the help of XDR, SecOps teams face **major challenges** from an organizational perspective—especially skills gaps, tool complexity, budget and resource constraints, and integration of tooling; not to mention a rapidly evolving threat landscape. **That's why many are turning to MDR**; the most effective way to detect and contain ever-changing, sophisticated threats.

HOW MDR ADDRESSES CONTEMPORARY THREATS

Although MDR varies from provider to provider, it should include at least some variation of the following:

- **24/7 Threat Monitoring and Detection**:
  Continuous monitoring of an organization's network, endpoints, and cloud environments.

- **Proactive Threat Hunting**:
  Unlike traditional security measures that react to alerts, MDR involves proactive threat hunting which helps in identifying APTs and zero-day vulnerabilities.

51%

is the number

of organizations that have formally established threat hunting methodologies in 2024, compared to 35% in 2023.
Source: *SANS: The Evolution of Enterprise Threat Hunting: Detailed Insights from the SANS 2024 Survey*.

- **Expert Analysis and Response**:
  The expertise of security professionals allows for nuanced analysis and rapid decision-making, which is crucial for addressing complex security incidents.

- **Global threat intelligence**:
  Accurate, current and relevant telemetry collected from across the globe provides actionable intelligence for rapid incident response and optimized threat hunting.

Organizations using telemetry can achieve up to a

60% improvement

in their ability to manage vulnerabilities and threats compared to those relying solely on traditional security measures..
Source: *Forrester: The Four Steps for More Proactive Security, 2024*.

- **Continuous Improvement**:
  By analyzing past incidents, using advanced threat intelligence, focusing on real threats, and providing regular security health checks and reports, MDR services help prevent the recurrence of similar attacks by enabling teams to improve cyber-resilience.

KEY FUNCTIONS OF MDR

MDR can bring tremendous benefits for organizations that want to mitigate cyber risk, but don't have the in-house resources effectively helping them to close skills gaps, save costs and enhance detection and response. A high-performance solution should enable organizations to:

Monitor

Experienced threat hunters keep track of the entire customer IT environment, and actively monitor malware and APT groups to provide the highest level of situational awareness.

Detect

Threat actors have countless ways to sneak through perimeter defenses, but by leveraging behavioral analytics, they can be spotted for rapid remediation.

Triage

An initial assessment and categorization of alerts filters out false positives and gathers necessary information.

Prioritize

Intelligent analytics rank these alerts by severity to ensure the most critical threats are addressed first. This is a critical phase of the MDR workflow, given how many IT teams struggle with alert overload.

Investigate

Automated tools and human expertise combine to dig deeper into alerts, performing data and log analysis in order to understand their nature and scope. They will need to calculate whether an alert is a true positive or not, and what steps must be taken to resolve it.

Respond

An effective MDR service will either provide basic response actions to block and contain the threat, or containment and full remediation of any compromized systems. The latter could entail a password reset, patching specific endpoints, or even reimaging computers.

The benefits of outsourcing detection and response are simple but compelling:

- The MDR provider takes care of all management of the back-end technology, freeing up staff to focus on high-value, strategic tasks rather than drowning in security alerts.
- The MDR provider may also optimize the backend technology to align with each customer's risk profile and infrastructure.
- With detection and response managed by a third party, there will be no need to pay hefty salaries to attract and retain the best cybersecurity talent.
- Customers can benefit from their provider's economies of scale, ability to attract the best talent, and insight into other customer organizations and threat environments.

ESSENTIAL FEATURES TO LOOK FOR IN AN MDR SOLUTION

With so many MDR solutions flooding the market, it can be challenging knowing **where to start**. Consider a provider capable of offering at least the following:

Speedy onboarding and fine-tuning

Detection rules, exclusions, and parameters will need to be customized for each IT environment and the threats facing the organization. Faster onboarding is desirable, but not to the detriment of detection performance which should be optimized from day one.

➜ Remember MDR protection will usually improve with time.

Speed

Reduce your incident detection and response time from months to minutes with your MDR provider. You need to stop the attack in the initial phases (discovery, lateral movement, persistence) before the payload is executed.

24/7 service

Threat actors operate from all time zones and often strike in the early hours or at weekends/during public holidays. That means MDR must work round-the-clock. Indicators of compromize and attack must be investigated immediately, in real time.

Easy to use solution with a simple interface and low learning curve

This makes the solution accessible for even those new to IT security. Easy-to-use dashboard gives a clear view of security status and important alerts.

Customizable notifications and advanced reporting options

In order to automatically or on-demand receive reports about incidents, the status of environment, and other updates.

This makes it easy to present cybersecurity status to executives, receive timely alerts, and generate actionable reports for audits and compliance.

Seamless compatibility with diverse infrastructures

Effective integration with tools such as SIEM, SOAR, ticketing tools, and many others. Whether you have multi-OS environments, existing security software, or both on-prem and cloud setups, you want to integrate without any issues.

A comprehensive tech stack

A key part of an MDR solution is the underlying technology. It should include endpoint or extended detection and response (XDR), security information and event management (SIEM), and security orchestration and response (SOAR). These should be either provided by the MDR vendor or third-party tools linked via APIs.

Automation and AI

AI can play a great role in identifying anomalous behavior and analyzing large volumes of data to find signs of compromize or attack.

Automation can also rapidly execute a set of actions to isolate systems and contain threats. But these should always be viewed as assistive rather than replacing the expertise of human analysts.

Human intelligence

As important as AI and automation are, they have limitations that only human experts can address effectively. Experienced cybersecurity professionals can add contextual understanding of behavioral anomalies flagged by the

➜ AI to determine if an alert is truly malicious. This helps to reduce false positives. Humans are also more capable of adapting to new and emerging threats in real time.

Threat intelligence
Regularly updated threat intelligence feeds, generated by the MDR provider or third parties, are a key component of any effective MDR service. Updates should be gathered from telemetry and curated by expert threat intelligence teams to reveal attack methods and effective countermeasures.

Threat hunting
Ongoing, systematic threat hunting should come as standard in any MDR service, in order to root out the more evasive attacks.

Remediation
There's no established rule about whether the service provider or customer should handle remediation/mitigation once a threat has been discovered. IT buyers should look for the offering which best aligns with their requirements and in-house capabilities.

Alignment
Ensure the MDR service operationally aligns with the rest of the IT environment, such as whether outputs integrate with ticket management systems and internal workflows.

A provider should be able to generate incident reports and status updates for full transparency.

Compliance
The MDR service must be able to adhere to any data privacy, residency, or retention requirements that the customer might have, and any stipulations demanded by insurance policies.

The MDR market is expected to grow at a compound annual growth rate (CAGR) of about

24%

from 2024 to 2029.
Source: *MarketsAndMarkets: Managed Detection and Reponse (MDR) Market, 2024*.

Chapter 2: Implementing MDR with ESET

ESET offers one of the fastest and most effective MDR services on the market. The key to its power is a winning combination of human and machine. That means world-class security research and threat intelligence—built on more than 30 years of expertise and 11 R&D centers—plus leading AI capabilities to identify anomalous behavior that human eyes might miss.

Also, ESET MDR service delivery teams are spread across the globe what helps customers bridge potential language barriers better and makes the whole experience smoother.

For business customers: ESET offers MDR in two tiers. ESET MDR is a powerful but affordable service designed to meet the needs of SMBs starting from 25 seats. ESET MDR Ultimate is a highly customized service tailored to the specific requirements and security profile of enterprise customers.

It works like a seamless extension of the client's IT function—whatever the vertical—featuring full Digital Forensic Incident Response (DFIR). The result is enterprise-grade MDR designed to see more and act faster, in order to proactively stop and contain threats before they can cause any damage.

For MSPs: ESET understands that your business can also suffer resource constraints, especially when working to support potentially hundreds of customers across a growing attack surface. Your organization is an increasingly attractive target, for example as a means for threat actors to remotely access client environments.

With ESET MDR, you can diversify your portfolio with rapid detection and response (in potentially as little as 20 minutes) and optimize internal resources to continue offering the best service possible for clients.

MDR AS PART OF HOLISTIC SECURITY

ESET MDR or ESET MDR Ultimate services can be purchased as part of specific ESET PROTECT subscription tiers to support multilayered holistic security. These are more comprehensive options combining products and services covering prevention, detection, and response. Managed via a single pane of glass, these include:

ESET PROTECT MDR

Ideal for small and mid-sized businesses

- Management Console
- Modern Endpoint Protection
- Server Security
- Advanced Threat Defense
- Full Disk Encryption
- Vulnerability & Patch Management
- Extended Detection & Response
- Multi-factor Authentication
- **MDR Service**
- **Premium Support Service**

ESET PROTECT MDR Ultimate

Ideal for enterprise-grade organizations

- Management Console
- Modern Endpoint Protection
- Server Security
- Advanced Threat Defense
- Full Disk Encryption
- Vulnerability & Patch Management
- Extended Detection & Response
- Multi-factor Authentication
- **MDR Ultimate Service**
- **Premium Support Ultimate Service**

Conclusion

Cybersecurity is an essential part of organizations' IT operations. Yet in most cases, it isn't their primary focus, nor should it be. They need to be able to concentrate on their core business, and leave the battle against a diverse, determined, and growing cohort of threat actors to the experts. This is where trusted security partners come in, bringing extensive resources and decades of industry expertise.

MDR can offer a comprehensive solution by integrating prevention, protection, detection, and response. Tailored services are available to meet the diverse needs of various organizations, whether they are SMBs, MSPs, or large enterprises. It's time to snuff out cyber risk with expert assistance.

Schedule free consultation

WHAT DOES A SUCCESSFUL DEPLOYMENT OF MDR LOOK LIKE?

Electrical Consultants, Inc.

ECI is a premier design and engineering consulting firm specializing in power utility and infrastructure projects. With over 37 regional offices across the United States and Canada, ECI supports the engineering and construction of high-voltage, utility-scale facilities, ensuring each project is approached with innovation, precision, and a dedication to excellence.

ECI faced a significant staffing challenge, with only a small team dedicated to managing cybersecurity, making after-hours monitoring and quick response to threats particularly difficult. The organization needed a reliable and cost-effective way to monitor and respond to threats around the clock to protect its assets and operations.

For ECI, the implementation of ESET MDR was straightforward, requiring minimal adjustments The ESET security team conducted a thorough initial assessment and fine-tuned alert settings to optimize threat detection. Throughout the setup process, an ESET engineer provided hands-on support, ensuring a smooth and efficient transition.

"ESET MDR has detected many threats and incidents that we would have either missed or not responded to in as timely a manner. In at least one instance, the MDR detection and response kept a small incident from becoming a much larger problem for our company."

This is ESET

Proactive defense. Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach**, **powered by AI and human expertise**.

Experience best-in-class protection, thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network, led by **industry-acclaimed researchers**. ESET protects your business so it can unlock the full potential of technology.

Book a demo

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

ESET
Cybersecurity
Progress. Protected.