



Leveraging MDR in Manufacturing:

A Strategic Cybersecurity Guide to Managed Detection & Response



Digital Security
Progress. Protected.

Introduction: A Multilayered Preventive Approach

The manufacturing sector is facing unprecedented cyber threats, with attackers leveraging advanced techniques to exploit digital transformation efforts. According to the [2025 Verizon Data Breach Investigations Report \(DBIR\)](#), ransomware was involved in 35% of all manufacturing-related breaches in 2024. These incidents increasingly target critical infrastructure, industrial control systems, and supply chains, dramatically increasing the risk and potential impact of a successful breach.

The cost of such incidents is staggering. SOC Radar reports that the average cost of a data breach in the manufacturing sector is steadily rising due to increased digital complexity and attacker sophistication ([SOCRadar Threat Landscape Report](#)).

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

Ransomware was involved in

35%

of all manufacturing-related breaches in 2024.

Source: [2025 Verizon Data Breach Investigations Report \(DBIR\)](#).

Security staffing remains a core challenge. According to Verizon, skills gaps and shortages in the manufacturing sector significantly limit organizations' ability to operate round-the-clock security operations, making them vulnerable to persistent threats ([Verizon DBIR 2025](#)).

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, many manufacturers struggle with:

SKILLS GAPS AND KNOWLEDGE SHORTAGES:

Difficulty in staffing 24/7 security operations centers (SOCs).

THE COMPLEXITY:

Limited expertise in operating advanced detection and response platforms.

SOPHISTICATED CYBER-THREATS:

Increasing attacker use of AI and automation to accelerate and scale breaches.

BUDGETS CONSTRAINTS:

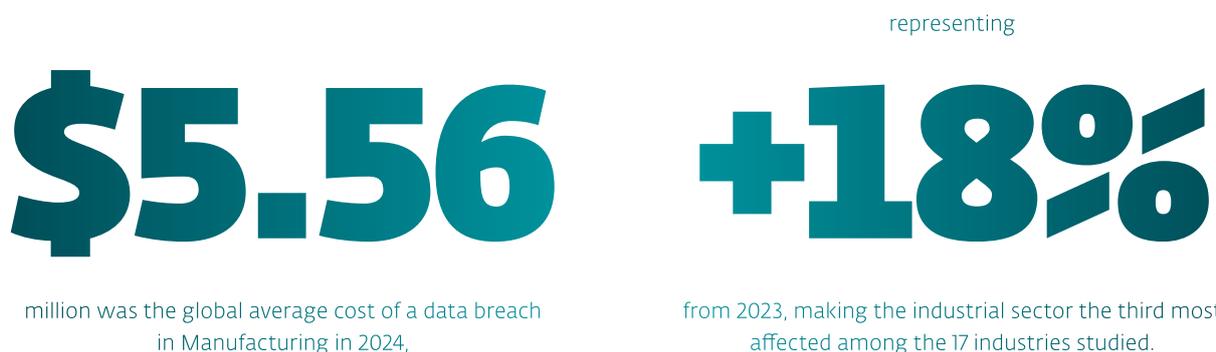
High upfront costs for security infrastructure and qualified personnel.

COMPLIANCE PRESSURES:

Regulatory requirements add urgency to cybersecurity readiness.

This is why many manufacturers 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, freeing internal teams to focus on core manufacturing operations.



Source: [OnWire: Cost of a data breach: The industrial sector, 2024.](#)

Why Your Manufacturing Business Needs MDR

Modern manufacturing operations are built on a foundation of cloud-based tools, IoT-enabled machinery, and complex supply chains—all of which expand the attack surface. The [2025 DBIR](#) confirms that 73% of breaches in manufacturing involved external actors, with system intrusion being the most common vector.

Notably, 15% of breaches involved third-party suppliers, reflecting a 68% year-over-year increase in supply chain risk. Threat actors are also becoming more organized and professionalized. As noted in the [SOCRadar Threat Landscape Report](#), attackers are leveraging Ransomware-as-a-Service (RaaS), AI tools, and stolen credentials to breach manufacturing networks faster and more efficiently.

To counter these risks, manufacturers need MDR - an agile, scalable cybersecurity approach. MDR's integration of telemetry, analytics, and human expertise has been shown to improve vulnerability and threat management effectiveness by up to 60% over traditional security methods ([SOCRadar Report](#)).

FROM PREVENTION TO MDR

In-house security teams often struggle to keep pace with the volume, variety, and sophistication of cyber threats. Ransomware remains a significant concern, with 33% of breaches involving ransomware or extortion techniques. A notable trend is the exploitation of zero-day vulnerabilities, which has seen a [180% increase](#) compared to the previous year. Additionally, the use of stolen credentials remains a prevalent method for attackers, appearing in almost one-third of all breaches.

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 manufacturing 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.

However, if these measures are bypassed by sophisticated actors, there is fast and reliable detection and response to mitigate advanced threats that manage to compromise 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 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?

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.

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 manufacturing companies 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 compromised 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 compromise 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 compromise 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 Response \(MDR\) Market, 2024](#).

5 Reasons Manufacturers Choose ESET MDR

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 AI capabilities to identify anomalous behavior.

- 1. Comprehensive protection for even the most regulated, air-gapped environments:** Services can be delivered through cloud, but also through on-prem boxes in air-gapped environments, allowing to serve the manufacturing industry that has stringent regulatory standards.
- 2. Real-time detection and resolution within 20 minutes, 24/7/365:** With ESET MDR, proactive threat hunting is powered by global intelligence from over 100 million endpoints. Expert-led investigations detect and contain threats in as little as 5-10 minutes, 20 minutes on average, depending on their severity. MDR provides rapid resolution at the chosen level: immediate threat containment followed by a customer notification with recommended next steps (if necessary), or with MDR Ultimate, threat containment and complete remediation by ESET experts.
- 3. Minimum noise, maximum protection:** AI and human expertise are combined to achieve 99.6% protection rates and minimum false alarms (AV Comparatives, Business Security Test 2024, August – November). ESET uses AI to reduce noise and automate processes, while cybersecurity experts (all in-house, none outsourced) maintain communications and quality control.
- 4. Consolidated dashboards and executive-friendly reports:** Customers get the visibility they need: On-the-ground IT staff access a customizable dashboard that provides single-pane-of-glass visibility with powerful drill-down capabilities; executives get easy-to-read weekly and monthly incident reporting.
- 5. Attractive bundling with flexible pricing:** MDR helps manufacturers save money while complying with industry regulations and cybersecurity insurance standards – through a complete package of protection that includes: next-generation endpoint security, multi-factor authentication (MFA), encryption, and vulnerability and patch management – plus mobile threat defense for each seat you buy at no additional cost.

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 manufacturers' 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.

ESET MDR, designed for compatibility with diverse manufacturing infrastructure, helps protect your supply chains and operational technology. It ensures seamless integration with your existing ICS and OT security systems, providing a unified security posture for manufacturing environments, reduces the risk of unauthorized access, secures your cloud infrastructure, and facilitates compliance with security governance and regulatory policies.

Tailored services are available to meet the diverse needs of manufacturing businesses of all sizes. It's time to snuff out cyber risk with expert assistance.

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.



**Multilayered,
prevention-first**



**Cutting-edge AI
meets human
expertise**



**World-renowned
threat intelligence**



**Hyperlocal,
personalized
support**



Digital Security
Progress. Protected.

© 1992–2025 ESET, spol. s r.o. – All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET, spol. s r.o. or ESET North America. All other names and brands are registered trademarks of their respective companies.