Top Cyberthreats in Manufacturing

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.

Ransomware was involved in

35%

of all manufacturing-related breaches in 2024.

Source: *2025 Verizon Data Breach Investigations Report (DBIR)*.

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.

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.

$5.56

million was the global average cost of a data breach in Manufacturing in 2024,

representing

+18%

from 2023, making the industrial sector the third most affected among the 17 industries studied.

Source: *OnWire: Cost of a data breach: The industrial sector, 2024*.

Strengthen Your Cybersecurity with ESET MDR

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.

LEARN MORE

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

Digital Security
Progress. Protected.