ARMIS | Industry Spotlight Series

Manufacturing

Top Trends

- **Manufacturing environments are converged -** ransomware attacks have shifted from only IT environments in 2021 to both IT and OT environments in 2023..
- Industrial manufacturers that **increased their technology investments** during the pandemic were better able to weather the downturn and emerge in better shape than those that pulled back tech spending.
- **Between 2023 and 2028, the fastest-growing industrial manufacturing segments by revenue will be solar power equipment (compound annual growth rate of 25.5%), 3D printers (24.1%), drones (24.1%), and hybrid and electric vehicles (22%)**

85%

According to NIST, 85 percent of ICS devices currently deployed in the field are between 10-15 years old. Many, such as Programmable Logic Controllers (PLCS), process sensors, gateways, and workstations are no longer patchable and can't be upgraded due to technical or operational constraints. NIST, 2024

↑↑↑ 37%

37% increase in ransomware attacks between April 2022 and April 2023.

Armis Labs

Why is the Manufacturing Industry Suffering?

Complex, sprawling environments with assets distributed and in motion. As a result, they are more easily susceptible to cyber exposure and attack.

Supply Chain Attacks Many manufacturing organizations are part of complex supply chains, so a cyberattack on one company can have a ripple effect—impacting other manufacturers, distributors, retailers, and even consumers downstream.

Insider Threats Historically, insiders have been a significant challenge for manufacturing organizations. Malicious or unintentional actions by employees, contractors, or trusted partners can pose considerable risks, data breaches or disruptions in manufacturing processes.

Inadequate Authentication and Access Controls Internal and third-party users often need remote access to industrial assets for maintenance and other purposes; however, this requires administrators to maintain costly, complex infrastructure.

Legacy OT systems in manufacturing are outdated and lack modern security, making them easy targets.

Interested to learn how Armis delivers a holistic, proactive cybersecurity solution to the manufacturing industry?

Read the solution brief

80%

80% of industrial organizations have cyber insurance policies, half of which are $500K or more. IBM, Threat Report 2024

USD 2.22M

The average cost savings in million for manufacturing organizations that used security AI and automation extensively in prevention versus those that didn't. IBM, Threat Report 2024

108 - day shorter

OT Organizations that used these [AI and automation security] capabilities extensively within their approach experienced, on average, a 108-day shorter time to identify and contain the breach.

IBM / Cost of a Data Breach Report, 2023

936 alerts

Manufacturing tops the Armis Centrix™ for Actionable Threat Intelligence early warning list with 936 alerts in 2024.

Armis Labs 2024

ARMIS | Industry Spotlight Series

Manufacturing

Interconnection of IT/OT relies on orchestration of complex systems that may contain cyber vulnerabilities, which you cannot take down to patch at a moment's notice.

USD **4.88M**

The global average cost of a data breach in 2024—a 10% increase over last year and the highest total ever. IBM, Threat Report 2024

Plant Engineer

You are responsible for the technology infrastructure and operational processes of assets on the ground that keep operations flowing.

Challenges:

Lack of visibility into complex sprawling networks makes maintenance difficult

Maintaining secure operations as attack surface grows

Digital transformation and innovation yet being aware that these changes increase security risks

Proactively working on risk resolution when you don't have the ability to prioritize vulnerabilities

Security Analyst

Every event logged within the organization is monitored by you. In Transportation and Logistics where uptime is essential, making sure your proactive defences and response to vulnerabilities are in good order is critical to operations.

Challenges:

Legacy hardware and software causing inefficiencies

Lack of asset situational awareness makes priortizing vulnerabilities impossible

Cybersecurity threats are faster than defenses

Choosing the right technology, and constant software updates after threats are dealt with

Early detection of vulnerabilities

Security Risk and Compliance Officer

You're strategic and focused on ensuring your organization has the right technology strategy and resources to deliver against mission critical goals and objectives.

Challenges:

The pressure of personal culpability if your organization fails audits

Transport has a heavy public touch point- if you get it wrong peoples lives are at risk

Staying up-to-date with local and global security challenges, new technologies and compliance issues

Delivering strategy and response reports to non-technical board and business leaders

18,382

Manufacturing trumps all OT industries with the highest number of Critical CVEs, totaling 18,382. Armis Labs, 2024

> "Ensuring robust cybersecurity in the manufacturing industry is not just a necessity; it's an imperative. As we increasingly rely on interconnected operational technologies (OT) to optimize supply chain management, maximize uptime, and streamline operations on the factory floor, the potential risks grow exponentially. Safeguarding these critical infrastructures against cyber threats is essential, not only to protect our assets but also to maintain the seamless production and distribution processes that our industry hinges upon. A breach could disrupt supply chains, halt production lines, and compromise sensitive data, jeopardizing the trust and reliability that our industry is built on.
>
> — Carlos Buenano, Chief Technology Officer, Armis

See, protect, and manage your attack surface with Armis for OT/IoT

Visit **Armis.com** to find out more