SOLUTION BRIEF

Auto Manufacturing

Traditional cybersecurity is ineffective in industrial environments. This is particularly pertinent in Auto Manufacturing with a complex web of IT, OT, and IoT assets needing interconnectivity to remain functional. Armis Centrix™ delivers the ability to manage the lifecycle of these assets and their users across sprawling environments.

Top Trends

- The global automotive cyber security market size was valued at **USD 3,090.6 million** in 2022 and is estimated to expand at a compound annual growth rate (CAGR) of **20.93%** from 2023 to 2030.[1]
- One minute of automotive production downtime costs an average of **$55,000**.[2]
- The automotive industry has experienced a **225%** increase in cyberattacks over the last three years. The most common attack types include ransomware, data, and control system breaches.[3]
- The annual count of Common Vulnerabilities and Exposures (CVEs) affecting automotive companies worldwide saw a noticeable upward trend from 2019 to 2022, with the number of CVEs reaching 151, a **457%** increase in just two years.[4]
- **64%** of automotive industry leaders believe their supply chain is vulnerable to cyberattacks, with many businesses inadequately prepared for a connected automotive era.[5]
- Vulnerability exploitation is the top vector for attacks on automotive manufacturers according to IBM's X-Force Threat Intelligence Index 2022 report.
- Connected automobiles gather data from more than 150 sensing devices placed all over the car.[6]
- The average car today contains up to 150 electronic control units and about **100** million lines of software code. That number is projected to reach 300 million lines of code by 2030.[7]

1 grandviewresearch.com/industry-analysis/automotive-cyber-security-market
2 pingdom.com/outages/average-cost-of-downtime-per-industry/
3 Edge Research
4 Statista
5 csoonline.com/article/652299/automotive-supply-chain-vulnerable-to-attack-as-cybersecurity-regulation-looms.html
6 grandviewresearch.com/industry-analysis/automotive-cyber-security-market
7 securityintelligence.com/posts/automotive-cybersecurity-new-regulations/

Recent Attacks

20

Japanese manufacturer Honda suffered a ransomware attack in 2020 that led to a temporary suspension of global operations, including production, sales, and development.

22

In late February 2022, Toyota had to halt production at several Japanese plants due to a severe cyberattack on one of its suppliers, underscoring the automotive industry's vulnerability to such incidents. The attack disrupted operations at 28 production lines across 14 plants, affecting the production of approximately 10,000 vehicles, equivalent to around 5% of the company's monthly output in Japan.

22

Denso, one of the world's largest technology and component manufacturers, faced a cyberattack in March 2022 when hackers infiltrated the company's network in Germany, prompting the network's disconnection from compromised devices once the breach was detected.

23

November 2023 production of Chrysler, Dodge, Jeep, and Ram models were affected after a cyberattack on an automotive supplier disrupted its operations.

The cyberattack affected Chinese supplier Yanfeng International Automotive Technology Co. Ltd., a manufacturer of a number of just-in-time parts, including seats, interiors, electronics and other components.

Common OT Manufacturing Protocols

Modbus	Profibus	Ethernet/IP	DeviceNet
CAN (Controller Area Network)	Profinet	EtherCAT (Ethernet for Control Automation Technology)	CANopen

Key Challenges

1

Growing Attack Surface

Automotive manufacturing relies heavily on automation, robotics, and interconnected systems. These automated processes create a larger attack surface, and securing them is vital to prevent potential disruptions and compromises.

2

Convergence of IT and OT Systems

The gap between traditional IT systems and OT systems in manufacturing processes is diminishing, reducing or eliminating airgapping as a method of protection. Different processes, protocols, and technologies have been integrated into larger systems where a single security vulnerability can still generate an attack. Once the attack is successful, it can move laterally anywhere in the network.

3

Connected Supply Chains

Automotive manufacturers have complex and interconnected supply chains that often employ just-in-time technology. Securing the entire supply chain and third party interconnections requires real-time control and precision. Implementing security measures without causing delays or disruptions in the production process is crucial for maintaining efficiency.

4

Legacy Systems and Equipment

It is not uncommon for automotive manufacturing facilities to operate with legacy ICS and OT systems that are decades old and not initially designed with robust cybersecurity features. Updating and securing these older systems poses a significant challenge.

5

Tight Tolerance Production Requirements

Vehicles are safety-critical systems, and any compromise to their manufacturing processes could result in safety risks for consumers. Regulations require exact tolerance thresholds in car manufacturing, as even a small deviation from specs can lead to catastrophic failure, injury, or death.

6

Regulatory Compliance

The automotive industry is subject to various regulations and standards related to safety, quality, and environmental concerns. Ensuring compliance with these regulations while also adhering to robust cybersecurity frameworks can be challenging.

7

Remote Access and Maintenance

Remote monitoring and maintenance of ICS and OT systems are common practices in automotive manufacturing. Securing remote access points is crucial to preventing unauthorized access and potential cyber threats.

8

Security of Testing and Development Environments

Securing the environments where vehicle testing and development take place is crucial. These environments may contain sensitive information about upcoming vehicle models and technologies, in addition to data that drives key design decisions for each vehicle.

Common Auto Manufacturing Use Cases

Asset Inventory

Failing to see and contextualize all connected asset information when building a map of the attack surface.

Interconnections and Access

Data sharing of OT to IT and collaboration between component vendors has greatly data-driven insights and cooperation. It has also increased the risk of threat actors.

Cyber Hygiene

Not staying up to date with new cyber threats. Ie: attacks, interconnections, cybersecurity frameworks - leaves major holes in the organization's defense strategies, which are constantly targeted by adversaries.

Vulnerability Management

No single view into all vulnerabilities, no ability to prioritize, and poor/ non optimized patch management.

Securing The Automotive Manufacturing Process

The automotive manufacturing industry relies heavily on operational technology (OT) to achieve efficiency and minimize downtime, all while adhering to rigorous engineering and safety standards. Striking this delicate balance becomes even more challenging when introducing the ever-present threat of cyberattacks.

Automakers across the world depend on a secure supply chain and manufacturing processes to produce thousands of cars daily. Today's automobiles are manufactured with more technology than ever before, meeting exacting standards. Even the slightest deviation in the manufacturing process can lead to catastrophic failures and extensive and expensive recalls once the cars hit the road.

The potential for production slowdowns or shutdowns due to unauthorized intrusions or security incidents poses a significant financial risk. In the auto industry, downtime costs rise to about $55,000 per minute, which translates to about $3 million per hour. Nearly 70% of the time, downtime issues can be attributed to people being unaware of their equipment's maintenance or update requirements[8]. In light of these realities, ensuring security throughout the industrial operations process including but not limited to supply chain, automotive manufacturing, and subsequent consumer use is of paramount importance.

8 pingdom.com/outages/average-cost-of-downtime-per-industry/

How Armis Can Help

Deep Contextual Awareness

Automotive OT environments can contain a mix of IT, OT and IoT assets. Keeping up-to-date on exactly what is in the environment can be challenging. The legacy method of manually running an asset inventory is inefficient and error prone. Moreover, the dynamic nature of the environment means that the inventory may already be out of date the moment it's completed. The result is an inaccurate and siloed snapshot in time that cannot possibly provide a real-time status. This leads to significant security issues.

Read More About OT/IoT Security

Armis Centrix™ provides an automated real-time asset inventory of exactly what is in your network. Armis leverages its own proprietary asset intelligence engine that contains profiles of over 3.5 billion assets.

It provides known profiles for each asset and can append data where appropriate to provide unparalleled intelligence on each and every asset and its expected behaviors, as well as an organization-wide view of everything from the make and model of all assets, to more granular information including OS, patch level, access information, and full detail all the way down to the backplane.

It identifies dependencies and applications on devices that affect the business criticality of assets and classifies assets owned vs maintained by 3rd party partners and vendors. Knowing exactly what is in your environment is the first step to securing and gaining control over the environment.

Read more about Asset Management and Security

Efficiently Addressing Vulnerabilities

New vulnerabilities are announced everyday. However, due to their always-online needs, OT environments are a challenge to take offline to patch identified vulnerabilities uncovered in the asset inventory process. This means vulnerabilities can stay open for a very long time- from discovery until the product run is completed and critical systems can be taken down for maintenance. Armis Vulnerability Prioritization and

Remediation offers risk based vulnerability management that enables security teams to quickly identify and remediate the vulnerabilities that are most likely to be exploited and negatively impact the business. Armis Centrix™ Vulnerability Prioritization and Remediation seamlessly integrates with existing vulnerability assessment solutions, aggregates vulnerability data, and adds data for any uncovered assets. Armis's comprehensive asset intelligence engine adds risk scores, business criticality, and threat intelligence feeds, to provide a single pane of glass for organizational assets, their vulnerabilities, and their business impact. Armis Centrix™ Vulnerability Prioritization and Remediation also enables automatic ITSM ticket creation to accelerate response time and reduce operational overhead and helps track progress over time. Furthermore, this information can be shared with your existing security ecosystem such as SIEM, SOAR, and ticketing systems to raise the effectiveness of your security practice across the distributed infrastructure.

Read more about Vulnerability Prioritization and Remediation

Securing The Environment

To secure the environment against attacks, it is essential to identify suspicious behaviors. Armis Centrix™ utilizes multiple detection engines including:

1. **Device mapping and traffic visualization:** With Armis' network traffic analysis and deep packet inspection, IT and security teams can visualize network communications and display asset risks in order to more efficiently manage network segmentation and enforcement.

2. **Anomaly detection:** Our world class anomaly detection, based on single device baselines and known good behaviors, empowers security operations teams to detect network threats with a high degree of accuracy.

3. **Signature-based detection:** Identify known threats used by attackers for known attacks.

Integrations with common network enforcement systems and SOC tools deliver automated workflows to improve incident response time and reduce Mean-time-to-Resolution.

Read more about Telemetry Data

Achieving Process Integrity

Auto manufacturing requires a vast supply chain composed of numerous third-party component suppliers and various departments within the manufacturing facility. This complexity requires synchronized operations and access to credentials by a wide, heterogeneous audience. Maintaining access and configuration control from the main facility to all locations is crucial. Armis Centrix™ monitors and audits changes of ICS assets to ensure they are within acceptable tolerance limits.

It also provides constant insights and reporting on PLC usage, if any OT assets produce errors, and tracks and reports misconfigurations and default settings that are unchanged. The OT security solution periodically queries individual devices at all locations, identifying any changes. This approach ensures security across headquarters, regional, and remote locations.

Read more about Process Integrity

Achieving Adherence To Regulations and Security Frameworks

To comply with IATF, NIS2, ICA/IEC 62443, MITRE ATT&CK and ISO standards, maintaining a proper paper trail is essential. Armis Centrix ™ provides deep awareness of every device's state and characteristics, accurate matching with vulnerability knowledge bases, and real-time capture of deviations. Customizable dashlets and reports proactively demonstrate regulatory compliance and adherence to security frameworks and can provide a detailed paper trail that captures user activity, processes, code downloads, and environmental changes, and helps speed incident response while demonstrating and enabling proactive compliance.

Read more about Compliance Reporting

Quick Time To Value

Armis has deep expertise in a variety of different verticals. With Asset Intelligence, Armis gathers intelligence in over 4 billion assets and uses this intelligence to offer customers access to over 35 value packs. These ready to run value packs help administrators easily address common security challenges, discover security gaps, and unlock innovation with predefined security policies dashboards and reports that are relevant to their specific vertical or business challenge.

Business Deliverables with Armis in Automotive Environments

Customer testimonials reveal some core themes achieved when Armis is deployed in Auto Manufacturing organizations:

- **ROI** with production agility and efficiency, resources can be used more effectively.
- **Cyber Resilience** with complete asset discovery ensures visibility of all assets connected to your organization.
- **Future-Proofed** cybersecurity with Armis, organizations are ready for future digitalization.
- **Operational** resilience with Armis, organizations are reducing ransomware attacks on their networks.
- **Compliance** and safety across the entire production process in manufacturing and critical infrastructure.
- **Reputation and trust**. Organizations using Armis are industry leaders upholding best cybersecurity practices.

Asset Inventory

Armis collects information from many data sources to provide a unified view of all managed and unmanaged assets, physical or virtual.

OT/ICS - Process Integrity

Provides a dynamic overview of the Process Integrity aspects of the OT/ICS environment, including a detailed view of all of the critical configuration activities, operational status of the controllers, errors and more.

Active Directory

Make the most of your newly connected integration by adding hand-picked modules and content to the platform.

Summary: Prioritizing Cybersecurity in Industrial Operations

Industrial cybersecurity is paramount in mitigating the core risks associated with new trends and challenges in the automotive manufacturing industry. The ability to see, secure, and manage IT, OT, and IoT assets is essential. Armis offers an advanced multi-detection engine for comprehensive visibility and control across the manufacturing process, ensuring an up-to-date inventory, and helping prioritize and address vulnerabilities while maintaining capacity planning and maintenance schedules. Finally, keeping a full paper trail aids in proactively demonstrating compliance, empowering engineering and security teams to maintain peak efficiency without compromising the manufacturing process's security.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial