Securing AI-Enabled Smart Factories

Addressing security challenges and solutions in the era of industry 4.0

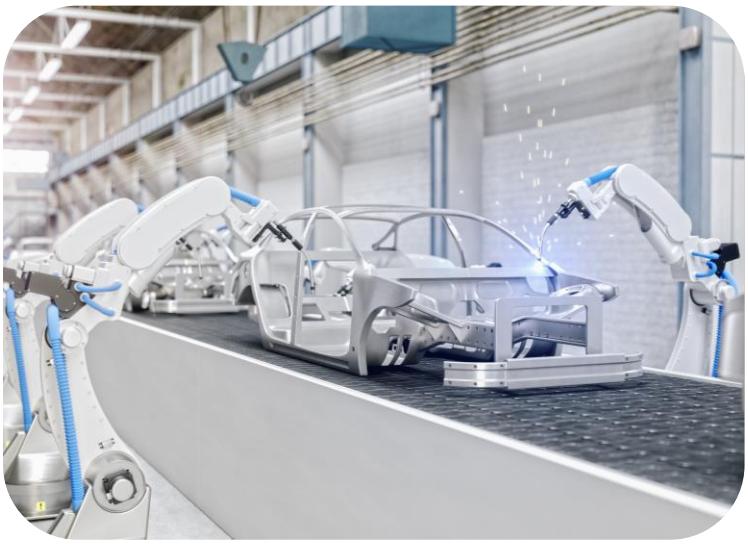
The manufacturing sector is a cornerstone of the global economy, driving innovation, employment, and economic growth. Factories play a pivotal role in manufacturing enterprises, serving as the hubs where raw materials are transformed into finished products. The significance of data in manufacturing operations cannot be overstated, as it enables efficiency, productivity, and informed decision-making.

Since it was first unveiled in 2011, Industry 4.0 has defined the emergence of digital industrial technology and cyber-physical systems. In recent years, the deployment of the Industrial Internet of Things (IIoT) and Artificial Intelligence (AI) in smart factories has revolutionized the industry. These technologies offer numerous benefits, including enhanced machine health monitoring, the creation of digital twins for simulation and optimization, productivity initiatives, sustainability reporting, predictive maintenance, and operational efficiency. However, the integration of IIoT and AI systems also brings new security concerns that must be addressed to protect sensitive data and ensure the smooth operation of smart factories.

Challenge: Securing IIoT and AI systems

IIoT devices potentially expand vulnerabilities in two ways. First, the data they produce, along with AI-generated insights and data, can itself be the target in industrial espionage scenarios, including attacks sponsored by state-backed hackers. Secondly, these devices and AI systems can provide entry points into the larger enterprise IT network, potentially allowing bad actors to access less-protected avenues of penetration and exploit sensitive data.

Securing the smart factory without interfering with its smooth operations grows more difficult as the number of IIoT devices and AI applications expands. Additionally, backhauling data and applications to a centralized data center introduces latency that could slow production or cause other disruptions in process control.



Key applications of AI in smart factories

Robotics and automation
AI-powered robots perform complex tasks with precision, helping to increase productivity and reduce human error.

Production planning and scheduling
AI enhances production efficiency by optimizing resource allocation and streamlining workflows.

Predictive maintenance
AI predicts equipment failures and schedules maintenance to help reduce downtime and extend machinery lifespan.

Quality control
AI enables real-time quality inspection and defect detection, helping to ensure high product standards and reduce waste.

Supply chain optimization
AI optimizes supply chain management by forecasting demand, managing inventory, and improving logistics efficiency.

Enhanced safety
AI-powered sensors help robots and machines understand and navigate their surroundings, reduce the risk of collisions and ensure safe interactions with human workers.

LUMEN® TECHNOLOGIES

Solution: Move security to the edge

All this IIoT and AI activity is happening at the edge of the network. Security must move to the edge as well.

Secure Access Service Edge (SASE) provides a technology framework for securing these remote accesses. SASE is a set of integrated technologies that builds profiles for users, devices, and access channels to properly authenticate who, or in this case what device, is authorized to access certain resources. SASE can be configured for devices (such as certain IIoT devices) that need access to data from other devices. SASE helps isolate components of your network to contain worst-case security scenarios. Those IIoT devices and AI systems expand the attack footprint for attackers and must be secured.

SASE is one way to converge security and network management into a single approach. When paired with other security functions such as Security Operations Centers (SOC) that can monitor network traffic looking for anomalies, these modern approaches can improve security and enhance operations.

While IIoT and AI are pushing a lot of computing out to the edge, it is imperative that smart factories are properly protected at the edge.

Results: Security for the smart factory

By leveraging AI and IIoT, there are many ways manufacturers can help secure their smart factories, including: optimizing supply chain management, improving sustainability practices, and driving innovation in manufacturing. The combination of these technologies helps smart factories operate more securely and efficiently, fostering continuous improvement and innovation.

In addition, it is crucial to enable strong security solutions, particularly at the edge, to safeguard against potential cyberthreats.

To stay ahead of security threats without compromising productivity, manufacturers should implement SASE into their smart factory operations. By integrating SASE, manufacturers can benefit from enhanced security and operational efficiency.

By leveraging Lumen partnerships and security expertise, manufacturers can create a robust security framework that helps ensure the protection and reliability of their smart factory operations.

Rather than viewing the factory as a remote island, manufacturers can recognize it as part of a larger digital infrastructure. This perspective allows factory and plant operations to better align with broader enterprise needs and realities, enhancing overall efficiency and connectivity.

Why Lumen?

With a comprehensive portfolio, Lumen can help your business deliver high-quality connectivity, minimize costs and complexity, and enhance your security posture. Rely on the extensive and deeply peered Lumen global network, Black Lotus Labs' threat intelligence, and our team of experts to help deploy and manage the solution.

866-352-0291 | lumen.com | info@lumen.com

LUMEN® TECHNOLOGIES