Edge-enabled security enhances and protects the smart factory

The manufacturing sector is a huge part of the global economy. The factory is the heart of any manufacturing enterprise. Factories literally have many moving parts from inventory to partially finished goods to the manufacturing machines themselves. Maintaining the flow of all those components is key to driving the global economy and maintaining profitability for each company.

Data is a crucial enabler and byproduct of that flow. The smart factory deploys the Internet of Things (IoT) to collect data on equipment and the rest of the operation. Sensors can measure vibrations and temperatures within manufacturing gear to assess machine health in real time. That data can be used to improve operations and avoid unscheduled downtime. That data can also be used to power digital twins of the factory in a simulator or metaverse environment so those models reflect the real factory conditions as engineers chart a course to the factory's future. Data produced in the factory can be linked to other productivity initiatives such as warehouse automation, supply chain management. This data can also be integrated into the enterprise's overall IT system to aid many other functions such as the growing responsibility of sustainability reporting.

However, those IoT devices also expand the potential attack surface that can be exploited by bad actors. Security is a key concern for the modern manufacturer.

Challenge: Securing the proliferation of IoT devices

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

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

Solution: Move security to the edge

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

Secure Access Services 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 IoT devices) that need access to data from other devices. SASE helps isolate components of your network to contain worst-case security scenarios. Those IoT devices expand the attack footprint for attackers and have to 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.

IoT is already pushing a lot of computing out to the edge and the smart factory can be secured at the edge as well.

Results: Security for the smart factory

Manufacturers must stay ahead of security threats without bogging down productivity. SASE is a key edge-based security measure for the manufacturing industry as it automates factories and related functions such as inventory and supply chain management. Deploying SASE requires the integration of different technologies that must work together seamlessly to avoid interfering with manufacturing operations. Manufacturers can take advantage of Lumen's partnerships and experience integrating technologies into a robust solution.

Rather than viewing the factory as a unique island of operations, manufacturers can see it as part of a larger digital infrastructure. That view can marry the automation that's already going into the factory with other enterprise needs and realities.

Visit Lumen today for more information or contact a Lumen Expert for consultation to get started.

LUMEN® TECHNOLOGIES