asimily

Connected Device Security and Vulnerability Management for Manufacturing

Manufacturers face the dual pressure of securing their environments while still hitting revenue targets. Implementing an Industrial IoT (IIoT) solution enables organizations to reduce operating costs, manage supply chains, and anticipate maintenance needs. However, securing these devices cost-effectively is challenging as the process often requires specialized technologies and skills.

The Role of IoT and IIoT in Converging IT and OT

IIoT devices act as a bridge between the OT and enterprise IT technologies. OT connects machines like physical plant equipment. IT focuses on storing, processing, and delivering data to business users for enhanced decision-making and improved productivity.

IIoT devices typically have an application that enables the users to leverage analytics. The IIoT devices that monitor OT technology collect data. That data is sent across the enterprise IT network to the associated application which applies analytics so that the business gains insight.

As a subset of IoT, the devices that enable operational monitoring and efficiency create similar security challenges to their digital cousins. However, within the context of the OT environment, these issues pose a broader risk to businesses. From a business perspective, a cyberattack that compromises the OT environment can disrupt business operations, leading to lost revenue. IIoT's connection to OT also creates a risk to physical safety, requiring organizations to integrate cybersecurity risk with safety hazard evaluations.

Top IIoT Security Challenges

Growing Attack Surface

Convergence of IT and OT Systems

Connected Supply Chains

Legacy Systems and Equipment

Accurate IoT Inventories

Regulatory Compliance

Manufacturing: the Most Targeted Industry in 2023

Within the past year, a few industries have borne the brunt of the increased number of cyberattacks. According to IBM X-Force data, this has included manufacturing, services firms, and energy companies among others. Manufacturing companies sitting near the top of the list of attacked firms shouldn't be surprising. Firms across the various forms of manufacturing have a lot of intellectual property and proprietary designs; financially motivated cybercriminals can sell those designs to foreign governments or foreign corporations where intellectual property laws are less stringent.

Inclusive of this data from IBM, there are a few industries that we're going to examine in terms of recent attacks. This will include specific examples, as well as an examination of the reasons why threat actors view these spaces as potentially valuable targets.

It's important to note that these attacks, while not necessarily originating with IoT devices, are nevertheless incredibly damaging to operations. An attack can start anywhere in critical systems, and the increased number of IoT endpoints means that they can be used for lateral movement deeper into the organization as well as an origin point.

Recent Cyberattacks on Manufacturers

Manufacturing companies experienced 54.5% of attacks in 2023, according to Zscaler research, with an average of 6,000 attacks against them per week. Given that manufacturing companies tend to have tens and hundreds of thousands of OT and IoT devices in their networks, they have some unique weaknesses among other firms.

Manufacturing companies are also some of the most critical to a country's economy. Interrupting operations of the right manufacturing company can cause failures throughout certain market sectors.

A few of the most recent attacks on manufacturers include:

- Ingersoll Rand, a maker of compressors, experienced a ransomware attack in March 2023 where malicious actors leaked an estimated 3% of stolen data.
- Johnson Controls International experienced a ransomware attack that also impacted two of its subsidiaries and encrypted the company's VMware ESXi machines. Malicious actors stole more than 27 terabytes of data in the attack, potentially also including Department of Homeland Security floor plans and security information.
- Fortive Corp, which makes test and measurement tools and asset management software, reported a $5 million one-time expense on its earnings report related to the remediation and operational impact of a ransomware attack from BlackBasta.
- Mueller Water Products, Inc. reported a cyberattack in October 2023 that affected its IT and OT systems alike, and wasn't fully contained until the end of November. Mueller is one of the largest manufacturers and distributors of fire hydrants, gate valves, and other water infrastructure products in North America. They delayed filing a 10-K with the SEC and didn't resume normal operations until mid-December.

Unmanaged IoT Devices Leads to Increased Attack Surface and Risk

Shadow IT is one of the most persistent cybersecurity challenges today. Already, researchers estimate that 53% of departments refuse to use IT-approved tools and 80% of workers admit to using SaaS applications at work without getting approval from the IT department.

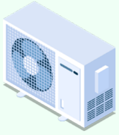
Connected devices often have at least a network interface, like ethernet, Bluetooth, Long-Term Evolution (LTE), Zigbee, Wi-Fi, 5G, or Ultra-Wideband (UWB). Once deployed in a network using these connection methods, IoT systems can be readily discovered and connected to the open internet. This is a major issue because they're not designed to have any setup protocols before connecting to the internet.

Once threat actors gain initial access into a network from a discoverable IoT device, they're able to laterally move deeper into the information architecture to achieve their goals. At the individual device level, IoT equipment is particularly vulnerable to common security pitfalls.

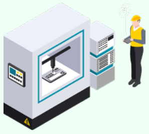
In terms of which categories of connected devices organizations tended to buy, Keyfactor research found that companies tended to deploy the following IoT solutions:

Hybrid work technologies	53%
Security cameras	53%
Real-time monitoring and location tracking	52%
Inventory and asset management	46%
Door locks or physical security	43%
Smart lighting	40%
Space utilization technology/tools	38%
Air quality monitoring	35%

Common Unmanaged IoT Devices


HVAC

Sensors


Equipment

Routers

Smart Energy Meters

Manufacturing Workstations

Drones

Printers & Scanners

TVs

Alarms

Badge Readers

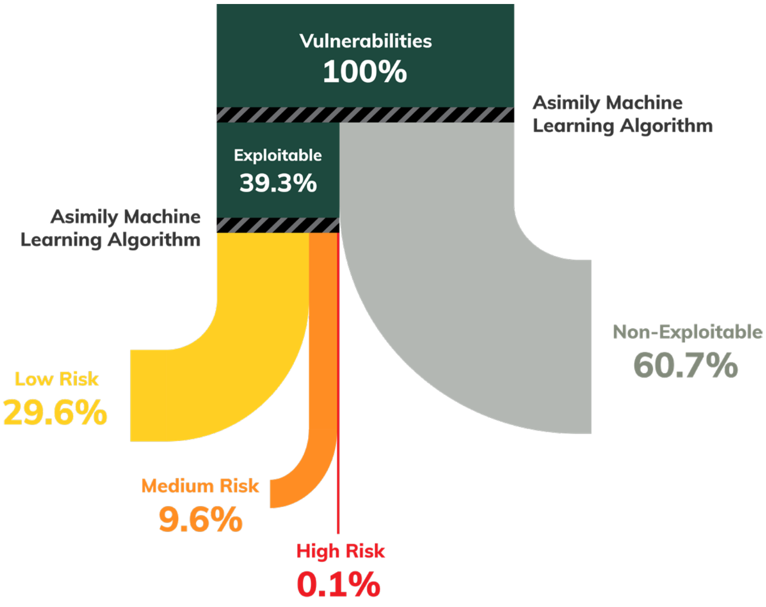
Security Cameras

Autonomous Vehicles

Secure Your Connected IoT Devices and Reduce Vulnerabilities 10x Faster with Half the Resources

Your reputation depends on timeliness and avoiding delays. When threats are kept out, everything stays on time and business can grow. Asimily IoT security solutions help you ensure that outside attackers don't affect your operations.

Asimily empowers vulnerability management teams to tackle the riskiest issues first. Instead of just giving you a list of vulnerabilities to fix, Asimily combines that information with unique Impact and Likelihood analyses to get a risk-ranked set of devices whose vulnerabilities can be mitigated.



Accurate Inventory & Unmatched Visibility

Harness Asimily's powerful protocol analyzer and deep packet inspection (DPI) to safely discover and automatically categorize your IoT assets, services, connections, and apps giving you the power to proactively manage risks, optimize resources, and fortify your security like never before.

Vulnerability Prioritization & Efficient Mitigation

Asimily's unique Impact, Likelihood and Utilization analyses show which vulnerabilities attackers will take advantage of in your environment. Allocate your resources to the riskiest devices first to promptly address vulnerabilities.

Threat Detection & Incident Response

Set device behavior rules that instantly identify any suspicious activities. Our engine swiftly spots deviations from normal behavior, ensuring that you can respond promptly to potential threats. Detect misconfigurations as well, keeping security posture high.

Risk Modeling & Simulations

Envision, predict, and act with unparalleled confidence, and unlock a new era of proactive risk mitigation. Calculate the least risk associated with a device before configuration and connection.

Connected Device Security, Reimagined

Securing the Internet of Things is far more complex than securing traditional IT equipment. Poor security practices at IoT device manufacturers paired with minimal visibility by IT and security teams make connected equipment a major security risk. The distributed and broadly installed nature of these devices means that a risk-based approach is required. This can be done, and thankfully Asimily can help companies implement and manage a risk-focused method of securing IoT devices for a more secure future.

Asimily's IoT Risk Management Platform

- Creates a complete IoT inventory, collecting 100+ attributes for each device;
- Identifies and prioritizes the riskiest vulnerabilities; Recommends simple, validated mitigation actions;
- Conducts a full flow analysis for each device, recording all communication patterns across the network;
- Calculates risk for every connected device based on device attributes, dataflows, vulnerabilities, anomalies, configuration, and overall criticality of the device on operations;
- Generates ACLs for targeted segmentation for use by a NAC;
- Flags anomalous device behavior based on profiling data from millions of IoT devices;
- Makes it easy to set policies to monitor accepted risks and identify suspicious activity proactively;
- Automates packet capture for forensic analysis of any IoT device to support root cause analysis;
- Documents when the device is being used so users can understand utilization and operational efficiency;
- Allows device configuration snapshots to be taken, to thwart ransomware and simply recovery; and
- Risk simulator helps determine the benefit of work before it is performed, increasing team efficiency.

Asimily can help enterprise organizations drastically reduce cyber risk while minimizing resource and time costs.

To see how Asimily can help your organization, **arrange a demo today.**

About Asimily

Asimily is an industry-leading risk management platform that secures IoT devices for medical, diagnostic, life sciences, pharmaceutical, and enterprise companies.

Connect With Us

info@asimily.com
440 N Wolfe Road
Sunnyvale, CA 94085
(833) 274-6459
(833) ASI-MILY