asimily

Connected Device Security and Vulnerability Management for Utilities

The companies that underpin critical infrastructure often use tens or hundreds of thousands of Internet of Things (IoT) devices for several use cases. Water utilities use remote sensors to monitor water quality and reservoir levels. Power companies leverage connected equipment to monitor for outages and higher usage levels throughout the system. Oil and gas companies use connected devices to monitor miles of geographically distributed pipelines.

The use of IoT devices brings with it the risk of cyberattack. Connected devices are deployed incredibly quickly in large numbers, adding more possible entry points to the networks of critical infrastructure organizations.

Utilities and other critical infrastructure reported 60 incidents in the first three months of 2023 that they characterized as physical threats or attacks on major electric grid infrastructure, in addition to two cyberattacks, according to mandatory disclosures with the Department of Energy. This is more than double the same period in 2022 and is indicative of the desire of criminals to cause mass blackouts.

IoT Risks for Utilities and Critical Infrastructure Organizations

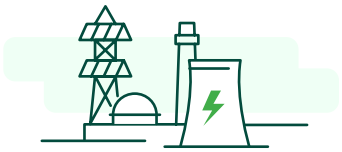
IoT devices are often insecure. They come with default passwords that are easy to guess and difficult to change before connecting to the internet. Their firmware is often built with speed to market instead of security at the forefront. Further, the reality that IoT devices lack agreed-upon security standards means that device manufacturers have no real best practices to adhere to. This creates what amounts to thousands of potentially insecure devices out in the real world.

Even without the basic lack of security in IoT devices, however, cybercriminals still find the utilities and critical infrastructure sector a target-rich environment.

Top IoT Security Challenges

- Growing Attack Surface
- Connected Supply Chains
- Legacy Systems and Equipment
- Accurate IoT Inventories
- Third-party Security Standards
- Regulatory Compliance

Recent Attacks on Utilities and Critical Infrastructure Organizations



As part of our analysis of the IoT risks to critical infrastructure, we examined a few recent cyberattacks on individual sectors. There was not enough information to determine whether these attacks originated in connected devices, unfortunately. Whether they started with IoT devices or not is immaterial, however; what's more important is understanding that cybercriminals regularly target critical infrastructure. Anything that creates more cyberattack risk, including unprotected IoT devices, needs to be defended.

Different critical infrastructure categories experience distinct threats. For water utilities, an IoT breach won't necessarily stop operational technology from functioning or create downtime. That might be a good thing, but that doesn't mean these attacks aren't damaging. A more salient point is that these attacks on water systems may also occur in rural areas that have more limited budgets.

Co-ops and rural organizations are getting targeted because they're the ones with the smallest amount of resources. In 2022, there were a total of 1,665 security incidents involving the U.S. and Canadian power grids; 60 of those incidents led to outages. Although IoT attacks may not cause major disruptions given how they're connected to a network, the reality is that they can still impact energy company terminals and other IT rather than OT.

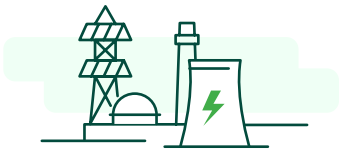
At least 10 water facilities throughout the United States were hacked through the same method the Cyber Av3ngers, according to federal investigators. The devices that the Iranian group shut down were manufactured in Israel and displayed a message that said all Israeli tech is fair game for the Cyber Av3ngers.

Oil and gas companies typically have larger organizations with distributed networks and riskier IoT assets because of how geographically dispersed their operations are. Overall, these companies are less regulated in terms of how and where to invest in cybersecurity. Everything relies on IT defenses as opposed to the OT side of things with other utility and critical infrastructure companies.

A few recent attacks on utilities and critical infrastructure include:

- The Municipal Water Authority of Aliquippa in Pittsburgh had to shut down its OT systems after a cyberattack from the Iran-backed group "Cyber Av3ngers" on one of its booster stations. The attack shut down equipment that monitors water pressure at the station, forcing the water company to switch to manual monitoring.
- In May 2021, financially motivated cybercriminals launched a ransomware attack on Colonial Pipeline. The hack locked up IoT sensors on the pipeline, making it impossible for the company to track how much to bill customers. In response, the company shut down all 5,500 miles of pipeline. This pipeline makes up 45% of the East Coast's supply of diesel, petrol, and jet fuel. Because of the shutdown, there were fuel shortages and panic buying in multiple U.S. states.
- Suncor Energy, a Canadian oil and gas company, experienced a cyberattack in June that one expert said would likely cost the company millions of dollars in recovery. Customers trying to get gas at Suncor Petro-Canada retail locations were unable to pay with credit or debit cards while the company recovered. It took until nearly August to almost completely recover regular operations.
- Chicago-based engineering firm Sargent & Lundy, which designed more than 900 power stations in the US, experienced a ransomware attack in October 2022. Sargent & Lundy holds sensitive data on its power station and power line projects. Data on electrical systems was exfiltrated, but there is as yet no indication of any downstream impacts.

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). Utilities can use Modbus, DNP3, IEC 61850, ENIP or other less common technologies for communication. 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.

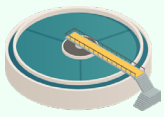
Once threat actors gain initial access into a network from a discoverable IoT device, they're able to laterally move deeper into the information architecture to achieve their goals. At the individual device level, IoT equipment is particularly vulnerable to common security pitfalls.

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


Air Sensors


Treatment


Facility Cameras


Wireless


Meters


Electrical Generation


Chemical Sensors


Flow Analysis


Printers & Scanners


Displays


Leak Detection


Badge Readers

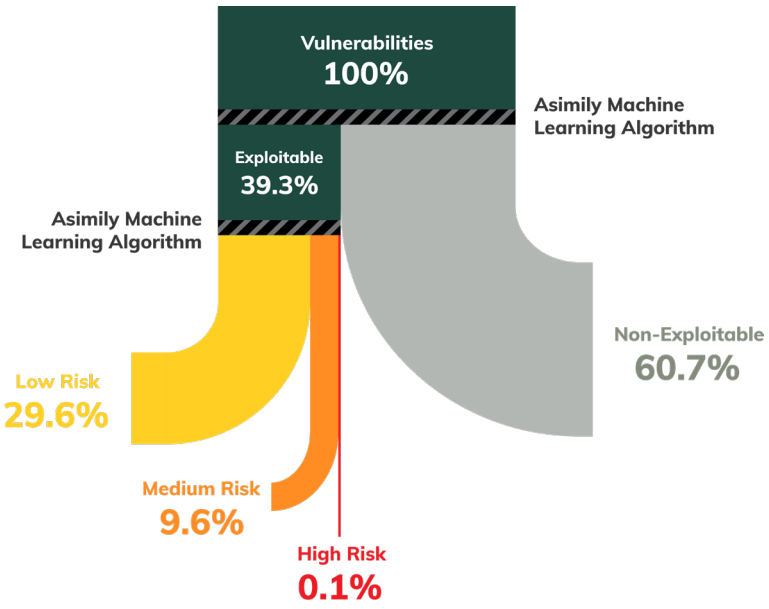

Lighting


Thermal Sensors

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