Connected Device Security and Vulnerability Management for Life Sciences

Life Sciences organizations rely heavily on technology and data to drive their research, development, and operations. The industry has increasingly adopted Internet of Things (IoT) devices to enable better research, development, and manufacturing monitoring and management. As the industry continues to drive digital transformation, the use of IoT will become critical to maintaining a competitive edge.

Life Sciences organizations manage critical sensitive data, including patient information, customer details, and intellectual property. According to IBM's 2023 Cost of a Data Breach Report, the pharmaceutical vertical spends an average of $4.82 million on a data breach.

Although data breaches are a moment-in-time incident, they can have long-term reputations and financial outcomes. At a minimum, the organization needs to pay to recover from the incident and notify impacted parties. However, as filing class action lawsuits against breached companies becomes the norm, Life Sciences organizations need to consider everything from defense attorney fees to potential damages to long-term identity theft monitoring costs. Further, they should consider the increased scrutiny that insurance companies place on their security posture. Even with cyber liability policies, an organization can find that the insurer denies coverage due to negligent security practices.

IoT Risks for Life Sciences

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.

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 Life Sciences and the Consequences

Whether seeking to steal intellectual property as part of corporate espionage or consumer data for financial gain, attackers want to find an organization's weakest security link. They want to gain unauthorized access to their target as quickly as possible without being detected. The most notable breaches in the Life Sciences industry highlight the ease with which they can target connected systems to achieve their objectives.

Life Sciences companies including those in pharmaceuticals, biologics, biotech, medical devices, food processing, and others have increased their use of sensitive customer data in the past few years. As a result of this, plus valuable intellectual property and high turnovers, the average cost of a data breach in pharmaceuticals was $4.82 million in 2023.

Life Sciences companies are heavily targeted in general. The CISO of global pharmaceutical company Johnson & Johnson, for example, said in 2021 that the company experienced 15.5 billion potential cyberattacks per day. There's no telling how that may have increased in the past few years.

Life Sciences companies would do well to account for their critical equipment and protect it against threats. Cybercriminals and nation-state groups seeking to either steal data or intellectual property will continue to target them. This state will require tighter analysis of security risks and a more nuanced method of protecting connected devices and other necessary manufacturing or scientific equipment. And that's even outside of discussing the threats facing critical infrastructure.

Healthcare organizations would do well to shift additional spend to cybersecurity, especially in light of the risk of HIPAA fines and a greater focus on data privacy in the year ahead.

A few of the most recent attacks on Life Sciences include:

- Novartis in June 2022 saw its data hijacked by Industrial Spy, a well-known online extortion ring. The group claimed they stole data related to DNA and RNA-based technologies from the Swiss pharmaceutical company.
- PharMerica, one of the largest providers of pharmacy services in the United States, revealed in March that an unknown actor accessed its systems in March and extracted personal data pertaining to 5.8 million individuals. PharMerica operates 2,500 facilities directly and over 3,100 pharmacy and healthcare programs throughout the country. They notified affected individuals and the next-of-kin for any deceased people whose personal information was impacted.
- Pharmaceutical giant Merck lost $1.4 billion in 2017's NotPetya attack linked to Russian threat actors. The attack started with an infection in Ukrainian accounting software, eventually spreading to 65 countries. Merck was one of the biggest victims and has been locked in a lengthy court fight against insurers trying to avoid paying out. Just recently, the courts ruled that insurers couldn't use the war exclusion clause to avoid making a payout in this case.
- Postmeds, a mail-order pharmacy, revealed in late August that the personal data of more than 2.3 million patients was exposed in a cyberattack.

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

Scientific Equipment

Thermostats

Air Quality Sensors

Networking

Meters

Process Workstations

Laboratory Equipment

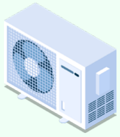
Printers & Scanners

Displays

Alarms

Badge Readers

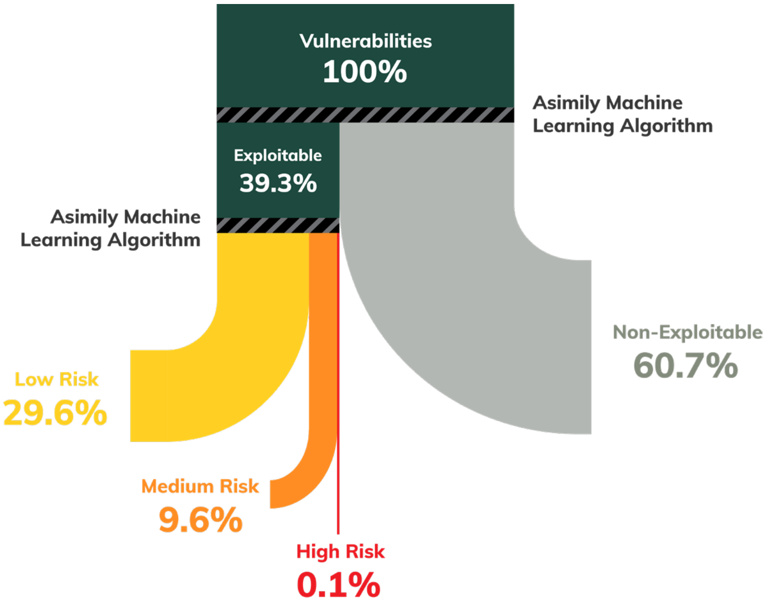
Security Cameras


Climate Control

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