Connected Device Security and Vulnerability Management for Retail

The retail industry is evolving, transforming transactions into shopping experiences. To do this, retail businesses have adopted a wide range of technologies, from e-commerce platforms and in-store IT systems to connected devices such as beacons, sensors, and trackers.

This increased use of technology makes retail businesses an enticing target for cybercriminals, who can profit by stealing customer data, scraping payment card information from POS devices, and disrupting operations as leverage for hefty ransom demands.

The Sophos State of Ransomware in Retail report found that 69% of retail businesses were hit by ransomware in 2023. Almost three-quarters of these ransomware attacks resulted in data being encrypted, up from 68% and 54% in the two previous years.

The average cost of a retail data breach in 2023 was $2.96 million, and the industry accounted for 6% of all data breaches worldwide, up from 5% the previous year. This makes retail the 8th most targeted industry, up from 10th in 2022.

IoT Risks for Retail

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 Retail 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 Retail Organizations

The retail sector attracts cybercriminals because it processes and handles large amounts of personal data and financial information. Every retail store is likely to have valuable credit card data, and devices in that store are logical pivot points to get that data. The complexity of physical stores with e-commerce sites creates opportunities for cybercriminals due to the mix of technologies, including cloud-based services.

Retailers also sell a wide range of goods purchased from third-party suppliers and their software supply chains tend to be just as complex and deep. Any cyber-attacks that happen to these suppliers can affect the retailers who rely on them as well. The supply chain is an operational dependency which represents many points of ingress for an attacker.

The 2023 Data Breach Investigations Report identified system intrusion, web application attacks, and social engineering as the most significant threats to retail businesses. Additionally, a report by Trend Micro notes that 30 percent of retail IT and business leaders cite too many tools and vendors as one reason that it's difficult to manage security; 40 percent say it's spiraling out of control.

Balancing security with operational efficiency is also a significant challenge for retailers. Retailers must ensure that their security measures do not impede day-to-day operations or cause unnecessary disruptions to customer experiences. Retailers must strike a delicate balance between robust security measures and operational efficiency. This can be achieved by implementing security solutions that are designed to integrate seamlessly with existing operations and workflows, and by providing comprehensive training to employees to ensure that they understand and can comply with security policies and protocols.

Securing a retail enterprise—especially one that encompasses both brick and mortar and online sales—can be a complex task. So, while the attacks described here are concerning, they're hardly surprising. Many cyberattacks against retail businesses go unreported—and of those that do make headlines, it's rare that the full extent of the damage is publicized.

A few recent attacks on retailers include:

- In late October 2023, hardware giant Ace Hardware was hit by a cyberattack that compromised over a thousand assets—1,202 devices, including 196 servers, were hit during the attack and had to be repaired or recovered. The result was widespread disruption across the chain's 5,600 stores around the world.
- In early 2023, fashion retailer JD Sports was hit with a major cyberattack. The breach occurred after a server containing online order information for customers was hacked. Cybercriminals stole 10 million unique customers personally identifiable information.
- VF Corporation, the corporate owner of apparel brands such as Timberland, Dickies, North Face, Vans, and many more, suffered a serious cyberattack in December 2023. Cybercriminals stole 35 million unique customers personally identifiable information.
- On Cyber Monday 2023, a cyberattack began against Staples, disrupting the company's ability to process and deliver online orders during the critical promotional period. The attack also affected communications and customer service, with all customer service employees reportedly being sent home for several days.

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.

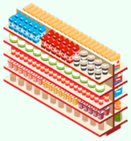
Once threat actors gain initial access into a network from a discoverable IoT device, they're able to laterally move deeper into the information architecture to achieve their goals. At the individual device level, IoT equipment is particularly vulnerable to common security pitfalls.

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%

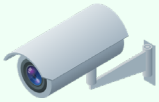
Common Unmanaged IoT Devices

Point of Sale Systems

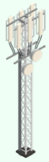

Smart Shelves

Barcode Scanners

Inventory Systems


Cameras

People Counters


Wireless

Printers

Displays

Call Buttons

Badge Readers

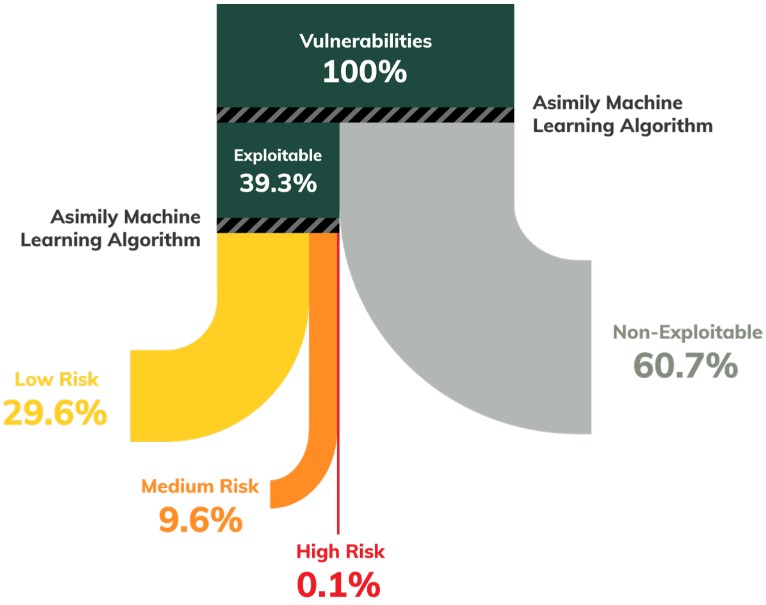
Air Sensors

Occupancy 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