ARMIS®

WHITE PAPER

AGENTLESS DEVICE SECURITY FOR RETAIL ENVIRONMENTS

Table of contents

EXECUTIVE SUMMARY

As a retailer, digitally transforming your brick-and-mortar stores can grow revenue, reduce costs, and deliver new, exciting shopping experiences that attract and retain customers. However, the connected devices that make digital transformation possible can also put your business at risk.

The connected devices that make digital transformation possible are, more often than not, unmanaged, which means they are not seen or controlled by your security or IT teams. That leaves your security team blind to what the devices are doing. Adding complexity is the fact that many retail devices like remote vending machines are now connected through a dedicated IoT cellular network. Because these devices are not part of the traditional IT network, they cannot be seen or protected by traditional security solutions.

So increasingly, cybercriminals focus on these devices as targets taking advantage of their ubiquity and inherent security weaknesses.

The digital transformation to modern, connected retail devices shouldn't come at the cost of incurring unacceptable levels of cyber risk. Deployments of devices like these require security that can cover the full landscape of managed, unmanaged and IoT devices, and that includes continuous device discovery and monitoring allowing retailers to detect both operational and cyber threats and quickly respond to mitigate risk.

This white paper explores the cyber security and operational challenges in retail environments and proposes ways to address them.

THE CONNECTED RETAIL AGE IS HERE

Today's visionary retailers are deploying a wide variety of assets to deliver better customer service and optimize their supply chain and inventory management:

- Self-service checkout can help customers complete the purchase process more quickly.
- Sensors can track customers' paths through a store, and you can use the tracking information to improve layout and merchandise placement.
- Interactive kiosks and smart displays can provide store layouts, directions, and product information.
- Standalone Vending Machines in remote locations like airports and train stations help deliver a familiar brand experience and drive sales outside of the branch stores.
- Automated inventory systems that include devices like robots that continuously scan store floors for restocking needs and for general orderliness of shelves or displays.

These innovations depend on devices that can be a big security risk. These devices expose an increasingly vulnerable attack surface because they aren't visible to traditional IT operations or security solutions and thus are not monitored for potential compromises.

THE AGE OF THE DIGITAL, CONNECTED DEVICES

This new age of connected retail also brings in a new age of digital devices driving that transformation. From smart displays and customer sensors to mobile point of sale devices to inventory robots in a store to internet connected forklifts unloading new goods, each of these devices are the new endpoint. However, these new devices do not come with security, nor can they host an agent. In fact, many are not even connected to the corporate IT network but utilize a cellular connection. This means the very devices used to drive connection, productivity, and interaction do not have the required protection. That's because traditional IT and security tools were not designed to deal with today's digital, connected devices.

1 **Barcode Scanners**
May use Bluetooth or Wi-Fi. Hard to patch, but remotely exploitable.

2 **Smart Lighting**
On the network with no security.

3 **Smart TV**
Can't take an agent, but on the network. Hard to upgrade.

4 **Point of Sale**
Tablets & handheld devices. Taking credit cards and digital payments.

5 **Tablets**
Used for mobile Point of Sale, inventory lookup, support, and more.

6 **Security Systems**
On the network, but security on these devices is questionable.

7 **Smart HVAC**
Smart HVACs and thermostats can't take agents.

8 **Security Camera**
No security, but often the target of botnets and other attacks.

9 **Smartphone**
Transient devices used by customers and vendors. Should identify and track

SECURITY BREACHES ARE COMMON

Retail experiences higher levels of security incidents compared to other industries. Account takeover - a risk for consumers who have login accounts that store their credit card or payment information on eCommerce sites - affected 32.8% of online retailers in 2021, compared to the average logins (25.5%) across all other industries.[1]

Just weeks before the 2021 holiday season, an international ransomware attack left electronics retailer MediaMarkt incapable of collecting or returning packages ordered online.[2]

In the UK, the supermarket chain Spar has been forced to close approximately 300 stores following a cyber attack. And that was just 2 months after the one of the largest grocery retailers in the UK website & app crash, leaving thousands of shoppers frustrated.[3, 4]

High-end department store chain Neiman Marcus Group had to notify about 4.6 million US customers that their personal information including names, contact information and credit card numbers may have been accessed in a data hack.[5]

[1] *https://www.helpnetsecurity.com/2021/11/09/retail-industry-security-incidents/*

[2] *https://www.retaildetail.eu/en/news/electronics/mediamarkt-victim-international-cyber-attack*

[3] *https://www.retailgazette.co.uk/blog/2021/12/cyber-attack-hits-over-300-spar-shops-forcing-many-to-close/*

[4] *https://www.retailgazette.co.uk/blog/2021/10/customers-left-unable-to-shop-online-as-tesco-website-app-crash/*

[5] *https://www.reuters.com/business/retail-consumer/neiman-marcus-says-notified-46-mln-customers-about-data-breach-2021-09-30/*

These are just the exposures we know about. More likely is the case that breaches occur every day that we don't know about — until we do. That's because vulnerabilities in devices are far more elusive to retailers than they are to bad actors. And it only takes one vulnerability to put an entire business at risk.

These connected devices are the new targets for hackers. New research[2] shows cyberattacks on IoT devices surged 300%, targeted billions of devices across multiple industries including retail. The lack of any security on these devices makes them the new attack surface.

SECURITY BREACHES **ARE COSTLY**

With a worldwide average cost of $4.65 million per incident in 2021, retail experienced a large increase in costs vs. the prior year.[1]

Perhaps the most high profile data breach in memory was Target in 2013, which resulted in an $18.5 million settlement.[3] But the overall cost was much higher. Target also paid $10 million to settle a class-action lawsuit in 2015, and the company agreed to pay up to $10,000 to consumers who suffered losses from the data breach. With a loss of customers in the first few quarters following the breach, the total cost was an estimated $300 million as of mid-2017.[4]

Aside from expensive downtime and breach recovery, retailers today have to concern themselves with regulators that could impose heavy fines on top of lost revenue and diminished customer trust.

[2]Forbes, Cyberattacks On IoT Devices Surge 300% In 2019, 'Measured In Billions', Report Claims, Sept. 2019

[1]https://www.statista.com/statistics/387861/cost-data-breach-industry/

[3]"Target will pay $18.5 million in settlement with states over 2013 data breach", L.A. Times, May 23, 2017

[4]"The Supply Side: Walmart cybersecurity team handles over 200 billion events annually", Talk Business & Politics, May 22, 2019

REGULATIONS LOOM OVER RETAILERS

Many organizations are adopting the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to outline their current state of cybersecurity and strengthen their security posture. The framework provides cybersecurity governance best practices for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. In conjunction with Arims, it can be used to help identify and prioritize actions for reducing cybersecurity risk in your environment.

A retailer must also comply with the Payment Card Industry Security Standard (PCI DSS) as they conduct their business. They must look at how they will meet these standards, documenting, monitoring, and enforcing policy on all devices in the cardholder data environment — including unmanaged or IoT devices beyond the reach of traditional controls such as endpoint security or network firewalls.

Real threats in the digital retail environment

Smart displays and kiosks:
Internet-connected devices can be attacked remotely to give attackers access to your network.

Self-serve checkout and point-of-sale (POS) devices:
Theft of shopperr credit/debit card information costs time and expense to fix but also causes millions in regulatory fines and damage to your brand.

Bluetooth-enabled price scanners:
Hackers can attack these devices through Bluetooth-related vulnerabilities to change the pricing of items or stage a broader attack for customer information.

Printers connected to Wi-Fi:
A printer with an open hotspot can enable hackers to circumvent network access control and gain access to yourr data.

Production-line sensors:
Sensors and automated controls in warehouses can be compromised causing production or delivery delays.

Remote vending machines:
Often rely on cellular connectivity, leaving them vulnerable to remote attacks.

TRADITIONAL SECURITY WASN'T BUILT FOR THE NEW DIGITAL AND CONNECTED DEVICES

In the rush toward digital transformation, the primary focus has been to acquire and deploy digital retail devices at scale to quickly reap their rewards—like helping to grow revenue, reducing costs, gathering critical data, and delivering new shopping experiences. Security has not been a front-and-center concern. However, once these devices are on your network, their vulnerabilities become a risk you have to face.

The traditional security products most organizations have come to know and trust simply won't help manage the risks and consequences of the new connected retail frontier. These products were built for traditional computing devices. And while some security vendors have reengineered their products, or have offered new bolt-on modules that attempt to make them work for IoT and unmanaged devices, most fail for a variety of reasons:

- Security agents won't work. You cannot install an agent on most retail unmanaged and IoT devices. This renders invalid an entire class of security tools that are often used to help identify, protect and monitor devices on enterprise networks.
- Network scanners can't be used. Designed for IT networks, they can't cover cellular-IOT devices. In addition, many of these devices do not tolerate network scans or probes, which can crash or disrupt the device. That makes obtaining an inventory of hardware, software, and vulnerabilities are far more challenging for IoT devices than for normal computers.
- Conventional network security products are insufficient. The traditional placement of network IPS systems is at the perimeter and in the core of the network. This makes protecting IoT devices at the edge of the network difficult and protecting IoT devices on cellular networks virtually impossible. Furthermore, network equipment can be compromised by a determined hacker, so relying exclusively on network controls (e.g. firewalls and network segmentation) is not enough.
- Wireless connectivity evades legacy security controls. Manufacturers of network devices like access points and routers as well as OT security products are increasingly building wireless connectivity into their devices. These protocols, which include Bluetooth, Near Field Communication, Zigbee, etc. are invisible to traditional security controls.

ARMIS: MITIGATING SECURITY RISKS ACROSS ALL YOUR ASSETS

Since traditional security tools are unable to monitor and secure unmanaged retail and IoT devices, security professionals must seek a new approach. This new way forward in security must be purpose-built for today's unmanaged, connected environments. That includes the ability to discover all the devices in remote locations, proactively assess the risk of every device, and detect threats by monitoring and analyzing device behavior continuously. And it must be able to respond to incidents immediately and automatically to stop attacks from unraveling your business.

An Agentless Approach

As previously discussed, several security products use proprietary software agents and even additional hardware to scan devices for information. For managed devices, agent-based tools can provide detailed information — but they are difficult to deploy and maintain, and are effective only when the agents are working properly. More importantly, the scope of agent-based products does not extend to unmanaged or IoT devices.

Armis is designed to address managed, unmanaged and IoT devices on any network using an agentless approach. Without installing or licensing separate software or hardware, Armis can discover every device in your organization, managed and unmanaged, and the connections those devices make. With no agents to deploy or manage, it works equally well for any unmanaged and IoT devices. And it is completely passive, so as not to disrupt the operation of any device in your retail operations.

Armis is cloud-based and integrates easily with your existing network and security products — nothing to install on devices, and no configuration or programming required. It integrates with your existing enforcement points like firewalls and NAC, and enables you to create fine-grained policies for managed, unmanaged and IoT devices to extend the value of your security investments.

Discover devices other products miss

The right device security product should discover every device on and off your network, and analyze their behavior, including connections and activity history. Specifically, you need a security solution that can monitor both wired and wireless traffic on your network and in your airspace to identify every device and to understand their behaviors.

Armis can detect, classify, and profile every managed, unmanaged, and IoT device in your environment, giving you a complete, real-time device inventory and an unprecedented level of visibility and control. Armis can even identify off-network devices using Wi-Fi, Bluetooth, and other IoT protocols in your environment — a capability no other security product offers.

Our partnership with Eseye extends the platform's coverage to remote devices connecting through Eseye's global cellular IoT platform. The unified Armis and Eseye solution protects all of these devices out of the box and scales dynamically to support device requirements for each network.

Assess the risk of attack surfaces

Investing in risk assessments can help you manage your organization's attack surface and enable you to pinpoint risky devices and activities. Armis provides modern retailers with ongoing device risk scoring based on multiple risk factors, including software vulnerabilities, known attack patterns, and the behaviors that Armis observes of each device on your network. The risk score helps your security team understand your attack surface and meet compliance with regulatory frameworks that require identification and prioritization of vulnerabilities.

ARMIS: MITIGATING SECURITY RISKS ACROSS ALL YOUR ASSETS

Detect threats with continuous monitoring

Continuous monitoring is essential for maintaining security with unmanaged and IoT devices. Core to the Armis platform is our Device Knowledgebase. It is the only crowd-sourced, cloud-based device behavior knowledgebase—the largest in the world. It tracks 200 million devices broken out into distinct device profiles. These device insights enable Armis to fingerprint and classify new devices and detect threats with a high degree of accuracy.

Armis compares real-time device state and behavior to “known-good” baselines to similar devices we have seen in other environments. Using it’s unique threat detection and prevention technology, Armis can detect changes in device states and anomalies that could indicate threats or attacks and can automate threat response. Armis continuously monitors every device on your network to detect suspicious or malicious activity and automatically quarantines suspicious devices to stop attacks and any exposure to the rest of your business.

Reduce your response time

Visibility and continuous monitoring are not enough. You need to take action and quarantine suspicious or malicious devices. When Armis detects a threat, it can alert your security team providing added context about the device, it’s owner and even it’s physical location. Optionally, Armis can trigger automated policies in response to an attack. This helps reduce security team workload by providing otherwise difficult to obtain information, shorting the response time by days or even weeks.

Conclusion

The digital transformation in retail is already underway, as businesses look to find new ways to engage with customers while simultaneously driving productivity, operational efficiency, and increased revenue. That transformation comes with a new generation of managed, unmanaged and IoT devices designed to connect, but with no inherent security.

This transformation of retail places thousands of unmanaged devices in your stores and on your network at any given time. Those new security risks are real, especially with the advent of connected unmanaged and IoT devices. Designed to connect in an increasingly wireless world, IoT devices. Cybercriminals are already exploiting that fact.

Armis is the first agentless, enterprise-class security platform to address the new threat landscape that exposes any device on any network, including cellular IoT. Armis fills a massive gap, providing agentless security from the warehouse to the shelf and checkout aisle for the growing number of devices in modern retail. Armis security helps you fulfill the promise of the future of digital retail: to conduct business, attract customers, and manage resources faster and more efficiently.

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

armis.com

1.888.452.4011

20220412-1

ARMIS®