SOLUTION BRIEF

From the Warehouse to the Checkout, Armis Centrix™ is Empowering the Retail Industry with Complete Lifecycle Cybersecurity

Introduction

Operations in retail are changing, from warehouse logistics to the checkout experience, digitalization is on the rise. Retailers are increasingly adopting connected devices, Internet of Things (IoT) technologies, and cloud platforms to streamline processes, enhance customer service, and improve supply chain visibility. However, these innovations also bring new cybersecurity risks, expanding the attack surface and exposing vulnerabilities that could disrupt operations and compromise sensitive data.

The retail ecosystem, spanning from warehouses to store floors, is a dynamic and distributed environment where protecting all assets is essential to maintaining smooth, uninterrupted operations. To secure this vast landscape, retailers need a comprehensive, exposure management cybersecurity solution capable of safeguarding every aspect of their business, from inventory management systems to customer payment terminals.

Armis Centrix™ for OT/IoT Security is empowering retailers to do exactly that, offering complete lifecycle cybersecurity across IT, OT, IoT, and cloud platforms. With Armis Centrix™, retailers can maintain operational resilience, protect sensitive data, and secure every device — from the warehouse to the checkout.

Key Takeaways: Trends in the Retail Industry

Rising Cyber-Physical Threats

More connected devices in retail (IoT, POS) expand the attack surface, increasing cyber risks to both digital and physical assets.

Surge in Ransomware and Supply Chain Attacks

Ransomware and supply chain attacks disrupt retail operations by targeting logistics and critical systems.

Growing Compliance Pressure

Retailers face stricter data privacy regulations, needing strong security for customer data and cloud platforms to avoid fines and protect trust.

Expanding Attack Surface in Retail

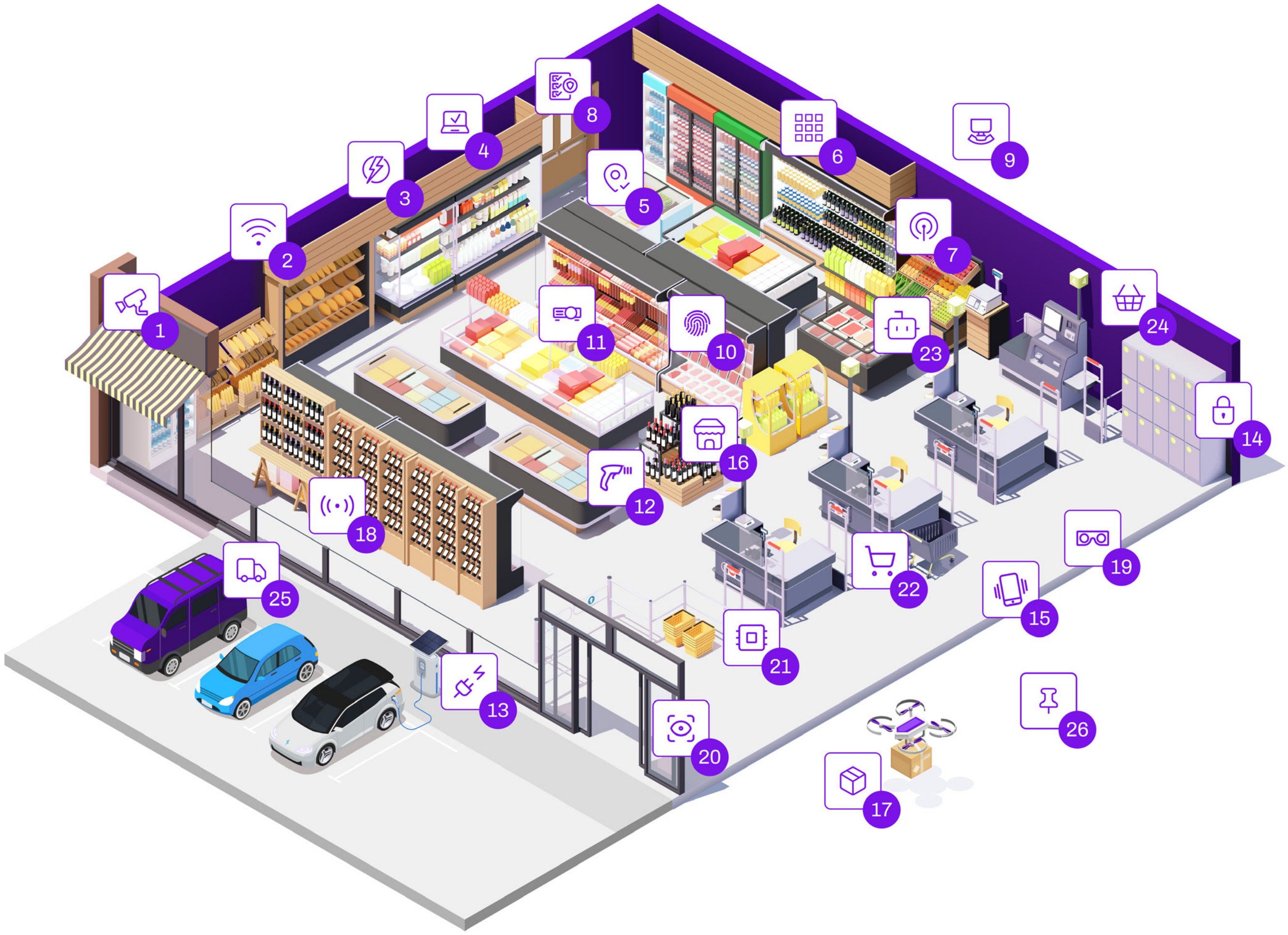
Retailers are adopting more connected technologies than ever before to stay competitive and efficient, but with that growth comes an increase in the attack surface. Every connected device, whether in a warehouse, a distribution center, or on the sales floor, becomes a potential entry point for cyberattacks.

The rise in cyber-physical threats targeting the retail industry, including ransomware, data breaches, and supply chain attacks, has only exacerbated the need for robust security measures. In 2023, the global average cost of data breaches in the retail sector was more than $4.73 million[1], with incidents affecting both IT and OT systems—disrupting operations and eroding customer trust.

These disruptions can have devastating consequences. A ransomware attack that locks a retailer out of its inventory system can result in delayed shipments and empty shelves. A breach in a POS system can expose sensitive customer payment data, damaging both reputation and the bottom line.

[1] IBM, 2024

The Retail Store of the future has infinitely more Attack Pathways



1 Video monitoring

2 Access points streaming video

3 IoT, HVAC energy monitoring system

4 Electronic menu board

5 In store, location-based services

6 Shelf-edge display

7 RFID gondola labels

8 Employee/manager dashboard

9 In-store back office

10 Biometrics contactless reader

11 Volumetric holographic interactive consumer display

12 Point-of-sale peripherals

13 Electric car charging stations

14 Pickup lockers

15 Consumer phones, NFC/RFID/BLE/WIFI

16 Holographic in-store kiosk

17 Drone delivery

18 IoT gateway & sensor fusion: proximity beacons and temperature and pressure sensors

19 Augmented reality lens/wearables

20 Smart mirror, facial recognition iris scan

21 Bottom of basket detection

22 Consumer phones, NFC/RFID/BLE/WIFI

23 Store robots

24 Self-service cashless checkout

25 Curbside execution BOPIS/ROPIS

26 Geo-fencing

Key Components that need Protection in Retail Environments

Sensing and Actuation

POS Systems: These devices handle billions of transactions daily, but they are also common targets for attacks that aim to steal credit card data or disrupt the customer experience.

Radio Frequency (RFID) Sensors and Barcode Scanners: These are integral to inventory tracking, generating valuable operational data but often overlooked from a security standpoint.

Control and Automation

Automated Checkout Systems: Self-checkout kiosks offer convenience but introduce vulnerabilities that need robust protection.

Warehouse Automation Systems: Robotic and automated systems used for order picking, packing, and shipping can be compromised, leading to operational shutdowns.

Data Management and Analytics

Customer Relationship Management (CRM) Systems: These store personal customer data and are attractive targets for hackers aiming to steal sensitive information.

Supply Chain Management Platforms: Connected supply chains allow real-time data sharing between retailers, suppliers, and logistics partners, but they also increase the risk of supply chain cyberattacks.

Networks and Integration

Cloud Platforms: Retailers are increasingly moving operations to the cloud, but with that shift comes data security and compliance challenges.

Warehouse Integration Systems: These platforms facilitate the seamless connection of inventory, logistics, and vendor management but must be protected to ensure uninterrupted supply chain operations.

Challenges in the Retail Industry

Securing POS Systems

Challenge: POS systems process millions of customer transactions daily, making them a prime target for cyberattacks aimed at stealing credit card data or inserting malware to disrupt operations.

Solution: Armis Centrix™ monitors and analyzes real-time activity across POS devices, identifying unusual behaviors that may indicate an attack. It automatically detects threats like unauthorized access, malware, or vulnerabilities, helping retailers protect customer data and maintain operational uptime.

Warehouse and Supply Chain Security

Challenge: Retail warehouses are increasingly automated with robotic systems, IoT devices, and connected platforms to manage inventory, shipments, and deliveries. Cyber threats targeting these systems can disrupt the entire supply chain.

Solution: Armis Centrix™ provides visibility and security across warehouse automation systems, monitoring connected devices like RFID sensors, automated packing robots, and inventory management platforms. It helps prevent ransomware or malware attacks that could shut down warehouse operations, ensuring uninterrupted fulfillment and supply chain continuity.

Protecting Self-Checkout and Kiosk Systems

Challenge: Self-checkout kiosks and other automated retail systems offer convenience to customers but also create potential security vulnerabilities. Cybercriminals may attempt to tamper with these systems, introduce malware, or extract sensitive customer data.

Solution: Armis Centrix™ secures self-checkout kiosks by monitoring for unauthorized access, detecting suspicious activities, and providing real-time alerts on potential security threats. It also ensures that kiosks are running the latest security patches and updates, reducing the risk of vulnerabilities being exploited.

Securing Remote Vendor Access

Challenge: Third-party vendors often need remote access to maintain or troubleshoot store systems, such as POS terminals or warehouse automation platforms. However, unsecured or overly permissive access can introduce vulnerabilities.

Solution: Armis Centrix™ ensures secure remote access by providing vendors with "just-in-time" access, allowing them to only access necessary systems for a limited time. It tightly controls and monitors remote access, reducing the risk of unauthorized entry or data breaches stemming from third-party interactions.

Inventory Management and Asset Tracking Security

Challenge: Retailers rely on technologies like RFID tags, barcode scanners, and IoT-enabled tracking systems to manage inventory in real time. These devices, however, can be exploited if not adequately protected, leading to potential theft, fraud, or operational disruption.

Solution: Armis Centrix™ ensures the security of inventory tracking systems by continuously monitoring connected devices for anomalies. It detects potential threats to these systems—whether through device tampering or network attacks—ensuring accurate, secure tracking and reducing the risk of inventory-related fraud or loss.

Cybersecurity for Digital Signage and Advertising Displays

Challenge: In-store digital signage and displays are often part of the store's network but may not receive the same level of cybersecurity attention as other critical devices. These can be targeted to spread malicious content or disrupt operations.

Solution: Armis Centrix™ monitors and protects digital signage and advertising displays, identifying vulnerabilities or unusual activity that could indicate a cyberattack. This ensures the security of promotional systems and prevents attackers from compromising these devices to disrupt marketing efforts or inject malware.

Ensuring Compliance with Security Regulations (PCI DSS)

Challenge: Retailers must comply with stringent data security regulations, such as PCI DSS, to protect cardholder information. Non-compliance can result in heavy fines and damage to the brand's reputation.

Solution: Armis Centrix™ helps retailers maintain compliance by continuously monitoring all connected devices for security risks, ensuring the protection of sensitive data. It also provides detailed reporting that can be used to demonstrate compliance with regulatory requirements, helping retailers avoid fines and regulatory action.

Preventing Ransomware Attacks on Critical Retail Systems

Challenge: Ransomware attacks targeting retail networks can lead to severe disruption, including the inability to process payments, access inventory, or run store operations.

Solution: Armis Centrix™ detects ransomware activity in real-time by monitoring for early warning signs such as abnormal file access patterns or suspicious encryption activities. By alerting security teams to potential threats early, Armis Centrix™ helps retailers prevent ransomware from taking hold of their systems and causing operational downtime.

Enhancing Customer Experience through Secure IoT Devices

Challenge: Retailers are using IoT-enabled devices like smart mirrors, digital fitting rooms, and customer engagement kiosks to enhance in-store experiences. However, these IoT devices are often vulnerable to cyberattacks.

Solution: Armis Centrix™ secures IoT devices by providing comprehensive visibility into their behavior, ensuring they operate securely without being compromised by cyber threats. This allows retailers to confidently deploy innovative customer experience solutions without introducing security risks.

Securing Cloud-Based Retail Platforms

Challenge: Many retailers are migrating critical business operations to cloud platforms, including inventory management, customer data, and point-of-sale systems. Ensuring the security of cloud infrastructure and data is essential.

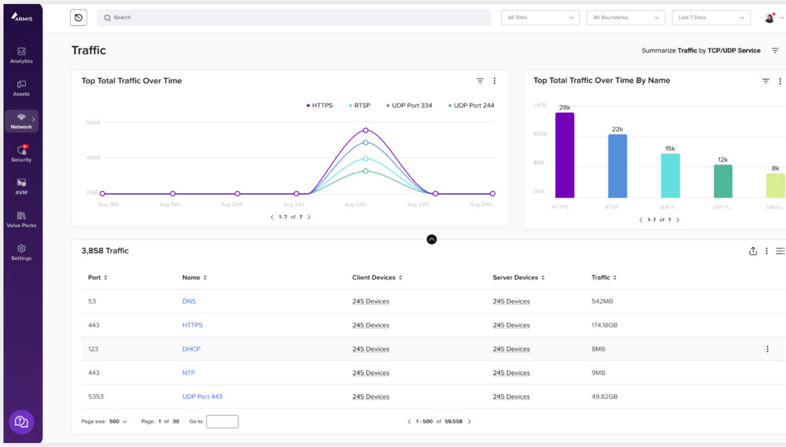
Solution: Armis Centrix™ protects cloud-based retail environments by monitoring all connected assets, providing insight into cloud configurations, and detecting vulnerabilities or misconfigurations that could expose data. This allows retailers to maintain secure cloud operations while taking advantage of scalable, flexible cloud technologies.

Armis Centrix™: Complete Lifecycle Cybersecurity for Retail

Armis Centrix™ is providing the retail industry with an end-to-end security platform that secures every aspect of the retail environment, from the warehouse to the checkout. Now, retailers can gain complete visibility into all assets, proactively detect threats, secure remote access, and manage all security findings efficiently.

Asset Visibility Across IT, OT, and IoT

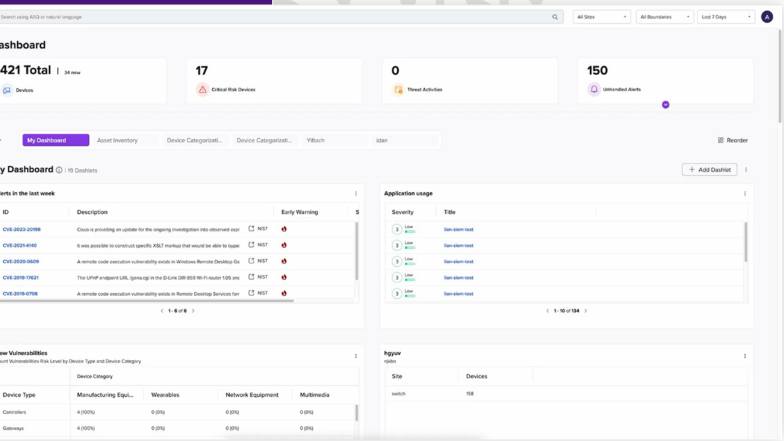
They lack real-time visibility into the assets and devices that comprise their operations. This “situational blindness” hampers their ability to maintain a clear compliance posture and understand the security status of each and every asset.



3,858 Traffic

Port	Name	Client Devices	Server Devices	Traffic
53	DNS	245 Devices	245 Devices	542MB
443	HTTPS	245 Devices	245 Devices	174.18GB
123	DHCP	245 Devices	245 Devices	8MB
443	NTP	245 Devices	245 Devices	9MB
5353	UDP Port 443	245 Devices	245 Devices	49.82GB

Page size: 500 Page: 1 of 30 Go to 1-500 of 59,558



lerts in the last week

ID	Description		Early Warning
CVE-2023-20198	Cisco is providing an update for the ongoing investigation into observed expl	NIST	🔥
CVE-2021-4140	It was possible to construct specific XSLT markup that would be able to bypa:	NIST	🔥
CVE-2020-0609	A remote code execution vulnerability exists in Windows Remote Desktop Ga	NIST	🔥
CVE-2019-17621	The UPnP endpoint URL /gena.cgi in the D-Link DIR-859 Wi-Fi router 1.05 anc	NIST	🔥
CVE-2019-0708	A remote code execution vulnerability exists in Remote Desktop Services forr	NIST	🔥

1-6 of 6

Application usage

Severity	Title
3 Low	ilan-siem-test
3 Low	ilan-siem-test
3 Low	ilan-siem-test
3 Low	ilan-siem-test
3 Low	ilan-siem-test

1-10 of 134

ew Vulnerabilities
unt Vulnerabilities Risk Level by Device Type and Device Category

	Device Category			
Device Type	Manufacturing Equi...	Wearables	Network Equipment	Multimedia
Controllers	4 (100%)	0 (0%)	0 (0%)	0 (0%)
Gateways	4 (100%)	0 (0%)	0 (0%)	0 (0%)

hgyuv
njkbn

Site	Devices
switch	158

Proactive Threat Detection and Real-Time Response

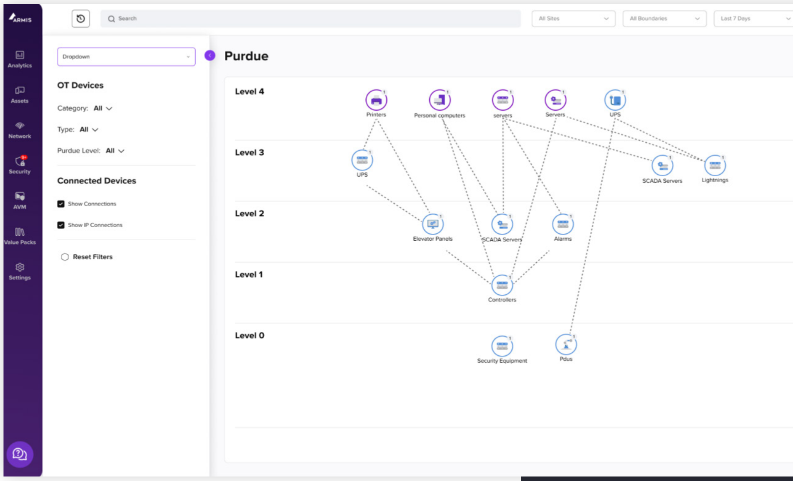
Armis Centrix™ uses advanced AI and machine learning to identify anomalies and detect cyber threats in real-time, allowing retailers to address security issues before they cause significant damage. From ransomware targeting supply chain systems to malware on POS devices, Armis Centrix™ offers fast, actionable intelligence to stop attacks in their tracks.

Secure Remote Access for Vendors

As third-party vendors often need remote access to maintain devices like automated checkout kiosks or warehouse management systems, securing these connections is vital. Armis Centrix™ provides granular, “just-in-time” remote access, ensuring that vendors only access what is necessary and when needed, without exposing the network to unnecessary risks.

Network Segmentation and Policy Enforcement

Armis helps retail organizations create and enforce network segmentation policies that protect critical systems. By providing comprehensive visibility into connected assets and their communications, Armis can segment or recommend network segmentation policies that are automatically enforced via existing firewalls and network access control (NAC) solutions. This ensures critical systems are isolated from potential threats, enhancing overall cybersecurity resilience.



Category: All

Type: All

Purdue Level: All

☑ Show Connections

☑ Show IP Connections

Risk Prioritization: Addressing Vulnerabilities and Security Findings in the Retail Industry with Armis Centrix™

Retailers face an overwhelming volume of security alerts across IT, OT, IoT, and cloud platforms, with no scalable way to effectively prioritize and address them. Armis Centrix™ offers a comprehensive solution that consolidates security findings from various sources and automates the prioritization process.

By integrating asset knowledge from complex retail environments—such as POS systems, automated checkout kiosks, and inventory management platforms—Armis Centrix™ leverages AI and machine learning to reduce alert volume and deduplicate findings. It contextualizes security issues with threat intelligence and assesses their operational impact, enabling retailers to prioritize fixes based on business significance and risk likelihood.

Armis Centrix™ also simplifies remediation workflows by streamlining ownership assignment, integrating with existing systems, and tracking progress through a consolidated dashboard. This ensures that retailers can address vulnerabilities efficiently, maintain operational uptime, and continuously improve their security posture across all connected assets.

Future-Proofing Retail with Armis Centrix™

As retailers continue to evolve their operations with digital transformation, cybersecurity must keep pace. From securing automated warehouses to protecting checkout systems, Armis Centrix™ delivers comprehensive lifecycle cybersecurity, empowering retailers to defend against modern threats while maintaining seamless, efficient operations.

With Armis Centrix™, retailers can safeguard their entire environment—from the warehouse to the checkout—ensuring operational resilience and protecting both business and customer data against ever-evolving cyber threats.

Trust Armis to protect your retail operations and learn more here.

Armis, the asset intelligence and cybersecurity company, Protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, Protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

To learn more or see a demo, contact us today.
Armis - armis.com/contact-us

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial