ARMIS®

WHITE PAPER

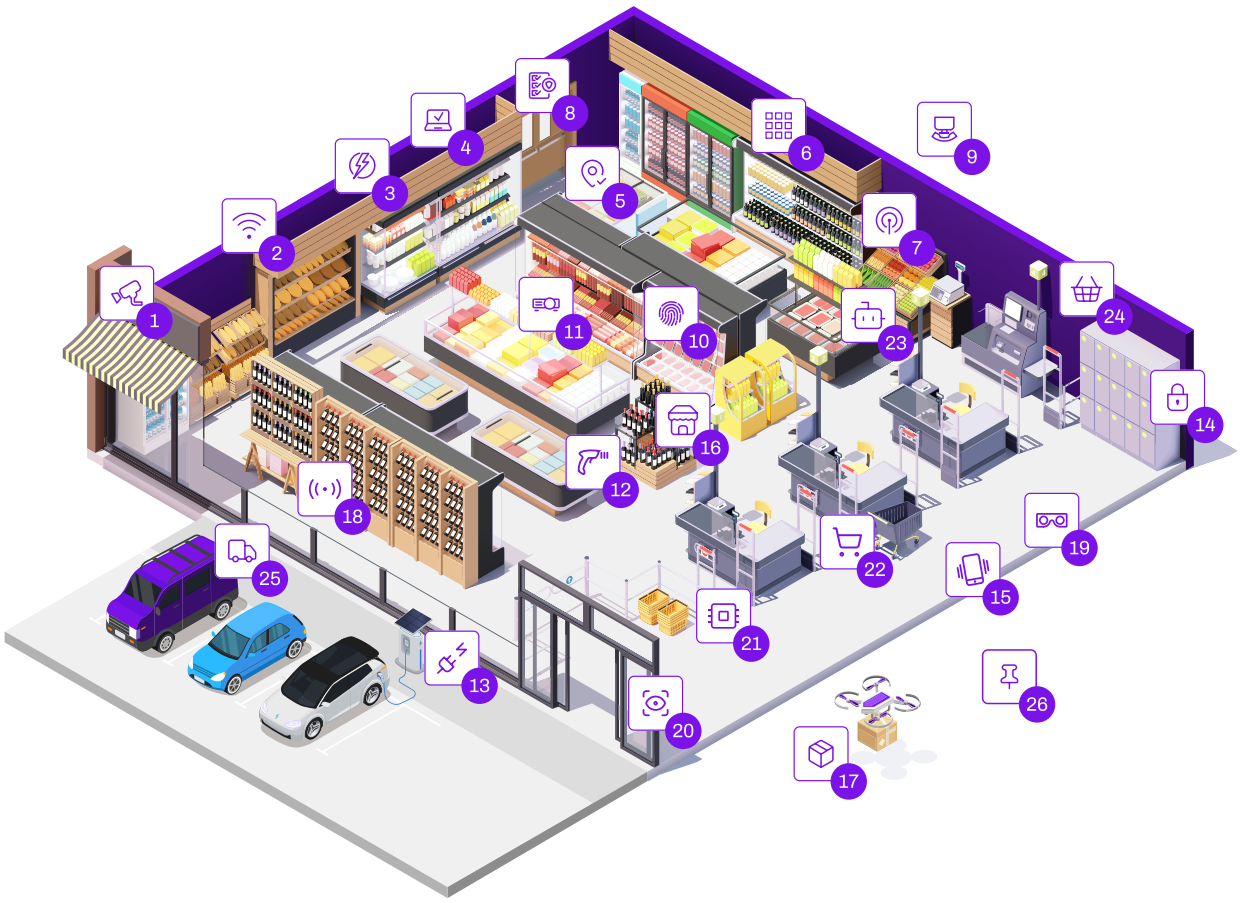
# Cyber Exposure Management for Modern Retail: Securing the Future of Connected Commerce

Digital transformation has redefined the retail landscape. From frictionless checkout and interactive signage to AI-powered inventory systems and mobile points-of-sale, retail organizations are embracing connectivity to enhance customer experiences and operational efficiency. However, this transformation introduces new risks: the growing presence of unmanaged, IoT, and cyber-physical systems (CPS) has created a massive, often invisible, attack surface. Traditional security tools were never designed for this reality.

Armis Centrix™ is the leading agentless cybersecurity platform purpose-built for this new era. We help the world's largest retailers gain complete visibility, continuous security, and real-time protection across every asset in every store, distribution center, and corporate office. This paper explores the modern risks retailers face and how Armis Centrix™ empowers retail organizations to secure every connected asset from warehouse to checkout.

# The New Retail Reality: A Vast, Unseen Attack Surface

Each asset type in a retail operation plays a unique role in the retail value chain, and together they form an interconnected digital infrastructure that must be continuously monitored and secured against emerging cyber threats. This ecosystem of digital assets range from smart self-checkout kiosks and mobile point-of-sale systems to Bluetooth-enabled barcode scanners, interactive displays, inventory robots, and shelf-scanning devices. Even behind-the-scenes infrastructure such as HVAC and energy management systems, networked security cameras, and remote vending machines connected via cellular networks contribute to this environment. These devices often operate outside of IT's visibility and cannot support security agents. Many evade network-based tools entirely, relying on non-IP protocols or separate communications methods. Each one presents a potential entry point for threat actors.



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

In 2023, a Fortune 500 retailer relied on Armis to uncover a rogue access point spoofing a Bluetooth beacon to intercept payment data. In another instance, a large retail chain used Armis to locate legacy Windows-based point-of-sale terminals still vulnerable to EternalBlue exploits, which had remained hidden from conventional vulnerability scanners.

# The Cyber Threat Landscape: Common Retail Exposure Attacks

Retail environments today are high-value targets for cybercriminals. Unlike traditional IT networks, retail networks are distributed, filled with diverse and often insecure devices, and dependent on rapid transaction processing and real-time connectivity. This makes them uniquely vulnerable to a wide array of cyber exposure threats.

In 2024, Armis Labs revealed that retail organizations faced an average breach cost of $5.1 million. Additionally, there was a 32% surge in attacks targeting IoT devices in retail environments. These statistics underscore the urgency for robust, modern security measures.

One of the most prevalent attack vectors is the exploitation of vulnerable point-of-sale (POS) systems. These systems, often running outdated software, have historically been exploited to steal payment card data using malware like BlackPOS or JackPOS. Equally concerning are Bluetooth-based attacks that target barcode scanners or beacons used in customer tracking—attackers can hijack these devices or spoof legitimate ones to conduct man-in-the-middle attacks.

Another increasingly common tactic involves ransomware campaigns that disable access to critical systems across a retailer's digital ecosystem. These attacks often originate through phishing emails, unsecured remote access points, or through lateral movement from poorly secured IoT devices like smart cameras, HVAC systems, or inventory scanners. Once inside, threat actors can encrypt entire store networks or distribution center operations, halting business and demanding multimillion-dollar payouts.

Supply chain compromises are another area of growing concern. Retailers often connect with third-party vendors and service providers for operations like vending machine management, digital signage, or energy systems. If these partners have poor cybersecurity hygiene, attackers can exploit their credentials or devices to pivot into the retailer's core environment.

Additionally, credential stuffing and account takeover attacks plague eCommerce portals and customer-facing applications. With access to customer data, attackers can impersonate legitimate users, conduct fraudulent purchases, or sell stolen data on the dark web; all while eroding brand trust and triggering regulatory scrutiny.

These exposures represent a modern, multifaceted attack surface that retailers must address holistically, across every layer of digital operations.

## Compliance Pressure Is Growing

Retailers are under increasing regulatory scrutiny. Compliance with PCI DSS version 4.0, which mandates stronger requirements for asset inventory, risk scoring, and segmentation, has become essential. Simultaneously, adherence to the expanded scope of NIST CSF 2.0 emphasizes continuous monitoring and comprehensive cyber exposure management. Adding to this pressure are state-level privacy laws that demand swift breach notification and stringent data protection. Meeting these requirements demands full visibility and control over all assets, not just traditional IT-managed systems.

## Why Traditional Tools Fail in Retail Environments

Retail environments have evolved into highly connected ecosystems that blend traditional IT infrastructure with a wide array of cyber-physical systems (CPS) and Internet of Things (IoT) devices.

One of the most significant limitations of traditional security tools is their reliance on software agents. However, in retail environments, many connected devices are agentless by design. They often run on proprietary operating systems, have limited processing capabilities, or are locked down by manufacturers, making it impossible to install traditional security agents.

Retail infrastructures are also highly dynamic and distributed. Devices are frequently added, replaced, moved between store locations, or temporarily disconnected. Traditional tools struggle to maintain accurate, real-time visibility in this type of environment. Unmanaged or unauthorized devices such as rogue Wi-Fi access points or consumer-grade plug-and-play peripherals can easily appear on the network without triggering any alerts, giving threat actors a pathway into the system.

In retail, not all devices are equal in terms of operational importance or business risk. A digital price tag going offline is far less critical than a smart freezer that stores temperature-sensitive pharmaceuticals or food. Traditional tools, however, often fail to recognize this distinction. Without deep contextual understanding, security teams are left reacting to alerts without insight into what truly matters, which leads to wasted effort and slower response times.

Traditional tools fall short in securing the broader retail supply chain, which now includes warehouses, cloud platforms, delivery logistics, and third-party service providers. The modern retail operation extends well beyond the four walls of a store, but most legacy security solutions were not designed to provide visibility or protection across such a wide and complex landscape. This creates additional exposure as attackers can target these external systems to gain access to the core retail network; a tactic seen in several recent, high-profile breaches.

## Key Steps For Reducing Cyber Risk - Right Now

Retailers are prime targets for ransomware, data breaches, and supply chain attacks due to the volume of consumer data they process and their reliance on uptime for operations. Fortunately, there are actionable steps retail organizations can take today to improve visibility, reduce cyber risk, and enhance resilience across all locations and endpoints. These steps involve understanding what assets exist, how they behave, and where risk is accumulating, so that threats can be identified, prioritized according to asset criticality and mitigated before they impact operations or customers.

# Strategic Cyber Exposure Management Checklist

Retailers can follow this checklist to implement a modern cyber exposure management program:

- **Establish full asset visibility** across all locations, including IT systems, IoT devices (e.g., smart cameras, sensors), cyber-physical systems (CPS like HVAC or refrigeration), and cellular-connected devices.
- **Maintain a real-time inventory** of all connected assets, enriched with contextual data such as device type, manufacturer, firmware version, operating system, location, and behavioral baselines.
- **Conduct continuous risk assessments** using dynamic scoring that combines vulnerability data, threat intelligence, exploitability, and observed device behavior to prioritize high-risk exposures.
- **Monitor devices and communications** for anomalies and deviations from known baselines to identify early indicators of compromise, rogue devices, or lateral movement within the network.
- **Automate threat response** through integrations with NAC, SIEM, EDR, firewall, and orchestration tools to isolate, quarantine, or block suspicious devices and contain threats in real time.
- **Align cybersecurity operations with compliance frameworks** such as PCI DSS 4.0 and NIST CSF 2.0, ensuring your organization maintains appropriate controls, auditability, and readiness for regulatory requirements.

> **Extend protection to third-party systems** such as vendor-managed services, cloud-based platforms, and unmanaged or remote infrastructure operating outside the traditional IT perimeter.

> **Harden physical retail environments** by monitoring digital signage, kiosks, surveillance systems, and payment infrastructure for security gaps or misconfigurations.

> **Test incident response plans regularly** to ensure your team is prepared to respond swiftly to breaches, ransomware attempts, or coordinated attacks across multiple stores or systems.

## Armis Centrix™ for Retail: Purpose-Built Cyber Exposure Management

Armis addresses these challenges through a comprehensive, agentless approach to cyber exposure management. The platform enables retailers to discover and monitor every connected asset in their environment, whether it is managed, unmanaged, IoT, or CPS. Armis provides a real-time inventory that includes hardware, firmware, operating systems, and behavioral context. This inventory extends across wired, wireless, and cellular networks, ensuring nothing is missed.

Through continuous risk and vulnerability assessment, Armis assigns real-time risk scores to devices based on observed behavior, known vulnerabilities, and threat intelligence. These scores are informed by contextual data, allowing security teams to identify the most critical risks and align mitigation strategies with industry standards like MITRE ATT&CK, NIST, and PCI.

Armis Centrix™ also excels in threat detection and automated response. Using its cloud-based asset intelligence knowledgebase, which tracks billions of behavioral traits across device types, Armis identifies anomalies in real time. When threats are detected, the platform can alert security teams with detailed context including device ownership and location, or initiate automated responses such as isolating devices or triggering segmentation policies through integrations with network access control systems, endpoint detection tools, and firewalls.

## Use Case: Securing the Store of the Future

A global retail brand launched next-generation stores featuring RFID-enabled smart shelves, mobile checkout systems, and AI-powered cameras for queue monitoring. With Armis, the retailer rapidly mapped and gained deep situational awareness on every connected asset within each store in less than 48 hours. The platform uncovered point-of-sale devices communicating with unauthorized international IP addresses and detected rogue Bluetooth tags mimicking loyalty program beacons. By integrating Armis with their NAC and SIEM systems, the retailer automated incident response and significantly improved operational resilience. As a result, their mean-time-to-response improved by 83%, and the time required for compliance audits dropped by 60%.

# Conclusion: Unlock Digital Innovation, Without the Risk

The future of retail hinges on secure digital transformation. Armis Centrix™ equips retail security and operations teams with complete asset visibility, continuous risk assessment, rapid threat detection, and prioritized & automated response capabilities. These foundational pillars not only protect customer data and critical systems but also enable compliance with evolving regulatory frameworks. Whether securing ten stores or ten thousand, Armis provides the cyber exposure management capabilities retailers need to protect every transaction, interaction, and innovation.

**Armis: From warehouse to checkout, protect the future of retail.**

**Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.**

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. 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.

1.888.452.4011


**Website**

Platform
Industries
Solutions
Resources
Blog

**Try Armis**

Demo