Cybersecurity for Retail: The new edge of customer experience

Retail

Forces reshaping Retail

The retail world has always been built on connection, the instinctive, immediate exchange between people and products. Today, that connection runs on technology. Customers browse, buy and return across apps, kiosks and marketplaces; warehouses run on automation, sensors and algorithms. Every moment of convenience becomes an opportunity — and an entry point.

As retail accelerates into an AI-driven, omnichannel era, cybersecurity becomes more than an IT requirement. It becomes the foundation of trust, reputation, continuity and seamless customer experience.

Forces reshaping Retail

Artificial Intelligence (AI) in every part of the value chain

From demand forecasting to hyper-personalization, AI now powers assortment planning, inventory optimization, fraud detection and customer engagement.

Hyper-personalized experiences

Generative AI and real-time pricing reshape customer journeys while retail media ecosystems expand rapidly.

Smart warehouses and stores

Autonomous robots, computer vision, smart shelves and cashierless experiences bring efficiency and new attack surfaces.

Seamless omnichannel operations

Unified commerce, item-level RFID and distributed order management blur the boundaries between digital and physical retail.

Together, these forces are propelling retailers forward at high speed and raising the stakes of every digital decision.

100% +

increase in retail cyber incidents between 2023 and 2025

64%

of retail cyber incidents are caused by human error

Expanding the retail experience without expanding the risk

More convenience, personalization and seamless movement between channels, but growth only works when the systems behind it stay secure, available and compliant. Retailers face three core imperatives:

Keep the customer experience frictionless and safe

Customers expect instant, secure interactions across every channel, from mobile checkout to in-store payments. Any interruption damages trust immediately.

What retail needs: Always-on, tamper-resistant, fraud-aware digital touchpoints that customers never have to think twice about.

Maintain resilient operations across a sprawling retail network

Retail infrastructures span warehouses, branches, HQ systems, logistics hubs and cloud platforms. Complexity is powerful but fragile.

What retail needs: A unified, centrally managed digital backbone that stays stable, scalable and secure regardless of location or traffic.

Automate with confidence as AI and robotics scale across the value chain

Automation drives modern retail, from smart shelves and robotics to AI-driven inventory and forecasting, but it expands exposure.

What retail needs: Secure automation where innovation is never slowed by hidden vulnerabilities, insider risks or supply-chain weaknesses.

How Kaspersky protects Retail

We've spent decades tracking how attacks unfold across sprawling retail networks, from warehouses to POS terminals to cloud-native e-commerce stacks. Our approach builds more than protection: it builds continuity, trust and the freedom to innovate:

Protecting your infrastructure from sophisticated attacks

What's at stake: Sophisticated attacks can cause significant harm to companies: from data breach to extended downtime.
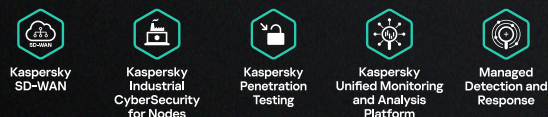
What this means for you: Retailers should deploy a complex approach to cybersecurity, protecting the internal and external perimeter of the company to stay ahead of threats — and the competition.

- Kaspersky Next XDR Expert
- Kaspersky Anti Targeted Attack
- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Threat Intelligence
- Managed Detection and Response

Helping you manage complex and distributed infrastructures

What's at stake: The growing retail footprint expands your attack surface and creates gaps that attackers can exploit.

What this means for you: Centralized, unified security to keep every branch, warehouse and cloud workload protected — and running without interruption.

- Kaspersky SD-WAN
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Penetration Testing
- Kaspersky Unified Monitoring and Analysis Platform
- Managed Detection and Response

Protecting your perimeter from supply chain attacks

What's at stake: Partner and supplier systems are often less secure, giving attackers indirect access to your environment.
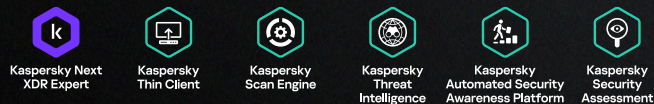
What this means for you: You need strong visibility and threat detection across all third-party connections to prevent attackers entering through trusted channels.

- Kaspersky Next XDR Expert
- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Anti Targeted Attack
- Kaspersky Threat Intelligence
- Kaspersky Incident Response
- Managed Detection and Response

Protecting your organization against insider attacks

What's at stake: Human actions and error drive most retail incidents, from phishing to misuse of access.
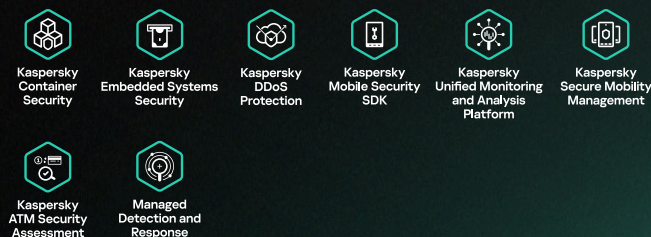
What this means for you: Regular training, monitoring and fast detection help reduce employee-driven risks and strengthen overall protection.

- Kaspersky Next XDR Expert
- Kaspersky Thin Client
- Kaspersky Scan Engine
- Kaspersky Threat Intelligence
- Kaspersky Automated Security Awareness Platform
- Kaspersky Security Assessment

Supporting payment transaction continuity

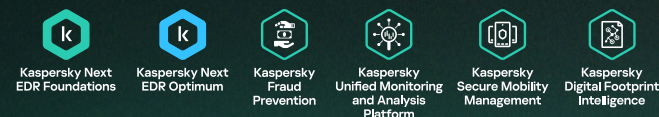**What's at stake**: PoS malware and DDoS attacks can disrupt payments, hitting revenue and customer trust.

What this means for you: Standards-aligned controls and specialized payment protection keep transactions secure and uninterrupted.

- Kaspersky Container Security
- Kaspersky Embedded Systems Security
- Kaspersky DDoS Protection
- Kaspersky Mobile Security SDK
- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Secure Mobility Management
- Kaspersky ATM Security Assessment
- Managed Detection and Response

Protecting your customers' personal data

What's at stake: Data breaches trigger major financial penalties and damage trust and reputation.

What this means for you: Strong detection, secure device management and consistent data controls help you stay compliant and protect customer information.

- Kaspersky Next EDR Foundations
- Kaspersky Next EDR Optimum
- Kaspersky Fraud Prevention
- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Secure Mobility Management
- Kaspersky Digital Footprint Intelligence

How Retail can build resilience against cyberattacks

A comprehensive, long-term strategy that equips people, strengthens processes and fortifies technology across the retail footprint.

Preparation
Audit

Audit infrastructure, assess risks and identify vulnerabilities across stores, warehouses, data centers and cloud environments.

Technologies
Solutions

Equip in-house teams with powerful tools for detection, investigation, response and prevention integrated across all digital channels.

Knowledge
Training and analytics

Strengthen security culture with awareness training, advanced analyst development and up-to-date threat intelligence.

Expertise
Services

Bring in specialists for penetration testing, compromise assessment, SOC maturity improvement and incident response.

Secure the future of Retail

Retail is entering an era of AI-driven commerce, hyper-personalized experiences and borderless omnichannel journeys. With it comes a new era of risk. The retailers that will thrive are those that treat cybersecurity not as infrastructure but as a competitive advantage powering trust, resilience and growth.

Secure your Retail future now

Learn more

#kaspersky
#bringonthefuture