

AI in Retail: Rapid Growth and Rising Security Stakes



AT-A-GLANCE

Key Findings from the ThreatLabz 2026 AI Security Report

Retail runs on data, from how customers shop to how inventory and orders move between stores, e-commerce platforms, and distribution centers. Artificial intelligence (AI) is helping retail organizations turn that data into faster insights, automated decisions, and operational continuity. While AI-enabled functions and operations yield clear business value, they also amplify cyber risk. The **ThreatLabz 2026 AI Security Report** highlights just how quickly AI adoption is advancing across retail and why securing it is essential.

Retail AI activity surged **193% year over year**

AI transactions from the Retail & Wholesale sector increased **193%**, reaching **49 billion AI/ML transactions in 2025** and making up 5% of enterprise AI activity observed in the Zscaler cloud. Growth at this pace shows that AI is becoming part of routine retail business operations. Across the industry, organizations are expanding AI use in areas such as customer engagement, personalization, and inventory management.^{1,2}

At the same time, Retail & Wholesale accounted for just 2% of all blocked AI/ML transactions in the Zscaler cloud. Because a relatively smaller share of retail AI is restricted, more data and systems are vulnerable to AI-driven access, expanding the sector's attack surface and increasing opportunities for exploitation.

¹ <https://www.businessinsider.com/how-major-retailers-using-ai-shopping-experience-2025-11>

² <https://www.businessinsider.com/walmart-target-use-ai-to-prevent-inventory-shortages-2025-6>



Risks amplified alongside AI transformation

The interconnected nature of retail environments that links stores, distribution centers, e-commerce platforms, SaaS applications, and partner systems creates a large digital attack surface.

As AI is embedded in these environments and interacts with enterprise data and systems, it amplifies the security risks retail organizations must manage, including:

Unauthorized data disclosure through AI tools and prompts:

Ungoverned prompts and access controls in public/SaaS AI applications risk exposing sensitive customer and inventory data, complicating the continuous reporting required for due diligence.

Attack surface expansion through AI integrations: Connections between AI tools and retail SaaS, fulfillment, and payment platforms extend trust relationships and create additional pathways into enterprise environments.

Over-privileged AI assistants: AI agents integrated with customer service or operations often inherit permissions to sensitive systems, such as point-of-sale and inventory databases, allowing them to retrieve data or trigger operational actions if compromised.

AI-powered social engineering: Generative AI also enables threat actors to scale highly convincing phishing and deepfake attacks that steal credentials and provide entry into e-commerce platforms, payment systems, and supplier portals.

Several of these common attack vectors, vulnerabilities, and real-world attack scenarios are explored in the [ThreatLabz 2026 AI Security Report](#).



Securing AI across retail operations

Retailers need visibility and control over how AI systems access enterprise data and connect to business systems. Zscaler's unified platform for AI security empowers retail organizations to safeguard every aspect of their enterprise AI lifecycle.

With Zscaler in place, retailers can:

- **Protect sensitive customer and payment data** using unified DLP, CASB, and inspection powered by Zscaler AI across web, SaaS, cloud, and endpoints.
- **Control AI access to business systems** by enforcing least-privileged access and continuously verifying users, devices, and AI-enabled workflows.
- **Reduce the attack surface created by AI agents and third-party integrations** through inline inspection, and use posture management to identify misconfigurations and risky sharing.
- **Provide continuous evidence of control efficacy**, and support enhanced security posture with centralized visibility into data flows, encrypted traffic inspection, and policies aligned to PCI DSS, GDPR, and CCPA requirements.
- **Adopt AI confidently by securing AI workflows** without slowing innovation across distributed environments, simplifying your security stack and eliminating tool sprawl.



Learn more about the latest enterprise AI adoption trends, AI-powered threats, and security guidance for retail organizations in the **ThreatLabz 2026 AI Security Report**.

[Read Now](#)

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at zscaler.com or follow us on Twitter [@zscaler](https://twitter.com/zscaler).

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.com



**Act Fast.
Stay Secure.**