End-to-End AI Governance & Security for Retail

AT-A-GLANCE

AI Security Benefits for Retail

MITIGATE AI-ENABLED DATA LOSS
Enforce approved GenAI tools and tenants, and block PCI or other sensitive data prompts to unsanctioned GenAI.

BLOCK AI-DRIVEN ATTACKS
Inspect all traffic inline to detect and block phishing, malware and C2 attacks. Block or isolate high-risk GenAI apps or sites used for data exfiltration and prompt-based abuse.

GOVERN AI AT SCALE
Identify AI apps, agents and connectors (including shadow AI) to find vulnerabilities such as over-permissioned access, public links or misconfiguration. Generate audit-ready reporting for compliance with PCI DSS and other regulations.

ENSURE OPERATIONAL CONTINUITY
Deploy a cloud-native platform that secures AI innovation without the latency of legacy stacks, ensuring your systems remain resilient and available even during peak shopping period.

Enable AI across stores, omnichannel, and supply chain

Retail AI is accelerating. From customer service agents and associate copilots to personalization and supply chain planning, retailers are increasingly relying on AI-driven workflows and integrations to power their operations.

AI expands the attack surface from simple networks to a complex ecosystem of identities, data, prompts, APIs, third parties, and AI connectors. Expanded attack surface increases the risk of data leakage, abuse, and business disruption.

Zscaler helps retailers adopt AI confidently by securing AI usage end-to-end; discovering shadow AI and risky integrations, controlling data leakage and loss, and defending AI interactions inline.

Why Zscaler for AI Security

FULL AI LIFECYCLE
AI Security from discovery through deployment

UNIFIED PLATFORM
Proven platform integrates AI Security with Zero Trust

PROVEN PARTNER
Expertise in customer success and transformation

Retail AI Risks — How Breaches Can Happen

Prompt Data Leakage: An employee or partner in customer support, fraud review, or marketing pastes Personal Data, an order record, or even customer PCI information into an unsanctioned GenAI, leading to possible data exposure, regulatory risk, and higher breach probability—jeopardizing customer trust.

Malicious Prompts: Attackers manipulate a customer service chat bot on a website or in-app with a malicious prompt to reveal order or account information, leading to data exposure, unauthorized transactions, account takeovers, legal risks, and damaged brand reputation.

Risky AI Connectors & Plugins: A connector is set up with too broad permissions, risking misuse or malicious prompts and overexposure of sensitive data. Alternatively, a connector accesses internal systems, such as CRM, ERP or WMS, using credential or token access which can be stolen through phishing or malware. This allows attackers to pull data or trigger actions often without tripping traditional "perimeter" alarms.

Agentic Scraping & API Abuse: APIs supporting ecommerce and omnichannel experiences can be scraped by bad actors for pricing or competitive information, or to extract sensitive data unintentionally returned by the backend. High volumes can also hammer systems, leading to failed checkouts and downtime during peak shopping seasons.

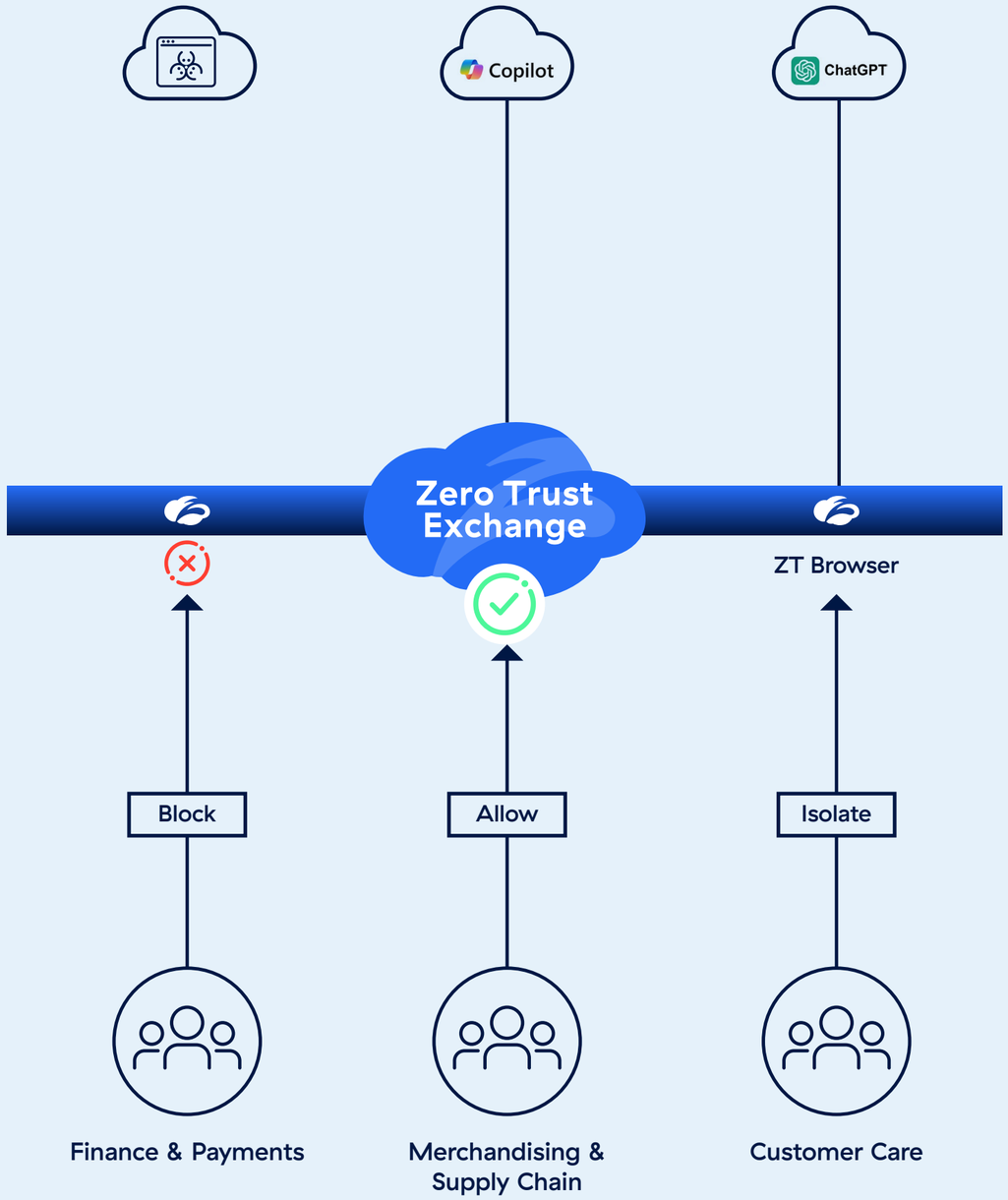
Key AI Security Solutions

DISCOVER AI ASSETS AND RISKS

Discovering your full AI footprint is challenging in the fast-paced environment required by retail operations. Shadow AI can exist across store operations, customer care, merchandising, supply chain, and in the growing number of connectors and agents. Zscaler AI-SPM provides full visibility into your AI ecosystem, including GenAI apps (whether sanctioned or unsanctioned), LLMs/models and AI services, as well as connectors/MCP servers and pipelines, so your team can identify any exposures involving sensitive data, customer records, or supplier and contract data. Faster containment of shadow AI reduces the risk of unknown data paths that can compromise your business operations, while eliminating the "human tax" of manually tracking and securing unmanaged AI sprawl across your enterprise.

SECURE AI ACCESS

Retailers need AI innovation to stay competitive, but controlling access and ensuring security for GenAI SaaS applications is increasingly complex. Enable AI without compromising sensitive or trade data. With secure AI access you can restrict GenAI users to approved tenants and tools (by user, role and location) and apply granular controls to govern which users or apps can interact with AI tools. Leverage DLP protection or isolation to contain and control data loss and enforce content moderation aligned to brand guidelines, legal requirements, and other corporate acceptable use policies.



INLINE PROTECTION

AI traffic is now a high-value target and LLMs can become a dangerous new vector for threats and data loss. Without high-performance inline inspection of these connections, retailers are vulnerable to data exposure, compromised systems, and malicious threats. Zscaler AI Guard can deliver high-performance inline inspection of AI prompts and interactions, detect risky threats like prompt injections and jailbreaking, prevent sensitive data loss, and moderate content to enforce safe usage and acceptable use policies. Built on the expertise of a trusted leader in inline inspection, Zscaler ensures robust protection for your critical AI traffic.

AUTOMATED RED TEAMING

Retail AI changes fast, especially when prepping for peak shopping seasons, and AI agents on the edge for omnichannel or storefront use cases could risk unsafe actions and data exposure. Testing AI systems for vulnerabilities can be a complex and time-intensive process, particularly if your organization does not have dedicated Red Team resources. Zscaler's Automatic and Continuous Red Teaming addresses these challenges with an innovative, automated red teaming engine that includes over 25 predefined probes, support for fully custom probes and dataset uploads tailored to your policies and risk scenarios. Enable continuous testing to discover disclosure and manipulation risks for remediation before production impact.

GOVERNANCE, COMPLIANCE & DATA PROVENANCE

As retailers scale AI, governance must keep up with the pace of AI innovation. Without proper oversight retailers risk exposure to legal, financial, and reputational harm to their brand. With Zscaler's approach to AI Governance you can automate compliance monitoring. Enable your team to prove control and due care by providing key audit-ready evidence for PCI DSS and other regulatory standards. Help mitigate risk, maintain operational integrity, and avoid negative impacts to brand and customer loyalty. Plus, gain continuous assurance and automated reporting, via Risk360™ Gen AI Reports, on the provenance of data used to train and interact with AI models to meet emerging global standards (like the EU AI Act), and improve regulatory agility and velocity.

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**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Act Fast.
Stay Secure.