SOTI RESEARCH

Commerce Under Attack: Protecting Retail — the Most Targeted Industry

Introduction

In 2024, global web application and API attacks surged to 311 billion, a 33% year-over-year increase, driven by cloud adoption, microservices, and AI-powered applications.

Commerce — encompassing both online retailers and brick-and-mortar stores — bears the brunt of this storm, with physical retail stores at particularly high risk. Commerce faced more than 230 billion web attacks from 2023 to 2024 — more than 40% of all global attacks and nearly triple those against high technology, the next most targeted industry. As retailers prepare in advance for the Black Friday to Christmas rush, robust security is critical to protect revenue and customer trust.

The scale of retail cyberattacks: By the numbers

It's no surprise that retail is particularly vulnerable. Retail operations maintain complex digital ecosystems with initiatives that often prioritize speed to market over extensive security — and relying on third-party suppliers creates numerous points at risk of compromise.

The most concerning attack vectors targeting retail include:

Web application attacks

64.25% of attacks targeted customer-facing systems, risking personal and payment data

API vulnerabilities

Commerce API attacks exceeded all other industries combined, threatening inventory, payments, and customer data

Layer 7 DDoS attacks

4.8 trillion attacks from 2023 to 2024 disrupted operations during peak periods

Bot attacks

There was a 137% spike in AI-driven bot fraud attacks in January 2024, with bots serving as enablers for broader attack campaigns

Case study

Ecommerce API abuse

In Q1 2025, an ecommerce company's SMS API that lacked proper authentication was exploited using multiple IP addresses and random mobile numbers. Attackers registered fraudulent numbers and sent SMS messages that sustained unexpected charges via the SMS gateway (often referred to as a leaky faucet attack), causing financial and reputational damage. This highlights the need for robust API security.

Evolving threats in retail

With technologies like AI advancing rapidly, new attack methodologies continue to emerge that specifically target retail vulnerabilities.

AI-powered attacks: Threat actors now use AI tools to scan retail APIs, pinpoint unique vulnerabilities, and create custom attacks designed specifically for each target's weaknesses.

Automated attack scaling: Cybercriminals can automate the entire attack process, significantly reducing the time and effort needed to identify and exploit security weaknesses in retail systems.

Year-over-year intensification: Global web attacks increased 33% year over year, with commerce bearing the largest share of this growth.

AI-driven escalation: Web attacks on commerce surged more than any other sector, making up the biggest share of the 33% year-over-year spike.

Regional attack patterns

Asia-Pacific (APJ)

- 18 billion web attacks, 18% of attacks targeted APIs
- Layer 7 DDoS attacks on APIs: 16%

Europe, the Middle East, and Africa (EMEA)

- 54 billion web attacks, 63% targeting APIs
- Layer 7 DDoS attacks on APIs: 43%

Latin America (LATAM)

- 17 billion web attacks, 11% targeting APIs
- Layer 7 DDoS attacks on APIs: 21%

These regional variations have significant implications for global retailers that prepare security measures across different markets. EMEA's high concentration of API-targeted attacks suggests that retailers should prioritize API security measures, while LATAM and APJ's lower API targeting necessitates a more diversified attack approach in their markets.

Preparing for peak season

Security tools alone won't protect your business during the holiday rush. Retailers must prepare for the scale and intensity of holiday traffic months in advance of Black Friday and winter holiday shopping.

Stress testing and capacity planning

Simulate real-world conditions: Test your website and everything connected to it by running load testing simulations that mirror expected Black Friday traffic, including sudden spikes and sustained high volumes.

Plan for traffic surges: Treat the winter holiday season as a prolonged high-traffic event rather than as isolated peak days. These days, customers start shopping earlier and promotional periods run longer, requiring sustained readiness from early November through January.

Traffic management and user experience

Set up waiting room capabilities: When traffic suddenly spikes beyond capacity, intelligent queue management systems can control user volume. These systems prevent site crashes while improving the customer experience.

Enhance omnichannel integration: Features like "buy online, pick up in store" and third-party logistics integrations see the highest growth during peak seasons. Make sure these integrations are functional, optimized, and secure.

Disaster recovery and business continuity

Plan for holiday-level recovery: Standard disaster recovery time frames may not be sufficient during peak season, when every hour of downtime costs serious revenue. Test your backup systems for holiday traffic levels.

Monitor what matters most: Use real-time monitoring to track technical performance and business metrics. When problems arise, retailers need to quickly understand what's broken and how it's impacting sales.

Retail security action plan

Now that you're prepared operationally, here are the security controls that are essential to implement across your retail infrastructure.

API security essentials

- [ ] Implement security from design to production
- [ ] Enable continuous discovery to identify shadow and zombie APIs
- [ ] Deploy real-time threat detection and monitoring
- [ ] Enforce authentication and authorization protocols
- [ ] Cache critical API responses (pricing, shipping) for peak performance
- [ ] Ensure compliance with PCI DSS v4.0.1 and DORA requirements

Bot defense strategy

- [ ] Use behavioral analysis to distinguish customers from bots
- [ ] Manage good bot activity so known bots don't negatively impact production
- [ ] Apply rate limiting during product launches
- [ ] Monitor for and block malicious bots that attempt scalping, scraping, and inventory hoarding

Distributed denial-of-service (DDoS) protection framework

- [ ] Install Layer 7 DDoS protection
- [ ] Review subnets and IP spaces for efficient protection deployment
- [ ] Configure alerts for high traffic volumes and pattern deviations
- [ ] Address DDoS attacks against web applications, network segments, and DNS infrastructure independently
- [ ] Configure content delivery network (CDN) caching for traffic spikes
- [ ] Test DDoS response plans before peak seasons
- [ ] Establish traffic baselines to quickly identify anomalies

AI-ready defenses

- [ ] Deploy AI-powered tools to detect evolving threats
- [ ] Protect systems using large language models (LLMs) from input and response abuse
- [ ] Assess vulnerabilities in AI-connected systems
- [ ] Implement Zero Trust models for APIs
- [ ] Adopt tools to defend against attacks that are unique to AI applications

Smart segmentation strategy

- [ ] Map critical assets (ecommerce platforms, payment systems, customer data)
- [ ] Apply microsegmentation to reduce attack surface and prevent lateral movement
- [ ] Implement software-defined segmentation strategies for observability and more granular control of lateral communication
- [ ] Implement Zero Trust principles for workload segmentation
- [ ] Consider Zero Trust Network Access (ZTNA) principles for users and for management of these environments

Performance optimization

- [ ] Cache frequently accessed API responses (pricing, shipping quotes) to maintain responsiveness
- [ ] Review and optimize caching settings for dynamic and static content
- [ ] Optimize images and video for faster load times
- [ ] Plan graceful degradation for noncritical features during peak loads
- [ ] Implement synthetic monitoring to catch issues before customers do
- [ ] Use unified logging to quickly correlate metrics during incidents

Postseason review

- [ ] Conduct a postmortem analysis to identify lessons learned
- [ ] Document operational gaps and automation opportunities
- [ ] Capture insights for better planning next season

Be prepared for every season

Attacks on commerce are massive in scale and growing in sophistication, which is no surprise given the industry's valuable customer data and direct financial incentives for attackers. However, with proper planning and modern security measures, you can protect your business and customers year-round.

Beyond implementing these security measures, you should assess the capacity and expertise of your internal security teams. During peak seasons when attack risks are highest, consider partnering with external security experts to supplement your internal capabilities.

Visit Akamai's retail security hub to learn more about our complete suite of retail-specific protections, including Akamai API Security, Akamai Bot Manager, and Akamai App & API Protector, that safeguard the world's largest retailers.

You can find additional details in Akamai's State of the Internet (SOTI) report: State of Apps and API Security 2025.