Strengthen retail security with dynamic zero trust architecture

Protect your omnichannel retail environment from evolving cyberthreats while enhancing customer experiences through modern security approaches

- Two out of three retailers were attacked by ransomware in 2022
- More than half of insider threats are caused by negligence

Source: Ponemon Institute, *Cost of Insider Threats Global Report*. (2022)

The retail industry faces growing security challenges as business models evolve to embrace omnichannel experiences. With supply chain disruptions, technology innovations, and expanding customer engagement channels, retailers must now connect customers with supplier data while allowing employees broader access to information resources. This environment, often leveraging partners and managed service providers, makes traditional perimeter-based security insufficient.

Defend against sophisticated cyberthreats across all endpoints

As ransomware, malware, fraud, and theft attacks grow in both number and sophistication, retailers need robust protection for their numerous endpoints. Zero trust architecture assumes nothing should be trusted by default, requiring strict authentication and authorization for each specific action or resource. This approach prevents unauthorized access and lateral movement even if initial breaches occur, protecting both physical and digital retail environments.

Meet expanding regulatory requirements for customer data protection

With increasing volumes of customer data being collected and processed, retailers must comply with regulations like GDPR and CCPA. Zero trust security segments sensitive data, ensuring only authorized personnel can access it while monitoring all interactions. This comprehensive approach safeguards customer information, builds trust, and protects your brand reputation—boosting customer loyalty and stakeholder confidence.

Simplify security across hybrid and cloud environments

Zero trust architecture often delivers greater simplicity and cost savings than expected. By consolidating disconnected technologies and replacing expensive legacy systems with more streamlined solutions, retailers can achieve better protection with lower overhead. This approach is particularly valuable for cloud environments where traditional perimeter defenses don't apply, providing consistent protection regardless of where services are located.

Enhance customer experiences through trusted personalization

When customers trust their sensitive information is being handled securely, retailers can deliver more personalized experiences. Zero trust enables flexible authentication methods including biometrics, voice recognition, or geolocation, while demonstrating to consumers that their privacy is protected. These capabilities, combined with self-service options and immediate threat response, create both security and satisfaction.

OpenText helps retailers build robust zero trust frameworks that ensure identity validation and dynamically managed access. As traditional security approaches fall short in today's environment of distributed users, multiple applications, and varied devices, our solutions centralize policy management and automate enforcement to close security gaps and simplify compliance. This comprehensive approach protects your business while enabling the seamless customer experiences required for retail success.

opentext™