aptos

Retail Under Siege: 5 Strategies Every Store Needs Now

How to Shield Your Enterprise from Cyber Threats Targeting Retailers

Retail cyberattacks are surging, with vulnerabilities jumping over 50% from last year alone[1]. The fallout is severe: breaches cost retailers millions in direct losses while eroding customer trust that drives long-term success.

Critical Impact: Consider that **58%** of consumers lose faith in companies after a breach, and **70%** will abandon the brand entirely[2].

With both profit margins and customer loyalty on the line, cyber resilience isn't optional. It's essential. Here are five critical steps to fortify your retail business against digital and physical security threats.

1 Build systems that bounce back

Create redundant infrastructure with cloud-based backups and automated failover systems that keep your stores running during attacks and enable rapid recovery.

Reality check: The average cost of a data breach reached $4.88 million last year, the highest average on record[3].

2 Turn employees into security champions

Empower associates to become your strongest defense with regular cybersecurity training, simulated phishing exercises and clear data handling protocols.

Wake-up call: 95% of successful cyberattacks start with human error[4]. Trained retail teams can prevent 19 out of 20 potential breaches[3].

3 Control who sees what and when

Give each employee exactly the system access they need through role-based permissions, multifactor authentication and session timeouts to minimize your attack surface.

Internal risk revealed: 83% of organizations reported insider attacks last year[5].

4 Deploy smart security that thinks ahead

Invest in next-generation AI and automation technologies that identify attack patterns, isolate threats and respond faster than manual security processes.

Proactive payoff: Organizations that applied AI and automation to security prevention saved an average of $2.22 million compared to those that didn't[3].

5 Partner with security-first vendors

Choose tech providers who embed security into their development process and maintain industry-leading standards with continuous monitoring.

Vendor reality: The cost of a third-party cyber breach is typically 40% higher than the cost to remediate an internal one[6].

aptos

Aptos ONE: Security-first POS

When cyber threats target retail stores, Aptos ONE POS serves as your strongest line of defense. Our security-first architecture protects your stores, transactions and customer data through comprehensive measures built into every layer of our solution. We maintain vigilant protection with vulnerability scans every four hours, annual penetration testing by certified professionals and enterprise-grade anti-virus coverage.

Our rigorous compliance with industry standards is verified through regular third-party audits with full transparency available at trust.aptos.com. Through always-on monitoring that combines automated threat detection with intelligent analysis, we identify and neutralize suspicious activities before they escalate into costly breaches, safeguarding both your profits and reputation with resilient, secure infrastructure.

1. Cyber Security News
2. Security Magazine
3. IBM
4. Infosecurity Magazine
5. Cybersecurity Insiders
6. SecurityScorecard

Learn more at **aptos.com**