# Walmart - Building trust in retail with cybersecurity

## Research Overview: Building Trust in Retail with Advanced Cybersecurity

As digital commerce continues to expand, the retail sector faces escalating cyber threats, making robust cybersecurity indispensable for protecting both consumers and business operations. Below is a synthesis of current research, emerging technologies, and innovative features that can position Walmart at the forefront of secure, trustworthy retail for Sparkathon 2025.

---

## Key Cybersecurity Threats in Retail

- **Credential Phishing:** 58% of attacks target login credentials, often via sophisticated phishing schemes.
- **Malware and Ransomware:** Malware (21.74%) and ransomware (13.04%) disrupt operations and target sensitive payment/customer data.
- **DDoS Attacks:** 10.14% of attacks aim to overwhelm retail networks, especially during peak seasons.
- **Insider Threats & Third-Party Vulnerabilities:** These account for a significant portion of breaches, highlighting the need for holistic security1.

---

## Cutting-Edge Technologies and Approaches

### 1. AI-Driven Fraud Detection

- AI and machine learning models can analyze massive volumes of transaction data in real time, identifying anomalies, predicting fraud, and minimizing false positives.
- Emerging trends include:
  - Anomaly detection algorithms
  - Predictive risk scoring
  - Network analysis for interconnected fraud patterns

    - Behavioral biometric authentication (e.g., typing patterns, mouse movements)
- Real-time data processing enables instant risk profiling, allowing fraudulent transactions to be blocked before completion2.

**2. Blockchain for Secure, Transparent Transactions**

- Blockchain provides a decentralized, tamper-proof ledger for all transactions, enhancing transparency and reducing fraud (e.g., chargebacks, counterfeit goods).
- Smart contracts automate and enforce agreements, reducing manual errors and conflicts.
- Blockchain-based loyalty programs and supply chain tracking build customer trust by ensuring authenticity and transparency from source to shelf3.

**3. Multi-Factor Authentication (MFA) and Biometric Security**

- MFA is now critical, given that 80% of breaches are linked to weak or stolen passwords.
- Combining traditional credentials with biometrics (fingerprint, facial recognition) or physical tokens significantly reduces unauthorized access.
- MFA is increasingly required for regulatory compliance and as a prerequisite by suppliers and insurers4.

**4. Zero Trust Security Frameworks**

- Zero Trust Architecture (ZTA) operates on the principle of “never trust, always verify,” continuously validating every access request regardless of origin.
- ZTA protects against both internal and external threats, replacing outdated perimeter-based models5.

---

# Stand-Out Features and Innovations for Sparkathon 2025

To distinguish Walmart’s approach from competitors and demonstrate true innovation, consider these advanced features:

| Feature/Technology | Description & Differentiator |
|---|---|

| | |
|---|---|
| **Generative AI for Threat Simulation** | Use generative AI to simulate evolving attack vectors, enabling proactive defense and continuous system hardening2. |
| **Decentralized Identity Management** | Leverage blockchain-based digital IDs for customers and employees, ensuring privacy and preventing identity theft3. |
| **Continuous Behavioral Authentication** | Implement AI that continuously monitors user behavior (e.g., navigation patterns, device usage) for ongoing authentication2. |
| **Quantum-Resistant Encryption** | Integrate next-gen encryption algorithms to future-proof transaction security against quantum computing threats. |
| **Self-Healing Security Systems** | Deploy AI-driven systems capable of detecting, isolating, and autonomously recovering from breaches or anomalies. |
| **Transparent Supply Chain Provenance** | Use blockchain to provide customers with real-time, immutable proof of product origin and authenticity3. |
| **Personalized Security Dashboards** | Offer customers a dashboard to view their security status, recent activity, and control privacy settings, enhancing trust. |
| **Zero Trust Micro-Segmentation** | Apply ZTA at a granular level, isolating applications, devices, and user groups to minimize breach impact5. |

# Implementation Recommendations

- **Embed Security in Every Layer:** Make cybersecurity a core part of all retail operations, from employee training to backend systems and supplier networks1.
- **Invest in Real-Time AI:** Prioritize AI models that adapt to new threats instantly, reducing detection-to-response time to milliseconds2.
- **Adopt Blockchain Beyond Payments:** Extend blockchain to loyalty programs, supply chain management, and digital identity for holistic trust-building3.
- **Prioritize User Experience:** Ensure that advanced security (MFA, biometrics) is frictionless for customers, balancing protection with

convenience4.

- **Lead with Zero Trust:** Position Walmart as a pioneer in Zero Trust retail, with continuous verification and adaptive access controls5.

---

## Sources


- [Securing Retail in 2025: Top Cybersecurity Threats and How to Prepare]1
- [AI in Retail for Fraud Detection: Navigating 2025 Trends]2
- [Blockchain in Retail: Revolutionizing Supply Chain and Customer Experience]3
- [Overcoming the Challenges of Multi-Factor Authentication in Retail]4
- [Rethinking Retail Security: Zero Trust Architecture]5


---

By integrating these advanced technologies and strategies, Walmart can set a new industry standard for secure, transparent, and trustworthy retail—making a compelling case for Sparkathon 2025 and beyond.

Untitled