SERKET-TECH SECURITY

Securing the Modern Retailer: Compliance, Resilience, and Risk Management

Cybersecurity, compliance, and resilience services for retailers, ecommerce brands, franchise systems, auto dealers, and consumer-facing businesses. Protect payments, customer data, store operations, loyalty programs, digital channels, and third-party ecosystems.

Retail organizations operate across stores, ecommerce sites, mobile apps, POS systems, call centers, loyalty programs, warehouses, payment providers, SaaS platforms, and third-party service partners. A cyber event can stop checkout, disrupt online orders, expose customer data, enable fraud, or damage brand trust during peak selling periods.

Serket-Tech Security helps retailers and consumer-facing businesses strengthen governance, protect payment and customer data, validate controls, reduce vendor risk, prepare for PCI and privacy reviews, respond to incidents, and operate a more resilient security program.

Protect Checkout, Payments, and Ecommerce

Strengthen PCI DSS readiness, cardholder data controls, payment page security, POS environments, cloud stores, mobile apps, APIs, and checkout workflows.

Keep Stores and Digital Channels Operating

Prepare for ransomware, outages, third-party disruptions, and peak-season incidents that can affect stores, ecommerce, warehouses, fulfillment, and customer service.

Reduce Fraud, Account Abuse, and Social Engineering

Improve identity controls, call center verification, loyalty and gift card defenses, vendor payment controls, phishing resilience, and executive response readiness.

Safeguard Customer, Employee, and Loyalty Data

Prepare for ransomware, outages, third-party disruptions, and peak-season incidents that can affect stores, ecommerce, warehouses, fulfillment, and customer service.

SERKET-TECH SECURITY

A Broad Security and Compliance Portfolio for Retail

Retail teams need coordinated services that protect revenue operations, reduce fraud, secure payment and customer data, satisfy audit expectations, and keep security aligned with stores, ecommerce, and fulfillment.

- **Governance, Risk, and Privacy**
  Security program design, policies, risk assessments, privacy governance, executive reporting, data retention review, and roadmap planning for retail operations.
- **Vendor and Supply Chain Risk**
  Reviews of payment processors, ecommerce platforms, franchisees, MSPs, marketplaces, 3PLs, marketing providers, SaaS vendors, and managed service partners.
- **Ecommerce, Application, and Cloud Security**
  Web, mobile, API, cloud, WAF, CI/CD, identity, OMS, CRM, CDP, and martech security reviews tied to digital commerce and customer data workflows.
- **Fraud, Identity, and Social Engineering Controls**
  Account takeover, loyalty fraud, gift card abuse, bot activity, BEC, vendor payment fraud, call center abuse, MFA, and identity governance support.
- **PCI DSS and Payment Security**
  PCI DSS v4.0.1 readiness, CDE scoping, SAQ or ROC preparation, segmentation review, POS control review, P2PE support, and payment page script management.
- **Incident Response and Managed Security**
  Breach response, ransomware readiness, tabletop exercises, forensics coordination, MDR support, vCISO advisory, and recurring compliance operations.
- **Store Network, POS, and IoT Security**
  Store network segmentation, wireless testing, remote access review, POS hardening, camera, kiosk, scanner, digital signage, and device security for inventory.
- **Security Assessments and Penetration Testing**
  Security posture reviews, internal and external testing, ecommerce and application testing, cloud testing, wireless testing, and prioritized remediation plans.

Who We Serve

- Specialty, regional, national, omnichannel, and ecommerce retailers.
- Direct-to-consumer brands, marketplaces, subscription businesses, and franchise systems.
- Grocery, convenience, fuel, pharmacy, apparel, luxury, electronics, home goods, and health retailers.
- Auto dealers and retailers offering financing, leasing, store credit, warranties, or recurring payments.
- Retail technology, POS, ecommerce, loyalty, payment, fulfillment, and customer data providers.

Common Drivers We Support

- PCI DSS v4.0.1, payment security, cardholder data scoping, and ecommerce script controls.
- CCPA, CPRA, state privacy laws, FTC Act expectations, and breach notification planning.
- GLBA Safeguards, Red Flags, ACH/Nacha, HIPAA, or SEC cyber support where business models require it.
- Ransomware, store downtime, ecommerce outage, social engineering, loyalty fraud, and account takeover risk.
- Third-party risk, franchise risk, processor reviews, cyber insurance, M&A diligence, SOC 2, HITRUST, and ISO needs.

SERKET-TECH SECURITY

How Retailers Can Engage Serket-Tech

Clients can start with focused work tied to payment security, privacy, fraud reduction, security validation, incident readiness, or ongoing operations. Each path can stand alone or expand into a broader program.

1. Readiness and Assurance Program

Built for retailers that need to satisfy PCI, privacy, customer, lender, processor, cyber insurance, board, or partner due diligence expectations.

What It Includes

- PCI DSS v4.0.1 readiness, CDE scoping, SAQ, ROC, and remediation planning.
- CCPA, CPRA, state privacy, FTC Act, and breach response program support.
- FTC Safeguards Rule, GLBA, Red Flags, and financing workflow support where applicable.
- SOC 2, HITRUST, ISO 27001, SEC cyber disclosure, or partner assurance support where relevant.
- Vendor review, evidence collection, policies, control mapping, and executive reporting.

2. Security Validation and Hardening

Built for teams that need to find gaps before peak season, payment review, digital launch, franchise rollout, M&A event, or cyber insurance renewal.

What It Includes

- Ecommerce, payment page, mobile app, API, cloud, and identity reviews.
- Store network, POS, wireless, kiosk, scanner, and remote access testing.
- Payment script authorization, change detection, and page integrity control review.
- Fraud, phishing, BEC, account takeover, and call center abuse control review.
- Prioritized remediation tied to checkout, customer data, uptime, and brand impact.

3. Continuous Operations and Resilience

Built for organizations that want security readiness to become a repeatable operating model rather than a one-time project.

What It Includes

- Managed detection and response support across endpoint, identity, cloud, and key systems.
- Control monitoring, evidence management, issue tracking, and compliance cadence support.
- Ransomware tabletop exercises, incident response retainers, and crisis coordination.
- Business continuity and disaster recovery planning for stores, ecommerce, and fulfillment.
- Recurring vCISO guidance, risk steering, board reporting, and security roadmap management.

SERKET-TECH SECURITY

Why Choose Serket-Tech Security

Serket-Tech Security gives retailers one partner for strategy, hands-on remediation, testing, response, vendor oversight, and ongoing operations. We help clients reduce cyber risk without disconnecting security from customer experience, revenue operations, and store realities.

01

Assess
Scope stores, platforms, data, vendors, payments, and operational risk.

02

Prioritize
Rank gaps by revenue impact, compliance need, and customer exposure.

03

Implement
Build policies, controls, evidence, workflows, and remediation plans.

04

Validate
Test controls, reduce attack paths, and prepare for review.

05

Operate
Monitor, report, respond, and sustain readiness year-round.

Build a retail security program that protects revenue, customers, payments, and brand trust.

Engage Serket-Tech Security for a retail readiness workshop, PCI and privacy review, security validation project, or managed security program design.