THE ARCHON

TECHNOLOGY INTELLIGENCE

EXECUTIVE BRIEF

Why E-commerce is a Prime Target

Online retailers handle high-value transactions and personal data, making them a top focus for cybercriminals. Attack volumes have surged across the sector, driving revenue loss and brand damage.

→ High-value payment data

→ Large volumes of customer PII

→ Fast-moving inventory and promotions attract ransomware

CONTROL FRAMEWORK

Modern Threat Landscape

Key threats facing e-commerce platforms today include:

- → Credential stuffing and credential-cracking bots
- → API abuse and data exfiltration
- → Supply-chain malware inserted into third-party plugins
- → Ransomware targeting order-fulfillment systems

CONTROL FRAMEWORK

Secure the Payment Flow

Protect cardholder data end-to-end with industry-standard controls:

→ Tokenization of stored card numbers

→ 3-D Secure (EMV 3-DS) for authentication

→ Full PCI DSS compliance across all payment components

CONTROL FRAMEWORK

Hardening the Front-End

Deploy defensive controls that stop attacks before they reach the back-end:

→ Web Application Firewall (WAF) with bot management

→ Content Security Policy (CSP) to block malicious scripts

→ SameSite and HttpOnly cookie flags

CONTROL FRAMEWORK

API Hardening Blueprint

Treat every public API as a critical security perimeter:

→ Rate limiting and anomaly detection

→ OAuth 2.0 with scoped access tokens

→ Mutual TLS for server-to-server calls

CONTROL FRAMEWORK

Incident-Response Playbook

A repeatable, timed process reduces impact and restores trust:

→ Detect – real-time alerts from SIEM and fraud monitoring

→ Contain – isolate compromised services, rotate secrets

→ Eradicate – remove malicious code, patch vulnerable components

→ Recover – restore from immutable backups, verify integrity

→ Communicate – coordinated internal and external notifications

CONTROL FRAMEWORK

Continuous Assurance & Monitoring

Shift security left and maintain visibility across the stack:

→ Automated SAST/DAST in CI/CD pipelines

→ Third-party component SBOM analysis

→ Security posture dashboards with KPI alerts

EXECUTIVE TAKEAWAY

Executive Takeaway

A resilient e-commerce operation blends layered technical controls with a disciplined, repeatable process. By securing payments, hardening APIs, automating testing, and rehearsing response, leaders turn security into a growth enabler rather than a cost center.

→ Use tokenization and industry-aligned security controls for every transaction

→ Deploy web-application firewalls, content-security policies, and bot mitigation at the web layer

→ Apply strong authentication, rate limiting, and mutual TLS on all APIs

→ Integrate a structured incident-response workflow into operations

→ Run continuous static and dynamic code analysis and software component inventories in CI/CD