

RETAIL & E-COMMERCE CYBERSECURITY

Keep the checkout safe.

Web, mobile and API VAPT, payment integration security, privacy, brand protection and SOC for retail and e-commerce.

Three questions every retail leader should be able to answer

Who can change the scripts on our payment page?

Skimming attacks ride on third-party scripts; an inventory, authorisation and tamper detection are now PCI DSS expectations.

Would our checkout survive the festive sale—and a bot attack during it?

Load, API and DDoS testing before the season decides whether peak day is a record or an outage.

If our customer database leaked tonight, could we report in six hours?

Knowing where customer data lives, who can reach it and how a breach is detected and reported is the core of CERT-In and DPDP readiness.

59%

Of retail web traffic is bad bots

£300 m

Estimated hit from one 2025 retail attack

~20 m

Customer records leaked in one Indian case

6 hours

Incident reporting to CERT-In

Built for every retailer

Retail chains and supermarkets · online marketplaces · D2C brands · quick commerce · omnichannel and fashion retailers · consumer electronics retail · payment, loyalty and gift card programmes.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
CERT-In Directions · audit guidelines (2022, 2025)	6-hour reporting, 180-day logs; independent audits
RBI payment rules · PCI DSS v4.0.1	No stored card data; tokenisation; payment page controls
Consumer rules · DPDP	E-Commerce Rules, dark-pattern guidelines; personal data safeguards

VAPT, payments, privacy, brand, festive readiness and SOC

Web, Mobile & API VAPT

Storefront, app, API, POS and business-logic testing with pre-season retests.

Payment Integration Security

Gateway, UPI, token and payment page controls; PCI DSS v4.0.1 and RBI PA readiness.

Privacy & DPDP

Customer, loyalty and seller data mapping, consent design, DPDP programme.

Brand & Fraud Protection

Fake app and domain monitoring, takedowns, loyalty and refund fraud controls.

Bot, DDoS & Festive Readiness

Load and DDoS testing, bot management, runbooks and war-room drills.

24/7 Retail SOC

Platform, cloud and store monitoring with fraud signals and 6-hour reporting support.

Choose your starting point

Foundation

Storefront, app and API assessment, payment integration review, cloud posture check, privacy quick assessment. For D2C brands and single-format retailers.

Assurance

Annual VAPT with retests, payment page and token controls, independent audit and PCI DSS readiness, 24x7 SOC. For regional chains and growing marketplaces.

Continuous Resilience

Continuous testing and red teaming, bot and festive-readiness programme, partner and seller risk, SOC with hunting and Board reporting. For national retailers, marketplaces and quick commerce.

Why Codec Networks

CERT-In empanelled

for information security auditing services, and empanelled with NISCI for application audit services.

Certified

ISO 9001:2015, ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018.

Regulation-mapped

Every finding mapped to OWASP, PCI DSS v4.0.1, RBI payment rules, CERT-In expectations and DPDP requirements.

One connected partner

Testing, audits, SOC, forensics and privacy linked from finding to closure.

Book a scoping session

Share your platforms, payment stack, partners and sales calendar. We will propose a practical, peak-aware assessment and assurance plan.

New Delhi: 507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place – 110001

Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018

Call: 011 430 496 96 · +91 99716 76124 · +91 88007 88220

Email: mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Services support risk reduction and assurance and do not guarantee prevention of all incidents or regulatory compliance. Sources: Imperva Bad Bot Report 2025, Marks & Spencer statements, public reporting, CERT-In. Confirm obligations against the official instruments.