

Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · RETAIL & E-COMMERCE

Keep the Checkout Safe. Keep the Customer's Trust.

Web, mobile and API VAPT, payment integration security, privacy, brand protection and SOC for retail chains, marketplaces, D2C brands, quick commerce, omnichannel retailers and payment and loyalty programmes.

Web, Mobile & API VAPT

Payment Integration Security

Privacy & DPDP

Brand & Fraud Protection

Bot, DDoS & Festive Readiness

24/7 Retail SOC

Coding Threats. Decoding Solutions.

www.codecnetworks.com

THE CHALLENGE

In retail, a cyber incident is a customer incident.

Indian retail runs on apps, APIs and payment integrations serving millions of shoppers—and attackers follow the money and the festive peak. Bad bots make up 59% of retail web traffic, skimming scripts steal cards at checkout, leaked passwords unlock loyalty accounts, and one 2025 ransomware attack cost Marks & Spencer an estimated £300 million. In India, leaks at BigBasket, Domino's India and boAt put millions of records on sale.

What keeps leadership teams awake

- Card and customer data stolen at the checkout
- Account takeover, loyalty and refund fraud
- Bots and DDoS during the festive sale
- A plugin, script or partner that opens the door
- Ransomware across stores and dark stores
- CERT-In, RBI, PCI DSS and DPDP obligations



59%

Of retail web traffic is malicious bots (Imperva, 2025)

£300 m

Estimated profit hit from the 2025 Marks & Spencer attack

~20 m

BigBasket customer records reported leaked (2020)

6 hours

To report cyber incidents to CERT-In

The rulebook has changed

Instrument	What it means for you
CERT-In Directions and audit guidelines (2022, 2025)	6-hour reporting, 180-day logs; independent cyber audits
RBI payment rules · PCI DSS v4.0.1	No stored card data; tokenisation; payment page script controls
Consumer protection (2020, 2023)	E-Commerce Rules duties; CCPA guidelines prohibit dark patterns
DPDP Act and Rules · SEBI LODR	Customer data safeguards (most from May 2027); quarterly disclosure

One partner from storefront to settlement

Built around our primary proposition for the sector: **Web, mobile and API VAPT, payment integration security, privacy, brand protection and SOC.**

Web, Mobile & API VAPT

- Storefront, app and API testing against OWASP ASVS, MASVS and API Top 10
- Business-logic tests: pricing, coupons, cart and refund flows
- POS, kiosk and store network assessments
- Pre-festive-season retests and release testing

Payment Integration Security

- Gateway, UPI, BNPL and tokenisation integration reviews
- Payment page script inventory and tamper detection
- PCI DSS v4.0.1 scoping, gap assessment and evidence
- RBI PA and card-on-file compliance support

Privacy & DPDP

- Customer, loyalty, seller and rider data mapping
- Consent, notice and retention design for apps and CRM
- DPDP gap assessment, DPO support and breach workflow
- Dark-pattern and consent-flow review

Brand & Fraud Protection

- Fake app, look-alike domain and social impersonation monitoring
- Takedown support and dark web monitoring
- Loyalty, gift card and refund fraud control reviews
- Account takeover and credential-stuffing testing

Bot, DDoS & Festive Readiness

- Load, API and DDoS resilience testing before sales
- Bot management and rate-limit design
- WAF, CDN and scrubbing runbooks
- Festive-season war-room exercises

24/7 Retail SOC

- Platform, cloud, store and endpoint monitoring
- Fraud and bot signals correlated with security alerts
- Threat hunting and peak-season watch
- 6-hour CERT-In reporting support

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

Packaged for how retailers buy

Eleven Codec Networks bundles apply directly to retail and e-commerce companies:

B1 Cyber Assessment & VAPT Assurance	B2 Application, API & DevSecOps Security	B3 Cloud, Infrastructure & Zero Trust
B4 Regulatory Cyber Audit & Compliance	B5 GRC, ISO, SOC 2 & PCI DSS Maturity	B6 Data Privacy & DPDPA Program
B7 Managed SOC, MDR & Threat Monitoring	B8 Forensics, Incident Response & Malware RCA	B9 Third-Party & Supply-Chain Risk
B10 Cyber Simulation, Awareness & Tabletop	B11 Emerging Tech, AI & Web3 Security	

Foundation

D2C brands and single-format retailers

- Storefront, app and API assessment
- Payment integration and PCI DSS scoping review
- Cloud posture and secrets review
- Privacy quick assessment and policy pack

Assurance

Regional chains and growing marketplaces

- Annual web, mobile and API VAPT with retests
- Payment page and tokenisation controls
- Annual independent audit and PCI DSS readiness
- 24x7 SOC with fraud signals

Continuous Resilience

National retailers, marketplaces and quick-commerce platforms

- Continuous testing and red teaming
- Bot, DDoS and festive-readiness programme
- Partner, seller and 3PL risk programme
- SOC with threat hunting and Board reporting

Mapped to your obligations

Requirement	How we help	Bundle
Incidents to CERT-In in six hours; 180-day logs (CERT-In Directions)	SOC, IR retainer and reporting support	B7, B8
No card data stored by merchants; tokenisation (RBI PA, CoF rules)	Payment integration and token reviews	B2, B4
Payment page and cardholder data controls (PCI DSS v4.0.1)	PCI DSS scoping, gap assessment, evidence	B4, B5
Grievance officer and disclosures (E-Commerce Rules 2020)	Platform governance and policy support	B5
No dark patterns in interfaces (CCPA Guidelines 2023)	Consent and interface review	B6
Customer, loyalty and seller personal data (DPDP)	DPDPA programme	B6
Quarterly incident disclosure, listed retailers (SEBI LODR)	Incident records, disclosure support	B4, B8

Why retailers choose Codec Networks

CERT-In empanelled

Independent audits recognised by regulators, payment partners and customers.

Certified and accountable

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

Peak-season aware

Testing and monitoring planned around sales calendars, code freezes and launches.

Standards-mapped

Findings mapped to OWASP, PCI DSS v4.0.1, RBI, CERT-In and DPDP expectations.

Full stack, one partner

VAPT, payment security, privacy, brand monitoring, SOC and forensics connected from finding to closure.

Certified experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI and CHFI professionals.

How we engage

Discover & scope

Storefronts, apps and APIs, payment integrations, cloud platforms, stores and dark stores, partners and sellers, and your sales and audit calendar.

Assess & test

Threat-led testing and regulatory audits executed by certified specialists.

Report in business terms

Findings, risk ratings and a compliance gap matrix for the Board and regulators.

Remediate

Practical, prioritised fixes with technology and compliance teams.

Validate & prove

Retesting and an evidence tracker for auditors, regulators and partners.

Monitor & improve

Managed SOC, recurring testing and quarterly governance reviews.

What you receive: executive summary for the Board or its committee · technical findings with evidence and CVSS ratings · compliance gap matrix · prioritised remediation roadmap · retest reports · audit evidence tracker · SOC dashboards and MTTD/MTTR metrics.



START WITH A SCOPING SESSION

Let's make your next festive sale, audit and incident a non-event.

Tell us 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, New Delhi – 110001

Gurugram

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

Call

011 430 496 96 · 011 437 522 99
+91 99716 76124 · +91 88007 88220 · +91 88003 31124

Write

mktg@codecnetworks.com
www.codecnetworks.com

Codec Networks

Coding Threats. Decoding Solutions.

Secure Today. Innovate Tomorrow. Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Packages are proposed groupings of Codec Networks bundles, finalised through scoping. 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.