

Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · FINTECH & DIGITAL FINANCIAL SERVICES

Build Fast. Ship Secure. Pass Every Diligence.

API security, cloud assessment, DevSecOps, third-party risk, fraud simulations and regulatory readiness for lending technology firms, Account Aggregators, embedded finance platforms and financial API providers.

API Security

Cloud Assessment

DevSecOps

TPRM

Fraud Simulations

Regulatory Readiness

Coding Threats. Decoding Solutions.

www.codecnetworks.com

THE CHALLENGE

Fintech runs on APIs. So do attackers.

Fintechs move fast, integrate with dozens of partners and hold sensitive financial data—while banks, NBFCs, investors and RBI's partner rules demand proof of security.

What keeps leadership teams awake

- Broken API authorisation and leaked keys
- Cloud misconfiguration exposing KYC files
- Malicious SDKs and open-source supply-chain risk
- Deepfake and synthetic-identity onboarding fraud
- Consent and data-retention obligations under DPDP
- Bank and NBFC partner security questionnaires



500 mn+

Account Aggregator
consents fulfilled
(Sahamati, Sept 2026)

1,100+

Regulated entities live on
the AA ecosystem

6 hours

To report specified
incidents to CERT-In

May 2027

Most DPDP Rules
obligations take effect

The rulebook has changed

Instrument	What it means for you
RBI (Digital Lending) Directions (2025)	LSP and digital lending app obligations; borrower-data collection, storage and sharing restrictions; lender accountability
RBI 2026 cybersecurity Directions for NBFCs (31 Jul 2026)	Apply to licensed NBFC-AAs and NBFC-P2Ps by layer; 6-hour incident reporting to RBI
Partners' rules: bank and NBFC Directions, Outsourcing Directions (2025–26)	Banks and NBFCs must oversee fintech partners—due diligence, audit rights and security controls flow down
CERT-In Directions · DPDP Act & Rules	6-hour CERT-In reporting, 180-day logs in India, consent, minimisation, safeguards and breach intimation

Security that keeps pace with your releases

Built around our primary proposition for the sector: **API security, cloud assessment, DevSecOps, TPRM, fraud simulations and regulatory readiness.**

API & Application Security

- REST, GraphQL and webhook testing
- Mobile app and SDK security
- Business-logic and authorisation testing
- Partner-ready VAPT reports

Cloud Assessment

- AWS, Azure and GCP posture reviews
- Kubernetes and serverless testing
- IAM, secrets and key management
- Continuous cloud assurance

DevSecOps

- SAST, DAST and SCA in CI/CD
- Secrets scanning and SBOM
- Secure code review and threat modelling
- Developer security enablement

Third-Party Risk Management

- Vendor and SDK risk assessments
- Partner questionnaire support
- Contract and data-sharing reviews
- Continuous vendor monitoring

Fraud Simulations

- Synthetic identity and deepfake KYC tests
- Account takeover and mule simulations
- Business-logic abuse testing
- Fraud-signal SOC use cases

Regulatory Readiness

- Digital Lending Directions alignment
- NBFC-AA and P2P cyber Directions readiness
- ISO 27001 and SOC 2 readiness
- DPDPA consent and privacy programme

Who we serve: lending technology firms and LSPs · Account Aggregators · embedded finance platforms · banking-as-a-service and financial API providers · P2P lending platforms · KYC and identity providers · wealthtech and insurtech apps · fintech SaaS vendors.

Packaged for how fintechs actually buy

Eleven Codec Networks bundles apply directly to fintech 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

Seed and early-stage fintechs

- Pre-launch API and app VAPT
- Cloud posture quick review
- ISO 27001 / SOC 2 gap review
- Partner questionnaire pack

Assurance

Growth-stage fintechs and NBFC-AAAs

- Release-based API and app testing
- DevSecOps and secrets scanning
- DPDPA readiness and TPRM
- Extended-hours SOC + IR retainer

Continuous Resilience

Scale-ups and multi-partner platforms

- Continuous testing and red teaming
- Continuous cloud assurance
- 24x7 SOC with fraud correlation
- Board and investor reporting

Mapped to your obligations

Requirement	How we help	Bundle
Digital Lending Directions 2025: lenders accountable for LSPs; borrower-data restrictions	LSP security assessment, data-flow and API review	B2, B6
RBI 2026 NBFC Directions: requirements by layer for NBFC-AAAs and NBFC-P2Ps	Applicability assessment and gap remediation	B4
Bank and NBFC partner due diligence, audit rights and security controls	Partner-ready assurance pack, VAPT, ISO 27001 / SOC 2	B1, B5
CERT-In: 6-hour reporting, 180-day ICT logs in India, clock sync	Logging review, IR retainer, playbooks	B7, B8
Cloud and secrets security across the platform	Cloud posture, IAM and secrets reviews	B3
DPDP Act and Rules: consent, minimisation, safeguards, breach intimation	DPDPA programme and breach drills	B6
Vendor and SDK supply-chain risk	TPRM and software composition analysis	B9, B2

Why fintechs choose Codec Networks

CERT-In empanelled

Empanelled for information security auditing services; NISCI empanelled for application audit services.

Certified and accountable

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

Partner-ready evidence

Reports and evidence packs designed to satisfy bank, NBFC, investor and enterprise due diligence.

Built for release velocity

Testing that plugs into CI/CD, with retests aligned to your sprint cadence.

Full stack, one partner

AppSec, cloud, SOC, forensics, privacy and TPRM connected from finding to closure.

Fintech-grade expertise

OSCP, CEH, CPENT, cloud and AppSec specialists using OWASP API Top 10, MASVS and MITRE ATT&CK.

How we engage

Discover & scope

Licences or partner model, products, APIs, cloud stack, partners and your diligence deadlines.

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 diligence, release and incident a non-event.

Tell us your product, partners and deadlines. We will propose a practical, partner-ready 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. Statistics: Sahamati press release (September 2026); CERT-In Directions; DPDP Rules 2025.