



Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · SAAS & ENTERPRISE SOFTWARE

Ship Secure Software. Win Every Security Review.

Product VAPT, SAST/DAST/SCA, API testing, tenant isolation, cloud security and SOC 2 readiness for ERP, CRM, HRMS, collaboration, cybersecurity and business application vendors.

Product VAPT

SAST / DAST / SCA

API Testing

Tenant Isolation

Cloud Security

SOC 2 Readiness

Coding Threats. Decoding Solutions.

www.codecnetworks.com

THE CHALLENGE

Your customers trust your tenant model. Attackers test it.

SaaS platforms hold the business data of thousands of customers. Enterprise buyers now expect SOC 2 or ISO 27001, product test reports and an SBOM before they sign—and regulated customers pass on their regulators' vendor rules.

What keeps leadership teams awake

- A tenant isolation flaw exposing one customer's data to another
- Stolen OAuth and integration tokens
- Customer account takeover through credential stuffing
- Support and admin tools abused by attackers
- Vulnerable open-source dependencies without an SBOM
- SOC 2, ISO 27001, CERT-In and DPDP obligations



6 hours

To report cyber incidents to CERT-In

Oct 2024

CERT-In SBOM technical guidelines issued

Sep 2026

EU Cyber Resilience Act reporting obligations apply

May 2027

Most DPDP obligations take effect

The rulebook has changed

Instrument	What it means for you
CERT-In Directions, audit and SBOM guidelines (2022–25)	6-hour incident reporting, 180-day logs; risk-based audits; SBOM practices for software
DPDP Act & Rules	Processor safeguards for customer data and controller duties for your own users; breach intimation from May 2027
Customer regulator flow-down	RBI, SEBI and IRDAI vendor and cloud controls for BFSI customers; MeitY empanelment for government
SOC 2, ISO 27001 and international rules	Enterprise assurance expectations; GDPR for EU data; EU CRA for in-scope products

One partner from code to customer trust

Built around our primary proposition for the sector: **product VAPT, SAST/DAST/SCA, API testing, tenant isolation, cloud security and SOC 2 readiness.**

Product VAPT

- Web, mobile and desktop product testing
- Admin and support console testing
- Business-logic and abuse testing
- Retest and customer-ready reports

SAST / DAST / SCA

- Secure code review
- Dynamic application testing
- Open-source and licence risk
- SBOM generation and governance

API Testing

- Public and partner APIs
- OAuth and integration scopes
- Rate limiting and abuse controls
- Webhook and event security

Tenant Isolation

- Cross-tenant authorisation testing
- Data partitioning and encryption reviews
- Shared-service and cache isolation
- Automated isolation tests in CI

Cloud Security

- Cloud posture and IAM reviews
- Infrastructure-as-code scanning
- Kubernetes and container security
- Secrets management

SOC 2 Readiness

- SOC 2 gap assessment and readiness
- ISO/IEC 27001:2022 alignment
- Security questionnaire support
- Trust centre evidence

Who we serve: ERP vendors · CRM vendors · HRMS and payroll vendors · collaboration platforms · cybersecurity product companies · vertical and business application SaaS vendors.

Packaged for how SaaS companies buy

Eleven Codec Networks bundles apply directly to SaaS and enterprise software vendors:

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

Early-stage SaaS

- Product VAPT and API testing
- SCA and secrets scanning
- SOC 2 gap assessment
- Cloud posture review

Assurance

Growth-stage SaaS

- Tenant isolation and API testing
- DevSecOps and SBOM programme
- SOC 2 readiness and ISO 27001
- 24x7 managed SOC

Continuous Resilience

Enterprise software vendors

- Continuous testing and red teaming
- Integration and supply-chain assurance
- SOC with identity and tenant signals
- Customer and Board reporting

Mapped to your obligations

Requirement	How we help	Bundle
Cyber incidents to CERT-In within six hours; 180-day logs (CERT-In Directions)	SOC monitoring, IR retainer and reporting support	B7, B8
Software bill of materials practices (CERT-In SBOM guidelines, 2024)	SCA and SBOM programme	B2
Processor safeguards for customer personal data (DPDP)	DPDPA programme and data mapping	B6
Vendor controls for BFSI customers (RBI, SEBI, IRDAI)	Flow-down assessments and evidence	B4
Secure multi-tenant architecture (customer contracts)	Tenant isolation and product VAPT	B1, B2
SOC 2 and ISO/IEC 27001 expectations	Readiness and implementation	B5
Cloud security (MeitY empanelment for government customers)	Cloud and IaC reviews	B3

Why SaaS companies choose Codec Networks

CERT-In empanelled

Independent product testing and audits that enterprise customers recognise.

Certified and accountable

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

Product-security depth

Tenant isolation, OAuth, API and support-tool testing built for SaaS.

Sales-ready evidence

Reports, retests and SOC 2 support that close security reviews.

Full stack, one partner

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

Certified experts

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

How we engage

Discover & scope

Product architecture, tenant model, integrations, customer sectors and your certification 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 release, security review and incident a non-event.

Tell us your product, tenant model and target customers. We will propose a practical product security 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: CERT-In, MeitY, European Union. Confirm obligations against the official instruments.