Codec Networks
Coding Threats. Decoding Solutions.

SAAS & ENTERPRISE SOFTWARE CYBERSECURITY

Secure by design. Trusted by customers.

Product VAPT, SAST/DAST/SCA, API testing, tenant isolation, cloud security and SOC 2 readiness for SaaS vendors.

Three questions every SaaS leader should be able to answer

Could one customer see another's data?
Tenant isolation must be enforced server-side on every endpoint, cache and job—and tested continuously.

Which integrations hold tokens to our customers?
OAuth apps and partners need narrow scopes, short lifetimes and monitoring of bulk exports.

Could we report an incident within six hours?
CERT-In requires reporting within six hours of noticing an incident; customers will expect prompt notice too.

6 hours
Incident reporting to CERT-In

Oct 2024
CERT-In SBOM guidelines

Sep 2026
EU CRA reporting obligations

May 2027
Most DPDP obligations take effect

Built for every SaaS vendor

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

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
CERT-In Directions · SBOM guidelines (2022, 2024)	6-hour reporting, 180-day logs; SBOM practices
DPDP · customer flow-down	Processor safeguards; RBI, SEBI, IRDAI vendor controls; MeitY empanelment
SOC 2 · ISO 27001 · EU rules	Enterprise assurance; GDPR; EU CRA for in-scope products

WHAT WE DO

Product VAPT, code and API testing, tenant isolation, cloud and SOC 2

Product VAPT
Web, mobile, admin and support console testing with customer-ready reports.

SAST / DAST / SCA
Secure code review, dynamic testing, dependency risk and SBOM.

API Testing
Public and partner APIs, OAuth scopes, webhooks and abuse controls.

Tenant Isolation
Cross-tenant authorisation, partitioning, caches and CI tests.

Cloud Security
Cloud posture, IAM, IaC, Kubernetes and secrets management.

SOC 2 Readiness
SOC 2 gap assessment and readiness, ISO 27001, questionnaire support.

Choose your starting point

Foundation
Product VAPT and API testing, SCA and secrets scanning, SOC 2 gap assessment, cloud review. For early-stage SaaS.

Assurance
Tenant isolation and API testing, DevSecOps and SBOM, SOC 2 and ISO 27001, managed SOC. For growth-stage SaaS.

Continuous Resilience
Continuous testing and red teaming, integration assurance, SOC with tenant signals, customer reporting. For enterprise vendors.

Why Codec Networks

CERT-In empanelled
for information security auditing services, and empanelled with NICSI for application audit services.

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

Regulation-mapped
Every finding mapped to CERT-In, DPDP, customer flow-down, SOC 2 and ISO 27001 requirements.

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

Book a scoping session

Share 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 – 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: CERT-In, MeitY, European Union. Confirm obligations against the official instruments.