CLOUD / SAAS

# Cloud & SaaS Security Assessment

Application, tenant-isolation, identity and cloud-configuration testing for SaaS and cloud-native products, with post-quantum readiness and AI security — reported as the paths that reach your customers' data.

**Read-only** FIRST

**Attack paths** NOT ALERT LISTS

**CycloneDX** CBOM & ML-BOM OUTPUT

**Senior** PRACTITIONER-LED

## What we assess

**AI security**
Assistants, retrieval over customer data, and agents and integrations that act inside customers' accounts.

**Post-quantum readiness**
TLS at the edge and between services, key management, customer-data encryption, and pipeline signing keys.

**Product & platform testing**
Application, APIs and tenant isolation, plus identities, privilege paths, containers and the pipeline that deploys them.

## What you get

- ✓ Starting-position table: what a leaked key or CI runner reaches
- ✓ Attack paths with break points, not forwarded tool output
- ✓ Findings traced to their origin in console, template or module
- ✓ Tenant-isolation results for multi-tenant products
- ✓ Third-party app access revoked and re-tested, with timings
- ✓ CBOM and AI-BOM in CycloneDX format
- ✓ One round of retesting to confirm the fixes landed

## How it works

1. Scope your architecture, tenancy model, and provider rules
2. Review configuration and identity read-only, across all accounts
3. Test application, tenants and paths with purpose-built resources
4. Deliver paths and break points, then retest the fixes

## A good fit if

- ✓ Enterprise customers are sending security questionnaires you struggle to answer with evidence.
- ✓ You run many accounts or projects and nobody is sure non-production is isolated from production.
- ✓ Your posture tool produces thousands of alerts and you need to know which ones matter.
- ✓ Your product holds customer data, and some of it acts on customers' behalf.

## Probably not, if

- × You want the cloud provider's own infrastructure tested — that is theirs to authorize, not yours.
- × You want a report that forwards scanner output — a posture tool already does that.
- × You need an audit opinion or certification — we test; auditors attest and certification bodies certify.

## How we engage

**Fixed scope**
A fixed-scope proposal at a fixed price. No hourly meter running.

**Senior-led**
The practitioner who scopes the work does the work and writes the report.

**Plain language**
One report your engineers and your board can both act on.

**Retest included**
We verify the fixes landed — one round of retesting is in scope.



Security that locks down risk, not your business. · © 2026 verrou