SHOMAR SECURITY PLATFORM

Enterprise Capacity and Concurrency Proof

Multi-client, multi-project scan and compliance operating model for regulated customers.

Document Control
Audience: Tier-1 banks, fintechs, procurement teams, CISOs, compliance leaders, and platform operators
Classification: Customer-facing readiness guide
Generated: August 01, 2026
Website: https://shomar.io
Application: https://app.shomar.io

Shomar is a security and compliance evidence platform for regulated Nigerian and African teams. It combines security scanning, findings operations, compliance evidence, customer-controlled scanning, and auditor-ready reporting in one operating workspace.

Contents

1. Reference Scenario

The baseline enterprise proof scenario is 10 customer organizations, 10 workloads per organization, 25 developers per organization, and 30 concurrent scan requests across SAST, SCA, secrets, IaC, CI/CD, and VAPT.

Compliance evidence, remediation, reporting, ticket sync, SIEM export, and MCP playbooks can operate beside the scan workload because they are tenant-scoped and governed by quotas, worker pools, and approvals.

Dimension	Baseline	Evidence to collect
Organizations	10	Tenant list, quotas, API-key policies, audit logs.
Projects	100 total	Project registry, source-control bindings, scan histories.
Developers	250 total	RBAC assignments, IDE/CI keys, remediation ownership.
Concurrent scans	30	Queue depth, worker saturation, p95 agent latency, autoscale recommendation.
Compliance workload	Active	Evidence vault, gap status, reports, attestation manifest.

2. Capacity Controls

Shomar keeps multi-client operation stable by combining hard tenant scoping with queue controls and enterprise policy.

Control	Purpose	Why a bank cares
Tenant isolation	All operating data is scoped by organization.	One client cannot see another client's scans, evidence, or tickets.
Worker pools	Scan families are processed by matching pools.	Slow active testing does not block code or compliance evidence work.
Tenant quotas	Limits are applied to concurrent scans, pending scans, VAPT, CI/CD, and reports.	A noisy tenant cannot starve the platform.
Incremental reruns	Changed-file and targeted retest paths reduce unnecessary scan volume.	Developers get faster feedback after fixes.
Autoscale recommendation	Queue pressure is turned into recommended worker capacity.	Operators can scale before backlog becomes user pain.
Agent observability	MCP failures, p95 latency, approvals, and top tools are visible.	Automation is measurable and governable.

3. Proof Workflow

Run the following proof sequence before a Tier-1 bank production launch or large procurement review.

Step	Action	Output
1	Run enterprise.status_get.	Current operating posture, SLA, queue, connector, and evidence summary.
2	Run enterprise.capacity_simulate for expected load.	Decision status and additional slot recommendation.
3	Run enterprise.autoscale_recommend.	Worker-pool targets and saturation flags.
4	Run enterprise.connector_health.	Connector readiness for ticketing, SIEM, source control, and evidence workflows.
5	Run enterprise.evidence_verify.	Checksum/signature verification output.
6	Generate enterprise attestation.	Signed readiness run and pack manifest.
7	Validate VAPT scope and ROE.	Approved targets, test window, stop conditions, and scan metadata.
8	Validate CI/CD incremental rerun from a real pipeline.	Pipeline scan, gate result, rerun evidence, and developer feedback loop.