TARA INNOVA

Quicksand Deployment Guide

Deployment Models, Requirements, and Sizing Guidelines

Deployment Models

Model	Description
On-Premise	Full deployment within your data center. All data stays on your infrastructure. Maximum control and data sovereignty.
Private Cloud	Container-based deployment in your private cloud environment. Same isolation as on-premise with cloud operational benefits.
Hybrid	Edge enforcement on-premise with centralized management and reporting in your private cloud. Distributed enforcement with unified visibility.
Managed	Fully managed by a TARA INNOVA certified partner. Deployment, monitoring, and operations handled on your behalf.

Infrastructure Requirements

Minimum requirements per Quicksand enforcement node:

Resource	Requirement
CPU	4 vCPU (8 recommended for high-traffic environments)
Memory	8 GB RAM (16 GB recommended)
Storage	50 GB SSD (for logs and local cache)
Network	1 Gbps NIC minimum. 10 Gbps recommended for high-throughput deployments
OS	Linux (container-based deployment). No specific distribution requirement
Container Runtime	Docker or any OCI-compliant runtime

Sizing Guidelines

Traffic Volume	Recommended Configuration
Up to 10,000 req/sec	2 enforcement nodes + 1 admin node. Single MariaDB + Redis instance
10,000–50,000 req/sec	4 enforcement nodes + 1 admin node. Clustered database and cache
50,000–200,000 req/sec	8+ enforcement nodes with load balancing. Dedicated analytics tier
200,000+ req/sec	Custom architecture. Contact TARA INNOVA for sizing consultation

Supporting Services

Service	Purpose
MariaDB	Configuration storage, user management, license data. Deployed alongside or use existing instance
Redis	Distributed session state, enforcement caching, real-time counters
ClickHouse	Analytics and reporting engine. Handles high-volume log storage and query

Service	Purpose
NATS	Internal message bus for real-time event distribution between components

Network Architecture

Quicksand deploys as a reverse proxy at your network edge. Incoming traffic passes through Quicksand before reaching your application servers. Typical deployment:

- **Internet** → **Load Balancer** → **Quicksand nodes** → **Application servers**
- **TLS termination** at Quicksand or pass-through to backend — configurable per deployment
- **Health checks** on all enforcement nodes with automatic failover
- **mTLS** between Quicksand and backend services for zero-trust internal communication

Deployment Process

Standard deployment is completed within one business day:

- **1. Environment provisioning** — Deploy containers from TARA INNOVA registry. Automated via provided compose files
- **2. Network integration** — Configure DNS and load balancer to route traffic through Quicksand
- **3. Policy configuration** — Initial security policies deployed via Admin UI or API
- **4. TI Cloud connection** — Connect threat intelligence feeds and configure adoption policies
- **5. CRP activation** — Enable compliance reporting and configure regulatory framework mappings
- **6. Validation** — Traffic verification, enforcement testing, and monitoring confirmation