TARA INNOVA

Platform Architecture Overview

How Quicksand, CRP, TI Cloud, and Oasis Work Together

Platform Components

The TARA INNOVA platform consists of four integrated products. Each can be deployed independently, but together they form a unified security, compliance, and integration layer.

Component	Role
Quicksand WAAP	Edge enforcement — inspects, controls, and enforces web and API traffic in real time
Compliance Report Portal (CRP)	Evidence engine — turns enforcement decisions into audit-grade compliance documentation
Threat Intelligence Cloud (TI Cloud)	Intelligence coordination — aggregates, validates, scores, and distributes threat indicators
Oasis	Integration streaming — connects IoT, industrial, and enterprise systems with security governance

Data Flow

The platform operates as a closed-loop system:

- **Inbound traffic** → Quicksand inspects at the edge, consulting TI Cloud for threat intelligence. Decisions are made in sub-milliseconds
- **Enforcement decisions** → Every block, challenge, allow, and monitor action is logged to CRP as an evidence record
- **Threat intelligence** → TI Cloud receives observations from Quicksand and Oasis, scores indicators, and pushes updates back to enforcement points
- **Integration traffic** → Oasis governs IoT/OT/API streams with channel security. Enforcement events feed into CRP and TI Cloud
- **Compliance evidence** → CRP continuously maps all enforcement data to regulatory frameworks and generates reports on demand

Multi-Tenant Architecture

The platform supports full multi-tenant isolation:

- **Enforcement isolation** — Each tenant has independent policies, rules, and enforcement decisions
- **Evidence isolation** — CRP generates separate evidence chains and reports per tenant
- **Intelligence isolation** — TI Cloud maintains per-tenant indicator sets with optional cross-tenant sharing
- **MSP operations** — Centralized management with per-customer dashboards, reporting, and SLA tracking

High Availability

The platform is designed for zero-downtime operation:

- **Horizontal scaling** — Multiple Quicksand enforcement nodes behind load balancing. Scale with traffic

- **No single point of failure** — Each component operates independently. Node failures do not disrupt enforcement
- **Stateless enforcement** — Quicksand nodes share state through distributed caching. Any node can handle any request
- **Automatic failover** — Health monitoring with automatic traffic redistribution on node failure

API and Integration

Every component exposes management APIs for automation and integration with your existing toolchain. SIEM integration via standard log forwarding. Webhook-based alerting. Full REST API for policy management, report generation, and threat intelligence operations.