Getting Started Guide

From First Contact to Full Protection — Your Onboarding Journey

Engagement Process

Whether you purchase directly or through a TARA INNOVA partner, the path to production follows a structured process designed to minimize disruption and maximize time-to-value.

Phase	What Happens
1. Discovery	We assess your infrastructure, traffic patterns, compliance requirements, and integration landscape. Typically a 1-hour technical call.
2. Architecture Design	Based on discovery, we design the deployment architecture: node count, deployment model, network integration, and compliance framework selection.
3. Deployment	Container-based deployment using provided compose files. Standard deployments complete within one business day.
4. Policy Configuration	Initial security policies configured in partnership with your security team. Starts in monitor mode — no traffic disruption.
5. Validation	Traffic analysis in monitor mode confirms correct operation. Fine-tune policies based on real traffic patterns before switching to enforcement.
6. Go Live	Switch from monitor to enforcement mode. Real-time protection active. CRP begins generating compliance evidence immediately.
7. Optimization	Ongoing tuning based on traffic analysis and threat landscape. TI Cloud continuously improves intelligence quality.

What You Need to Provide

- **Infrastructure** — Compute resources per sizing guidelines (see Deployment Guide). Linux hosts or container orchestrator
- **Network access** — DNS control for routing traffic through Quicksand. Load balancer configuration if applicable
- **SSL certificates** — For your domains, or we configure ACME-based automated certificate management
- **Security team availability** — 2-4 hours during deployment week for policy configuration and validation
- **Compliance requirements** — Which frameworks (NIS2, DORA, ISO 27001, etc.) you need CRP to report against

What We Provide

- **Deployment automation** — Container images, compose files, and deployment scripts
- **Initial policy set** — Baseline security policies tuned to your traffic profile and industry
- **TI Cloud configuration** — Pre-configured threat intelligence feeds relevant to your sector
- **CRP framework mapping** — Compliance framework configuration for your regulatory requirements
- **Documentation** — Operations runbook, API reference, and administrator guide
- **Training** — Platform training for your security and operations teams

Timeline

Milestone	Typical Timeline
Discovery call	Day 1
Architecture design	Day 2–3
Deployment	Day 4–5
Monitor mode validation	Day 5–10
Go live (enforcement)	Day 10–14
Optimization period	Day 14–30

Most organizations are fully operational within two weeks of engagement. Complex multi-site deployments may require additional time for phased rollout.

Support

All deployments include:

- **Deployment support** — Engineering assistance during initial deployment and validation
- **Ongoing support** — Technical support for platform operations, policy guidance, and troubleshooting
- **Platform updates** — Regular updates with new features, security patches, and threat intelligence improvements
- **Partner support** — For partner-managed deployments, your partner provides first-line support with TARA INNOVA escalation