

v3.4-SEC-001 – Zero-Trust Architecture & Runtime Isolation Policy

Document Title	Zero-Trust Architecture & Runtime Isolation Policy
Version	v3.4
Document ID	v3.4-SEC-001
Date	2025-03-22
Author	Take Back Your Data – Sovereign Security Division
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the Zero-Trust security principles and runtime isolation mechanisms implemented in MaxOneOpen. It ensures that no execution unit, identity, or data source is implicitly trusted and that all runtime logic remains fully contained and auditable.

2. Zero-Trust Enforcement Logic

- All actors (users, models, services) must be explicitly validated
- No global or pre-granted permissions exist
- Tokens define all access rights, time-scoped and revocable
- Forks must implement runtime-bound ZK validation

3. Isolation Strategies

Layer	Isolation Type	Enforcement Control
Twin Runtime	Container-per-request	Token-triggered + sealed
Inference Layer	Model-internal sandbox	Schema + context-bound
Data Layer	Encrypted vaults	Key split + access token
Network	Peer-scoped transport mesh	No fallback route memory

4. Policy Application

- Policies must bind to runtime context and be enforced locally
- No central config or rule propagation allowed
- Each execution must be evaluated independently
- Misconfigurations must be auto-rejected and logged

5. Certification Enforcement

- Forks must demonstrate Zero-Trust flows via simulated breach tests
- Runtime logs must verify isolation integrity and token flow
- No execution bypass or shared context reuse is allowed

6. Certification Relevance

Zero-Trust enforcement and runtime isolation are mandatory for MaxOneOpen certification. All forks must implement fully auditable isolation logic, verified in both design and runtime.