

v3.4-SEC-001 – Security Architecture & Threat Model

Document Title	Security Architecture & Threat Model
Version	v3.4
Document ID	v3.4-SEC-001
Date	2025-03-22
Author	Take Back Your Data – Security Core Unit
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the core security architecture and the formal threat model for MaxOneOpen. It serves as a foundational reference for resilience design, audit requirements, and zero-trust implementation across all components.

2. Core Security Principles

- Zero-Trust at every layer (no implicit trust, ever)
- Principle of least privilege (PoLP)
- Full decentralization of sensitive processing
- UDUH compliance (User Data in User Hands)
- Cryptographic validation of all runtime events

3. Threat Classification Matrix

Category	Threat	Mitigation	Residual Risk
External	DDoS, Port Scanning	Service cloaking + mesh routing	Minimal
Internal	Twin privilege escalation	Policy-scoped token gating	Low
Supply Chain	Backdoored container	Hash verification + provenance	Minimal
Inference	Prompt leakage	Masked prompt flow logic	Low
Data	Central storage breach	UDUH / no central DB	None

4. Resilience & Detection Measures

- Self-monitoring container runtime
- Integrity-pulse mechanism (signed checksums)
- Behavioral anomaly detection via twin logs
- Secure twin fallback (shadow clone strategy)
- No trust in timestamps or external clocks

5. Defensive Isolation Zones

- Each twin executes in an isolated runtime
- No twin can access memory or signals from another

- MaxControl cannot override cryptographic boundaries
- Memory and prompt streams are sandboxed per interaction

6. Certification Relevance

Security architecture and threat model compliance is mandatory for MaxOneOpen certification. Forks must demonstrate equal or stronger protections and must explicitly document their threat assumptions and countermeasures.