# Global Threat Model – Capsule-Based Risk & Trust Boundary Framework

Version: 4.1 | Classification: CTO-Mandatory | Language: EN

Scope: Threat Vectors, Attack Surfaces, and Countermeasure Matrix for MaxOneOpen v4.1

## 0. Purpose & CTO Enforcement Context

This document defines the global threat and mitigation model for MaxOneOpen v4.1. It is mandatory under CTO-level certification and required for validating the system’s resistance against misuse, trust exploitation, signature bypass, replay attacks, forked governance, and capsule manipulation. All listed threats are linked to countermeasure capsules, control flows, and audit trace enforcement.

## 1. Threat Vector Classes & Attack Taxonomy

The following vector classes are addressed:  
- 🔐 Identity & Trust Abuse  
- 🔁 Replay Injection  
- 🧬 Capsule Forgery / Tampering  
- 🛰️ Forked Surveillance Layers (Soft Fork Takeovers)  
- 🛑 Rule Bypass & Signature Spoofing  
- 📤 Add-on Escalation & Runtime Leakage  
- 📚 Governance Drift (Unverified Global Authority Spread)

## 2. Threat-to-Mitigation Mapping Matrix

|  |  |  |
| --- | --- | --- |
| Threat Vector | Risk Description | Mitigation Capsule / Enforcement Module |
| Identity & Trust Abuse | Privilege escalation via compromised tokens or broken trust tiering | Module 12 – Trust Downgrade, TVC Capsule |
| Replay Injection | Reusing a valid execution capsule or message in an invalid session | Module 09/10 – TTL + Hash Trace, Replay Block Capsule |
| Capsule Forgery | Injection of tampered or off-ledger capsules | Module 13 – Ledger Verification, Signature Root Chain |
| Soft Fork Surveillance | Governance hijack via non-consensual forks | Module 18 – Reentry Verification, Fork Divergence Ledger |
| Rule Bypass | Injection of unverified rule sets or policies | Module 04/05 – Rule Validation Capsule, Binding Enforcement |
| Add-on Escalation | OSS Add-ons invoking higher-tier runtime commands | Module 06/07 – Trust Scope Isolation, Add-on Sandbox Capsule |
| Governance Drift | Deployment of central authority without global consensus | NEW: Global Consent Ledger (to be implemented) |

## 3. Enforcement Interfaces & Capsule Types

Each mitigation path uses standardized capsule logic:  
- Trust Violation Capsule (TVC)  
- Replay Block Capsule (RBC)  
- Rule Injection Capsule (RIC)  
- Fork Trace Capsule (FTC)  
- Ledger Root Capsule (LRC)  
- Add-on Sandbox Capsule (ASC)  
All are committed via Module 13 and auditable via Module 14 forensic routines.

## 4. CTO Control Anchor & Certification Scope

This threat model is mandatory for any system seeking sovereign certification or high-assurance CTO-level deployment. It anchors directly into Module 17 (Certification) and must be validated in capsule-replay environments and during reentry reviews (Module 18). Absence of this model invalidates audit trace completeness and runtime trust guarantees.