

## v3.4-SCAN-001 – Security Scanning & Compliance Automation

Document Title	Security Scanning & Compliance Automation
Version	v3.4
Document ID	v3.4-SCAN-001
Date	2025-03-22
Author	Take Back Your Data – Compliance Automation Unit
Document Type	Public / Certification / Internal

### 1. Purpose & Scope

This document defines the security scanning and compliance automation logic within MaxOneOpen. It ensures that all deployments, forks, and updates can be continuously verified against security policies and certification baselines.

### 2. Scanning Framework Architecture

- Each module includes a self-check interface
- MaxControl periodically initiates scan requests
- Results are signed and optionally forwarded to mesh validators
- Scan logic is container-isolated and non-invasive

### 3. Compliance Ruleset Structure

Rule Type	Enforced Condition	Violation Action
Memory Retention	Only ephemeral or signed user-initiated	Terminate + log
ZK Compliance	ZK signature required for sensitive output	Block + alert
Container Drift	Runtime hash mismatch	Rebuild + quarantine
Quota Abuse	Exceeds defined limits	Suspend + force audit

### 4. Automation Pipeline Logic

- Scan jobs are scheduled by Control Layer
- Twin modules self-initiate internal probe
- Outcomes include: Pass / Deviation / Breach
- Forks must expose scan endpoints and allow policy hooks

### 5. Certification Maintenance Workflow

- Certified systems must pass full scan at deployment + updates
- Failure results in revocation unless corrected
- Periodic proofs of scan history must be available
- Manual override is allowed only under ZK-verified emergency scope

## 6. Certification Relevance

Security scanning and compliance automation is required for all certified MaxOneOpen deployments. Certification can be suspended or revoked on automated breach detection.