

## v3.4-SCN-001 – Autonomous Vulnerability Scanning & Threat Surface Modeling

Document Title	Autonomous Vulnerability Scanning & Threat Surface Modeling
Version	v3.4
Document ID	v3.4-SCN-001
Date	2025-03-22
Author	Take Back Your Data – Scan Intelligence Division
Document Type	Public / Certification / Internal

### 1. Purpose & Scope

This document defines the framework for continuous autonomous vulnerability scanning and threat surface modeling for MaxOneOpen-certified forks. It ensures early detection of security gaps, pattern-based anomaly indicators, and schema-specific risk correlation.

### 2. Scanning Architecture

- Scanners operate locally and within twin-isolated runtime
- Signature DBs are schema-bound and hash-pinned
- Live correlation against twin logs and AI anomaly engines
- Forks define scanning intervals and exemption boundaries

### 3. Threat Surface Modeling

Domain	Exposure Metric	Modeling Outcome
Network Entry	Port entropy + route disclosure	Ingress risk map
Runtime Scope	Token surface + container drift	Execution risk profile
Schema Integrity	Policy drift + override vector	Data access exposure
Fork Behavior	Heuristic deviation	Alert escalation path

### 4. Scanner Compliance Rules

- All forks must implement integrated, self-validating scanners
- Scanning results must be ZK-sealed and exportable
- Forks may not suppress or filter vulnerability class
- False positive handling must be schema-declared

### 5. Certification Triggers

- Certification requires threat surface map and scanner log integrity
- Missing coverage in declared risk domain voids certification
- Failing to expose false positive logic or log path results in rejection

## 6. Certification Relevance

Vulnerability scanning and dynamic threat surface modeling are required for all MaxOneOpen-certified forks. Auditable, schema-bound and runtime-coupled scanning must be provable at all times.