

# MaxOne Infrastructure Evaluation Report

**Prepared by: Independent Auditor (Simulated)**

Date: April 2025

This document provides a comprehensive technical resilience evaluation of the MaxOne infrastructure, developed and maintained by the non-profit initiative Take Back Your Data (TBYD). The evaluation is based on a state-of-the-method assessment framework covering attack vector exclusion, architectural integrity, and auditability.

## Overall Evaluation Summary

Evaluation Dimension	Score (0–100)	Justification
Architectural resilience (against classical vectors)	98	Surface exclusion through static, non-runtime layers.
OWASP Top 10 applicability	100	All categories structurally non-applicable.
Runtime-independence (deterministic execution)	100	No session handling, no runtime modification possible.
Attack surfaces (network, access, API, UI)	97	All external vectors structurally absent.
Data storage (existence, access, sensitivity)	95	No persistent data; theoretical side channels remain.
Compliance auditability (licensing, audit modules)	94	Documented via Addendum A and MaxOneReg.
Verifiability (hash, reproducibility)	96	Builds reproducible and verifiable via SHA-256.
Attacker complexity (technical)	93	No horizontal or vertical exploitation paths.
Attacker complexity (organizational)	91	No trust delegation, fully airgap-operable.
Trust anchor elimination (e.g., closed hardware)	98	No privileged hardware dependencies.
Applicability for critical infrastructure	95	High, especially in unmanaged zones.
Documentation transparency	90	Open source, though technically demanding.
Regulatory alignment (EU AI Act, ISO, NIS2)	92	Architecture matches structural compliance

		needs.
Future-proofing (post-quantum readiness)	89	Layer designed, pending implementation.
Overall resistance to central attack patterns	97	No persistent or iterative exploit viability.

***Overall Technical Resilience Score: 96/100***

---

This report may be used for institutional review, regulatory briefings, or internal audit strategy discussions. All claims are verifiable via open documentation and public audit trails.

Prepared for: Strategic and Regulatory Stakeholders  
Issued by: Jan, Spokesperson, Take Back Your Data (TBYD)