

See the gaps. Keep the plant still.

Offline assurance for exported firewall, router, managed-switch and industrial security-device configurations.

WHAT TECHWIZ DOES

TechWiz automatically detects readable device exports, normalises configuration evidence and runs deterministic OT-aware checks. It exposes policy weaknesses, management-plane risk, segmentation gaps, ransomware-relevant paths and meaningful configuration drift - without credentials or contact with the live device.

ZERO

live-device contact

OFFLINE

local analysis

TRACEABLE

evidence-led findings

THE SALES PROPOSITION

Assessment-grade configuration assurance across mixed and legacy OT estates, delivered without scanning or disrupting operations.

[REQUEST A TECHWIZ EVALUATION](#)



FROM EXPORT TO EVIDENCE

Deep configuration assurance. No operational disruption.

01

Add exports

Readable files from firewalls, routers, managed switches and comparable appliances.

02

Confirm context

Native, compatible or universal analysis route with transparent coverage warnings.

03

Review findings

Evidence-linked gaps, risk priority and OT-safe remediation guidance.

04

Share outputs

HTML, Excel, CSV, JSON and SARIF with a SHA-256 integrity manifest.

CAPABILITIES

Policy hygiene

Permissive, shadowed, redundant and unlogged rules.

Zones and conduits

Does the deployed configuration enforce the intended design?

Exposure review

Risky management paths and ransomware-relevant connectivity.

Configuration drift

Semantic comparison of previous and current exports.

Mixed estates

Native, compatible and vendor-neutral analysis levels.

Standards mapping

IEC 62443, NIST SP 800-82, CSF and applicable CIS/STIG.

CLEAR SCOPE

Designed for readable network-device configurations. PLC, DCS, RTU, relay, camera and storage engineering require separate specialist assessment. Findings must be validated against the exact model, firmware, safety constraints and approved OT change process.