OTOPIQ SECURITY

Device-Level OT Security
For Critical Operations

Secure every change. Restore any device.

OTOPIQ protects the PLCs, HMIs, and engineering workstations behind critical operations, and brings them back to a trusted state in one click when something goes wrong.

THE CHALLENGE

Every incident ends at the controller

Whether it starts with an attacker, a contractor, or a failed update, the damage happens at the controller. Network tools can see it. Few sites control who touches a controller, and fewer can restore it to a trusted state fast.

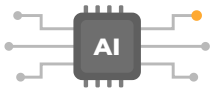
External Threats

IT breaches that move into OT and reach the controller



Persistent AI Threats

Ongoing campaigns using AI generated scripts to target PLCs



Internal Threats

Contractors, shared credentials, and human error



Multiple Vendors, Legacy & New

Mixed fleets, many too old to patch or replace

Schneider Electric · SIEMENS · Rockwell Automation · OMRON



THE OTOPIQ PLATFORM

One lifecycle for every controller

Protection and resilience at the device itself, backed by full visibility and run from one centralized platform.

01 Discover
Know every asset and connection

02 Protect
Control every session and change

03 Detect
Catch unauthorized change live

04 Recover
Restore any device in one click

Centralized Management is the single source of truth for every device, user, and change, across all vendors and sites.

AI Workflow Engine learns a device operation once and turns it into a reusable workflow the engineer controls.

AT THE CORE

Protect every change. Recover from anything.

PROTECTION

Control every session and change

- Zero trust access at the engineering workstation
- MFA and role based permissions per device
- Every change authorized before it executes
- Every action tied to a named person
- Secure PLC programming with encryption

For the CISO: a defensible answer for auditors, regulators, and insurers.



BACKUP, RESTORE & RESILIENCE

Restore any device in one click

- Automatic backup on every change
- Full version history for every device
- One click rollback to a known good state
- Compare versions to see what changed, and who
- Encrypted Fail Safe Kit for offline recovery

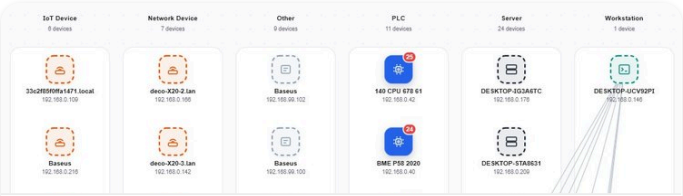
For operations: uptime when a vendor, a person, or an update gets it wrong.



FULL VISIBILITY

Discover and Detect power the core

You can only protect and recover what you can see. Discover maps every asset, and Detect flags every change, so Protect and Recover always act on the full picture.

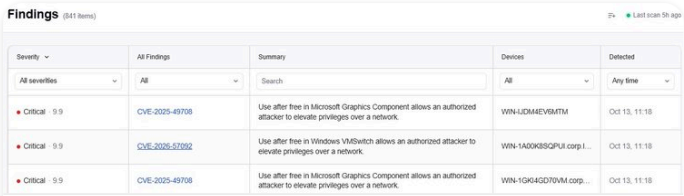


DISCOVER

Know every asset you protect

- Passive & active learning
- Live communication mapping
- Automatic classification
- Asset & risk visibility

Feeds Protect: every device found can be secured



DETECT

See change as it happens

- Human presence detection
- Communication anomalies
- CVE findings by severity
- Weak credentials

Feeds Recover: shows what changed and what to restore

HOW IT WORKS

Every change secured. Every change backed up.

1. **Request** — Engineer opens a session from the workstation
2. **Verify** — MFA and role checked for that device
3. **Execute** — Authorized change runs, logged to a person
4. **Back Up** — Every change saved and versioned automatically
5. **Restore** — Any verified version, in one click

PROTECTION | BACKUP & RESTORE

Attack alters PLC logic

See exactly what changed against the last verified version.

Restore the verified logic

Wrong config uploaded

The change is tied to a named person and saved as a version.

Roll back in one click

Platform or network down

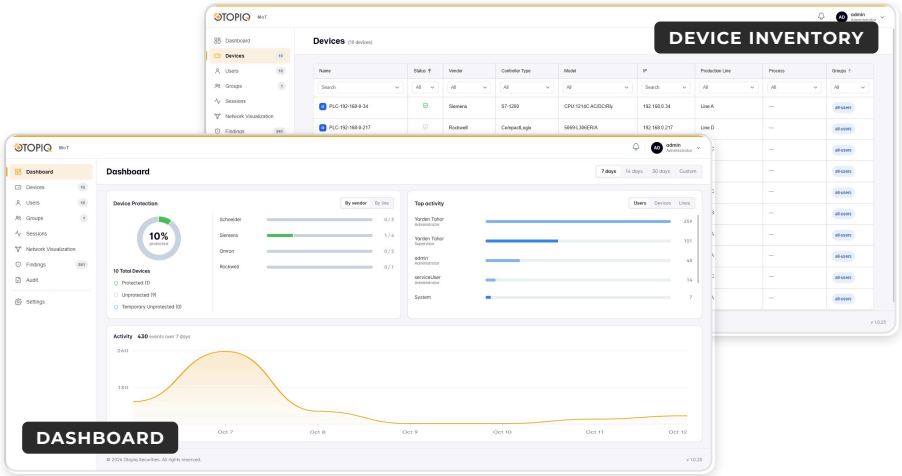
The encrypted Fail Safe Kit keeps the latest valid config at hand.

Recover offline

ONE PLATFORM

Every vendor, every generation, every site

- **Device protection at a glance:** protected and unprotected devices by vendor and process
- **Live inventory:** controller type, model, IP, and process for every device
- **Legacy and current:** compensating protection for devices that can't be patched
- **Any site:** connected, remote, air gapped, and offline environments



Comply with Rising Global Regulations

OTOPIQ turns regulatory requirements into automated, verifiable processes: authenticated access, full traceability, configuration integrity, and recovery evidence that auditors, regulators, and insurers ask for. Built to support frameworks including NIST SP 800-82, IEC 62443, NIS2, and the Singapore CCoP.