OTOPIQ SECURITY

Securing the Core of Industrial Operations

AI-BASED ZERO-TRUST DEVICE-LEVEL OT SECURITY & MANAGEMENT

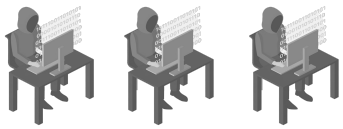
The Challenge

Industrial OT environments are harder than ever to secure. They face constant pressure from external cyber threats, internal risks such as operator mistakes and third-party contractor actions, and the growing complexity of managing multiple vendors and generations of equipment.

Together, these challenges create blind spots, operational instability, and unnecessary risk.

External Threats

Exploiting IT breaches and OT weaknesses



Internal Threats

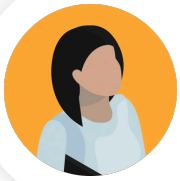
Including 3rd party OT automation contractors and human errors

Multiple Vendors, Legacy & New

Schneider Electric · SIEMENS · ABB · Rockwell Automation · OMRON · EMERSON

The Cybersecurity & Operations Gap

Security teams need tighter control, while operations teams need quick access and flexibility to keep systems running. When these priorities collide, risk increases and uptime suffers.



Security Teams

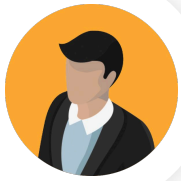
Face Escalating Risks

- Rising Cyber Threats
- Insider & Third-Party Risks
- Human Error

Operation Teams

Struggle to Maintain Oversight

- Multi-Vendor Environments
- Limited OT Visibility
- Accountability Gaps



The OTOPIQ Solution

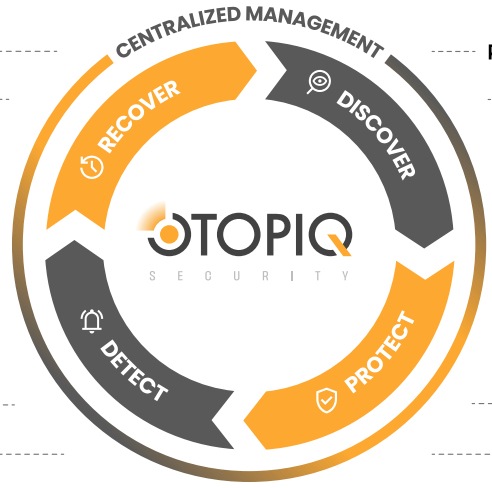
A One-Stop, Centralized Platform for Holistic OT Security & Management

RECOVER

- Automatic Backup & Version History
- One-Click Rollback
- Failsafe Kit

DISCOVER

- Passive & Active Learning of Environment
- Asset & Risk Visibility
- Live Communication Mapping



DETECT

- Human Presence Detection.
- Communication Anomalies
- CVE's & Weak Credentials

PROTECT

- Device Access Control
- Secure PLC Programming
- EWS/ HMI hardening

AI-Driven Platform Intelligence

Applies ML-based analysis of device state changes, communication patterns, and user actions to highlight real risk, reduce manual investigation, and accelerate incident resolution.

Discover

Continuously identifies Level 1-2 devices using passive, probe-less technology, building a live, vendor-agnostic inventory for full visibility.

Protect

Zero-Trust access controls with MFA, role-based permissions, and secure workflows — ensuring verified actions and rapid recovery, with encryption applied both in transit and at rest for protected execution.

Detect

Monitors PLC logic, HMI and workstation projects, and configuration changes in real time, correlating behaviors with known weaknesses and CVEs to expose vulnerabilities and unauthorized edits.

Recover

Automatically backs up every configuration change and enables one-click rollback to a known-good state, with the encrypted Fail Safe Kit ensuring a smooth recovery if a disaster occurs.

Prevention, Detection & Access Control + Device-Level Visibility, Configuration History & Management = Guaranteed Uptime → Proven ROI

Strengthen Visibility & Traceability Across All OT Assets

Gain unified oversight of your most critical OT devices, users, and configurations in real time

- User and Device Management: Complete visibility into every user, device, and interaction
- Configuration changes are automatically saved and traceable, maintaining a complete configuration history
- Seamless Auditing: Generate real-time audit trails for security and operational reporting

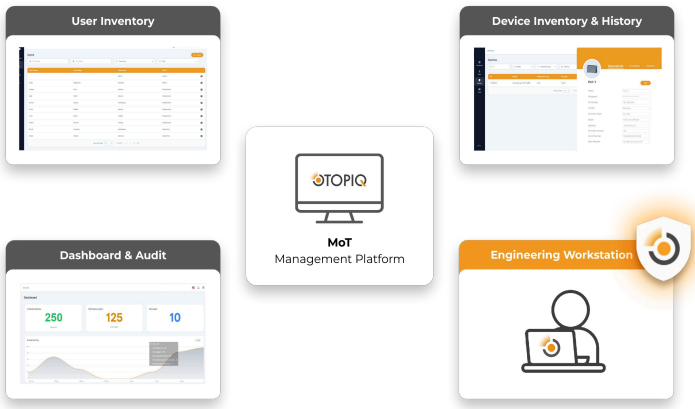
Device-Level Protection Against Insider & External Threats With Access Control

- **Enforce identity-based access:** Apply Zero-Trust controls with MFA, role-based permissions, and secure workflows to prevent unauthorized device actions
- **Validate every change before execution:** Ensure every action, update, and configuration change is authorized and logged—fully traceable to both user and device
- **Protect operations with rapid incident response:** Restore devices to previously verified states using configuration history—minimizing downtime caused by unauthorized changes, failed updates, or human error

Unify Multi-Vendor, Legacy & Modern Devices Under One Platform

Brings mixed generations and device types together under one secure management platform — simplifying control across diverse OT environments

- **Centralized Oversight:** Single interface for all types of Industrial Control Systems (ICS)
- **Legacy Modernization:** Extends lifespan with consistent, compensating security controls
- **Standardized Governance:** Ensures common policies and visibility across distributed operations



Comply with Rising Global Regulations

OTOPIQ turns regulatory requirements into automated, verifiable processes — helping teams meet global standards with secure access, full traceability, and configuration integrity. Built to support evolving mandates, including future post-quantum cryptographic requirements for long-life industrial systems.

CISA · NIST · CSA SINGAPORE · NIS2