

Hi, I'm Roy. I make complex security products easy to buy, sell and back.

Product marketing in OT cybersecurity.

Roy Bar Or.

Product Marketing & GTM

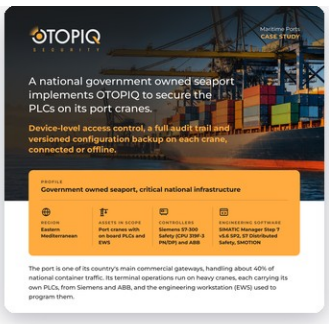
Customer names redacted where required



01 · p. 2
Platform Brief



02 · p. 5
Partner Battlecard



03 · p. 8
Customer Case Studies

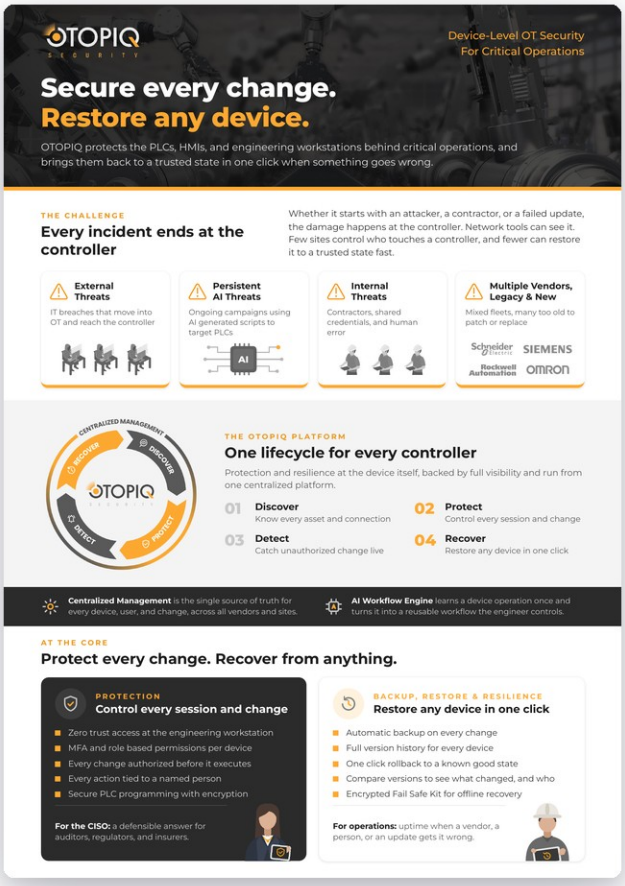


04 · p. 15
Investor Update

01

Platform Brief

One promise, four stages, two buyers.



THE BRIEF

Explain a deep OT security platform to security and operations buyers at once.

MY ROLE

Message hierarchy, copy and layout.

LOOK FOR

- Six word headline
- CISO vs. operations split
- Compliance mapping

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.

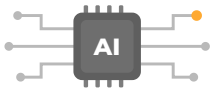
External Threats

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

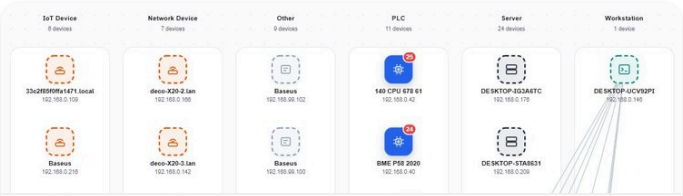
For operations: uptime when a vendor, a person, or an update gets it wrong.



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.

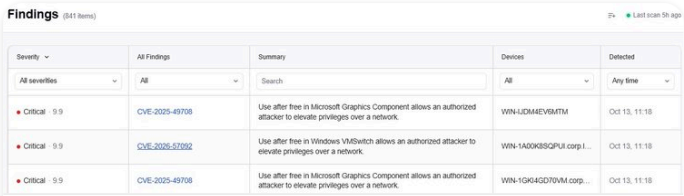


DISCOVER

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

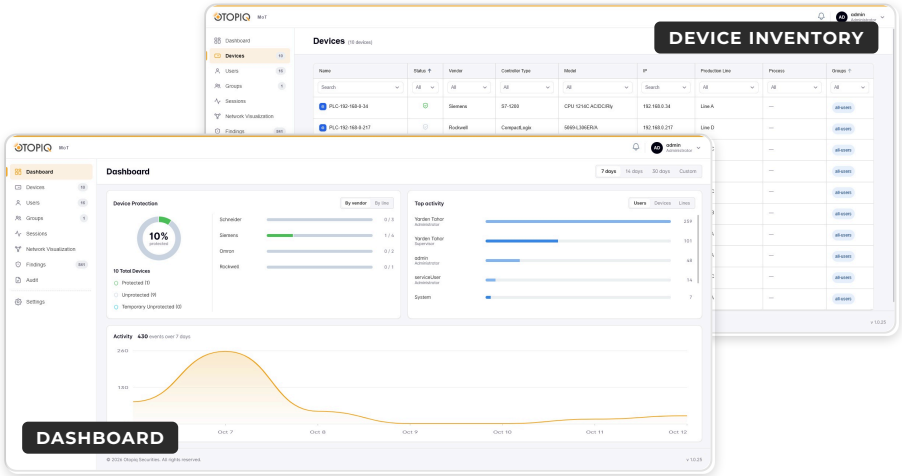
The encrypted Fail Safe Kit keeps the latest valid config at hand.

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



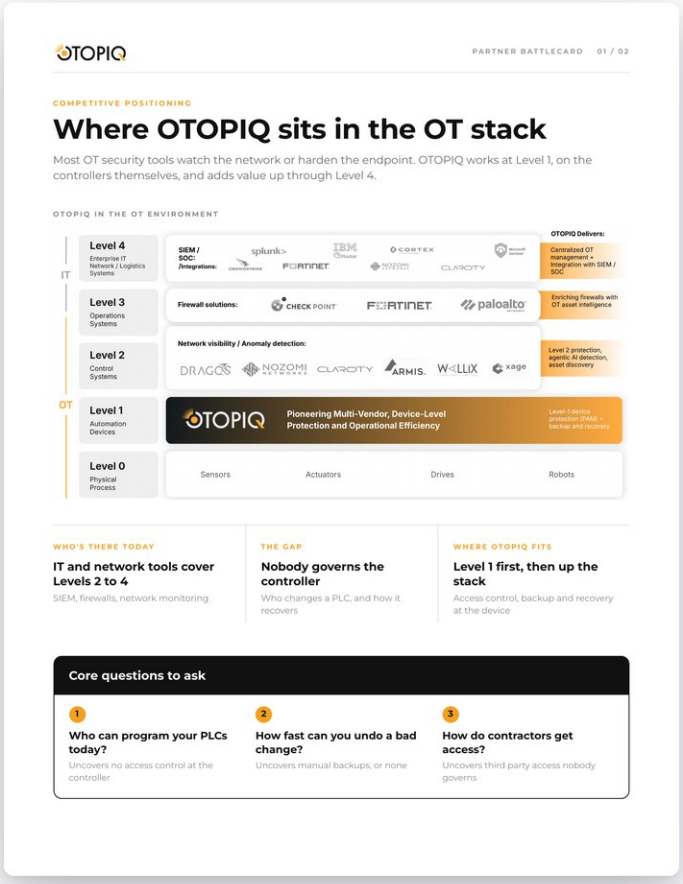
Comply with Rising Global Regulations

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.

02

Partner Battlecard

Where we fit, not just how we compare.



OTOPIQ

PARTNER BATTLECARD 01 / 02

COMPETITIVE POSITIONING

Where OTOPIQ sits in the OT stack

Most OT security tools watch the network or harden the endpoint. OTOPIQ works at Level 1, on the controllers themselves, and adds value up through Level 4.

OTOPIQ IN THE OT ENVIRONMENT

IT

Level 4 — Enterprise IT Network / Logistics Systems
SIEM / SOC: /Integrations: splunk> IBM QRadar CORTEX Microsoft Sentinel FORTINET Nozomi Networks CLAROTY
OTOPIQ Delivers: Centralized OT management + integration with SIEM / SOC

Level 3 — Operations Systems
Firewall solutions: CHECK POINT FORTINET paloalto
Enriching firewalls with OT asset intelligence

Level 2 — Control Systems
Network visibility / Anomaly detection: DRAGOS NOZOMI NETWORKS CLAROTY ARMIS. WALLIX xage
Level 2 protection, agentic AI detection, asset discovery

OT

Level 1 — Automation Devices
OTOPIQ Pioneering Multi-Vendor, Device-Level Protection and Operational Efficiency
Level-1 device protection (PAM) + backup and recovery

Level 0 — Physical Process
Sensors Actuators Drives Robots

WHO'S THERE TODAY
IT and network tools cover Levels 2 to 4
SIEM, firewalls, network monitoring

THE GAP
Nobody governs the controller
Who changes a PLC, and how it recovers

WHERE OTOPIQ FITS
Level 1 first, then up the stack
Access control, backup and recovery at the device

Core questions to ask

1. **Who can program your PLCs today?** Uncovers no access control at the controller
2. **How fast can you undo a bad change?** Uncovers manual backups, or none
3. **How do contractors get access?** Uncovers third party access nobody governs

THE BRIEF

Equip partners who meet established OT vendors in nearly every account.

MY ROLE

Competitive research, capability matrix and discovery questions.

LOOK FOR

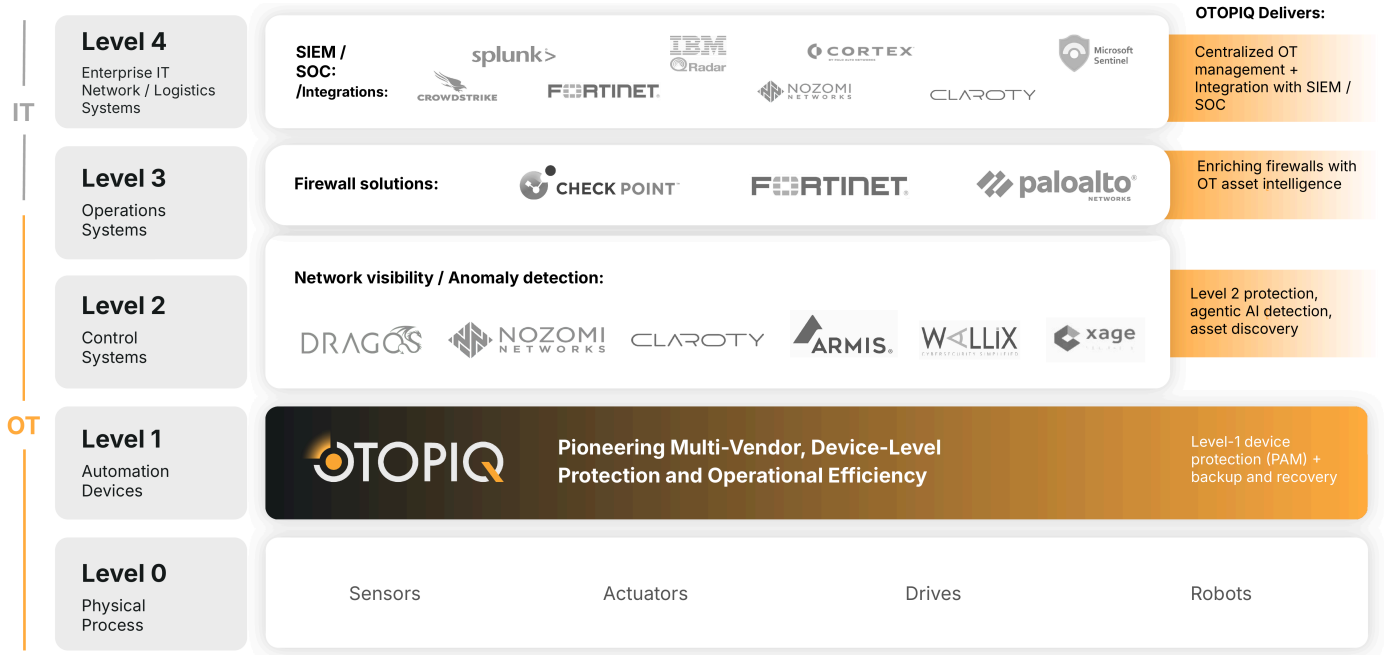
- Market mapped by Purdue level
- Honest three point scale
- Questions tied to gaps

COMPETITIVE POSITIONING

Where OTOPIQ sits in the OT stack

Most OT security tools watch the network or harden the endpoint. OTOPIQ works at Level 1, on the controllers themselves, and adds value up through Level 4.

OTOPIQ IN THE OT ENVIRONMENT



WHO'S THERE TODAY

IT and network tools cover Levels 2 to 4

SIEM, firewalls, network monitoring

THE GAP

Nobody governs the controller

Who changes a PLC, and how it recovers

WHERE OTOPIQ FITS

Level 1 first, then up the stack

Access control, backup and recovery at the device

Core questions to ask

1

Who can program your PLCs today?

Uncovers no access control at the controller

2

How fast can you undo a bad change?

Uncovers manual backups, or none

3

How do contractors get access?

Uncovers third party access nobody governs

COMPETITIVE COMPARISON

Capability comparison by vendor

Core OT security capabilities across the vendors partners meet most often.

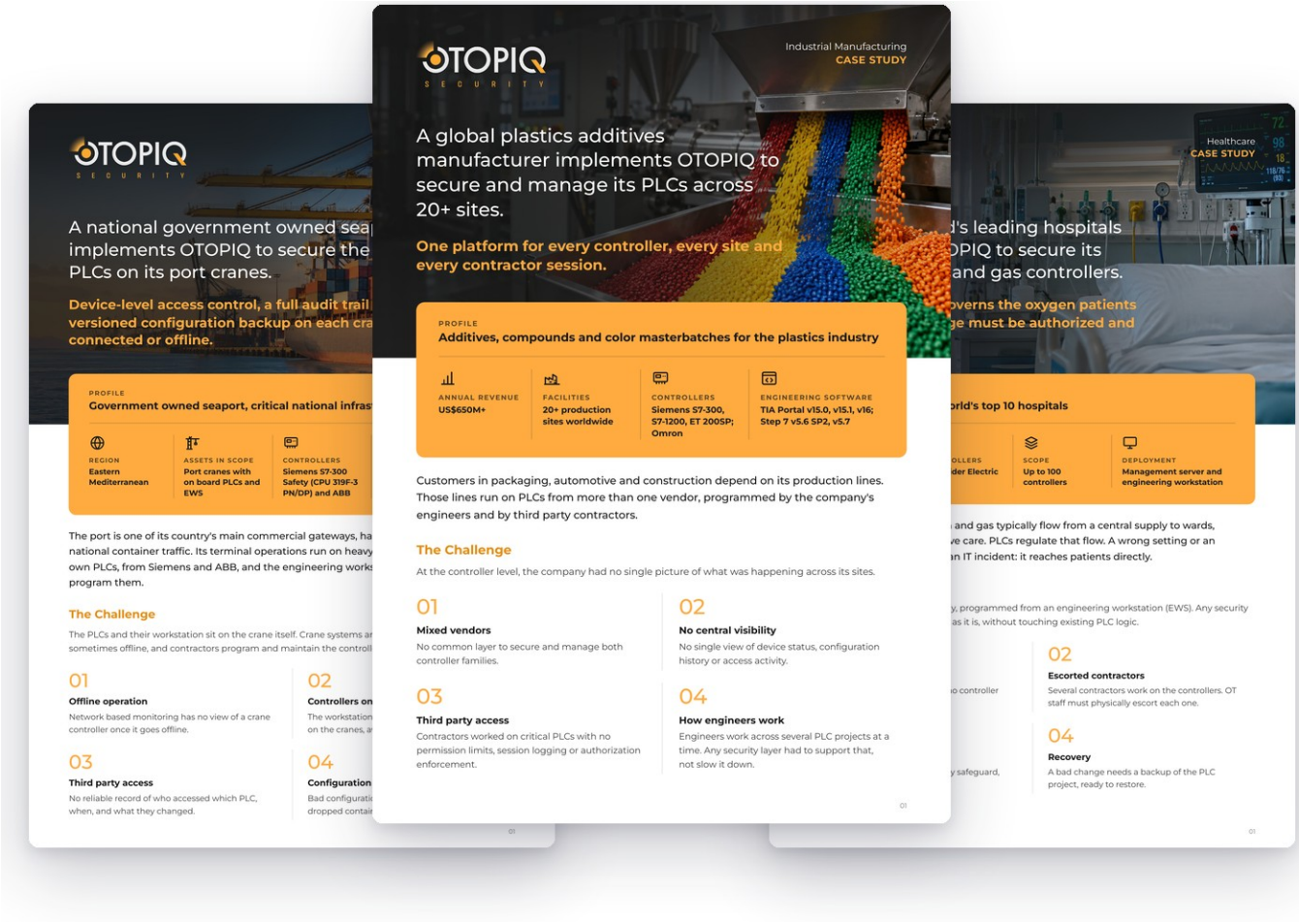
CAPABILITY	CLAROTY NOZOMI DRAGOS	ARMIS	TXONE	OPSWAT	OCTOPLANT	OTOPIQ
Passive learning of the OT network	✓	✓	✓	◐	–	✓
Active discovery of the OT network	✓	✓	✓	◐	–	✓
Flags PLC changes with no human at the keyboard	–	–	–	–	–	✓
Secure PLC programming, authorized users only	–	–	–	–	–	✓
Automatic backup and rollback of PLC configs	–	–	–	–	◐	✓
Automatic backup of EWS and HMI files	–	–	–	–	–	✓
USB, app and IP control on EWS and HMI	–	–	◐	◐	–	✓
CVEs pinpointed to exact firmware	◐	✓	◐	–	◐	✓
Deploys in air gapped environments	◐	◐	✓	◐	✓	✓

✓ Yes ◐ Partial or limited – Not offered

03

Customer Case Studies

Three industries, three buyers, one story structure.



THE BRIEF

Prove the platform to buyers in ports, manufacturing and healthcare.

MY ROLE

Story structure, copy and anonymization for each customer.

INDUSTRIES

Maritime ports

Industrial manufacturing

Healthcare



Maritime Ports
CASE STUDY

A national government owned seaport implements OTOPIQ to secure the PLCs on its port cranes.

Device-level access control, a full audit trail and versioned configuration backup on each crane, connected or offline.

PROFILE
Government owned seaport, critical national infrastructure

REGION	ASSETS IN SCOPE	CONTROLLERS	ENGINEERING SOFTWARE
Eastern Mediterranean	**Port cranes with on board PLCs and EWS**	**Siemens S7-300 Safety (CPU 319F-3 PN/DP) and ABB**	**SIMATIC Manager Step 7 v5.6 SP2, S7 Distributed Safety, SMOTION**

The port is one of its country's main commercial gateways, handling about 40% of national container traffic. Its terminal operations run on heavy cranes, each carrying its own PLCs, from Siemens and ABB, and the engineering workstation (EWS) used to program them.

The Challenge

The PLCs and their workstation sit on the crane itself. Crane systems are sometimes connected and sometimes offline, and contractors program and maintain the controllers on site.

01

Offline operation

Network based monitoring has no view of a crane controller once it goes offline.

02

Controllers on the crane

The workstations that can change the PLCs sit on the cranes, away from central oversight.

03

Third party access

No reliable record of who accessed which PLC, when, and what they changed.

04

Configuration incidents

Bad configurations disrupted operations, like dropped containers, with no version history.

The Solution

OTOPIQ runs on the engineering workstation on each crane, where the PLCs are programmed, and stays in place whether the crane is connected or offline. It covers the port's Siemens controllers today, with support for its ABB PLCs being added.

Runs on the crane

Installed on the crane's EWS. No dependency on connectivity.

Access by role

Only authorized users can program or change a PLC.

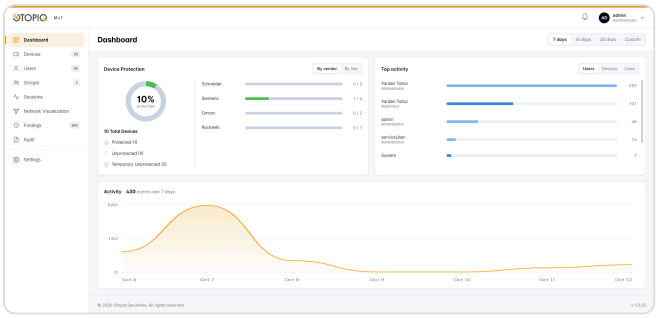
Sessions logged

Who accessed which PLC, when, and what changed.

Versioned backup

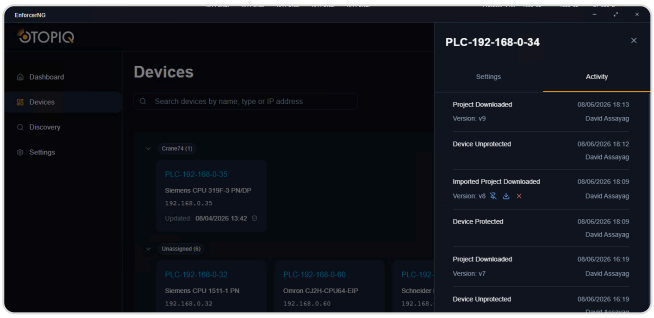
Every change saved as a version, with rollback to a known good one.

DASHBOARD



Protection status, users and activity in one view.

BACKUPS



Every change saved as a version on the workstation, ready to download, pin or restore.

Results and Benefits

- Control over who changes each crane PLC, connected or offline
- Contractor work traceable to a named user
- A known good version to return to after a bad change
- A clear record of which configuration was running when an incident occurred
- No hardware changes to the cranes

> When something goes wrong on a crane, the first question is always what changed. Now we have the answer, even if the crane was offline when it happened.

CISO, GOVERNMENT OWNED SEAPORT

For more information:

info@otopiqsecurity.com | www.otopiqsecurity.com

OTOPIQ SECURITY

OTOPIQ SECURITY

Industrial Manufacturing
CASE STUDY



A global plastics additives manufacturer implements OTOPIQ to secure and manage its PLCs across 20+ sites.

One platform for every controller, every site and every contractor session.

PROFILE

Additives, compounds and color masterbatches for the plastics industry

ANNUAL REVENUE	FACILITIES	CONTROLLERS	ENGINEERING SOFTWARE
US$650M+	**20+ production sites worldwide**	**Siemens S7-300, S7-1200, ET 200SP; Omron**	**TIA Portal v15.0, v15.1, v16; Step 7 v5.6 SP2, v5.7**

Customers in packaging, automotive and construction depend on its production lines. Those lines run on PLCs from more than one vendor, programmed by the company's engineers and by third party contractors.

The Challenge

At the controller level, the company had no single picture of what was happening across its sites.

01

Mixed vendors

No common layer to secure and manage both controller families.

02

No central visibility

No single view of device status, configuration history or access activity.

03

Third party access

Contractors worked on critical PLCs with no permission limits, session logging or authorization enforcement.

04

How engineers work

Engineers work across several PLC projects at a time. Any security layer had to support that, not slow it down.

The Solution

OTOPIQ brings both controller families and every site into one platform, and puts every contractor session under control.

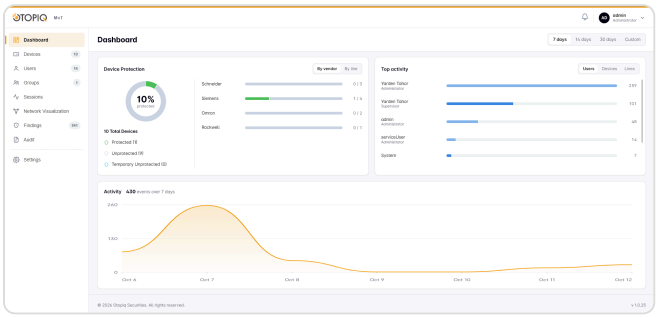
Central visibility
Protection status, inventory and access activity in one view.

Contractor access
Who is accessing which PLC, when, and from where.

Config history
Every authorized change versioned, per device.

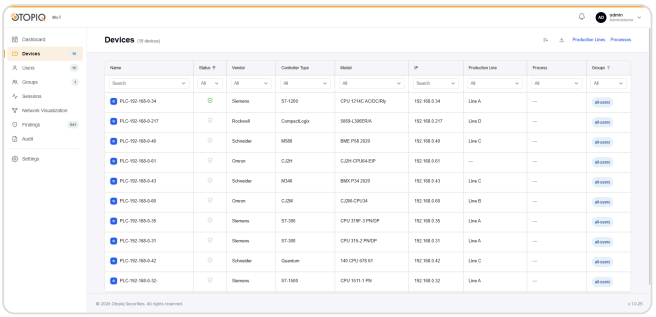
Multiple projects
Support for parallel PLC projects, built at the company's request.

DASHBOARD



Protection status, users and activity across vendors and production lines.

DEVICES



Every controller by vendor, model and protection status.

Results and Benefits

- Consistent security across every site and both controller vendors
- Contractor work accountable to a named user
- A known history behind every configuration change
- Engineers keep their workflow, including parallel projects
- Leadership visibility into OT without relying on day to day OT teams

> For the first time, I can actually see what's happening on our controllers at every site. What's protected, who's working on them, and what changed.

CISO, GLOBAL PLASTICS ADDITIVES MANUFACTURER

For more information:
info@otopiqsecurity.com | www.otopiqsecurity.com

OTOPIQ SECURITY



Healthcare
CASE STUDY

One of the world's leading hospitals implements OTOPIQ to secure its medical oxygen and gas controllers.

When a controller governs the oxygen patients breathe, every change must be authorized and recoverable.

PROFILE
Ranked among the world's top 10 hospitals

SYSTEMS	CONTROLLERS	SCOPE	DEPLOYMENT
Medical oxygen and gas systems	**Schneider Electric Twido**	**Up to 100 controllers**	**Management server and engineering workstation**

In a hospital, medical oxygen and gas typically flow from a central supply to wards, operating rooms and intensive care. PLCs regulate that flow. A wrong setting or an unauthorized change is not an IT incident: it reaches patients directly.

The Challenge

The controllers are a legacy family, programmed from an engineering workstation (EWS). Any security layer had to fit that environment as it is, without touching existing PLC logic.

01

Life sustaining supply

Oxygen delivery cannot pause, so no controller change can be left to chance.

02

Escorted contractors

Several contractors work on the controllers. OT staff must physically escort each one.

03

Locked doors as protection

Locked control rooms were the only safeguard, and some were found unlocked.

04

Recovery

A bad change needs a backup of the PLC project, ready to restore.

The Solution

OTOPIQ runs on the hospital's management server and on the EWS, where the controllers are programmed, so every change to the systems behind the oxygen supply passes through it first.

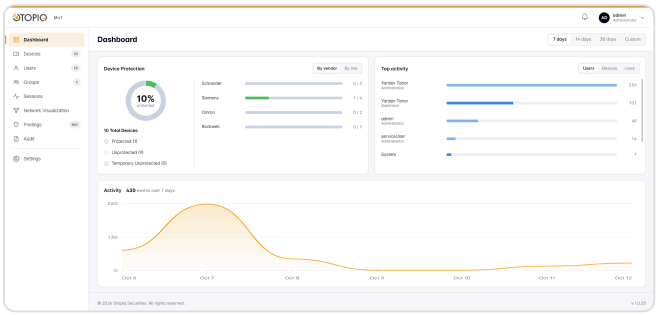
Secure programming
Controller programming runs through OTOPIQ on the EWS.

Contractor groups
Contractors organized into groups, each with its own permissions.

Automatic backup
PLC project files backed up, ready to restore.

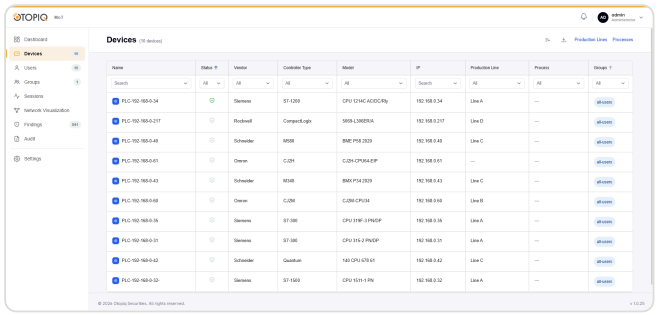
FailSafe kit
Encrypted USB kit keeps controllers maintainable if the server is down.

DASHBOARD



Users, protection status and activity in one view.

DEVICES



Every controller and its protection status.

Results and Benefits

- Changes to oxygen and gas controllers limited to authorized users
- Contractors organized into groups, each limited to its own permissions
- A known good project to return to after a bad change
- Maintenance continues even when the platform is down
- Admins and OT operators trained on their part of the platform

> Every time a contractor came in, one of us had to walk them to the control room and stay with them the whole time. Now I know exactly what each of them can touch, and if something changes, we can see it and put it back.

OT SUPERVISOR, LEADING MEDICAL CENTER

For more information:
info@otopiqsecurity.com | www.otopiqsecurity.com

OTOPIQ SECURITY

04

Investor Update

Where the market is heading, told through the product.



THE BRIEF

One report on rollouts, validation, market context and product.

MY ROLE

Narrative arc, copy and the CEO letter draft.

LOOK FOR

- Advisories mapped to capabilities
- One customer format
- Validation with limits

OTOPIQ SECURITY

OCTOBER 2026

INVESTOR UPDATE

Customer rollouts, market context and product developments

Device-level OT security for manufacturing and critical infrastructure



OTOPIQ Security · info@otopiqsecurity.com · www.otopiqsecurity.com

A NOTE FROM OUR CEO

From first release to production

Dear investors and friends,

In February we shared our first platform release and our first deployment with a global manufacturer. Eight months on, OTOPIQ is securing critical operations across several environments: manufacturing sites around the world at [redacted], port cranes at [redacted], oxygen and medical gas systems at [redacted], and chemicals operations at [redacted].

What stands out most is the feedback from our customers. Plant leaders tell us that, for the first time, they can see and govern who changes their controllers, and bring them back to a known good state when something goes wrong.

Much of what we built this year came straight from the field. Concurrent multi-project work was built at [redacted]'s request. Automatic backup and one-click recovery turn a bad change or an incident into a recovery step rather than an outage. Discovery and risk assessment give security teams a full picture of every device on the OT network.

We are also taking our first steps into the U.S. [redacted] is installing OTOPIQ in its OT lab, and [redacted] opens the path to public sector buyers.

This year's attacks and federal guidance point to the same place we started from: security and recovery at the device itself.

Thank you for your continued trust and support, and I look forward to sharing our next milestones with you.

Sincerely,

Tamar Milstein

CEO & CO-FOUNDER, OTOPIQ SECURITY

CUSTOMERS

Securing critical operations

Our customers span manufacturing, port infrastructure, healthcare and chemicals, and run on the controllers that keep their operations going.



[redacted]

Global manufacturer of plastics additives and color compounds

RUNS ON SIEMENS OMRON

MANUFACTURING

20

GLOBAL SITES

THE CHALLENGE

Mixed PLC estates across sites, with no single view of device status, configuration history or contractor access.

THE ENVIRONMENT

Production lines on several continents running **Siemens** (S7-300, S7-1200, ET 200SP) and **Omron** (CJ2M) controllers.

WHAT OTOPIQ DELIVERS

Device-level protection, backups and contractor governance in one view for leadership, plus multi-project support built at [redacted]'s request.



[redacted]

[redacted] critical national infrastructure

RUNS ON SIEMENS

PORT INFRASTRUCTURE

40%

OF [redacted] CONTAINER TRAFFIC

THE CHALLENGE

PLCs and engineering workstations sit on top of the cranes, with no network connection and ungoverned contractor access.

THE ENVIRONMENT

Crane controllers running **Siemens** S7-300 Safety (CPU 319F-3 PN/DP), managed from workstations on the crane itself.

WHAT OTOPIQ DELIVERS

Protection and a full change log run directly on the crane workstation, online or offline, where network tools cannot reach.



[redacted]

RUNS ON Schneider Electric

HEALTHCARE

THE CHALLENGE

Medical oxygen and gas systems that patients depend on, where an unauthorized change to a controller is not an option.

THE ENVIRONMENT

Hospital oxygen and medical gas systems running **Schneider Electric** controllers.

WHAT OTOPIQ DELIVERS

Device-level protection, access governance and recovery for the controllers that run the hospital's oxygen and gas supply.



[redacted]

Global specialty minerals and chemicals company

RUNS ON Schneider Electric

CHEMICALS

THE CHALLENGE

Large scale industrial operations where every change to a controller must be authorized and traceable.

THE ENVIRONMENT

Industrial environments running **Schneider Electric** Quantum 580 controllers.

WHAT OTOPIQ DELIVERS

Device-level security, change governance and recovery across its Schneider Electric controller environments.

INDEPENDENT VALIDATION

ICNL: Tried and Tested

OTOPIQ completed a controlled, third party validation at Israel's national ICS lab, covering engineering, misuse and incident response scenarios.

Why it matters. ICNL is Israel's national laboratory for cyber, industrial control systems, critical infrastructure and energy. Its findings give critical infrastructure buyers, integrators and regulators an independent reference before they deploy OT security controls.

ICNL ran OTOPIQ through nine use cases on live Siemens controllers, under normal operation and under simulated misuse and incident conditions.

ICNL ICS National Lab | INCD Israel National Cyber Directorate

TEST ENVIRONMENT

CONTROLLERS
Siemens S7-1200 and S7-1500

ENGINEERING SOFTWARE
Siemens TIA Portal v17

SCOPE
Authorization, configuration integrity and recovery

NINE USE CASES, ALL VALIDATED

- User and role management
- PLC registration
- Device protection
- Secure programming
- Unauthorized access attempts
- Automatic backup and versioning
- Cross group access restriction
- Disaster recovery
- Fail-safe recovery

RESULT 01

Authorization enforced at the PLC

Authorized users programmed normally. Unauthorized attempts were denied before execution.

RESULT 02

No unauthorized changes applied

No unauthorized programming or configuration change succeeded, across every misuse scenario.

RESULT 03

Recovery to a valid state

Restored after corruption, including through the Fail-Safe Kit with the server offline.

Next: This round covered two Siemens PLC models. ICNL noted that scale and multi-vendor coverage were outside its scope. OTOPIQ is returning to ICNL for an additional round of validation testing.

Full ICNL report available
Not public. Sent on request.

MARKET CONTEXT

The controller is now in focus

Across 2026, U.S. threat reporting and federal guidance point in the same direction: toward the controller itself. The two are not always directly linked, but the shift is consistent.

2026: ATTACKS REACHING THE CONTROLLER

APR → JUL 2026

AA26-097A; also DOE, CNMF, Treasury

Iranian affiliated actors disrupted PLCs across U.S. infrastructure.

- Malicious project file interactions and manipulated HMI and SCADA data
- Operational disruption and financial loss

PLC VENDORS TARGETED

Rockwell · Schneider Electric · Siemens

JUL 30, 2026

CISA alert with EPA and FBI, water sector

Actors changed PLC passwords to lock out operators and changed IP addresses.

- Boil water notices
- Sustained manual operations

SECTOR AFFECTED

Water and wastewater

AUG 2026

Joint advisory on Siemens S7; also DOE

An active threat to Siemens S7-200 through S7-1500 PLCs.

- AI generated scripts disguised as monitoring tools
- Read and write access to PLC memory, configuration and ladder logic

SECTORS TARGETED

Manufacturing · Energy · Water · Chemical

THE COMMON THREAD

In each case, the actors acted on the controller itself: its project files, passwords, configuration and logic.

WHAT THE AGENCIES ASK FOR	WHERE OTOPIQ FITS
Inventory every PLC Siemens S7 advisory	**Discovers and registers each controller**
Password protect PLCs; restrict programming to authorized workstations Siemens S7 advisory	**Enforces authorization at the PLC for every change**
Keep a known clean backup of each PLC CISA water alert	**Versions configuration automatically and restores to a known good state**
Flag logic or configuration changes made without a work order Siemens S7 advisory	**Logs who changed which PLC, what changed and when**

FEDERAL GUIDANCE IS FOLLOWING

NIST · SEP 2026

SP 800-82r4 draft (comments due Nov 30) calls for:

- Documented baselines and centrally tracked device changes
- A controlled change process for PLC logic
- Engineering workstation logs of sessions and project file access

NSA · OCT 2026

Zero Trust for OT environments calls for:

- Approved, maintained configurations for every controller
- Controller changes restricted, controlled and logged
- Engineering workstation access bound to each user's role

Agency marks identify the sources of the public advisories and guidance cited. No affiliation with, or endorsement of, OTOPIQ by any agency is implied. Sources: AA26-097A (Apr 7, 2026; updated Jul 22, 2026); CISA alert, Jul 30, 2026; joint CSA, Defending Against an Active Threat to Siemens S7 Series PLCs, Aug 2026; NSA CSI, Hardening DoW Critical OT Environments with ZT Principles, Oct 2026; NIST SP 800-82r4 ipd, Sep 2026.

PRODUCT AND R&D UPDATE

Platform updates and enhancements

New this period: discovery and risk assessment, and automatic backup with one-click recovery. Together they make OTOPIQ the only platform that sees, secures and restores the controllers running critical operations.

ONE PLATFORM, FOUR CORE PLC FAMILIES

Native protection, backup and recovery across the controller brands that run industrial operations.

Rockwell Automation · SIEMENS · Schneider Electric · OMRON

NEW

01 DISCOVER AND ASSESS

Maps every device on the OT network and scores its risk against known vulnerabilities (CVEs).

02 PROTECT

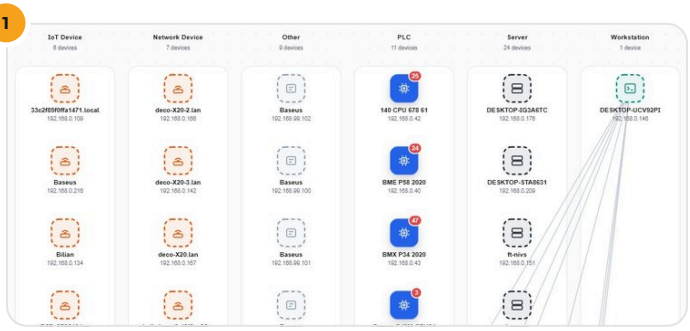
Authorization enforced at the PLC, inside the engineering tools teams already use. Every change logged.

NEW

03 RECOVER

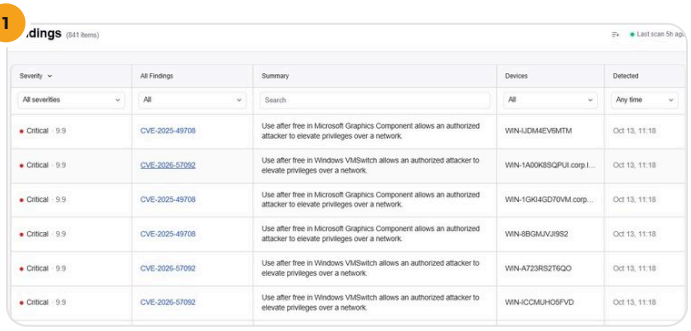
Every authorized change is backed up automatically. Restore any version in one click, for any reason.

1



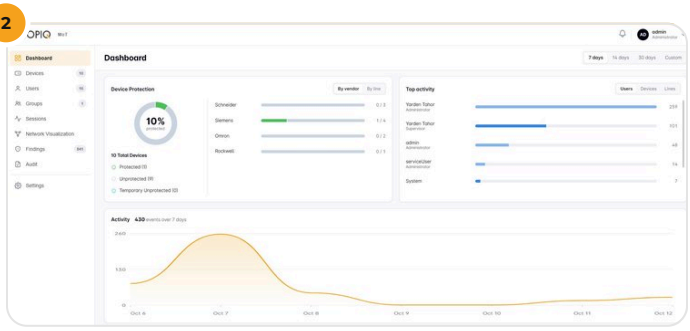
Network visualization: devices by type, with open risk counts per PLC

1



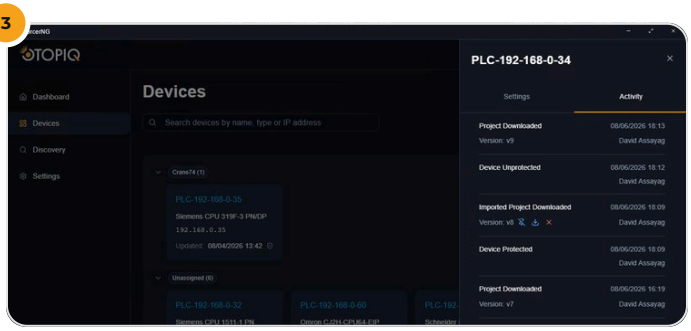
Findings: vulnerabilities ranked by severity

2



MoT dashboard: protection status by vendor, top activity and events over time

3



Enforcer: version history with one click restore



FOR THE CISO

Security and peace of mind

Full visibility of risk, enforced access to every controller, and proof of recovery readiness.



FOR OPERATIONS

Control and uptime

Teams keep their tools and workflows, and can roll back without waiting on anyone.