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

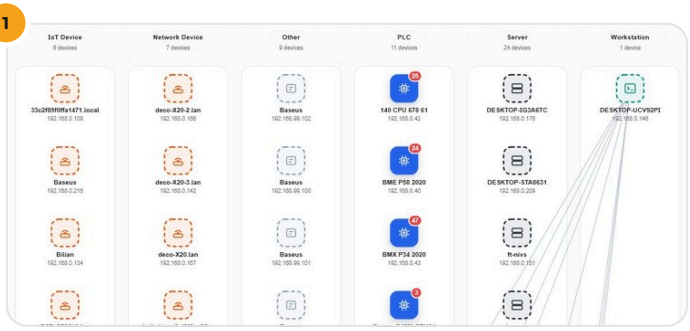
Authorization enforced at the PLC, inside the engineering tools teams already use. Every change logged.

NEW

03 RECOVER

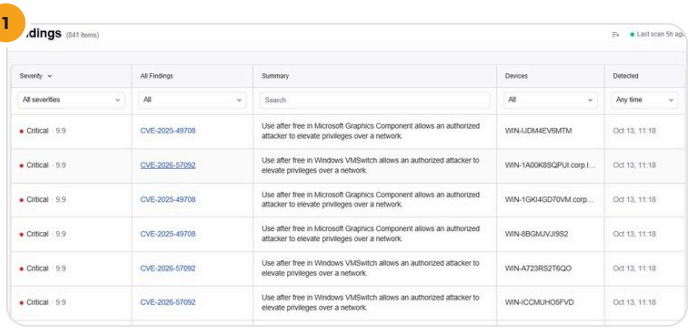
Every authorized change is backed up automatically. Restore any version in one click, for any reason.

1



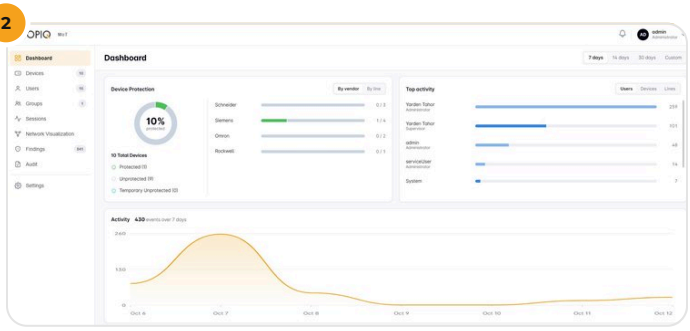
Network visualization: devices by type, with open risk counts per PLC

1



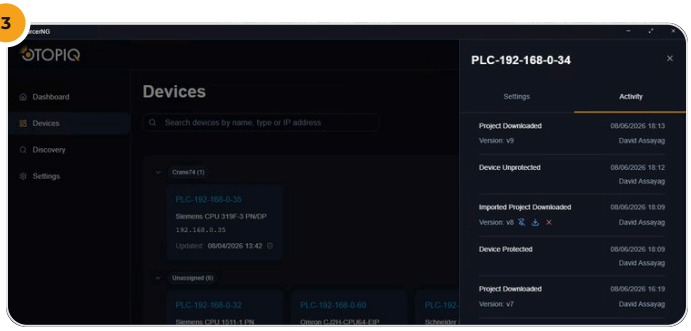
Findings: vulnerabilities ranked by severity

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.