OT SECURITY • SOLUTION BRIEF

Your OT environment doesn't need changes to the plant floor. It needs a better front door.

You can't easily patch decades-old controllers, modify certified systems, or install agents on the plant floor — and you shouldn't have to. TAC adds zero-trust access control to the systems that command your OT environment, cutting off the most common attack paths without touching a single device.

THE THREAT PATTERN

Most OT breaches don't start at the device. They start at the access path to it.

A vendor laptop with a compromised credential. A contractor's stolen SSH key. A flat network where the engineering workstation can reach anything. A jump host that nobody patched. The PLC isn't the weak link — the human path to the system controlling that PLC is.

VENDOR ACCESS

Third parties with broad reach

Equipment vendors, integrators, and maintenance contractors need access to engineering workstations and HMIs. Most are still authenticating with shared passwords on a VPN that gives them more network reach than they need.

REMOTE ENGINEERS

Engineers connecting from anywhere

Modern operations require remote engineering access — to diagnose, configure, and respond at any hour. Whatever device they're on, the path into the SCADA server needs the same controls as the corporate network has for any other sensitive system.

JUMP HOSTS

Bastion servers as soft targets

Traditional OT remote access funnels through jump hosts and bastion servers. They run software that needs patching, expose listening ports, and accumulate accounts over time. When one is compromised, everything behind it is reachable.

FLAT NETWORKS

No segmentation between zones

IEC 62443 zones and conduits, NERC CIP electronic security perimeters — every OT framework expects strong access control between IT and OT. Reality is often a single VLAN, a single VPN, and the assumption that "we trust everyone inside."

THE TAC APPROACH

We don't touch your OT devices. We control who reaches the systems that touch them.

TAC sits in the IT/OT DMZ as a reverse proxy. Every request from a human, a vendor, or a remote workstation goes through TAC before it can reach an HMI, a SCADA server, a historian, or a jump host. Identity is verified. Posture is checked. Policy decides what happens next. Every time.

WHAT TAC CONTROLS

Access to the systems that command OT

- SCADA servers and supervisory systems
- HMIs and operator consoles
- Engineering workstations and configuration tools
- Historians, data lakes, and OT analytics platforms
- Jump hosts, bastion servers, and remote-desktop gateways
- Vendor and contractor remote-access paths

WHAT TAC DOESN'T TOUCH

Your OT devices and protocols

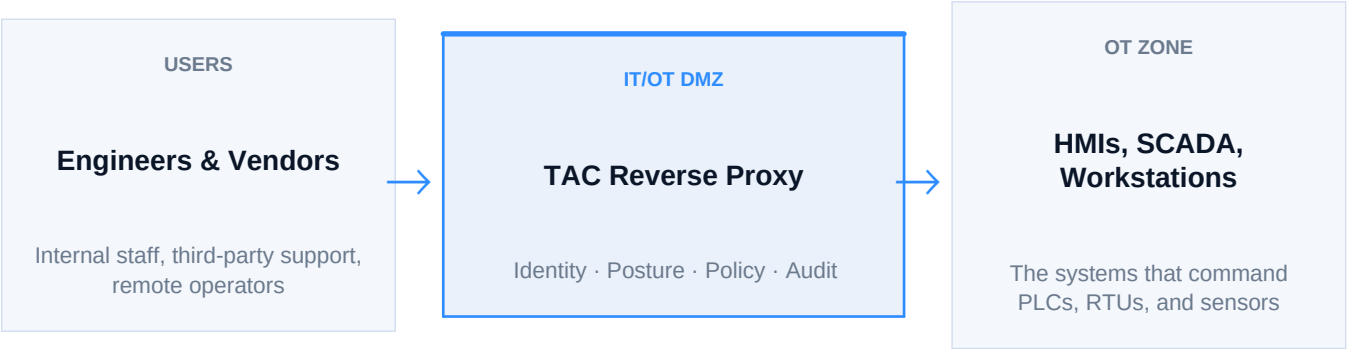
- No agents on PLCs, RTUs, or controllers
- No firmware modifications or patches required
- No Modbus, DNP3, or proprietary protocol inspection
- No interference with deterministic OT timing
- No changes to OT applications or vendor support contracts
- No protocol breaking — TAC is invisible to the OT side

Why this matters: Your OT plant is one of the most carefully tested, certified, and warranty-bound environments you operate. A security product that demands changes to the OT side is a security product that won't get deployed. TAC adds zero-trust to the access path — not to the plant floor.

HOW IT WORKS

Every path into your OT environment runs through TAC. No path bypasses it.

TAC sits in the IT/OT DMZ, taking the place of jump hosts, VPN gateways, and brittle remote-access tools. It's the only path remote users — engineers, vendors, contractors, IT staff — have to reach systems that command OT devices.



WHAT TAC ENFORCES

Five controls between a user and your OT systems

Every one of these happens at the proxy, before the request ever reaches the OT side.

1

Identity verified against your IdP — for everyone, including vendors

Engineers authenticate through your existing identity provider — Entra, Okta, AD. Vendors can authenticate through their own IdP via federation, or against a TAC-managed identity scoped to specific systems and time windows. No shared accounts. Every session is tied to a verified person.

2

MFA on every session — including vendor laptops you don't manage

FIDO2, hardware tokens, push notifications, or SafeLogin MFA on every connection to an OT-adjacent system. The vendor laptop you don't manage still needs the second factor before it can reach your HMI. A compromised credential alone isn't enough to get in.

3

Device posture checked — every session, not just at onboarding

OS version, patch level, antivirus status, disk encryption, domain join — verified before access is granted. The contractor whose laptop fell behind on patches isn't getting into the SCADA network until it's compliant.

4

Per-system, per-role policy — least privilege at the access layer

Policy operates at the system level — not the network level. A turbine vendor can be granted access to the specific HMIs for their turbines, during their scheduled maintenance window, from approved geographies. A flat VPN can't enforce this. TAC can.

5

Continuous evaluation and full session audit

Identity, posture, and policy are re-validated throughout every session — not just at login. If a device falls out of compliance mid-session or a policy changes, the session is revoked in real time. Every request is logged with full attribution, mapping directly to **NERC CIP-005**, **CIP-007**, and **IEC 62443** evidence requirements.

THE OUTCOME

What you get without changing a single OT device

A zero-trust access layer between your people and your plant.

Vendor remote access stops being your biggest risk

Every third-party connection is identity-verified, posture-checked, scoped to specific systems, time-bounded, and logged. The vendor laptop you can't manage is no longer a path into your plant.

Attack surface collapses to a single port

VPN concentrators, RDP gateways, jump hosts, vendor-specific tools — replaced by one encrypted TAC port. Inbound exposure shrinks to almost nothing.

Compliance evidence is generated automatically

NERC CIP-005 ESP boundary, CIP-007 session logging, IEC 62443 zone-and-conduit enforcement — produced as a byproduct of how TAC operates.

CUSTOMER OUTCOME • ENERGY

Oklahoma Municipal Power Authority

OMPA needed secure remote access across distributed power generation facilities while meeting NERC CIP compliance requirements. Legacy VPN left multiple inbound ports exposed with no application-level controls for OT and SCADA interfaces. TAC replaced VPN across all facilities, closing every inbound port except one encrypted TAC port. SCADA and OT interfaces are now published through TAC with MFA and device posture on every request.

1

Inbound port open. Everything else closed.

0

Changes required to OT applications

✓

NERC CIP access control and audit met

"With TAC, I can set up a connection within hours that would have taken days or even weeks with our previous approach. TAC makes our security posture significantly stronger while also making things much easier for our team to manage."

— IT Manager, Oklahoma Municipal Power Authority

READY TO SEE IT IN ACTION?

Cut off the most common OT attack path. Without touching a single device.

See how TAC adds zero-trust access to your OT environment in a live walkthrough.

www.portsys.com/contact