PORTSYS | TOTAL ACCESS CONTROL

Why TAC Is Different

Every access vendor promises Zero Trust. The difference is where they sit when they promise it.

Identity products verify you at login, then hand you off — bolting on separate gateways for the apps they can't reach. Cloud platforms enforce inline, but only through their cloud, in their jurisdiction. PortSys built the enforcement point itself: TAC is a reverse proxy standing in the traffic stream between every identity and every resource — applications, SSH, RDP, IoT, and OT systems alike. One policy engine verifies and controls every request, on your infrastructure, anywhere you need it.

They added enforcement to identity products. TAC IS the enforcement point.

EVERY RESOURCE. NOT JUST APPS.

One enforcement point for everything on your network — modern, legacy, and web applications, plus the SSH, RDP, IoT, and OT systems identity products and cloud platforms can't normally protect. No bolt-on gateways, no second console, no coverage gaps.

YOUR INFRASTRUCTURE. YOUR JURISDICTION.

Fully self-hosted — on-premises, in your cloud, or air-gapped. Traffic never transits a vendor's cloud. TAC runs where cloud-dependent platforms can't: federal agencies, defense contractors, financial regulators, even behind China's Great Firewall.

IN THE STREAM — NOT ON THE SIDELINES

TAC stands in the traffic itself, so enforcement is continuous: identity, device posture, and context verified on every request, payload-deep inspection, and the power to restrict or terminate mid-session — where out-of-band tools can only authenticate, then watch.

ONE LICENSE. EVERYTHING INCLUDED.

MFA, SSO, ZTNA, and DLP in a single platform and license — no modules, no edition upsells. One customer eliminated $1,000-per-device VPN hardware and saves $100,000+ a year, with MFA at zero additional cost.

$100K+	1,300+	0
one customer's annual savings vs. competitive alternatives	apps secured for a global consulting firm operating across 35 countries	exposed ports or vendor-cloud transit — every deployment

Over: the architecture view — and the record behind it.

portsys.com/contact · **info@portsys.com** · **US +1 781-996-4900** · **UK +44 208 196 2420**

NIST SP 800-207 • NSA Zero Trust • CISA TIC 3.0 • FBI CJIS • SOC 2 aligned

© 2026 PortSys, Inc. • 31 Hayward Street, Suite 2B, Franklin, MA 02038

Where enforcement lives decides what you can govern

Every access vendor can verify an identity. The question that separates architectures is what happens after the login — an identity provider sees an authentication event; a reverse proxy sees every request that follows. That single design choice drives everything below.

THE BOLT-ON MODEL

- — Identity checked at the door — then the platform goes blind to the traffic that follows
- — Legacy and on-prem apps need add-on gateways (Access Gateway, App Proxy)
- — Application ports stay open behind the identity provider
- — Cloud ZTNA routes your traffic through the vendor's cloud, in their jurisdiction

THE TAC MODEL

- | One reverse proxy in the path of every request — verification is continuous, not one-time
- | Web, thick-client, RDP, SSH, VDI, APIs, and OT through the same proxy — no add-ons
- | Inbound exposure collapses to a single encrypted port
- | Runs on your infrastructure — on-premises, your cloud, or fully air-gapped

The record behind the architecture

10,000+
users and 1,000+ applications — the scale at which a global consulting firm runs its enterprise on TAC

2015 → today
organizations that replaced Microsoft UAG at end of support still run TAC in production

2008
PortSys founded — access enforcement has been the architecture from day one

Fits what you already run — no rip-and-replace

FEDERATION, BOTH DIRECTIONS

Federates with Active Directory, Entra ID, Okta, and many more — or acts as a full identity provider using credentials from any repository. Your IdP investment stays; TAC becomes the enforcement point in front of it.

EVERYWHERE YOUR APPS LIVE

One policy engine across on-premises applications, private and public cloud, cloud-based datacenters, and SaaS — including the legacy, thick-client, and OT systems that may be most vulnerable.

CLIENTLESS OR CLIENT — YOUR CALL

Fully clientless access from any browser, with core policy and device signals intact — or add the TAC client for deeper device inspection where you need it.

UNMANAGED ENDPOINTS, HANDLED

Publish individual applications through Microsoft RDP App — TAC integrates with it seamlessly — so partner and BYOD devices get access without touching the endpoint.

And because enforcement lives at the proxy — not the identity provider — TAC is already in position for what's next: governing AI agents through the same enforcement point that governs your people. The proxy that verifies and controls every human request is the same one that will govern every agent's.

Humans today. Agents next.

portsys.com/contact · info@portsys.com · US +1 781-996-4900 · UK +44 208 196 2420

NIST SP 800-207 • NSA Zero Trust • CISA TIC 3.0 • FBI CJIS • SOC 2 aligned

© 2026 PortSys, Inc. • 31 Hayward Street, Suite 2B, Franklin, MA 02038