TOTAL ACCESS CONTROL | PRODUCT DATASHEET

# One zero-trust access platform.
# Every application. Every identity.

TAC is a reverse-proxy zero-trust access platform that controls who reaches what — across modern apps, legacy apps, OT systems, and AI agents. One policy engine, one inbound port, one audit trail. Every identity verified. Every request inspected. Every session logged.

THE CHALLENGE

## Access is the new perimeter.

Modern enterprises run a mix of SaaS, internal apps, legacy systems, OT environments, and increasingly AI agents — reachable by employees, contractors, vendors, and partners from any device, anywhere. Traditional VPNs, jump hosts, and point solutions can't keep up. Each new application and identity source adds another tool, another exposed port, another gap.

THE SOLUTION

## Total Access Control.

TAC sits as a reverse proxy between every user and every protected resource. Identity verified against your IdP. Device posture checked. Policy decides what happens next. One inbound port, one console, one policy engine — for every application your business depends on.

BUSINESS OUTCOMES

## What TAC delivers

ATTACK SURFACE

### One inbound port. Everything else closed.

VPN concentrators, RDP gateways, jump hosts — all replaced by TAC's single encrypted port. Inbound exposure shrinks to almost nothing.

IDENTITY

### Verified everyone, every session

MFA enforced on every session. No shared accounts, no anonymous API keys. Every session tied to a verified identity from your IdP.

OPERATIONS

### Works with what you already have

Modern apps, legacy apps, OT systems, AI agents — TAC governs access to all of them. No application code changes required.

VENDOR ACCESS

### Third parties without the risk

Contractor and vendor access scoped to specific systems, time-bounded, posture-checked, identity-verified, fully logged.

COMPLIANCE

### Audit evidence by default

Full session audit trail. Maps to NIST 800-207, ISO 27001, SOC 2, HIPAA, PCI-DSS, FedRAMP, NERC CIP, IEC 62443, and more.

LICENSING

### Simple per-user, annual subscription

No per-CPU fees, no bandwidth tiers, no add-on modules. Scale performance with infrastructure, not with your bill.

BUILT FOR

## Six use cases. One platform.

TAC is purpose-built for the access control problems that don't have clean solutions: legacy applications that can't speak modern auth, OT systems that can't be touched, AI agents that need the same governance as humans, and the explosion of contractor and vendor access that comes with every modern enterprise.

| Modern Apps | Legacy Apps | OT & SCADA | AI Agents | Vendor Access | Cloud Migration |
|---|---|---|---|---|---|
| SAML, OIDC, OAuth — secured at the proxy | No code changes. Wrap any web or thick-client app | Zero-trust to HMIs, SCADA, engineering workstations | Govern non-human identities like human users | Scoped, time-bounded, posture-checked | Same policies on-prem and cloud |

PROVEN IN PRODUCTION

## Deployed across regulated industries worldwide.

| 8+ | 5 | 10+ | ZERO |
|---|---|---|---|
| **INDUSTRIES SERVED** | **CONTINENTS** | **YEARS IN PRODUCTION** | **BREACHES** |
| Government, Healthcare, Energy & more | North America, Europe, Asia, Africa, South America | Continuous deployment since launch | No customer compromise via TAC |

GOVERNMENT — FEDERAL AGENCY

### Multi-facility rollout

**U.S. Federal Agency**

Legacy control systems and administrative applications secured with zero application changes. MFA injected into legacy apps. All inbound ports closed. NIST 800-171 compliance achieved.

ENERGY — UTILITY

### VPN replaced; NERC CIP achieved

**Oklahoma Municipal Power Authority**

OT and SCADA interfaces secured. Inbound attack surface reduced to a single port. VPN decommissioned across all generation facilities.

HEALTHCARE — NHS

### ICB-wide deployment

**UK NHS Acute Hospital Trust**

Single-tenant TAC deployment across the integrated care board. MFA injected into legacy clinical systems. SSO across all applications. NHS data security standards achieved.

HEALTHCARE — FEDERAL

### Microsoft UAG replaced

**Canadian Federal Health Agency**

Replaced in days, not months. Any-device, any-browser remote access. Contractors freed from supported-hardware lists. Mac users restored to full remote capability.

PUBLIC SECTOR — UK

### 8,000+ employees

**UK County Council (1M+ residents)**

Zero-trust access for public-sector employees. Application-aware policies replaced legacy VPN. Productivity gains aligned with UK public sector security requirements.

PHARMA — CONSULTANCY

### O365 gap closed

**Global Pharmaceutical Consultancy**

MFA and device posture enforced on every O365 session via TAC reverse proxy. Pharmaceutical client data protection requirements satisfied.

INDUSTRIES SERVED

| Government & Defense | Healthcare | Financial Services | Energy & Utilities | Manufacturing | Technology & SaaS | Education | Legal |
|---|---|---|---|---|---|---|---|

COMPLIANCE ALIGNMENT

## Audit-ready for the frameworks you operate under

TAC's audit trail and access controls map to the technical evidence requirements of every major security and compliance framework. Detailed alignment guides available for each.

| | | | | |
|---|---|---|---|---|
| NIST SP 800-207 | NIST SP 800-171 | ISO 27001:2022 | SOC 2 | PCI-DSS v4.0 |
| HIPAA / HITECH | FedRAMP | CISA TIC 3.0 | NSA Zero Trust | CJIS |
| GDPR | NERC CIP | IEC 62443 | NIST AI RMF | ISO 42001 |
| SAMA Cyber | | | | |

HOW TAC COMPARES

## VPN, Cloud ZTNA, TAC — an honest comparison.

| Capability | Traditional VPN | Cloud ZTNA | TAC |
|---|---|---|---|
| **Inbound exposure** | Concentrator + many open ports | Datacenter ports stay open — vendor cloud doesn't close them | **One encrypted port. Everything else closed.** |
| **Access model** | Network-level. Once in, you can roam. | App-level for web. Network tunnels for the rest. | **Application-level, every protocol, every app.** |
| **Application coverage** | Anything reachable on the network — no auth wrapping | Modern web/SaaS only. Legacy, thick-client, OT excluded. | **All apps: modern, legacy, thick-client, OT, AI agents.** |
| **Deployment** | Hardware concentrators per site | Vendor-cloud multi-tenant | **Single-tenant SVA — on-prem, cloud, or hybrid. You choose.** |
| **Identity & policy** | Static groups, network-based | Vendor IdP, opaque policy engine | **Your IdPs, your policy. Inspectable. Auditable.** |
| **Licensing** | Per-concentrator, per-bandwidth | Per-user **plus** per-module (MFA, posture, ZTNA, etc.) | **Per-user, all-inclusive. Every feature + 24×7 support in the base license.** |

ARCHITECTURE AT A GLANCE

## How TAC mediates every access request.

Every connection to every application flows through the TAC reverse proxy. Identity verified, device evaluated, policy applied — before any traffic reaches the target app.


Reverse-proxy enforcement — no agents on endpoints, no changes to applications, no vendor cloud in the path between your users and your data.

DEPLOYMENT OPTIONS

## Single-tenant. Wherever you need it.

ON-PREMISES
**Your datacenter**
Single-tenant SVA in your environment. You own the hardware, you control the policy.

CLOUD
**Your cloud account**
Single-tenant SVA in AWS, Azure, or GCP. Still your tenant, still your policy.

HYBRID
**Best of both**
Global array of SVAs across on-prem and cloud. One policy engine, one admin console.

PERFORMANCE & LICENSING

## Performance is in your control. Licensing is simple.

TAC is architected as a software virtual appliance (SVA), so performance is governed by the CPU and RAM you allocate — not by a vendor's hardware spec. Scale vertically per node. Scale horizontally by adding nodes to an array. There is no architectural ceiling.

**Licensing is per user, annual subscription. No per-CPU fees, no bandwidth tiers, no add-on modules, no surprise costs. 24×7 support included — no charge.**

READY TO SEE IT?

## Request a live walkthrough of TAC

**portsys.com/contact | info@portsys.com**