# Reverse-proxy zero trust. Architecture & specifications.

TAC is deployed as a software virtual appliance acting as a reverse proxy between every consumer of access — human users, third-party vendors, and contractors, with AI agents next on the platform — and every protected resource: modern web apps, cloud and SaaS apps, legacy apps, OT systems, thick-client applications, RDP, SSH, VDI, and APIs. Identity verified, MFA enforced, posture checked, policy applied, every session logged. This datasheet covers TAC's architecture, supported integrations, and platform specifications.

ARCHITECTURE

## Reverse proxy. Single port. Software-defined.

TAC sits between users and protected resources as a reverse-proxy enforcement layer. It terminates every inbound connection, re-establishes outbound connections to applications, and ensures no user device ever has direct access to internal systems. All inbound exposure collapses to a single TAC port; the integrated firewall closes everything else.

ENCRYPTION & SECURITY

## Defense-in-depth at the proxy

| | |
|---|---|
| **Transport encryption** | TLS 1.3 (TLS 1.2 supported) with strong cipher suites |
| **FIPS compliance** | FIPS 140-2 compliant cryptographic modules |
| **Network protection** | Integrated firewall — only the TAC port is exposed inbound |
| **SSL offloading** | Terminates TLS at the proxy; protected resources don't need their own certificates |
| **Session security** | Session ID binding to user + device; brute-force detection; latent-risk protection |

TRAFFIC FLOW

## Eight checkpoints, every request

Every request from consumer to resource passes through eight sequential checkpoints. None can be skipped. Each is logged. The session is monitored continuously — not just at initial authentication. MFA is enforced at TAC on every session, not just at the IdP.

1. **TLS handshake**
   Encrypted connection established at TAC's single inbound port
2. **Identity challenge**
   User or service identity authenticated via your IdP — SAML, OIDC, OAuth, AD, LDAP, RADIUS, KCD
3. **MFA enforcement**
   Strong second factor required on every session — FIDO2, YubiKey, RSA SecurID, Microsoft/Google/Duo Authenticator, push, OTP, smartcards, or certificates
4. **Device posture**
   OS, patches, AV, certificates, hardware ID, network, installed software validated
5. **Policy evaluation**
   ABAC/RBAC/CBAC/PBAC engine evaluates identity + posture + context against policy
6. **Server connection**
   TAC opens outbound connection to the application — no direct path from consumer
7. **Continuous authorization**
   Session continuously re-evaluated for posture, context, and policy changes; step-up MFA triggered when conditions change mid-session
8. **Session monitoring**
   Full lifecycle logged: every access, every decision, every change of state

PERFORMANCE & LICENSING

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

TAC is architected as a software virtual appliance — secure, fast, and customer-controlled. Performance is governed by CPU and RAM allocated to each TAC node, not by a vendor's hardware spec. Scale vertically by adding resources per node; scale horizontally by adding nodes to an array — with no per-node licensing penalty. Licensing is per-user annual subscription: no per-CPU fees, no bandwidth tiers, no add-on modules, no surprise costs.

IDENTITY & AUTHENTICATION

## Every supported identity source. MFA on every session.

TAC consumes identities from your existing identity providers and enforces strong authentication and MFA on every session — not just at the IdP, and not just at initial login. It does not replace your IdP; it sits in front of it as the policy and enforcement layer for everything downstream. MFA is required for human users, vendors, contractors, and the service accounts that act on their behalf — with agent-aware governance next on the platform.

| | |
|---|---|
| **Directory services** | Active Directory • Azure AD / Entra ID • Okta • LDAP • RADIUS • KCD (Kerberos Constrained Delegation) • Custom directories |
| **TAC native store** | TAC secure database — used for guest, vendor, and contractor identities when federation isn't viable |
| **Federation protocols** | SAML 1.1 / SAML 2.0 • OAuth 2.0 • OpenID Connect (OIDC) • NTLM • Client SSL certificates |

MULTI-FACTOR AUTHENTICATION

## Enforced at TAC, on every session

TAC enforces MFA independently of (and in addition to) any MFA configured at your IdP. This means MFA is mandatory even for users coming through federation, and it can be stepped up dynamically when posture, context, or sensitivity changes mid-session.

| | |
|---|---|
| **Hardware tokens** | YubiKey • RSA SecurID • Other FIDO2 / WebAuthn hardware tokens • Smartcards |
| **Authenticator apps** | Microsoft Authenticator • Google Authenticator • Duo • Symantec VIP |
| **Out-of-band** | SMS OTP • Email OTP • Phone OTP • Push notifications |
| **Primary auth (1FA)** | Password • Smartcards • Client SSL certificates |
| **Step-up MFA triggers** | Posture change • Sensitive resource access • Geo or network change • Policy-driven re-authentication |

CONDITIONAL AUTHENTICATION

## Context on every session — not just identity

TAC evaluates context on every session. The same user can be granted different access (or required to step up MFA) depending on:

| | |
|---|---|
| **Device** | Domain-joined status, certificates, hardware ID, posture compliance |
| **Location** | GeoIP, network type (corporate vs. public), specific IP ranges |
| **Time** | Business hours, scheduled maintenance windows, vendor access windows |

DEVICE & ENDPOINT SECURITY

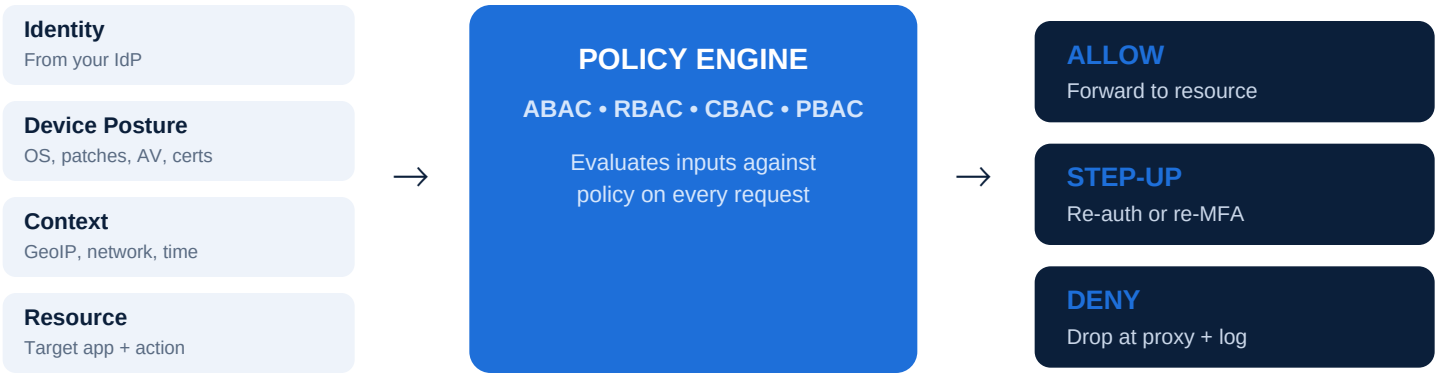
## Native posture, MDM coexistence

TAC checks device posture directly, without requiring a third-party MDM agent: core posture signals are gathered clientlessly, and the optional TAC client unlocks the deepest inspection. This lets TAC operate as a security overlay alongside any existing MDM — and because MDM architectures permit only one MDM controller per device, this approach prevents conflict. Where device posture for access decisions is the primary use case, TAC can reduce or eliminate MDM dependency.

| | |
|---|---|
| **Operating system** | OS version • Patch level • Domain-joined status |
| **Endpoint protection** | Antivirus / anti-spyware presence and currency • Disk encryption |
| **Identity proof** | Device certificates • Hardware ID binding • Installed software inventory |
| **Anomaly checks** | Hidden files • Unexpected processes • Network location anomalies |
| **Binding models** | Device → user • Device → certificate • Device → hardware ID |
| **EDR / threat-intel** | Ingested via API or syslog to inform policy decisions |
| **SIEM / SOAR** | All posture events exported to your SIEM via syslog |

POLICY ENGINE

## Continuous, context-aware decisions




| | |
|---|---|
| **Policy models** | ABAC (attribute-based) • RBAC (role-based) • CBAC (context-based) • PBAC (policy-based) • Time-restricted • Business-activity-based |
| **Microsegmentation** | Application-level segmentation. Users access specific resources — not network segments. No lateral movement on the network. |
| **Continuous evaluation** | Policy re-evaluated on every request, not just at session start. Sessions revoked in real time when conditions change. |

APPLICATION ACCESS CONTROL

## Anything users need to reach. Anything you need to govern.

TAC publishes web applications, cloud and SaaS applications, thick-client applications, remote desktops, virtual desktops, shell access, file collaboration, and APIs through a single reverse-proxy enforcement layer. Every published resource gets the same identity, posture, policy, and audit treatment.

| | |
|---|---|
| **Web applications** | Reverse proxy • Header injection • Form-based auth • HTTP 401 • Client SSL certs • SAML / OIDC federation |
| **Thick-client applications** | TCP socket forwarding • TLS tunneling • Legacy protocol encapsulation — replaces VPN for application access |
| **Remote desktop & VDI** | RDP (native client and HTML5 browser-based) • SSH (HTML5) • Citrix • VMware Horizon • Azure Virtual Desktop • AWS WorkSpaces |
| **File access & collaboration** | SharePoint • OneDrive • Exchange / OWA • ActiveSync • Microsoft 365 |
| **APIs** | Reverse-proxied API access with identity-aware policy on every call — one enforcement layer, with agent-aware governance next on the platform |
| **OT systems** | HMIs • SCADA servers • Engineering workstations • Historians — without touching the OT devices themselves |

MANAGEMENT & OPERATIONS

## Single console, real-time control, full visibility

| | |
|---|---|
| **Administration** | Single pane of glass • Delegated administration • Real-time configuration changes • Wizard-driven publishing • Config export/import |
| **Reporting** | User activity • Device usage • Performance • Security events • Compliance violations — HTML, XML, CSV, PDF |
| **Logging** | Syslog (compatible with all major SIEMs) • SQL logging • Session lifecycle monitoring • Automated alerts • Cross-log tracing |
| **Audit content** | Every authentication attempt, allow/deny decision, posture event, session start/end, and policy change — fully attributed: user, device, source, target, decision |

DEPLOYMENT & SCALABILITY

## Software-defined deployment, anywhere

| | |
|---|---|
| **Hypervisors** | VMware vSphere / ESXi • Microsoft Hyper-V • KVM |
| **Cloud platforms** | Amazon Web Services • Microsoft Azure |
| **Deployment models** | Stand-alone • Distributed (multi-site) • Hybrid (on-prem + cloud) • Multi-node arrays • Global arrays • Air-gapped and sovereign environments |
| **High availability** | Active/active with shared state • Integrated load balancing • Hyper-resilient session persistence • Global config sync |
| **Performance** | Customer-controlled via CPU/RAM allocation per node • Horizontal scaling by adding nodes • Low-latency proxying • SSL offloading • Optimized session caching |

COMPLIANCE ALIGNMENT

## Aligned to the frameworks your auditors use most

TAC's access controls, authentication, and audit evidence map to the frameworks your auditors use most — across zero trust, information security, healthcare, government, financial services, and OT.

**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 · FBI CJIS · GDPR · NERC CIP · IEC 62443 · SAMA Cyber**

PLATFORM ROADMAP — NEXT ON TAC

### AI Agent Governance

Agent-aware identity, scoped permissions, per-action policy, and full attribution — built on this enforcement point. Aligned to NIST AI RMF and ISO/IEC 42001 at module launch. Launch list: portsys.com/ai-agent-governance.

**Ready to evaluate? Architecture review · POC scoping · RFP support.**

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