TOTAL ACCESS CONTROL | TECHNICAL DATASHEET

Reverse-proxy zero-trust access. 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, contractors, and AI agents — and every protected resource: modern web 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 1.2 / TLS 1.3 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 agent 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 request, 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. No architectural ceiling.

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 AI agents and service accounts that act on their behalf.

Identity providers

Directory services	Active Directory • Azure AD / Entra ID • 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

TAC evaluates context on every session — not just identity. 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. 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. TAC can also replace MDM for organizations where device posture is the primary use case.

Posture checks

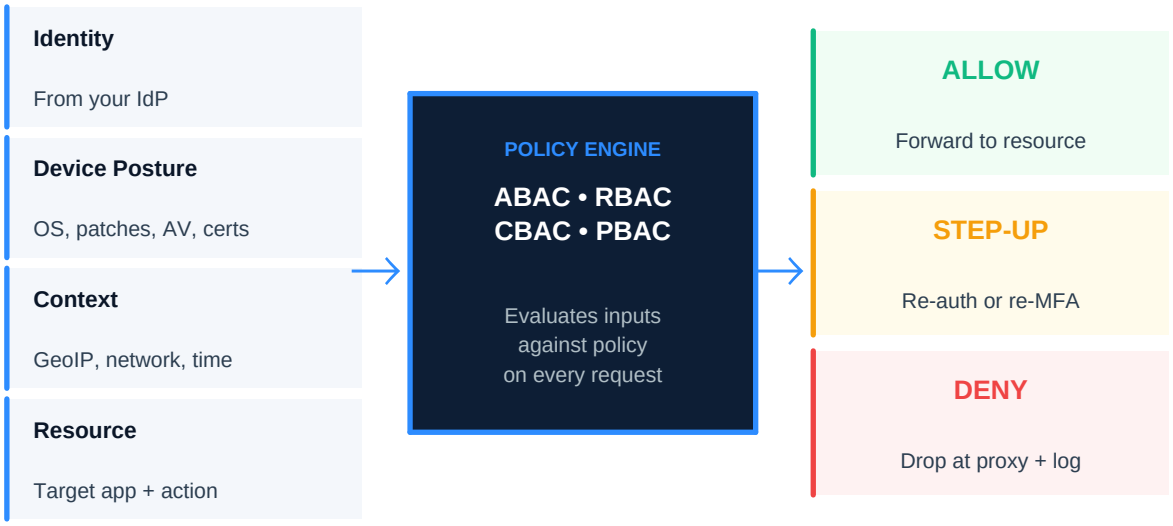
Operating system	OS version • Patch level • Domain-joined status
Endpoint protection	Antivirus / anti-spyware presence and currency • Disk encryption
Identity proof	Device certificates • Hardware ID binding • Installed software inventory
Anomaly checks	Hidden files • Unexpected processes • Network location anomalies

Device binding & integrations

Binding models	Device → user • Device → certificate • Device → hardware ID
EDR / threat-intel	Can be 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, 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 — same enforcement layer for human and non-human consumers
OT systems	HMIs • SCADA servers • Engineering workstations • Historians — without touching the OT devices themselves

MANAGEMENT & OPERATIONS

Single console, real-time control, full visibility

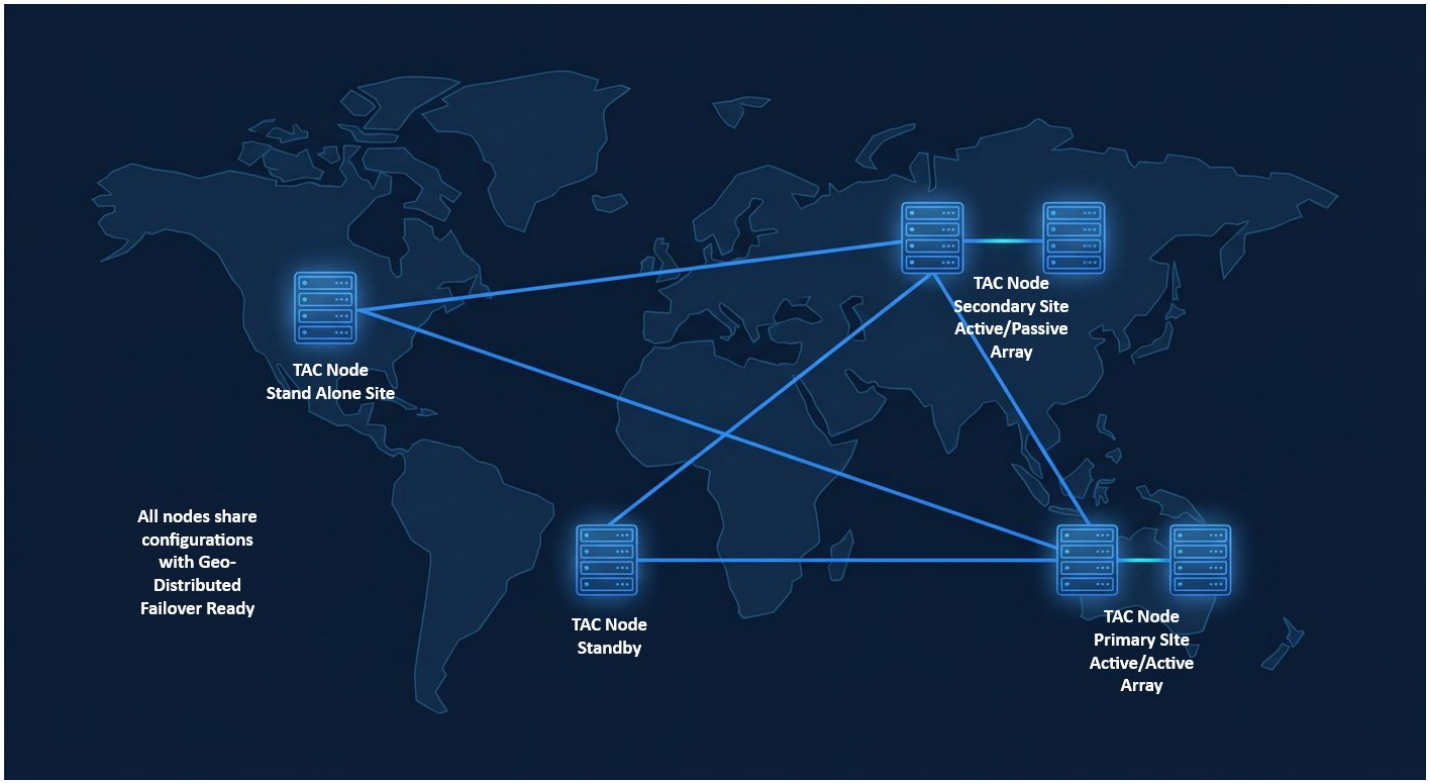
Administration	Single pane of glass • Delegated administration • Real-time configuration changes • Wizard-driven publishing • Config export/import
Reporting categories	User activity • Device usage • Performance • Security events • Compliance violations
Report formats	HTML • XML • CSV • PDF
Logging	Syslog (primary, 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
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

HA / DR Topology



COMPLIANCE ALIGNMENT

Frameworks TAC is aligned to

TAC's access controls, authentication, and audit evidence map to the technical requirements of every major security and compliance framework — across zero trust, information security, healthcare, government, financial, OT, and AI governance.

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				

READY TO EVALUATE?

Schedule a technical deep-dive

Architecture review • POC scoping • RFP support

portsys.com/contact | info@portsys.com