PORTSYS WHITE PAPER

Beyond ZTNA

A Technical Comparison of Five Access Architectures

Michael Oldham
Founder, PortSys, Inc.

November 2026

About this paper

This paper is published by PortSys, Inc., the developer of Total Access Control (TAC). It applies the same six evaluation criteria to every architectural category it examines, including the one PortSys competes in, and it identifies situations where other approaches are a better fit than ours. Statements about other vendors' products are drawn from their public documentation as of October 2026 and are cited so readers can verify them. No vendor briefings or paid placements were involved. This paper is the technical companion to The Enforcement Gap, a separate PortSys white paper that makes the business argument this analysis supports.

Introduction

Every access vendor can verify an identity. What separates architectures is what happens after the login: where enforcement sits, what triggers reevaluation, which applications are covered, how device trust is established, whose infrastructure the traffic crosses, and what the whole thing costs to operate. This paper compares five categories of access architecture against those six criteria, applied identically to each — including the category PortSys competes in: identity-centric platforms, cloud-delivered security service edge (SSE) platforms, application delivery controllers, traditional VPN appliances, and self-hosted unified enforcement proxies.

Vendor capability statements are drawn from each vendor's public documentation as of October 2026 and cited throughout so readers can verify them. The analysis names where each approach fits best, including situations where our own product is not the strongest choice.

This is the technical companion to The Enforcement Gap, which makes the business argument in brief: authentication has matured faster than authorization; "continuous" means different things to different vendors; and where enforcement sits determines what can be seen and controlled. No category is inline for every application type in every situation — and that includes unified platforms like ours.

1. An Evaluation Framework

To compare architectures fairly, we use six criteria and apply them identically to every category in Section 2, including our own.

Criterion	The question it answers	Why it matters
1. Enforcement location	Does the architecture make an admission decision at sign-in, or stay in the traffic path for the whole session?	Determines what the system can observe and act on after login.
2. Reevaluation triggers	What causes trust to be reevaluated: identity events, device changes, or every request?	Determines how quickly a change in conditions affects an open session.
3. Application coverage	Which application types are covered: SaaS, private web, non-web (RDP, SSH, thick-client), legacy authentication, OT?	Most enterprises run all of these; gaps become exceptions to policy.
4. Device trust model	Does it manage devices, inspect them at the moment of access, or both? Can it evaluate devices the organization does not own?	Contractors, partners and BYOD users are often the highest-risk population.
5. Deployment and data path	Is traffic brokered through the vendor's cloud, or can the customer self-host, including isolated or air-gapped environments?	Affects data sovereignty, resilience during outages and regulatory fit.
6. Operational model	How many products, consoles, licenses and specialist skills does it take to achieve the outcome?	Complexity is a cost and a source of misconfiguration risk.

These criteria do not produce a single score, and no category is strongest on all of them. They are intended to help an organization match an architecture to its own applications, risks and operating capacity.

2. The Architectural Landscape

The vendors named below are examples, not a complete market survey. Capability statements are drawn from each vendor's public documentation as of October 2026 and are cited so readers can verify them. Products change quickly, and buyers should confirm current capabilities directly with vendors.

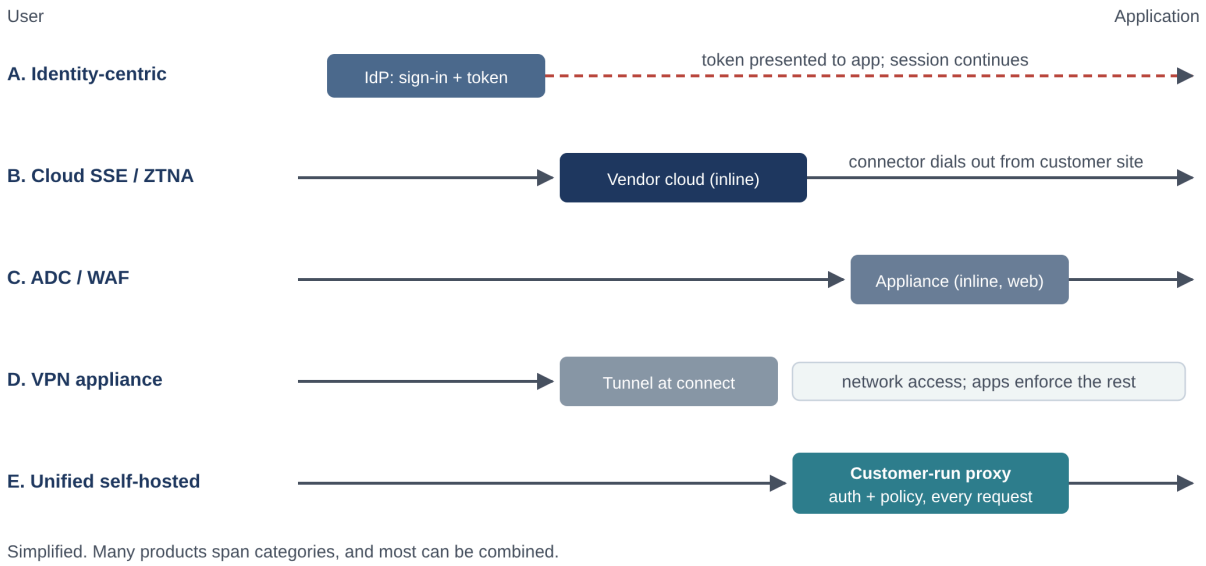


Figure 1. Where each category enforces policy in the traffic path

2.1 Identity-Centric Platforms

Examples: Microsoft Entra (with Intune, Defender and Global Secure Access), Okta, Ping Identity.

How it works. The identity platform authenticates the user and evaluates conditional access policy, then issues a token that applications accept. An example of this is Microsoft Entra ID, Microsoft's cloud identity service, which signs users into Microsoft 365 (Microsoft's productivity suite, including Outlook, Teams and SharePoint) and thousands of third-party applications. Device signals come from endpoint management tools such as Microsoft Intune, which checks whether a device meets the organization's configuration and security requirements.

Continuous evaluation. These platforms have invested heavily in shortening the time between a security event and its enforcement:

- Microsoft's Continuous Access Evaluation (CAE) lets Exchange Online, SharePoint Online, Teams and Microsoft Graph respond to critical events such as a disabled account, a password reset or high user risk without waiting for a token to expire [4]. Microsoft notes that event propagation can take up to 15 minutes, and that CAE-enabled sessions can receive tokens lasting up to 28 hours.

- Universal CAE extends this to any application reached through Microsoft's Global Secure Access service, including private resources such as Remote Desktop and file servers, without the application needing to support CAE. It responds to the same five identity events and, by default, operates opportunistically unless a stricter enforcement mode is enabled [5].
- Okta Identity Threat Protection evaluates policy conditions throughout a user's session and can respond to changes in a user's risk, network zone, device or behavior by terminating a session or prompting for MFA [10]. Okta both sends and receives security events using the OpenID Shared Signals Framework [11].
- PingAccess can apply risk evaluations to web applications on a recurring basis, every 20 seconds by default or on every request if configured [13].

In-session controls. Microsoft Defender for Cloud Apps can apply session controls in the browser, through a reverse proxy or, for Microsoft Edge, natively in the browser, to block downloads, copying, printing and specific in-app activities. Microsoft's documentation states that these session controls apply only to web browser–based access; native desktop and mobile clients, including the Teams desktop app, are not covered [6].

Private application access. Microsoft Entra Private Access, part of Global Secure Access, provides ZTNA to private resources through connectors that build outbound tunnels to Microsoft's cloud [7]. Entra Application Proxy continues to publish on-premises web applications, including Kerberos and header-based applications, natively or through partners such as PingAccess [8][40]. Okta offers Access Gateway, a customer-run reverse proxy for web applications [12], and the Okta Privileged Access gateway for SSH and RDP sessions [46].

Deployment. Microsoft's and Okta's core identity services are cloud-delivered. Ping offers self-managed software alongside its cloud options [14].

Strengths. Unmatched depth in identity, conditional access and risk detection; tight integration with device management and endpoint protection; and, for Microsoft customers, a single vendor relationship across productivity, identity and security.

Limits against our criteria. Reevaluation is driven largely by identity and risk events, plus network-location checks, rather than by each request. In-session activity controls depend on additional products and, in Microsoft's case, are limited to browser sessions. Full capability is spread across several products and licensing tiers. Microsoft's Entra Suite, for example, bundles Private Access, Internet Access, ID Governance, ID Protection and Verified ID [9].

Best fit. Organizations whose applications are predominantly cloud-based and that are already invested in the vendor's ecosystem.

2.2 Cloud-Delivered Security Service Edge (SSE) and ZTNA

Examples: Zscaler, Netskope, Palo Alto Networks Prisma Access, Cloudflare, Cisco Secure Access.

How it works. User traffic is routed through the vendor's global cloud, where it is inspected and policy is applied before it reaches the internet, SaaS applications or private applications. Lightweight connectors

inside the customer's network dial out to the vendor's cloud, so private applications do not need inbound firewall openings [20].

Protocol coverage. All five vendors in this category now offer browser-based access to RDP and SSH without a client, and several also support VNC [22][43][44][47][48]. Zscaler and Netskope market specific offerings for operational technology (OT) remote access [42][19], and Palo Alto Networks has announced browser-based privileged access for OT environments [49]. Coverage beyond that varies. Netskope documents support for server-initiated flows such as VoIP [19], while Palo Alto Networks notes that some dynamic-port applications cannot use its ZTNA connector [20].

Continuous evaluation. Approaches vary considerably:

- Zscaler's AppProtection inspects HTTP and HTTPS traffic to private applications inline for web attacks and Active Directory attack behavior [17], and Zscaler's adaptive access engine can receive continuous access signals from Okta [41].
- Cloudflare evaluates device posture on every request using a result cached for up to five minutes, but its documentation states that its Gateway "does not terminate an active session" when a later posture check fails [21].
- Cisco Secure Access offers continuous posture checks and can force reauthentication based on a dynamic trust profile, currently for client-based access only [22].

Deployment and data path. By default, private application traffic transits the vendor's cloud. Zscaler (Private Service Edge), Netskope (Local Broker) and Cisco (Hybrid Private Access) offer local enforcement for on-premises users, but each still depends on the vendor's cloud for policy, authentication or both. Netskope documents that if its management plane is unreachable, existing tunnels continue but new connections and periodic reauthentication fail [18]. Zscaler documents a business-continuity mode that keeps local access running on cached policy during internet outages, but configuration and policy still come from its cloud [16][45]. We found no mode documented by any of the five for permanently air-gapped operation.

Strengths. Global scale, and a broad bundle of internet and SaaS security services alongside ZTNA: secure web gateway (SWG) filtering of internet traffic, cloud access security broker (CASB) controls for SaaS applications, data loss prevention (DLP), remote browser isolation and firewall-as-a-service.

Limits against our criteria. Customer traffic and policy depend on a third party's infrastructure. Depth of private-application inspection varies by vendor and by protocol. Organizations with data-sovereignty, air-gap or operational-technology isolation requirements may find the cloud dependency difficult to accept.

Best fit. Distributed organizations whose main need is securing internet and SaaS traffic for a mobile workforce, with private application access as part of a broader cloud security program.

2.3 Application Delivery and Web Application Firewalls

Examples: F5 BIG-IP Access Policy Manager, Citrix NetScaler, Akamai Enterprise Application Access, Azure Application Gateway and Azure Front Door.

How it works. Application delivery controllers (ADCs) sit in front of applications to balance load, terminate encryption and filter malicious requests. Several have added substantial access capabilities. F5 BIG-IP APM, for example, describes per-request, context-based access policies, built-in SAML and OpenID Connect federation, translation of modern sign-ins into older Kerberos or header-based authentication, and device posture checks at login and continuously [23].

Deployment. F5 and NetScaler are deployed by the customer as hardware or virtual appliances. Akamai's service is cloud-delivered with on-premises connectors [34]. Azure Application Gateway and Front Door are Azure-managed services that primarily provide load balancing and WAF. User authentication is usually handled by the application or by a separate identity layer; Application Gateway's token-validation feature remains in preview and accepts only Entra-issued tokens [35].

Strengths. Inline by design, mature traffic management and WAF capabilities, and strong support for legacy web application authentication.

Limits against our criteria. Access features are often licensed and administered separately from delivery features and require specialist skills. Coverage centers on web applications. These gateways are also high-value targets: CISA's 2023 advisory on CitrixBleed described attackers bypassing passwords and MFA by hijacking sessions on NetScaler devices [25], and in October 2025 CISA issued Emergency Directive 26-01 after a nation-state actor exfiltrated a portion of F5's BIG-IP source code and vulnerability information [24].

Best fit. Organizations with large web application estates and existing ADC expertise.

2.4 Traditional VPN and Remote-Access Appliances

Examples: Ivanti Connect Secure, Fortinet FortiGate SSL-VPN, Palo Alto Networks GlobalProtect, Cisco ASA.

How it works. A VPN gives an authenticated device a network-level connection, after which access is governed largely by network segmentation and the applications' own controls.

Strengths. Universal protocol support and familiarity. Almost any application works over a VPN without modification.

Limits against our criteria. Trust is granted at the network level at connection time, which is the model Zero Trust was designed to replace. VPN appliances have also been among the most heavily exploited enterprise technologies of recent years:

- Under Emergency Directive 24-01 (January 2024) and its supplemental direction, CISA ordered federal agencies to disconnect, factory-reset and rebuild Ivanti Connect Secure and Policy Secure appliances, revoke connected credentials, and assume associated domain accounts were compromised [26].
- A maximum-severity vulnerability in Palo Alto Networks PAN-OS firewalls running GlobalProtect (CVE-2024-3400) was disclosed on April 12, 2024, after zero-day exploitation [29].
- In April 2025, the Canadian Centre for Cyber Security warned that attackers had maintained access to Fortinet SSL-VPN devices even after patches were applied [28].

- CISA Emergency Directive 25-03 (September 2025) addressed active exploitation of Cisco ASA devices [27].

NSA and CISA have published joint guidance on selecting and hardening VPN solutions for organizations that continue to rely on them [31].

Best fit. Short-term or narrowly scoped use while migrating to an application-level access model.

2.5 Self-Hosted Unified Enforcement Proxies

Examples: PortSys Total Access Control (TAC), PingAccess, Teleport, Pomerium.

How it works. A reverse proxy deployed and controlled by the customer sits between users and applications, combining authentication, authorization and policy enforcement at a single point that remains in the traffic path for the whole session. Products in this category differ in scope:

- PingAccess is a web-focused gateway that checks authorization on each request before forwarding it [50].
- Teleport focuses on infrastructure access (SSH, Kubernetes, databases and Windows desktops) using short-lived certificates [32].
- Pomerium is an identity-aware proxy that evaluates policy on each HTTP request, with an open-source core [33].
- TAC spans web, non-web, legacy and OT applications and includes MFA, SSO and device inspection in a single platform (described in Section 6).

Strengths. The customer controls the data path and can run the proxy on-premises, in the customer's own cloud environment (such as Azure or AWS), or fully isolated from the internet. Policy can be evaluated on each request rather than only at sign-in. Fewer separate products are needed to cover authentication, access and enforcement.

Limits against our criteria. For cloud and SaaS applications, a self-hosted proxy is in the traffic path only if users are routed through it, which in practice usually means it must also act as the identity provider for those applications. Products in this category generally do not match the depth of the large ecosystems in adjacent areas such as device management, endpoint detection, internet filtering or CASB. And because the proxy is the front door, it must itself be hardened and monitored like any internet-facing gateway.

Best fit. Hybrid environments: organizations with significant on-premises, legacy, thick-client or OT applications alongside cloud-based resources; multiple identity providers; data-sovereignty or air-gap requirements; or a need to reduce the number of products and consoles they operate.

2.6 Summary Comparison

Criterion	A. Identity-centric	B. Cloud SSE / ZTNA	C. ADC / WAF	D. VPN appliance	E. Unified self-hosted
Enforcement location	At sign-in and token issuance; browser-session proxy available as an add-on	Inline in the vendor's cloud for routed traffic	Inline at the appliance	At tunnel connection	Inline at a customer-run proxy
Reevaluation triggers	Identity and risk events; some periodic or per-request (varies by vendor)	Posture and risk; frequency and session behavior vary by vendor	Per-request policy possible (varies)	Mainly at connection	Per request; continuous device checks in some products
Application coverage	Strongest for SaaS; private apps via add-on services	Internet, SaaS and private; clientless RDP/SSH common	Primarily web	Broad, at network level	Broad for private apps (varies); SaaS when acting as identity provider
Device trust model	Device management and compliance at token issuance	Agent-based posture; limited clientless	Endpoint checks (varies)	Client posture at connect	Access-time inspection; continuous in some products
Deployment and data path	Vendor cloud (Ping also self-managed)	Vendor cloud; local brokers still cloud-dependent	Self-hosted or provider-hosted	Self-hosted appliance	Self-hosted on-premises or in the customer's cloud, including isolated environments
Operational model	Deep but spread across several products and tiers	Broad single platform; subscription bundles	Specialist skills; access licensed separately	Simple, but high exposure	Fewer products; less depth in adjacent areas

> **KEY TAKEAWAY**
>
> Every category makes tradeoffs. The useful question is which tradeoffs fit your applications, risks and team.

3. Cross-Cutting Issues

3.1 Device Management Versus Access-Time Device Inspection

Device trust is often treated as one capability. It is really two.

Device management platforms, such as Microsoft Intune, Jamf and Omnissa Workspace ONE, govern devices the organization owns: enrolling them, enforcing configuration baselines, deploying software and reporting compliance. Endpoint detection and response (EDR) tools such as Microsoft Defender for Endpoint and CrowdStrike Falcon watch for threats on those devices. These are essential, deep capabilities, and nothing in this paper suggests replacing them.

Access-time inspection answers a narrower question: is this device acceptable for this resource, right now? It examines the device when it requests access, and ideally keeps examining it while the session continues. Checks can include operating system state, running processes, registry values, certificates, the presence of specific files and whether security software is active.

The distinction matters in three situations:

- **Unmanaged devices.** Contractors, partners, students and vendors often use devices the organization does not own and cannot enroll. Management platforms cannot see them, but access-time inspection can still evaluate them when they request a resource.
- **Changes after login.** A compliance result is a snapshot. A device that was compliant at sign-in may not be twenty minutes later. In Microsoft's model, for example, a change in device compliance is not among the critical events CAE responds to [4].
- **Compliant but unsuitable.** A fully compliant device may still be running software that policy prohibits for a particular high-value system, such as an unauthorized remote-control tool.



Figure 2. Device management and access-time inspection answer different questions

3.2 A Note on AI Agents and Non-Human Identities

Software agents that act on behalf of users, including AI agents that call tools and APIs, are a fast-growing class of identity. During 2026, Microsoft, Okta, Ping Identity, Cloudflare and others announced or released capabilities for registering, governing and controlling agent access [36][37][38][39]. The principles in this paper apply directly: agents should authenticate, be authorized per action rather than per session, and have their access evaluated continuously, because an agent can perform many actions far faster than a human. This is an area where enforcement location will matter a great deal, and where standards are still forming.

3.3 The Operational Cost of Depth

The sixth criterion deserves more than a row in a table, because it is where many architecture decisions quietly fail. Feature depth has a cost structure: every product that is deep enough to be powerful is deep enough to require dedicated expertise — an administrator who knows its policy model, follows its release cadence, manages its patches and integrations, and can troubleshoot it under pressure. The large ecosystems are deep in many products at once, which means the fully realized version of that architecture carries a staffing plan: identity administration, device management, endpoint detection, data protection and network security as distinct specialties, each scarce and each expensive.

Licensing follows a similar accumulation pattern. Capability arrives in editions, add-ons and suites — Microsoft’s Entra Suite, for example, bundles Private Access, Internet Access, ID Governance, ID

Protection and Verified ID [9] — and gaps discovered during deployment tend to resolve to additional SKUs. The license bill at year three rarely matches the one modeled at purchase.

The security consequence matters more than the budget one. When staffing does not match the architecture's demands, consoles go unwatched, policies drift, and misconfiguration accumulates precisely where the product is most powerful. Organizations evaluating the operational-model criterion should ask not only how many products and consoles an outcome requires, but how many people, with which specialties, at what availability — and then compare that number honestly against the team they have. For large enterprises the answer may still favor depth. For mid-sized organizations, fewer products with one policy model is often not merely cheaper but better run — and better run is more secure.

4. Where Each Approach Fits Best

No single architecture is right for every organization. The table below summarizes where we believe each approach is strongest, including situations where our own product is not the best choice.

Situation	Typically strongest fit	Why
Predominantly cloud and SaaS applications, standardized on Microsoft 365 and Intune	Identity-centric platform (Microsoft)	Deepest integration across identity, device management and endpoint protection. An additional enforcement layer adds less value here.
Main need is securing internet and SaaS traffic for a distributed workforce	Cloud SSE platform	Secure web gateway, CASB and DLP at global scale are their core strength.
Large estates of on-premises, legacy, thick-client or OT applications	Unified self-hosted proxy	Inline coverage of non-web and legacy protocols, without relying on application changes.
Multiple identity providers, or many users on devices the organization does not own	Unified self-hosted proxy	One enforcement point across identity sources, with access-time device inspection that does not require enrolling the device in a management platform (full inspection uses an installed agent).
Data sovereignty, isolated or air-gapped requirements	Unified self-hosted proxy (or self-hosted ADC)	The customer controls the data path and the policy engine.
Large web application estate with an existing ADC team	ADC / WAF with access features	Builds on existing skills and infrastructure.
Mid-sized organization trying to reduce products and consoles	Unified self-hosted proxy	Authentication, MFA, SSO, device inspection and access enforcement on one platform.
Most real environments	A combination	Keep the identity platform as the store of users; put inline enforcement in front of private and sensitive applications.

Most real environments are mixed, and combinations are normal. A common and effective pattern is to keep an established identity platform, such as Microsoft Entra ID or Okta, as the authoritative store of users and credentials, while placing an inline enforcement point in front of the private, legacy and sensitive applications that the identity platform cannot see into. Organizations do not have to choose between identity depth and inline enforcement. They have to decide where each one belongs.

Cost is a legitimate part of this decision, and it extends beyond license prices. The number of products, consoles, integrations and specialist skills an architecture requires is often a larger long-term cost than its subscriptions, particularly for mid-sized organizations. Section 3.3 develops the staffing side of this in detail.

5. Questions to Ask Any Vendor

These questions are derived from the six criteria in Section 1. We encourage readers to ask them of every vendor they evaluate, including PortSys.

Criterion	Questions to ask
Enforcement location	Which of our applications will you be inline for, and which will you only gate at sign-in? What do you see after a session is established?
Reevaluation triggers	What causes an open session to be reevaluated, and how quickly does it take effect? If a device's state changes mid-session, what happens to that session?
Application coverage	Which of our non-web, legacy and OT applications can you protect without changes to the application? Do any of them require a client, and on which platforms?
Device trust model	How do you evaluate devices we do not own or manage? Which device attributes can you check, and how often?
Deployment and data path	Where does our traffic go, and where is policy stored and evaluated? What happens to access if your cloud, or our internet connection, is unavailable?
Operational model	How many products, licenses and consoles are required for the capabilities we have discussed? What skills does our team need to operate it day to day?
Security of the platform itself	How is the gateway hardened, how quickly are vulnerabilities patched, and what is your disclosure history?

6. How PortSys Approaches the Enforcement Gap

This section describes PortSys's own product. It applies the same criteria used throughout this paper, including where TAC's scope ends.

PortSys Total Access Control (TAC) is a self-hosted, unified access platform built on a secure reverse proxy architecture. TAC has been in production with enterprise customers for more than a decade, including customers with more than 10,000 users and more than 1,000 applications.

Enforcement location. For applications in the customer's own environment, on-premises or in the customer’s own cloud, TAC stays inline for the whole session and evaluates policy on each request. This includes web applications, Remote Desktop (RDP), SSH, thick-client and client-server applications, legacy applications that rely on Kerberos delegation or header-based authentication, and OT and IoT systems.

Cloud and SaaS applications. When TAC acts as the identity provider for a cloud application, it becomes the central point of access control: it issues the tokens that grant access and can proxy the application's traffic inline. It still validates credentials against existing repositories such as Active Directory or Microsoft Entra ID, so organizations do not need to move their users. When another platform remains the identity provider for a cloud application, TAC can protect access to it, but, like other products that are not in the traffic path, it does not continuously inspect that application's sessions.

Continuous device inspection. TAC is an access control platform, not a device management platform. It does not try to manage devices or watch everything they do. When a device requests a resource TAC protects, TAC inspects it deeply, and it keeps checking for changes in device state throughout the session, not only at initial access. Checks can include running processes, registry entries, certificates, the presence of specific files and other organization-defined markers, combined into multiple factors that are largely invisible to users. Full-context inspection requires the TAC agent. Installing it does not enroll the device in a management platform the way device management products do. Without the agent, TAC still evaluates policy and a limited set of device attributes, which matters for devices the organization does not own.

Integrated capabilities. MFA (with multiple methods), SSO, federation, device inspection, application publishing, load balancing and web application protection are part of one platform with one policy model and one console. TAC federates with Microsoft Entra ID, Okta and other identity providers, so it can work alongside an existing identity investment rather than replace it.

Deployment. TAC runs in the environment the customer selects: on-premises, in the customer’s own cloud environment (such as Azure or AWS), or fully isolated and air-gapped. In every case the customer controls the data path.

Licensing. TAC is licensed by number of users on an annual subscription, with all platform capabilities included. Customers do not buy separate products or tiers for MFA, SSO, device inspection or application publishing, which typically makes the total cost comparatively low.

Where TAC is not the strongest choice. For organizations that are almost entirely cloud-based, particularly those standardized on Microsoft, the Microsoft ecosystem offers deeper capabilities in areas

TAC does not try to cover, such as device management (Intune) and endpoint threat detection (Defender). For organizations whose main requirement is filtering internet and SaaS traffic, SSE platforms lead. TAC records access events with full user and device attribution; it is not a session-recording or full in-session activity audit tool. And like every gateway described in this paper, TAC is an internet-facing entry point that must be deployed, patched and monitored with care.

Where TAC fits best. Hybrid environments — organizations with significant on-premises, legacy, thick-client or OT applications in addition to cloud-based resources, which is to say most real enterprises; environments with multiple identity providers or many users on devices the organization does not own; organizations with data-sovereignty or isolation requirements; and teams that want to reduce the number of products and consoles they operate while closing the enforcement gap.

7. Conclusion

Zero Trust changed how organizations decide who gets in. The next stage of maturity is about what happens after they do.

The industry is converging on the right ideas. Identity platforms are adding event-driven session revocation, Shared Signals is giving vendors a common language for security events, and SSE and proxy vendors are moving enforcement closer to the application. These approaches differ in where they enforce policy, what triggers reevaluation, which applications they cover and who controls the data path, and those differences matter more than any feature checklist.

Organizations that map their own applications against those differences, and place enforcement where their real risk sits, will close the enforcement gap fastest. For most, that will mean combining an established identity platform with continuous, inline enforcement in front of the applications that matter most and the ones that are most vulnerable.

References

Vendor capability statements reflect public documentation reviewed in October 2026. Products change frequently; readers should confirm current capabilities with each vendor.

[1] NIST SP 800-207, Zero Trust Architecture, August 2020. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[2] CISA, Zero Trust Maturity Model, Version 2.0, April 2023. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

[3] NIST SP 1800-35, Implementing a Zero Trust Architecture, June 2025. https://www.nccoe.nist.gov/news-insights/nist-publishes-final-special-publication-1800-35-implementing-zero-trust-architecture

[4] Microsoft, Continuous access evaluation (Microsoft Learn), updated April 2026. https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-continuous-access-evaluation

[5] Microsoft, Universal continuous access evaluation (Global Secure Access), updated 2026. https://learn.microsoft.com/en-us/entra/global-secure-access/concept-universal-continuous-access-evaluation

[6] Microsoft, Conditional Access app control in Microsoft Defender for Cloud Apps, updated May 2026. https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad

[7] Microsoft, Global Secure Access connectors (Private Access and application proxy), updated September 2026. https://learn.microsoft.com/en-us/entra/global-secure-access/concept-connectors

[8] Microsoft, What is Microsoft Entra application proxy?, 2026. https://learn.microsoft.com/en-us/entra/identity/app-proxy/overview-what-is-app-proxy

[9] Microsoft, Microsoft Entra licensing, updated July 2026. https://learn.microsoft.com/entra/fundamentals/licensing

[10] Okta, Identity Threat Protection overview and session protection. https://help.okta.com/oie/en-us/Content/Topics/itp/overview.htm

[11] Okta, Shared Signals (Identity Threat Protection). https://help.okta.com/oie/en-us/content/topics/itp/shared-signals.htm

[12] Okta, About Okta Access Gateway. https://help.okta.com/oag/en-us/Content/Topics/Access-Gateway/about-oag.htm

[13] Ping Identity, PingAccess risk policies (PingAccess 9.1). https://docs.pingidentity.com/pingaccess/9.1/pingaccess_user_interface_reference_guide/pa_risk_policies_overview.md

[14] Ping Identity, Deployment options. https://www.pingidentity.com/en/platform/deployment-options.html

[15] OpenID Foundation, Shared Signals Framework 1.0 and CAEP 1.0 Final Specifications, 2025. https://openid.net/wg/sharedsignals/specifications/

[16] Zscaler, ZPA Private Service Edge data sheet. https://www.zscaler.com/resources/data-sheets/zpa-private-service-edge.pdf

[17] Zscaler, ZPA inspection (AppProtection) data sheet. https://www.zscaler.com/resources/data-sheets/zscaler-private-access-inspection-benefits.pdf

[18] Netskope, Local Broker best practices and FAQs. https://docs.netskope.com/en/local-broker-best-practices-and-faqs

[19] Netskope, Netskope One Private Access data sheet, September 2025. https://www.netskope.com/wp-content/uploads/2025/07/2025-09-Private-Access-DS-376-7.pdf

[20] Palo Alto Networks, ZTNA Connector in Prisma Access, updated October 2026. https://docs.paloaltonetworks.com/prisma-access/administration/ztna-connector-in-prisma-access

[21] Cloudflare, Non-HTTP applications and device posture checks (Cloudflare One documentation). https://developers.cloudflare.com/cloudflare-one/reusable-components/posture-checks/

[22] Cisco, Secure Access data sheet, updated July 2026; Hybrid Private Access documentation. https://www.cisco.com/c/en/us/products/collateral/security/secure-access/secure-access-ds.html

[23] F5, BIG-IP Access Policy Manager data sheet. https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf

[24] CISA, Emergency Directive 26-01: Mitigate Vulnerabilities in F5 Devices, October 15, 2025. https://www.cisa.gov/news-events/directives/ed-26-01-mitigate-vulnerabilities-f5-devices

[25] CISA, FBI, MS-ISAC and ASD's ACSC, Advisory AA23-325A: LockBit 3.0 Affiliates Exploit CVE-2023-4966 (Citrix Bleed), November 21, 2023. https://ic3.gov/CSA/2023/231121.pdf

[26] CISA, Supplemental Direction V1 to Emergency Directive 24-01 (Ivanti Connect Secure and Policy Secure), January–February 2024. https://www.cisa.gov/news-events/directives/supplemental-direction-v1-ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure

[27] CISA, Emergency Directive 25-03: Identify and Mitigate Potential Compromise of Cisco Devices, September 25, 2025. https://cisa.gov/news-events/directives/ed-25-03-identify-and-mitigate-potential-compromise-cisco-devices

[28] Canadian Centre for Cyber Security, AL25-005: Compromise and persistent access to Fortinet FortiOS products, April 2025. https://www.cyber.gc.ca/en/alerts-advisories/compromise-persistent-access-fortinet-fortios-products-cve-2022-42475-cve-2023-27997-cve-2024-21762

[29] Palo Alto Networks Unit 42, Threat Brief: Operation MidnightEclipse (CVE-2024-3400), April 2024. https://unit42.paloaltonetworks.com/cve-2024-3400/

[30] CISA, Binding Operational Directive 23-02: Mitigating the Risk from Internet-Exposed Management Interfaces, June 13, 2023. https://www.cisa.gov/news-events/directives/binding-operational-directive-23-02

[31] NSA and CISA, Selecting and Hardening Remote Access VPN Solutions, September 28, 2021. https://www.cisa.gov/news-events/alerts/2021/09/28/cisa-and-nsa-release-guidance-selecting-and-hardening-vpns

[32] Teleport, Architecture: agents and services. https://goteleport.com/docs/reference/architecture/agents/

[33] Pomerium, What is Pomerium? https://www.pomerium.com/what-is-pomerium

[34] Akamai, Enterprise Application Access connectors. https://techdocs.akamai.com/eaa/docs/conn

[35] Microsoft, JSON Web Token validation in Azure Application Gateway (preview). https://learn.microsoft.com/en-us/azure/application-gateway/json-web-token-overview

[36] Microsoft, What's new in Microsoft Entra Agent ID, 2026. https://learn.microsoft.com/en-us/entra/agent-id/whats-new-agent-id

[37] Okta, "Okta brings first-class identity to AI agents with Agent SSO," press release, August 2026. https://okta.com/newsroom/press-releases/okta-brings-first-class-identity-to-ai-agents-with-agent-sso/

[38] Ping Identity, Identity for AI release notes, 2026. https://developer.pingidentity.com/identity-for-ai/release-notes/idai-whats-new.html

[39] Cloudflare, Access changelog (MCP server portals), 2026. https://developers.cloudflare.com/changelog/product/access/

[40] Microsoft, Header-based single sign-on with Microsoft Entra application proxy. https://learn.microsoft.com/en-us/entra/identity/app-proxy/application-proxy-configure-single-sign-on-with-headers

[41] Zscaler, "Why continuous access evaluation matters now," April 2026. https://www.zscaler.com/blogs/partner/evolving-cybersecurity-landscape-why-continuous-access-evaluation-matters-now

[42] Zscaler, Privileged Remote Access for OT and IIoT data sheet. https://www.zscaler.com/resources/data-sheets/privileged-remote-access-for-OT-IIoT.pdf

[43] Netskope, Browser-based access for Netskope Private Access. https://docs.netskope.com/en/npa-browser-based-access

[44] Palo Alto Networks, Configure applications for Secure Agentless Access. https://docs.paloaltonetworks.com/prisma-access/administration/secure-agentless-access/configure-applications-for-secure-agentless-access

[45] Zscaler, On-premises ZTNA. https://www.zscaler.com/products-and-solutions/ztna-on-premises

[46] Okta, Okta Privileged Access gateways. https://help.okta.com/en-us/content/topics/privileged-access/gateways/pam-gateways.htm

[47] Zscaler, About Privileged Remote Access applications. https://help.zscaler.com/unified/about-privileged-remote-access-applications

[48] Cloudflare, Non-HTTP applications (browser-rendered SSH, RDP and VNC). https://developers.cloudflare.com/cloudflare-one/access-controls/applications/non-http/

[49] SecurityBrief, "Palo Alto Networks unveils AI-driven OT security solutions," October 30, 2024. https://securitybrief.co.uk/story/palo-alto-networks-unveils-ai-driven-ot-security-solutions

[50] Ping Identity, PingAccess use cases and deployment architecture (PingAccess 9.1). https://docs.pingidentity.com/pingaccess/9.1/reference_guides/pa_use_cases_and_deployment_architecture.html

About the Author

Michael Oldham is the founder of PortSys, Inc. His career in enterprise IT reaches back to the 1980s and spans each generation of access technology described in this paper, from centralized mainframe access and client-server computing to VPNs, single sign-on, mobile device management and cloud-delivered ZTNA.

About PortSys

PortSys, Inc., founded in 2008, develops Total Access Control (TAC), a unified access control platform built on a secure reverse proxy architecture. TAC is used by enterprises and public-sector organizations to secure access to cloud, on-premises, legacy and operational technology applications.

PortSys, Inc. · 31 Hayward Street, Suite 2B, Franklin, MA 02038

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