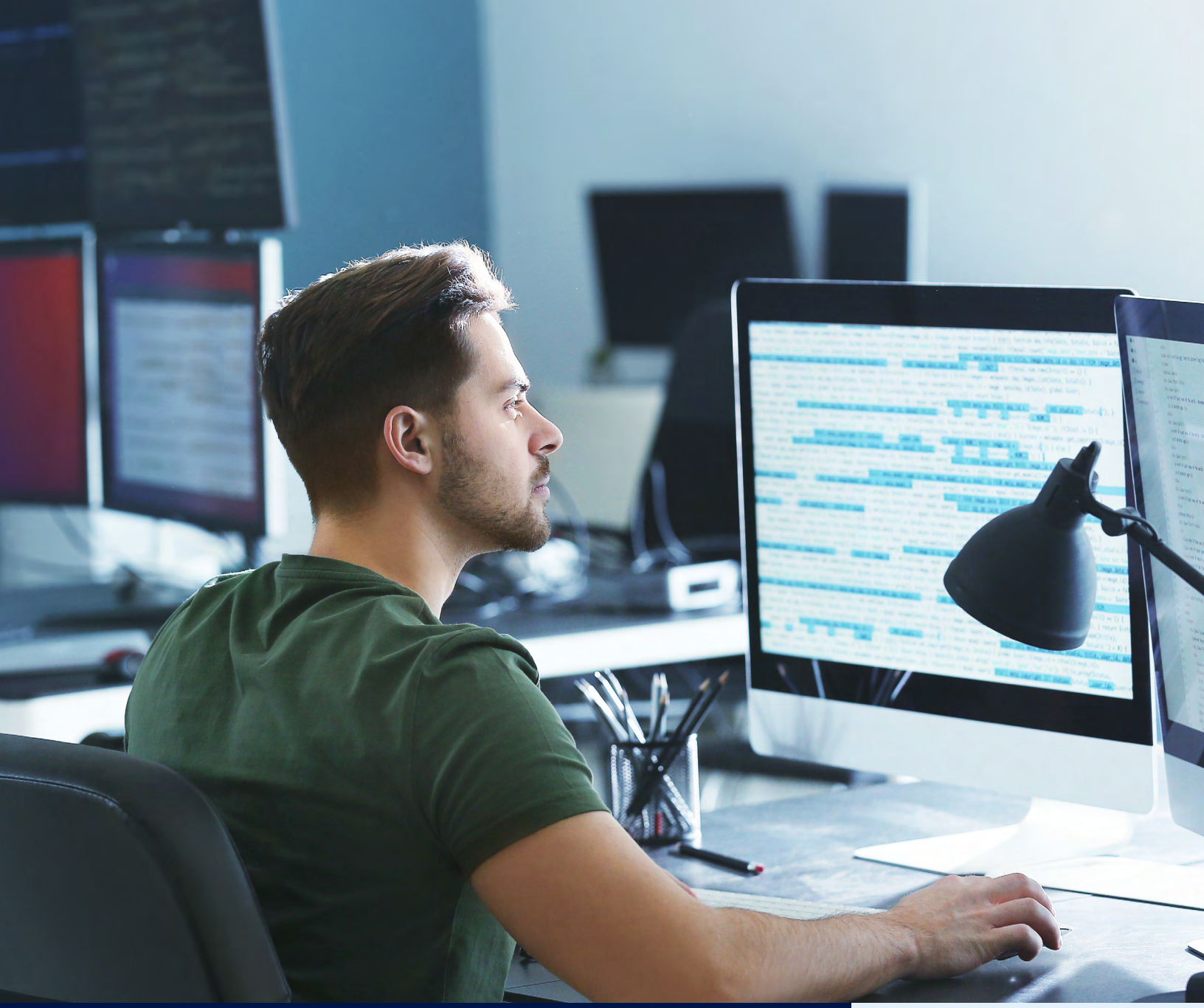

Cybersecurity > VPN

Zscaler Private Access™ (ZPA) overlays an organization's broader strategic vision and empowers its strategies (zero trust, cyber, cloud, CMMC, etc.) to secure dynamic operations across all environments

Solution Brief

E Pluribus Unum: 3 Capabilities, 1 Endpoint Agent, Anywhere

Zscaler Private Access (ZPA) is a part of the Zscaler Zero Trust Exchange™ platform, which simplifies and reduces software bloat on endpoints by consolidating security, threat intelligence, VPN/ZTNA, and network/data visibility capabilities. Combined with **Zscaler Internet Access**™ (ZIA) and **Zscaler Digital Experience**™ (ZDX), ZPA delivers a powerful software-defined perimeter (SDP) and zero trust network access (ZTNA) solution that provides comprehensive multitenant cloud security, enforcing unified policies to securely connect authorized users to authorized applications.

Together, ZPA, ZIA, ZDX connect, secure and enable users on/off premises across countless use cases.

ZPA, ZIA, and ZDX are all FedRAMP JAB-High & Moderate.

- **ZPA** secures user-to-app traffic and provides fast access to internally managed apps hosted in public, private, hybrid clouds and enterprise data centers. A complete VPN replacement, ZPA provides an SDP/ZTNA solution that enforces least privilege using unified policies from the organization's IdP, EDR/NDR, SIEM/SOAR.
- **ZIA** securely connects users to externally managed applications, including SaaS and internet destinations, no matter the location, device, or network. ZIA enforces least-privileged access using unified polices derived from the digital ecosystem.
- **ZDX** improves user experiences by giving IT teams unified visibility to rapidly detect and resolve app, network, and device issues. ZDX monitors SaaS and private application performance, inventories devices and software, and can work standalone or via native ZIA and ZPA integration.

Software-Defined Perimeter (SDP)
Zscaler's Response to a VPN-less world

The paradigm shift to a NIST Zero Trust Architecture (ZTA) emphasizes the need to transition to modern cybersecurity strategies and tools. To reduce and protect the attack surface and assets, commercial, federal, and defense agencies are moving away from a network perimeter-based security approach to zero trust network access (ZTNA), also known as the software-defined perimeter (SDP).

Zscaler Private Access **was the first ZTNA/SDP** solution of its kind to redefine private app connectivity by forming a virtual boundary around an organization's network perimeter, reducing its attack surface and effectively hiding resources from threats.

ZPA simplifies network operations by decoupling security from traditional network architecture, freeing up decades of network appliances and configurations, bloat, and blockages. ZPA secures the user, the application, and the connectivity in between using zero trust technical and policy controls, and enforcing least-privilege access to private applications that could be running on-premises, on hybrid clouds, or edge compute nodes-all while eliminating unauthorized access and lateral movement.
ZPA complies with SDP's four core requirements and delivers significant added value right out of the box:

1. Trust is never implicit.

2. No inbound connections.

3. Application segmentation, not network segmentation.

4. Leverage the internet, securely.

ZPA VALUE PROPOSITION	
Extend Zero Trust Security & Principles	Make applications invisible even when using insecure public internet connections.
Provide App Protection	Secure multicloud access in any form: public, private, or hybrid cloud or data center.
Reduce Operational Complexity	Reduce third-party risk and simplify administrative and operational burdens.
Increase Statewide Mobility/Flexibility	Accelerate unification of networks and securely expedite third-party access.
Enforce Comply-to-Connect	Provide adaptive access in a variety of environments.
Deliver a VPN Alternative	Eliminate lateral movement and reduce network complexity
Enhanced Logging	Stream tailored logs to multiple SIEMs simultaneously
ZPA LEVERAGES THE SAME APP FOR:	
Internet and SaaS Security (ZIA)	Combine secure web gateway (SWG), analytics, and enhanced visibility
Digital Experience Monitoring	Enhance endpoint, network, and resource performance by understanding what's happening within your environment, end-to-end, hop-by-hop

Analysis of [VPN] Alternatives

ZPA's simplicity of operations, API integrations, and versatility allow administrators and architects to plug and play ZPA into traditional and nonstandard environments while supporting use cases to work together with other VPN alternatives.

ZTNA/SDP	ZPA delivers ZTNA as an SDP. However, ZPA natively includes Comply-to-Connect functionality, logging, and 140+ API integrations.
SASE	Per Gartner, SASE equals SSE (ZIA+ZPA) + SD-WAN. While an SDP may bring a ZTNA component to SASE, SASE requires a SWG, CASB, FWaaS, and more.
SD-WAN	On its own, SD-WAN lacks the comprehensive security ZPA and ZIA deliver. ZPA and ZIA would secure user access to the internet, private apps, and SaaS.
UEM, MDM, and EMM	Compatible, Supportive, and Enhanced. ZPA integrates with UEMs to streamline secure access as well as provide Comply-to-Connect functionality coupled with logging.
VDI	Compatible and Supportive. Zscaler customers can use ZPA to access a VDI/DaaS environment, and then use ZIA to access the internet from the VDI/DaaS client.
Other VPN Alternatives	Other VPN alternatives can present challenges regarding compliance, scalability, integration, automation, and security requirements

ZPA Technical Coverage

One user, multiple devices	Security follows the user, instead of requiring separate reconfiguration on every device.
Platform-neutral	– Zscaler endpoint client works with Windows, MacOS, Chromebook, iOS, Android, Linux. – ZPA can operate as clientless (i.e., browser-based access). While using browser-based access, ZPA can integrate with Chrome browser to create and enforce approved device posture profiles.
Network-agnostic	Uncouples network and security to take advantage of all network scenarios.
PKI indifferent	– Encrypts using the organization's organic PKI for an added encryption layer. – Resistant to SAML and attacker-in-the-middle (AiTM) attacks. – Facilitates an encrypted Mutually. Authenticated Certificate-pinned connection.
Embedded Adaptive Access capability	API integration to enhance tailored Adaptive Access/Continuous Access policies.
140+ integrations	Integrates with multiple enterprise solutions simultaneously.
Network aware	Recognizes when user is not on the on-premises network and can enforce "off-premises" policies.
mTLS	works over low-bandwidth, high latency.
Logging	Tailored logs sent to multiple SIEMs simultaneously.

Beyond Traditional VPN Capabilities

Secure fast pass	– Internet is redefined as new secure network via end-to-end encrypted TLS tunnels. – Dynamically establishes and terminates connections .
Remove duplicative efforts	– Same enforcement of security policies on/off premises. – Same enforcement of security policies for managed and unmanaged devices (i.e., BYOD).
Remove human error	Zscaler can update its SDP components automatically.
Enable operational flexibility	ZPA's clientless functionality fills the gap between managed and unmanaged devices.
Empower help desk teams	– ZPA natively integrates with ITSM capabilities. – ZPA can incorporate ZDX, which can be leveraged by service desk teams and integrate with ITSM tools.
Data loss prevention	ZPA's endpoint agent allows the organization to take advantage of ZIA's DLP feature using the same app.
Inside-out connection	– No Active Listener. – Segmentation at the application level, not the network level, limits user access to application, restricting lateral movement.

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com