DATA SHEET

Zscaler Private Access™

Empower your workforce with fast, secure, and reliable access to private apps with the industry's first AI-powered ZTNA

Zscaler Private Access (ZPA) is a cloud-native solution that delivers zero trust access for all users with direct connectivity to private applications while minimizing the attack surface, eliminating lateral movement and protecting against sophisticated attacks.

Legacy network security approaches fail the needs of your hybrid workforce and your business. Traditional firewalls and VPNs create a massive attack surface for attackers to find and exploit. They also put users directly on your network, allowing lateral threat propagation. If your user's credentials are compromised, attackers have easy access to your sensitive data. Using a VPN to enable your hybrid workforce and third-party access increases cyber risk, creates poor user experiences, and adds to administrative overhead. To provide secure access to users from any device and location, you need a more effective approach.

According to Zscaler ThreatLabz 2025 VPN Risk Report – 92% of respondents share concerns that unpatched VPN flaws directly lead to ransomware incidents, highlighting how difficult it is to continuously patch VPNs in time.

Benefits:

- **Replace vulnerable VPN solutions**
  Reduce the attack surface and eliminate lateral movement by connecting users directly to applications – not the network, elevating your security posture.
- **Prevent cyber attacks**
  Minimize risk of a breach with private app protection against web and identity threats, advanced threat protection with full inline inspection and data loss prevention.
- **Empower your hybrid workforce**
  Seamlessly extend lightning fast access to private apps across users, HQ, branch offices, and third parties.
- **Reduce operational complexity**
  Offer secure, optimized access, without costly and complex point products, through a unified, cloud-native ZTNA platform for users, workloads, and OT/IT

©2025 Zscaler, Inc. All rights reserved.

Attackers can easily circumvent legacy network security approaches by taking advantage of the inherent trust and overly permissive access of traditional castle-and-moat architectures, including:

- **Legacy architecture can't scale or deliver a fast, seamless user experience:** VPNs require backhauling, which introduces cost, complexity, and too much latency for today's remote workforce
- **Traditional firewalls, VPNs, VDI, and private apps create a massive attack surface:** Attackers can discover and exploit vulnerable, externally exposed resources
- **Access to the full network allows free lateral movement:** VPNs put users on your network, giving attackers easy access to sensitive data
- **Compromised users and insider threats can bypass traditional controls:** Advanced attackers can steal credentials and subvert identity to access private apps with legacy remote access tools

It's time to rethink how we securely and seamlessly connect users to the applications they need and redefine private application security with a Zero Trust Network Access (ZTNA) solution.

Zscaler Private Access™ (ZPA)

Industry's first AI-powered ZTNA, Zscaler Private Access (ZPA) is a cloud-native solution that delivers zero trust access for all users with direct connectivity to private applications while minimizing the attack surface by hiding apps behind the Zero Trust Exchange, eliminating lateral movement using AI-powered user-to-app segmentation and protecting against sophisticated attacks with integrated traffic inspection, application and data protection.
As a resilient cloud native service built on a holistic security service edge (SSE) framework, ZPA can be deployed in a matter of hours to replace legacy VPNs and remote access tools to:

- **Minimize the attack surface:** Applications are made invisible to the internet preventing unauthorized users and devices from discovering them. The inside-out connections between user and app ensures apps and IPs are never exposed
- **Enforce least-privileged access:** Application access is determined by identity and context, not an IP address. Users are never put on the network for access
- **Eliminate lateral movement:** Applications are segmented so that users can only access a specific app, helping limit lateral movement
- **Stop cyberattacks with complete inspection:** Private app traffic is inspected inline to prevent the most prevalent web attack techniques
- **Prevent data loss:** Integrated DLP for private apps, advanced incident response and data classification to protect crown jewel apps
- **Deliver a superior user experience:** Connecting users directly to private apps eliminates slow, costly backhauling over legacy VPNs while continuously monitoring and proactively resolving user experience issues

92% of respondents share concerns that unpatched VPN flaws directly lead to ransomeware incidents, highlighting how difficult it is to continuosly patch VPNs in time

— Zscaler ThreatLabz 2025 VPN Risk Report

*Gartner, Emerging Technologies: Adoption Growth Insights for Zero Trust Network Access, Nat Smith, Mark Wah, Christian Canales. 8 April 2022

©2025 Zscaler, Inc. All rights reserved.

Key Use Cases

Secure remote access (VPN replacement)
Cloud-delivered or appliance-based VPNs leave you exposed to cyberattacks. They are plagued by vulnerabilities and regularly exploited by attackers. Their network-centric design backhauls traffic, expands attack surface, and allows for lateral movement by putting users directly on the network leading to ransomware attacks. VPNs are insecure, slow, and complex to manage.

ZPA resolves these challenges by delivering zero trust access for all users with direct connectivity to private applications while minimizing the attack surface by hiding apps behind the Zero Trust Exchange, eliminating lateral movement using AI-powered user-to-app segmentation and protecting against sophisticated attacks with integrated traffic inspection, application and data protection. ZPA provides fast, direct access to

applications via more than 160 globally distributed points of presence (PoPs) without the security risks inherent to VPN. ZPA's cloud native design means IT teams can eliminate inbound gateway appliances like load balancers, VPN concentrators, and other security devices, reducing costs, complexity, and management overhead. ZPA delivers zero trust access to all applications including network connected applications such as Voice over IP (VoIP) and server to client applications, and even business partner hosted (extranet) applications without the need to deploy additional infrastructure such as app connectors.

Secure app access for in-office and remote users
In the modern workforce, users work from their homes and other remote locations, branch offices, and headquarters, challenging legacy security paradigms. Organizations need uninterrupted access to applications, without compromising Zero Trust security during disasters or periods of degraded infrastructure access. Compliance and regulatory standards must be met for Business Continuity.

ZPA Private Service Edge enables you to deploy the power of the cloud to your premises, enforcing the same security controls as your remote users with the same high performance.

By deploying Zscaler Private Service Edges with private cloud controllers, ZPA supports fully automated switchover to Business Continuity Mode in the event of an outage detection. Policies and authentication are enforced even if the ZPA Cloud is not reachable.

BYOD and third-party user access
Traditional third-party access relied on costly, complex, and risky solutions like VDI, RDP, SSH, or VNC, which put users directly on the network and exposed internal systems to untrusted devices.

ZPA's Clientless Access capabilities make third-party access effortless, reduce costs and minimize risks. Third-parties like contractors, vendors, and partners can use any web browser from their own devices to connect to intranet websites, internal systems, and equipment—no client needed. It keeps third-party users and unmanaged devices isolated from your network and applications, ensuring sensitive data is protected from unauthorized copy/paste, printing, and upload/download. The integration of ZPA and Google Chrome Enterprise Browser will enhance security for unmanaged devices/BYOD by verifying Chrome Enterprise Browser and incorporating additional posture information into ZPA policy checks. With Clientless Access, IT can deliver a better and more secure experience for users without incurring the costs of managing legacy VDI. M&A and divestitures pose network integration challenges, but ZPA accelerates this process from months to weeks. ZPA offers seamless access to private apps, eliminating the need for network convergence or additional equipment.

Privileged remote access for OT/IT
Employees and third-party vendors need to access

©2025 Zscaler, Inc. All rights reserved.

OT/IT assets regularly to maximize production uptime as well as avoid disruptions from equipment and process failures. ZPA enables fast, secure, and reliable access to OT/IT environments from field locations, the factory floor, or anywhere else. ZPA for OT/IT provides fully isolated, clientless remote desktop access to internal RDP, SSH, and VNC target systems—without requiring users to install a client on their device using jump hosts and legacy VPNs.

VDI Alternative

IT and security teams lack control over unmanaged devices, creating business risks. To support application access on unmanaged devices, traditionally organizations have used VDI. VDIs put users directly on the network, exposing internal applications to unmanaged endpoints. In addition, VDIs are expensive, cumbersome to manage, and doesn't scale. In the wake of digital transformation, modernized applications are typically web or browser-based, and streaming an entire desktop via VDI does not provide a very good end user experience.

ZPA is an effective VDI alternative, offering secure agentless, browser-based access on unmanaged devices. Users get fast, seamless access to private apps brokered by the closest service edge. ZPA architecture provides direct access to applications, without placing the user on the network, making access to private applications secure. ZPA Browser Access allows users to leverage a web browser for user authentication and application access, without requiring Zscaler Client Connector installed on their devices. ZPA has integrated browser isolation, because of which only pixels are streamed to the end user device, instead of the actual content, data within apps stay safe. ZPA allows admins to create isolation policies to define how a user can interact within the isolated environment.

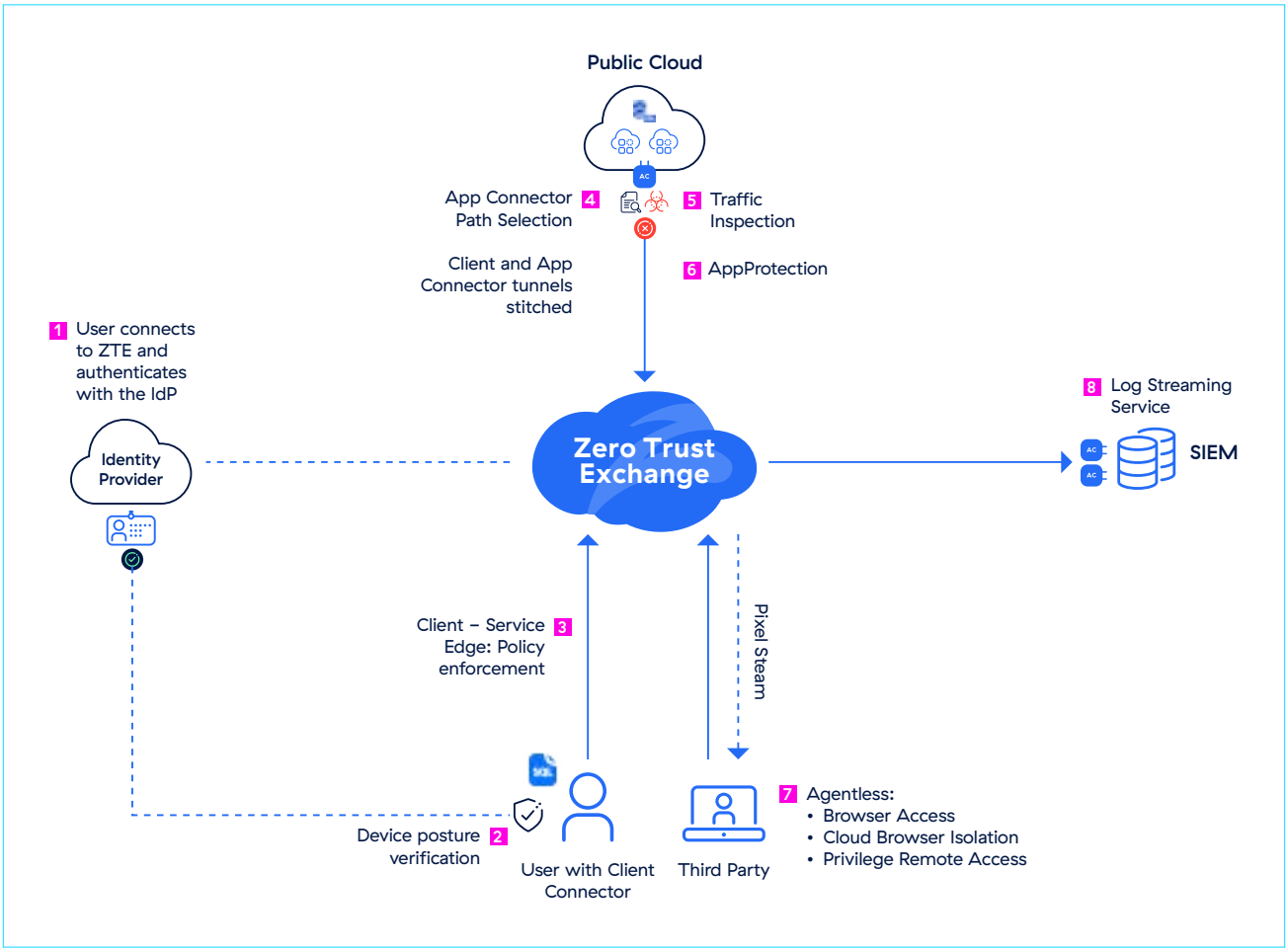
Microsegmentation (User-to-App Segmentation)

Remote access solutions like VPNs grant full network access, and they expose IPs and applications to the internet. VPNs extend the internal network to remote devices and, by design, require inbound traffic, exposing a public attack surface. Without proper network segmentation, a breach in one segment could compromise the organization's entire network. Having said that, implementing segmentation requires complex firewall rules that are difficult to maintain, often disrupt applications, and can complicate access for VPN users. Within large organizations, this often requires high-availability, complex routing, and costly private links.

Zscaler Autonomous user-to-app Segmentation delivers precise user-to-app segmentation and a robust solution for easily deploying consistent policies at scale and eliminating lateral threat movement. It automates the entire segmentation lifecycle by seeing every application through discovery, segmenting faster with AI-driven recommendations, and strengthening your posture with live insights.

©2025 Zscaler, Inc. All rights reserved.

How ZPA Works



How it works

When a user (employee, vendor, partner, or contractor) attempts to access an internal application, ZPA provides secure, direct connectivity by following these steps:

1. User connects to Zero Trust Exchange with the Client Connector and authenticates with the Identity Provider (IdP). Upon successful authentication, it reconnects to the Public Service Edge, establishing a single, permanent TLS connection to the Service Edge.
2. Upon user authentication and tunnel establishment to the Service Edge, the client connector downloads its configuration, including the device posture check.
3. The Zscaler app forwards the user's traffic to the closest ZPA Service Edge, which acts as a broker, where the user's security and access policies are checked.
4. Two outbound tunnels, one from the Client Connector on the device and the other from the App Connector, are stitched together by the Service Edge

©2025 Zscaler, Inc. All rights reserved.

5 Once a connection is established between the user's device and the application, App Connector automatically inspects the traffic inline to detect and stop potential threats coming from users or devices that may have been compromised

6 Zscaler AppProtection secures private apps from web and identity-based through a comprehensive Layer 7 inspection, enhancing overall security posture.

7 Third-party users can connect to private applications with integrated browser-based access or Zscaler Browser Isolation for clientless access on unmanaged devices

8 Log Streaming Service (LSS) streams various logs, including user activity to SIEM

A ZPA Service Edge can either be hosted by Zscaler in the cloud (ZPA Public Service Edge) or run on-premises within your infrastructure (ZPA Private Service Edge), providing a shorter path to local apps and supporting Business Continuity Planning.

Core Capabilities

App discovery	Automatically discover and catalog applications using specific domain names and IP subnets to get granular insight into your private application estate and potential attack surface.
User-to-app segmentation	Ensure all application access is granted on a need-to-know, least-privileged basis with user-to-app segmentation. Provide authorized users secure access to specific named applications, without ever placing users on the network. Avoid the need for complicated network segmentation with internal firewalls.
Autonomous user-to-app segmentation	Automate the entire segmentation lifecycle by seeing every application through discovery, segmenting faster with AI-driven recommendations, and strengthening your posture with live insights. Powered by ML models continually trained on millions of customer signals and your unique application access patterns, autonomous user-to-app segmentation can help you eliminate lateral threat movement, accelerate your ZTNA journey, and simplify and scale zero trust operations.
Risk-based policy engine	Continuously validate access policies based on user, device, content, and application risk posture with a powerful native policy engine to ensure only valid, authenticated users can access private applications.
Threat and data protection	Reduce the risk of threats with full content inspection. Find and control sensitive data across the user-to-app connection.
AppProtection	Protect private apps and infrastructure against the most prevalent attacks with high-performance, inline security inspection of the entire application payload that exposes threats. Identify and block known web security risks, such as the OWASP Top 10, and emerging zero-day vulnerabilities that can bypass traditional network security controls.
Privileged Remote Access	Allow privileged administrators and operators to securely connect to intranet websites, internal systems, and equipment without the need for VPN, VDI, or remote desktop clients such as RDP, SSH, and VNC.
Secure access to Legacy S2C Apps	Enable to secure access to legacy network connected applications such as VoIP, Follow me printer and other server-to-client applications.
B2B Application Access	Enable bi-directional secure access to applications and workloads hosted in your business partner's network (Extranet)

©2025 Zscaler, Inc. All rights reserved.

Client-based and clientless access	Choose the optimal method of protection for your hybrid environment. Client-based access ensures managed users are protected even when off the corporate network through the lightweight Zscaler Client Connector agent. Clientless access provides third-party contractors and BYOD users with frictionless app access from any device and web browser.
In-Office ZTNA	Enforce ZTNA for in-office users using ZPA private service edges, ensuring fast and seamless access to applications. Our universal ZTNA ensures consistent access and policies for users irrespective of the location of the users and the applications.
Business Continuity and Disaster Recovery	Ensure uninterrupted access to mission-critical applications even during a black swan event with a customer hosted or fully managed business continuity solution.

Benefits

Minimize the attack surface
Eliminating vulnerable VPNs and making apps invisible to the internet renders it impossible for unauthorized users to find and attack them. ZPA creates a segment of one between an authorized user and a specific private app, removing all inbound connectivity and allowing only inside-out connections via encrypted microtunnels to users' devices. Admins can automatically discover and segment rogue applications, services, and workloads using application discovery, further reducing the attack surface.

Eliminate lateral movement
Connectivity based on least-privileged access ensures application access is granted on a one-to-one basis from an authorized user to named applications, rather than full access to the network. Therefore, lateral movement between apps or across the network is impossible. As ZPA is not based on IP addresses, the need to set up and manage complex network segmentation, access control lists (ACLs), firewall policies, or network address translations is eliminated.

Prevent compromised users, insider threats, and advanced attackers
Integrated inline inspection and DLP capabilities, minimizes the risk of compromised users and active attackers. ZPA automatically stops web attacks with complete coverage for the most prevalent techniques, including the OWASP Top 10, and full custom signature support for immediate virtual patching against zero-day vulnerabilities. ZPA minimizes third-party and BYOD risks with fully isolated access to applications that keeps sensitive data off unmanaged devices using integrated cloud browser isolation.

Deliver an exceptional user experience
Consistently fast connectivity that doesn't require logging in and out of VPN clients gives remote users a more secure and efficient access experience. Third-party contractors, vendors, and partners benefit from frictionless access from any device and web browser without the need to install a client. Users enroll with their existing SSO credentials (Azure AD, Okta, Ping, etc.) Additionally, administrators can keep users productive by proactively detecting and resolving end user performance issues caused by private app access difficulties, network path outages, or network congestion.

A unified platform for secure access across apps, workloads, and devices
Extend zero trust across private apps and OT/IT devices to simplify and integrate multiple disjointed remote access tools, unifying security and access policies to stop breaches and reduce operational complexity.

©2025 Zscaler, Inc. All rights reserved.

Zscaler Private Access (ZPA): Multiple Options to get Started

	Zscaler Essentials Platform (ZS-ESS-PLATFORM)	ZPA Clientless Platform (ZPA-CLIENTLESS-PLATFORM)	Zscaler Private Access Platform (ZS-ZPA-PLATFORM)	Zscaler Platform (ZS-PLATFORM)
Private Access Platform Services				
Granular access control by user, group and ports	✓ 1 user per 20 subscribed users (Min: 500 subscribed users)	✓	✓	✓
Log Streaming Service				
Continuous Health Monitoring for all apps				
Source IP Anchoring: Selectively forward app traffic to the appropriate destination servers				
App Connector: Lightweight VM that enables inside-out connections to Zscaler ZTE	As many as required, up to system max	As many as required,up to system max	As many as required, up to system max	As many as required, up to system max
ZPA Private Service Edge: ZTNA for remote and in-office users	–	–		
ZPA for Legacy Apps (VoIP, S2C, etc.)	–	–	Add-On VPN Service Edges (Min: 50 users)	Add-On VPN Service Edges (Min: 50 users)
ZPA Business Continuity Cloud	–	–	Add-On (Min: 500 users)	Add-On (Min: 500 users)
User-to-App Segmentation	10 App Segments	20 App Segments	20 App Segments	20 App Segments
Autonomous user-to-app segmentation and insights	–	–	**Add-On**	**Add-On**
Third Party Access			Add-On (Min: 500 users)	Add-On (Min: 500 users
Browser-based Access for unmanaged devices	–	✓	✓ Additional guest users licenses can be purchased with ZPA-CLIENTLESS-PLATFORM	✓ Additional guest users licenses can be purchased with ZPA-CLIENTLESS-PLATFORM
User Portal: Single web portal for users to access authorized apps and privileged consoles				
Privileged Remote Access Standard: Clientless PRA to OT (up to 10) systems (RDP/SSH/VNC)				
Browser Isolation for Private and SaaS Apps		**Add-On**	**Add-On**	**Add-On**
Digital Experience Monitoring	–	–	✓	✓
ZDX Standard: Visibility into user, connectivity and application telemetry				
Protect Private Apps and Data	**Add-On**			
Data protection for private apps, incident response and data classification		–	**Add-On**	✓
Zscaler Deception: Integrated decoys to detect compromised users		–	✓ (Min 500 users)	✓ (Min 500 users)
AppProtection to protect private apps from OWASP Top 10 and web traffic inspection		**Add-On**	**Add-On**	**Add-On**

©2025 Zscaler, Inc. All rights reserved.

Key differentiators

As the industry's first AI-powered ZTNA solution, ZPA delivers superior security with an unrivaled user experience:

- **Built from the ground up for least-privileged access:** Allow authorized users to connect only to approved resources, not your network—which is impossible with legacy VPNs
- **Apps become invisible and inaccessible to attackers:** Stop app compromise, data theft, and lateral movement by making private apps, workloads, and devices invisible to the public internet
- **Full inline inspection:** Protect your applications by identifying and stopping exploitation of private apps, automatically preventing the most prevalent web attacks while protecting your data with industry-leading DLP
- **Enable global business continuity without compromising security:** Minimize impact of disruptions and enforce zero trust access to meet strict compliance requirements even when Zscaler cloud is unreachable
- **Secure browser access:** Leverage browser-based access for third parties with integrated DLP
- **Eliminate lateral movement with Autonomous user-to-app segmentation:** Delivers precise user-to-app segmentation, visualizes access, and fine-tunes policies using machine learning to minimize attack surfaces and prevent lateral threats
- **Global edge presence:** Gain unmatched security and user experience with 160+ cloud edge locations worldwide, as well as an optional local service edge to extend zero trust to your HQ
- **Cloud native foundation:** Leverage the scalability of a cloud-delivered platform without costly on-premises appliances or complex infrastructure as your business grows
- **Unified ZTNA platform for users, workloads, and devices:** Securely connect to private apps, services, and OT devices with the industry's most comprehensive ZTNA platform
- **Part of an extensible zero trust platform:** Protect and empower your business with the Zero Trust Exchange, built on a complete SSE framework

Gartner

Zscaler named a Leader in the 2025 Gartner® Magic Quadrant™ for Security Service Edge**

Learn More

**Gartner, Magic Quadrant for Security Service Edge, Charlie Winckless, Thomas Lintemuth, Dale Koeppen, April 15, 2024

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.

©2025 Zscaler, Inc. All rights reserved.

Foundational components

Zscaler Client Connector
Client Connector is a lightweight application that runs on users' laptops and mobile devices. By automatically forwarding user traffic to the closest Zscaler Service Edge, it ensures that security and access policies are enforced across all devices, locations, and applications.

Zscaler Clientless Access
Users can securely connect to apps, workloads, and OT devices via integrated browser–based access (Web, RDP, SSH, VNC) or Zscaler Browser Isolation for clientless access on unmanaged devices.

ZPA App Connector
App Connectors are lightweight virtual machines that sit in front of private applications deployed in the data center or public cloud, brokering security connectivity between an authorized user and a named app with an inside–out connection that doesn't expose apps to the internet.

ZPA Network Connector
Network Connectors are lightweight virtual machines that are deployed in front of the application servers in the data center, and connect to VPN Service Edges in the Zscaler Cloud with an inside–out tunnel.

ZPA Service Edges
Service Edges enforce security and access policies, stitching together the inside–out connection between an authorized user (via Client Connector and Browser Access) and a specific private application (via App Connector). Most customers use our Public Service Edges, which are hosted in more than 160 points of presence (PoPs) around the world and handle millions of concurrent users for the world's largest organizations. Private Service Edges, managed by Zscaler, are also available to be hosted on–site to provide on–premises users with the shortest path to on–premises applications without leaving the local network. It also ensures business continuity with uninterrupted access to mission–critical applications even during a black swan event.

ZPA Private Cloud Controller
Private Cloud Controllers are a per–tenant controller for users, ZPA Private Service Edges, and App Connectors to leverage when the Zscaler cloud is not available or reachable.

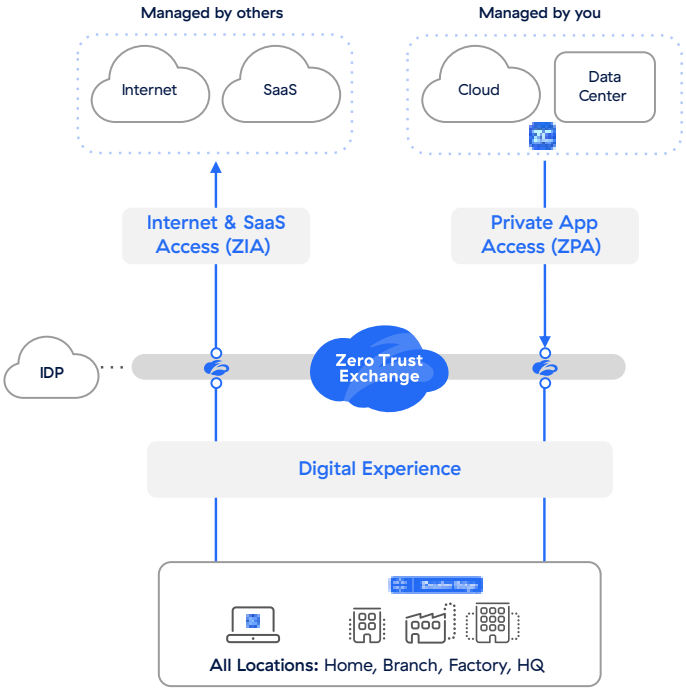
ZPA is part of the holistic Zero Trust Exchange

The Zscaler Zero Trust Exchange is a cloud native platform that powers a complete security service edge (SSE) to connect users, workloads, and devices without putting them on the corporate network. It reduces the security risks and complexity associated with perimeter–based security solutions that extend the network, expand the attack surface, increase the risk of lateral threat movement, and fail to prevent data loss.

©2025 Zscaler, Inc. All rights reserved.

Zscaler Secures the Workforce: Secure, Fast and Reliable App Access

Deployable in days to enhance cyber protection and user experience



Superior Threat & Data Protection, Great User Experience, Reduced Cost and Complexity

Technical Specifications

Zscaler Component	Supported Platforms & Systems	
Client Connector	iOS 17 or later Android 9 or later Windows 8 or later	ChromeOS version 137 or later Linux MacOS 14 or later
Clientless Access	Modern web browsers: (HTML 5–capable), Chrome, Edge, FireFox, Safari	
App Connector	AWS, GCP, Microsoft Azure, Nutanix, VMware, OpenShift, Docker, Red Hat	
Private Service Edge	AWS, GCP, Microsoft Azure, Nutanix, VMware, Docker, Red Hat	
Private Cloud Controller	AWS, Microsoft Azure, VMware, Red Hat	

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**.

© 2025 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at **zscaler.com/legal/trademarks** are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

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