DATA SHEET

Zscaler Private Access™

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

Zscaler redefines private application access with advanced connectivity, segmentation, and security capabilities to protect your business from threats while providing a great user experience.

Legacy networking and security approaches fail the needs of today's hybrid workforce

Connecting users to private apps shouldn't be slow, complicated, or risky. Hybrid work and cloud transformation have upended perimeter-based network security models, with private applications moving to the cloud, and users accessing applications over the public internet, on any device, from any location. Traditional approaches that rely on legacy VPNs and firewalls to control application access have become ineffective in the cloud and mobile-first world.

By 2025, at least 70% of new remote access deployments will be served predominantly by zero trust network access (ZTNA) as opposed to VPN services, up from less than 10% at the end of 2021, according to Gartner.

Benefits:

- **Boost hybrid workforce productivity**
  Get fast, seamless access to private apps whether you're at home, in the office, or anywhere
- **Mitigate the risk of a data breach**
  Minimize the attack surface and lateral movement by making applications invisible to the internet while enforcing least-privileged access
- **Stop the most advanced adversaries**
  First-of-its-kind private app protection and full inline traffic inspection minimize the risk of compromised users and active attackers
- **Extend zero trust across apps, workloads, and devices**
  The world's most complete ZTNA platform brings least-privileged access to private apps, workloads, and OT/IIoT devices
- **Reduce operational complexity**
  Our cloud native platform eliminates legacy remote access solutions like VPNs that are difficult to scale, manage, and configure

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 and first-generation ZTNA offerings

It's time to rethink how we securely and seamlessly connect users to the applications they need and redefine private application security with a new generation of ZTNA.

Zscaler Private Access™ (ZPA)

ZPA is the world's most deployed ZTNA platform, applying the principle of least privilege to give users secure, direct connectivity to private applications running on-premises or in the public cloud while eliminating unauthorized access and lateral movement. As a 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:

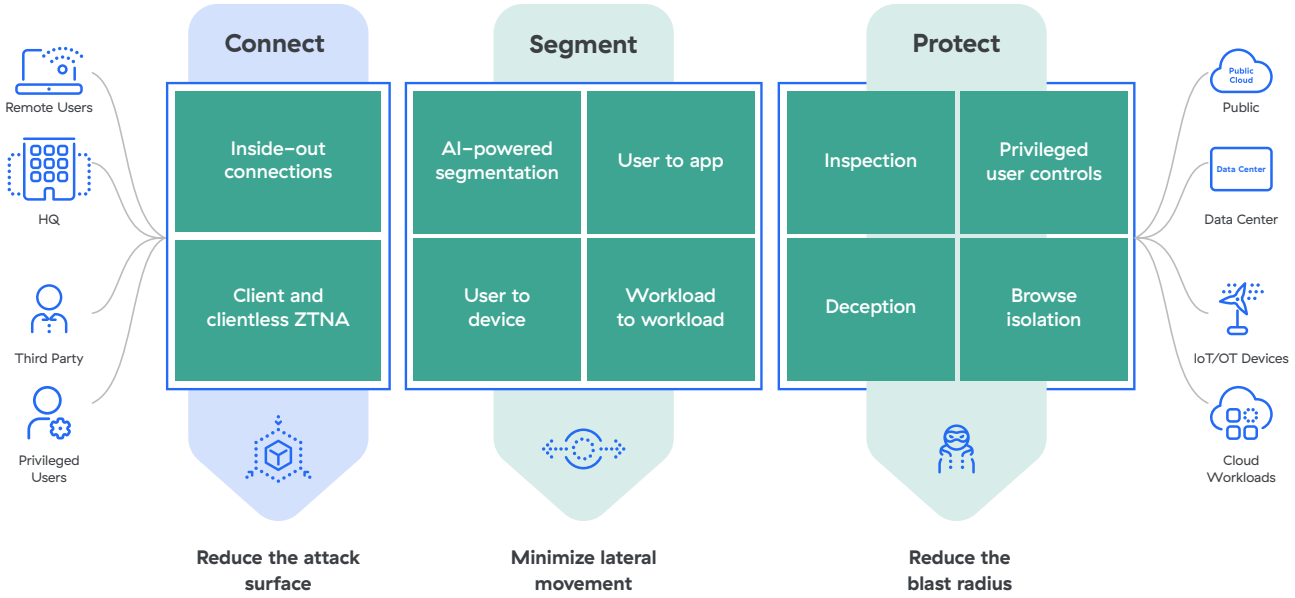
- **Deliver a superior user experience:** Connecting users directly to private apps eliminates slow, costly backhauling over legacy VPNs while continuously monitoring and proactively resolving user experience issues
- **Minimize the attack surface:** Applications are made invisible to the internet preventing 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—and 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
- **Detect compromised users and devices:** Integrated decoys work to quickly identify and remove malicious users and devices

By 2025, at least 70% of new remote access deployments will be served predominantly by ZTNA as opposed to VPN services, up from less than 10% at the end of 2021.*

— Gartner

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

How ZPA Addresses Emerging Use Cases for ZTNA



Key Use Cases

VPN alternative

VPNs were not designed with security, scalability, or user experience in mind. Traditionally, VPNs backhaul all remote user traffic to data centers that could be thousands of miles away, resulting in latency and user frustration. Once connected, VPNs tunnel users past the firewall and place them on the same network as your applications, which allows for free lateral movement.

ZPA overcomes these challenges by providing fast, direct access to applications via more than 150 globally distributed points of presence (PoPs) without the security risks inherent to VPN. Its inside-out connectivity ensures app access is decoupled from network access while eliminating internet-facing footprint. ZPA connects users to applications, not networks, and users can only access named apps, with no ability to move laterally. 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.

Secure hybrid workforce

In the modern workforce, users work from their homes and other remote locations, branch offices, and headquarters, challenging legacy security paradigms. ZPA enables seamless and secure access to private apps from wherever they need to work, on any device. On-campus users benefit from an identical experience through ZPA Private Service Edge.

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. ZPA is now able to provide Universal ZTNA capabilities for a fast and

consistent user experience. Moreover, with digital experience monitoring, you gain real-time visibility into performance degradation and outages, enabling productive hybrid work. As part of the Zscaler Zero Trust Exchange™, users benefit from an integrated SSE platform for safe, fast, and direct access to the internet, SaaS, workloads, devices, and private apps.

Third-party access/VDI alternative
In the past, third-party access relied on clunky, costly virtual desktop infrastructure (VDI) or other remote desktop clients, such as RDP, SSH, or VNC, which put users directly on your network and exposed internal systems to untrusted devices. ZPA's Clientless Access capabilities make third-party access as effortless as accessing the web while reducing costs and minimizing risks. Your vendors, contractors, and partners can freely 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 never outside your control and is protected from unauthorized copy/paste, printing, and upload/download. With Clientless Access, IT can deliver a better and more secure experience for users without incurring the costs of managing legacy VDI.

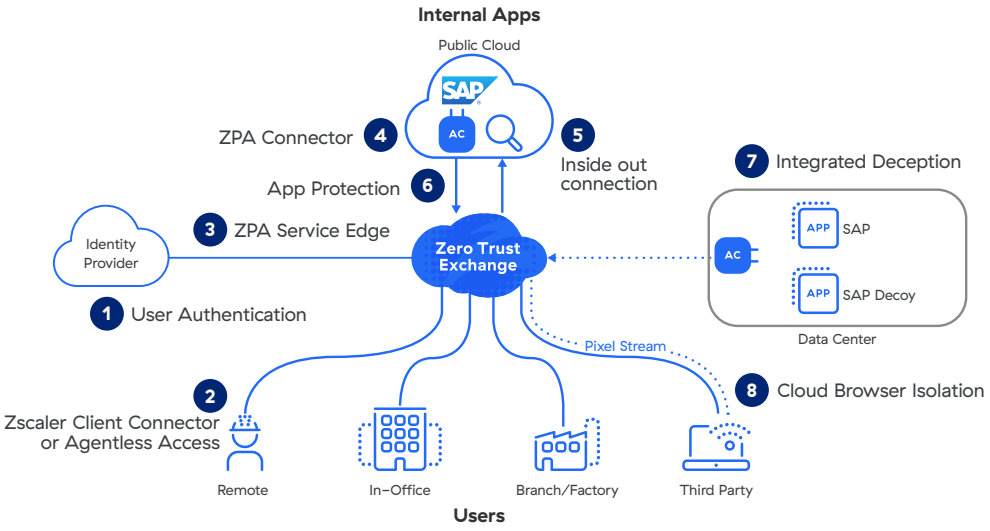
M&As and divestitures
M&A and divestitures often require combining networks, which can be challenging due to overlapping IP space and creating firewalls between the two entities. ZPA dramatically accelerates integration and time to value post-M&A, speeding the process to a matter of weeks instead of months. It provides seamless access to private apps—without the need for VPN—and eliminates the need to converge multiple networks or purchase additional networking equipment, freeing up resources to focus on high-impact work.

Secure operator access for OT and IIoT
Employees and third-party vendors need to access OT and IIoT 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 and IIoT environments from field locations, the factory floor, or anywhere else. ZPA for IoT & OT 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.

Secure workload-to-workload connectivity
Modern organizations require fast, secure workload-to-workload connectivity across private, hybrid, and multicloud environments. ZPA for Workloads reduces operational complexity and cost while enacting zero trust-based connectivity for workloads across all these environments. Because workloads are hidden behind ZPA, they are invisible to the internet and impossible to attack.

Zero Trust Branch Connectivity
Zero Trust Branch Connectivity securely connects branches, factories, and data centers without the complexity of VPNs, ensuring zero trust access between users, IoT/OT devices, and applications based on business policies. It eliminates the attack surface and prevents lateral threat movement by connecting users and IoT/OT devices to applications through the Zero Trust Exchange. Zero Trust Branch Connectivity dramatically simplifies branch communications by eliminating complex routing, VPNs, and firewalls while allowing for flexible forwarding and simple policy management with the proven ZIA and ZPA policy framework.

ZPA extends least-privileged access across the entire enterprise



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. The user is authenticating with IdP using their existing SAML SSO credentials.
2. The user's device posture is verified with Zscaler Client Connector, a lightweight forwarding agent installed on the user's laptop or mobile device. ZPA can also ingest device posture via third-party integration with all major EPP/EDR/XDR providers (e.g. CrowdStrike, Microsoft Defender, SentinelOne).
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. Next, the ZPA Service Edge determines the application in closest proximity to the user and establishes a secure connection to a ZPA App Connector, a lightweight virtual machine installed in the environment that hosts servers and applications.
5. Two outbound tunnels, one from the Client Connector on the device and the other from the App Connector, are stitched together by the ZPA Service Edge.
6. 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.
7. Integrated Zscaler Deception detects compromised users accessing decoy apps and can shut down access to internal resources across the Zero Trust Exchange.
8. Additionally, third-party users can connect to private applications with integrated browser-based access or Zscaler Browser Isolation for clientless access on unmanaged devices.

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). In either case, the service edge is managed by Zscaler without requiring any appliances.

Core Capabilities

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.
Unified client 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 unmanaged users with frictionless app access from any device and web browser.
Browser Access	Allow BYOD and third-party users to freely use their own devices to seamlessly and securely access internal apps leveraging any web browser, no client needed.
On-campus ZTNA	Experience ZTNA for on-campus users, securely connecting users to applications in your offices. Universal ZTNA ensures consistent access and policies for users irrespective of the location of the users and the applications.
Disaster Recovery	Ensure uninterrupted access to mission-critical applications even during a black swan event with a customer-controlled business continuity solution, creating the access path to critical private applications through ZPA Private Service Edge.
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.
AI-powered app segmentation	Apply ML-based segmentation recommendations automatically delivered to you in ZPA, making it fast and easy to identify the right application segments and build the right access policies. Powered by ML models continually trained on millions of customer signals and your unique application access patterns, ML-based segmentation can help you minimize your internal 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.
User-to-device segmentation	Ensure all access to OT/IIoT equipment and systems is granted on a least-privileged basis with user-to-device segmentation. Enable third-party vendors and remote users to connect to equipment from any location with ZPA for IoT and OT.
Workload-to-workload segmentation	Secure workload-to-workload connectivity and communication across hybrid and multicloud environments with ZPA for Workloads.
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.
Integrated deception	Detect and stop the most sophisticated attackers and insider threats with native app deception, including automated containment of compromised users across the Zero Trust Exchange.
Integrated Cloud Browser Isolation	Provide air-gapped, clientless access to critical web applications for contractors and employees using BYOD. Ensure unmanaged endpoints with vulnerabilities or malware infections do not compromise your network or applications. Enforce data exfiltration controls (copy/paste, printing, upload/download) to prevent sensitive data loss.
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.
Threat and data protection	Reduce the risk of threats with full content inspection. Find and control sensitive data across the user-to-app connection.
Zero Trust SD-WAN	Securely connect branches, factories, and data centers without the complexity of VPNs, ensuring zero trust access between users, IoT/OT devices and applications based on business policies.

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.

Minimize 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. ZPA's integrated deception capabilities let security teams immediately detect and isolate a malicious user or compromised device attempting to move laterally across the organization.

Prevent compromised users, insider threats, and advanced attackers
First-of-its-kind private app protection, with integrated inline inspection, deception, and data loss prevention 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. Integrated deception technology that utilizes decoy apps enables security teams to contain active in-network threats by cutting off compromised users from accessing resources.

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, workloads, and OT/IIoT devices to simplify and integrate multiple disjointed remote access tools, unifying security and access policies to stop breaches and reduce operational complexity.

Zscaler Private Access Editions

	Capabilities	Essentials	Business	Transformation	Unlimited
Platform Services	Secure access to private applications in the cloud and/or data centers along with real-time visibility	Std Device Posture enforcement, Log Streaming, Source IP Anchoring, Multiple IdP, Health Monitoring	(+) Extended DC Access	(+) Test Environment, Double encryption with Customer PKI	
Segmentation	**App Segments** AI generated recommendations for granular user-to-application segments based on access type, user privileges and app traffic	10	500	Unlimited	Unlimited
	App Connectors Lightweight VMs that securely connects a customer's servers to the Zscaler Zero Trust Exchange	20 pairs	50 pairs	Unlimited	Unlimited
	Private Service Edge Service edges deployed locally in customer environment for Universal ZTNA and business continuity	1 pair (Virtual)	1 pair / 5,000 users	1 pair / 2,000 users	1 pair / 1,000 users
Compromised User Protection	**Integrated deception** Integrated decoys to detect compromised users, stop lateral movement	Add-on	Standard[1]	Advanced	Advanced Plus
	AppProtection Prevent inline exploits of known vulnerabilities like log4j for private application traffic	Add-on	Add-on	✓	✓
Secure Clientless Access (3rd party users)	**Browser-based access** Browser Access for BYOD and unmanaged endpoints	Add-on	✓	✓	✓
	Privileged Remote Access Secure privileged remote access to OT systems (RDP/SSH/VNC) without a client	Add-on	PRA Essentials[2]	PRA Advanced[2]	PRA Advanced[2]
	Isolation data protection for Private Apps Prevent data loss to BYOD/ unmanaged devices accessing private apps	Add-on	Add-on	Isolation for Data Protection: Standard (100MB/user/mo.)	Isolation for Data Protection: Advanced Plus (1.5GB/user/mo.)
Protect Data	**Pvt apps, Classification, Incident Management** Data loss prevention for private apps, advanced incident response and data classification	Add-on	Add-on	Add-on	✓
Digital experience monitoring	Visibility into user, connectivity and application telemetry to help resolve user experience issues	–	Standard	Standard	Standard
Premium Support Plus	TAM support + 15min P1 response	Add-on	Add-on	Add-on	✓
	1. Min 1000 licenses of ZPA required 2. Up to 10 systems/consoles				

Key differentiators

As the industry's only next-generation ZTNA platform, Zscaler Private Access 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
- **Integrated deception:** Stop lateral movement attempts and the spread of ransomware with the only ZTNA solution with native app deception
- **Clientless access:** Leverage browser-based access for third parties with integrated DLP
- **Improved productivity:** Maintain complete visibility into access for private apps to detect user issues that impact user experience
- **Global edge presence:** Gain unmatched security and user experience with 150+ 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, 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.

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 Branch Connector
Branch Connector, available in physical and virtual appliance form factors, improves application performance by eliminating backhaul and forwarding all branch and data center traffic directly to the closest Zscaler edge location, minimizing latency. It allows for bidirectional communication between users, servers, and IoT/OT devices—where Client Connector cannot be installed—and applications, over any network via the Zero Trust Exchange.

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.

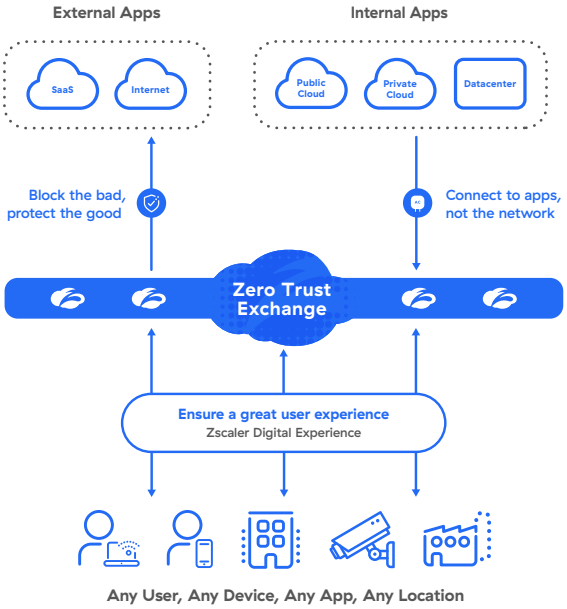
ZPA Service Edges
Service Edges enforce security and access policies, stitching together the inside-out connection between an authorized user (via Client Connector and Browser Access) and a specific private application (via App Connector). Most customers use our Public Service Edges, which are hosted in more than 150 exchanges 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.

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.

How Zscaler delivers zero trust for users, workloads, and IIoT/OT

Deploy in weeks to enhance cyber protection and user experience



Technical Specifications

Zscaler Component	Supported Platforms & Systems	
Client Connector	iOS 9 or later Android 5 or later Windows 7 or later	macOSX 10.10 or later CentOS 8 Ubuntu 20.04
Branch Connector	Centos, Redhat	VMware vCenter or vSphere Hypervisor
Clientless Access	Modern web browsers: (HTML 5–capable)	Chrome Edge FireFox
App Connector	AWS CentOS, Oracle, and Red Hat Microsoft Azure	Microsoft Hyper–V VMware vCenter or vSphere Hypervisor Docker host

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