Data Sheet

Zscaler Private Access™

Empower your hybrid workforce with fast, secure, and reliable access to private apps with the industry's 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**
  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 attackers while enforcing least-privileged access
- **Stop the most advanced adversaries**
  First-of-its-kind private app protection minimizes 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**
  Cloud-native platform eliminates legacy VPNs that are difficult to scale, manage, and configure.

Legacy network security approaches can be easily circumvented by attackers taking advantage of 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, and private apps create a massive attack surface:** Attackers can see and exploit vulnerable, externally exposed resources
- **Lack of least-privileged access 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. It's time to redefine private application security with a new generation of zero trust network access.

Zscaler Private Access

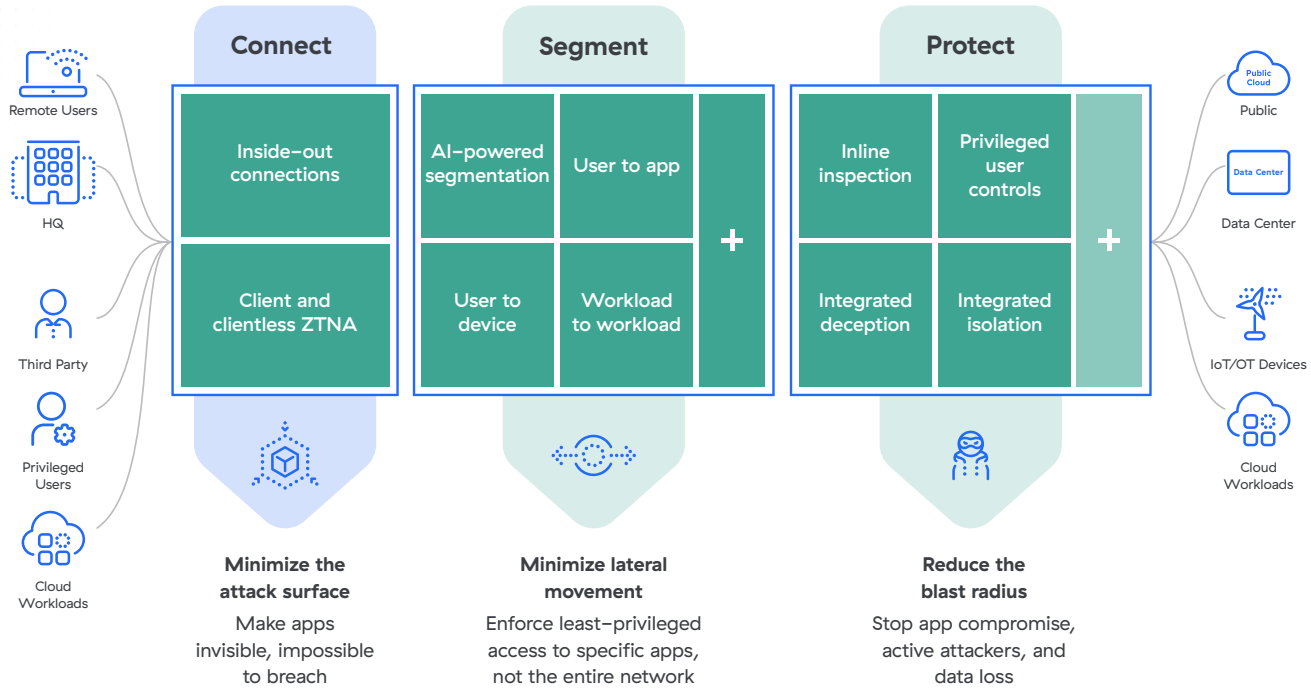
ZPA is the world's most deployed ZTNA platform, applying the principles of least privilege to give users secure, direct connectivity to private applications running on-prem or in the public cloud while eliminating unauthorized access and lateral movement. As a cloud-native service built on a holistic 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 lateral movement:** Applications are made invisible to the internet and unauthorized users, and IPs are never exposed using inside-out connections
- **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
- **Stop attacks with complete inspection:** Private app traffic is inspected in-line to prevent the most prevalent web attack techniques

By 2025, at least 70% of new remote access deployments will be served predominantly by zero trust network access (ZTNA).

— Gartner

Next-generation 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 and secure remote access without the backhaul latency or security risks inherent to VPN. Its inside-out connectivity ensures app access is decoupled from network access and only authorized users can access named apps, meaning no lateral movement. ZPA's cloud-native, multi-tenant design means IT teams can eliminate inbound gateway appliances (VPN concentrators, load balancers, DDOS, etc), and reduce network costs and complexity.

Secure hybrid workforce

Users require the ability to move fluidly between their homes, remote locations, branch offices, and headquarters. 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 the ZPA Private Service Edge, an on-prem broker, which replicates all of the policies and controls of the cloud. 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 was achieved through clunky and costly virtual desktops or other remote desktop clients, such as RDP, SSH or VNC, that 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 ensures third-party users and unmanaged devices are isolated from your network and applications, ensuring sensitive data is never outside your control and is protected from unauthorized clipboard, printing, upload/downloads. With Clientless Access, IT can deliver a better and more secure experience for users without incurring the costs of managing legacy virtual desktop infrastructure (VDI).

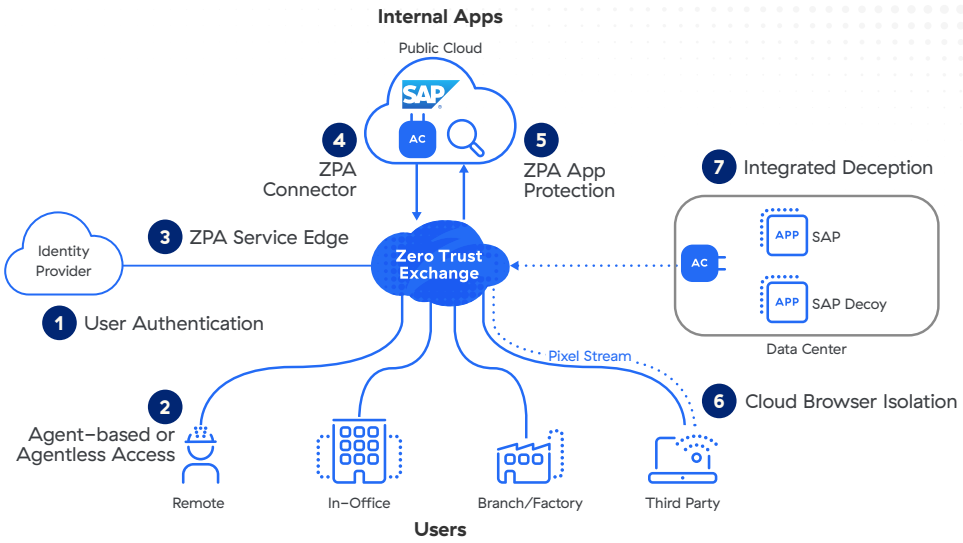
VDI alternative
Traditional VDIs are often slow, unresponsive, and introduce significant costs with racks of servers needed in the data center to support remote access needs. ZPA provides secure, direct connectivity to apps over RDP and SSH, enabling a faster, more secure experience for users. With built-in agentless access through the browser or Cloud Browser Isolation, employees and third-party users get seamless connectivity from any device without complicated desktop provisioning processes.

M&As and divestitures
Successful M&As and divestitures require that critical business apps be available and that newly acquired employees are productive on day one. ZPA simplifies IT integration during M&As and divestitures, 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 and purchase additional networking equipment (e.g., firewalls, routers, switches), freeing up resources to focus on high-impact work.

Secure operator access for OT and IIoT
OT and IIoT assets regularly need to be accessed by employees and third-party vendors to maximize production uptime and 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, for that matter. ZPA for IoT & OT provides fully isolated, clientless remote desktop access to internal RDP and SSH target systems—— without having 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 hybrid and multi-cloud environments. ZPA for Workloads reduces operational complexity and cost by eliminating the need for virtual DMZs and VPN meshes with least-privileged access-based connectivity across clouds. In addition, because workloads are hidden behind ZPA, they are invisible to the internet and impossible to attack.

Zero Trust SD-WAN connectivity
Traditional branch and data center connectivity relies on legacy WANs, mesh VPNs, and firewalls to control access, which create a broad attack surface, extensive privileges, and routing complexity. Zscaler Zero Trust SD-WAN replaces traditional approaches with a zero trust connectivity solution – for users, servers, and IoT/OT devices – and provides sites with fast, secure access to the internet and private applications. It simplifies branch communications by establishing direct branch-to-private app connections while allowing for flexible forwarding and policy management in ZPA.



How it works

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

1. Authenticating the user with IDP using their existing SAML SSO credentials.
2. Verifying a user's device posture with the 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, and 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, the 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 Deception detects compromised users accessing decoy apps and can shut down access to internal resources across the Zscaler Zero Trust Exchange.
8. Additionally, third-party users can connect to private applications with integrated browser-based access or Cloud 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 can run on-premises within the customer's infrastructure (ZPA Private Service Edge). In either case, they are 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 they are off the corporate network through a lightweight agent, the Zscaler Client Connector. Clientless access provides unmanaged users with frictionless app access from any device and web browser, no client needed.
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	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, as well as your 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 machine learning 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 (clipboard, printing, upload/download) to prevent sensitive data loss.
Privileged Remote Access	Allow privileged admins 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	Replaces traditional WAN connectivity solutions like firewalls and VPNs in branches and data centers that expose routable networks with a zero trust connectivity solution for users, servers and IoT/OT devices.

Benefits

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

Minimize lateral movement
Connectivity is based on least-privileged access, ensuring that 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 made 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. With integrated deception, security teams can detect and stop the most sophisticated adversaries 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 threat isolation capabilities minimizes the risk of compromised users and active attackers by:

- Automatically stopping web attacks with complete coverage for the most prevalent web attack techniques, including the OWASP Top 10, and full custom signature support for immediate virtual patching against zero-day vulnerabilities
- Minimize third-party and BYOD risks with fully isolated access to applications that keeps sensitive data off unmanaged devices using integrated Cloud Browser Isolation
- Utilizing decoy apps created by integrated deception and enabling security teams to contain active in-network threats by cutting off compromised users from accessing resources

Deliver an exceptional user experience
By providing consistently fast connectivity that doesn't require logging in and out of VPN clients, remote users gain a faster, more secure 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 login credentials such as Azure AD, Okta, Ping, etc. Additionally, admins 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

	ZPA Essentials Edition	ZPA Business Edition	ZPA Transformation Edition	ZPA Unlimited Edition
Platform services	Source IP Anchoring, Multiple IdP, LSS	(+) Extended DC Access	(+) Test Environment, Customer PKI	(+) Test Environment, Customer PKI
User-to-app segmentation	10 App Segments	300 App Segments	Unlimited App Segments	Unlimited App Segments
App Connector	20 Pairs	50 Pairs	Unlimited Pairs	Unlimited Pairs
On-campus ZTNA[1]	—	1st Private Service Edge Pair included, add'l Pair for every 10,000 users	1st Private Service Edge Pair included, add'l Pair for every 5,000 users	1st Private Service Edge Pair included, add'l Pair for every 1,000 users
Clientless Access[2]	—	✓	✓	✓
Integrated digital experience monitoring	—	Standard	Standard	Standard
Integrated deception	—	Standard	Advanced	Advanced + Add'l Decoys
AppProtection	—	—	✓	✓
Integrated isolation	—	—	Standard	100%
Data protection (private apps)	—	—	—	✓
Premium support	—	—	—	✓

Key differentiators

As the industry's only next-gen 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:** Identify and stop the exploitation of private apps with automatic prevention of the most prevalent web attacks
- **Integrated deception:** Stop lateral movement attempts and the spread of ransomware with the only ZTNA solution with native app deception
- **Global edge presence:** Gain unmatched security and user experience with 150+ cloud edge locations worldwide. An optional local service edge extends zero trust to your HQ

[1]ZPA Business Edition supports up to 5 Private Service Edge Pairs; required to buy additional pairs after 50,000 users. ZPA Transformation Edition supports up to 10 Private Service Edge Pairs; required to buy additional pairs after 50,000 users. ZPA Unlimited Edition supports up to 50 Private Service Edge Pairs; required to buy additional pairs after 50,000 users.

[2]Clientless Access includes Browser Access and Privileged Remote Access (for up to 10 systems).

- **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 security service edge (SSE) framework

Foundational components

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

Zscaler Branch Connector
Branch Connector is a virtual machine that runs at a branch or data center and forwards traffic from all resources to the closest Zscaler Service Edge. It allows for bidirectional communication between users, servers and IoT/OT devices – where the Client Connector cannot be installed – and applications, over any network via the Zscaler Zero Trust Exchange.

Zscaler Clientless Access
Users can securely connect to private apps, workloads, and IIoT/OT devices via integrated browser-based access (web, RDP, SSH, VNC) or Cloud 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.

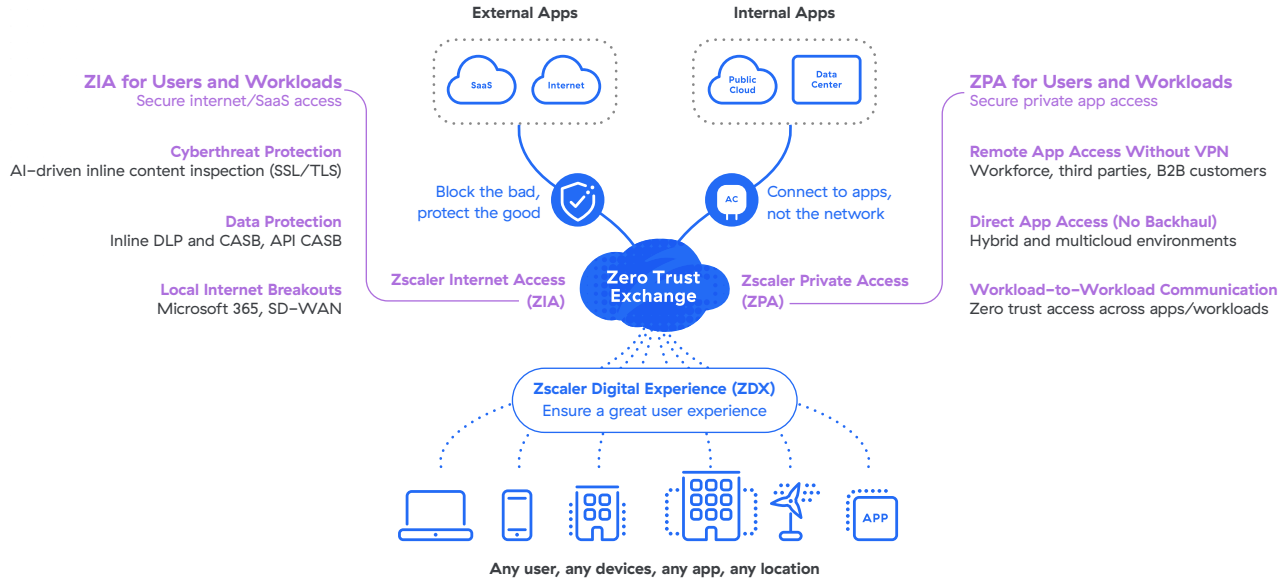
ZPA Service Edges
Service Edges enforce security and access policies, stitching together the inside-out connection between an authorized user (via Client Connector and Browser Access) and a specific private application (via the App Connector). Most customers leverage our Public Service Edges, which are hosted in over 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 at the customer site for providing on-prem users with the shortest-path access to on-prem 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 Redhat Microsoft Azure	Microsoft Hyper-V VMware vCenter or vSphere Hypervisor

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