Zscaler Private Access™

Fast, direct, secure private app access for all users, devices, and locations

Zscaler Private Access (ZPA) redefines private app connectivity and security for today’s hybrid workforce with the industry’s only next-generation zero trust network access (ZTNA) platform.

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 eliminate 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 IoT**
  The world’s most complete ZTNA platform brings least-privileged access to private apps, workloads, and OT/IoT devices

- **Reduce operational complexity**
  Cloud-native platform eliminates legacy VPNs that are difficult to scale, manage, and configure in a cloud-first world
Legacy network security approaches can be easily circumvented by attackers 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, and private apps are 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 the attack surface:** 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.

• **Eliminate lateral movement:** Applications are segmented so that users can only access a specific app, which helps limit lateral movement.

• **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
Key Use Cases

VPN alternative
Legacy VPNs fail to deliver the security, visibility, and user experience today’s distributed workforce requires. ZPA delivers fast, direct access to private apps by eliminating VPN traffic backhauling that creates latency, resulting in lost productivity. Without the need for a VPN client requiring constant authentication, remote access becomes effortless. Least-privileged access is enforced as users are no longer tunneled past firewalls directly onto the network. With ZPA, IT teams can eliminate the full VPN gateway appliance stack or duplicate inbound security (firewalls, load balancers, DDoS detection, etc.) infrastructure.

Secure a hybrid workforce through an integrated SSE platform
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. Local users benefit from an identical experience through an on-prem broker that replicates all of the policies and controls of the cloud. 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 internet, SaaS, workloads, devices, and private apps.
Third-party agentless access
Third-party partners, contractors, and vendors require secure, direct access to business applications and OT systems from unmanaged devices. ZPA provides secure, direct connectivity from authorized users to named applications without putting third parties on the network. With integrated agentless access, users can access applications from any browser, on any device, without the need to install a client or log into a VPN.

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, providing 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 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 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 multicloud environments. ZPA for Workloads reduces operational complexity and cost by eliminating the need for virtual DMZs and VPN meshes, instead providing least-privileged access connectivity across clouds. In addition, because workloads are hidden behind ZPA, they are invisible to the internet and impossible to attack.
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 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 Zscaler 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 agentless access on unmanaged devices.
A ZPA Service Edge can either be hosted by Zscaler in the cloud (ZPA Public Service Edge) or can be 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**

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk-based policy engine</td>
<td>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.</td>
</tr>
<tr>
<td>Agentless and agent-based access</td>
<td>Securely connect users to private applications through an agent, Zscaler Client Connector, or without the need for an agent for unmanaged devices via native browser-based access or Cloud Browser Isolation.</td>
</tr>
<tr>
<td>User-to-app segmentation</td>
<td>Connect users directly to private apps through a micro-tunnel created between the app and user, providing a zero trust segment of one between, without ever placing the user on the network to eliminate lateral movement.</td>
</tr>
<tr>
<td>User-to-device segmentation</td>
<td>Connect remote employees to IIoT/OT devices on the factory floor for maintenance and troubleshooting using least-privileged access, and not placing the user on the network with ZPA for IoT.</td>
</tr>
<tr>
<td>Workload-to-workload segmentation</td>
<td>Secure workload-to-workload connectivity and communication across hybrid and multicloud environments with ZPA for Workloads.</td>
</tr>
<tr>
<td>App discovery</td>
<td>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.</td>
</tr>
<tr>
<td>AppProtection</td>
<td>Stop compromised users and insider threats with automatic protection against the most prevalent Layer 7 web attacks with complete coverage of the OWASP Top 10 attack techniques and full custom signatures support to virtually patch zero-day vulnerabilities. Inline inspection of all private app traffic provides real-time visibility into suspicious user and application behavior.</td>
</tr>
<tr>
<td>Integrated deception</td>
<td>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.</td>
</tr>
<tr>
<td>Privileged Remote Access</td>
<td>Securely connect internal and third-party admin users to RDP and SSH target systems via client-less sessions from users’ web browsers. This eliminates the need to install a client on unmanaged devices or connect through VPN or VDI.</td>
</tr>
<tr>
<td>Cloud Browser Isolation</td>
<td>Provide a safe air gap between users and private applications with integrated Cloud Browser Isolation technology to enable safe access for unmanaged devices, including BYOD and third-party users, to prevent cyberattacks and data loss attempts.</td>
</tr>
</tbody>
</table>
Benefits

Minimize the attack surface
By eliminating vulnerable VPNs and making apps invisible to the internet, ZPA makes it 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 rogue applications, services, and workloads using application discovery, further reducing the attack surface.

Eliminate 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.
• Minimizing third-party and BYOD risks with fully isolated access to applications that keeps sensitive data off unmanaged devices with integrated Browser Access and 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 OT 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.
### ZPA for Users Editions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User-to-app segmentation (ZTNA)</td>
<td>10 app segments</td>
<td>300 app segments</td>
<td>Unlimited app segments</td>
</tr>
<tr>
<td>App connectors</td>
<td>Pair/1,000 users (max: 10)</td>
<td>Pair/500 users</td>
<td>Pair/300 users</td>
</tr>
<tr>
<td>Agentless access for third-party users &amp; BYOD</td>
<td>—</td>
<td>Browser-based access</td>
<td>Browser-based access &amp; cloud browser isolation</td>
</tr>
<tr>
<td>Local ZTNA</td>
<td>—</td>
<td>1 pair Private Service Edge</td>
<td>1 pair Private Service Edge</td>
</tr>
<tr>
<td>Log streaming</td>
<td>—</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>App protection</td>
<td>—</td>
<td>Add on</td>
<td>Advanced</td>
</tr>
<tr>
<td>Integrated deception</td>
<td>—</td>
<td>Standard</td>
<td></td>
</tr>
<tr>
<td>Privileged remote access</td>
<td>—</td>
<td>Add on</td>
<td></td>
</tr>
<tr>
<td>ZPA for workloads (1 workload per 100 users)</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Digital experience monitoring (3 apps)</td>
<td>—</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Platform services</td>
<td>—</td>
<td>Source IP anchoring Bandwidth premium</td>
<td>Source IP anchoring, multiple IdP, bandwidth premium, test environment, PKI</td>
</tr>
</tbody>
</table>

Licensing model: Zscaler Private Access Editions are priced per user. For certain products inside of a ZPA Edition, pricing may vary outside of user count, including ZPA for Workloads (Priced per workload/server, with one workload per 100 users provided as part of Transformation Edition). For more information on pricing, speak with your Zscaler account team.

### 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.
• **Unified agentless and agent-based access:** Enforce least-privileged access across BYOD and corporate-owned devices with agentless and agent-based options.

• **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 OT/IoT access:** 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 and 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 Agentless Access**
Users can securely connect to apps, workloads, and OT devices via integrated browser-based access (web, RDP, or SSH) or Cloud Browser Isolation for agentless 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 agentless 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.

---

**Gartner**
Zscaler named a Leader in Gartner’s SSE MQ, positioned highest in Ability to Execute. Learn More →
ZPA is part of the holistic Zero Trust Exchange

The Zscaler Zero Trust Exchange enables fast, secure connections and allows your employees to work from anywhere using the internet as the corporate network. Based on the zero trust principle of least-privileged access, it provides comprehensive security using context-based identity and policy enforcement.

How Zscaler delivers zero trust for users, workload, and OT

Deploy in weeks to enhance cyber protection and user experience

ZIA for Users and Workloads
Secure Internet/SaaS Access
Cyber Threat Protection
AI driven inline content inspection 95SL/TLS
Data Protection
Inline DLP and CASB, API CASB
Local Internet Breakouts
Microsoft 365, SD-WAN

ZPA for Users and Workloads
Secure Private App Access
Remote App Access without VPN
Workforce, third parties, B2B Customers
Direct App Access (no backhaul)
Hybrid and multi-cloud environments
Workload to workload Communication
Zero Trust access among apps/workloads

Technical Specifications

<table>
<thead>
<tr>
<th>Zscaler Component</th>
<th>Supported Platforms &amp; Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Connector</strong></td>
<td><strong>Supported Platforms &amp; Systems</strong></td>
</tr>
<tr>
<td>iOS 9 or later</td>
<td>macOSX 10.10 or later</td>
</tr>
<tr>
<td>Android 5 or later</td>
<td>CentOS 8</td>
</tr>
<tr>
<td>Windows 7 or later</td>
<td>Ubuntu 20.04</td>
</tr>
<tr>
<td><strong>App Connector</strong></td>
<td><strong>Supported Platforms &amp; Systems</strong></td>
</tr>
<tr>
<td>AWS</td>
<td>Microsoft Hyper-V</td>
</tr>
<tr>
<td>Centos, Oracle, and Red hat</td>
<td>VMware vCenter or vSphere Hypervisor</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td></td>
</tr>
</tbody>
</table>

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 SASE-based Zero Trust Exchange is the world’s largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.