DATA SHEET

Zscaler Private Access™

Fast, secure access to private applications with cloud-delivered zero trust network access (ZTNA)

Businesses are moving private apps that once ran solely in the data center to public clouds. At the same time, they are searching for ways to enable productivity as users work from anywhere and on any device. The key to success begins with finding the right balance of security and user experience.

Today, the security perimeter extends beyond the corporate network to anywhere users connect and wherever applications run. Traditional network security architectures have become less relevant for modern workflows, as they are anchored in the data center and rely on appliances. These architectures were not built for the cloud and mobile world and were never designed to scale like a cloud service.

Network-based architectures are also vulnerable as a result of excessive trust. Remote users connecting from an approved list of IP addresses (via VPN) are assumed to be trusted and are granted access to the network through a firewall, which is often exposed to the internet. On-premises users on the network can move laterally across it. Ultimately, this inherent trust leads to risk and overprivileged network access.

The security paradigm needs to shift from a static network perimeter and, instead, focus on the entity, resource, and user device. This shift in focus is why Gartner recommends that organizations adopt a zero trust network access service (ZTNA) to secure access to private applications.

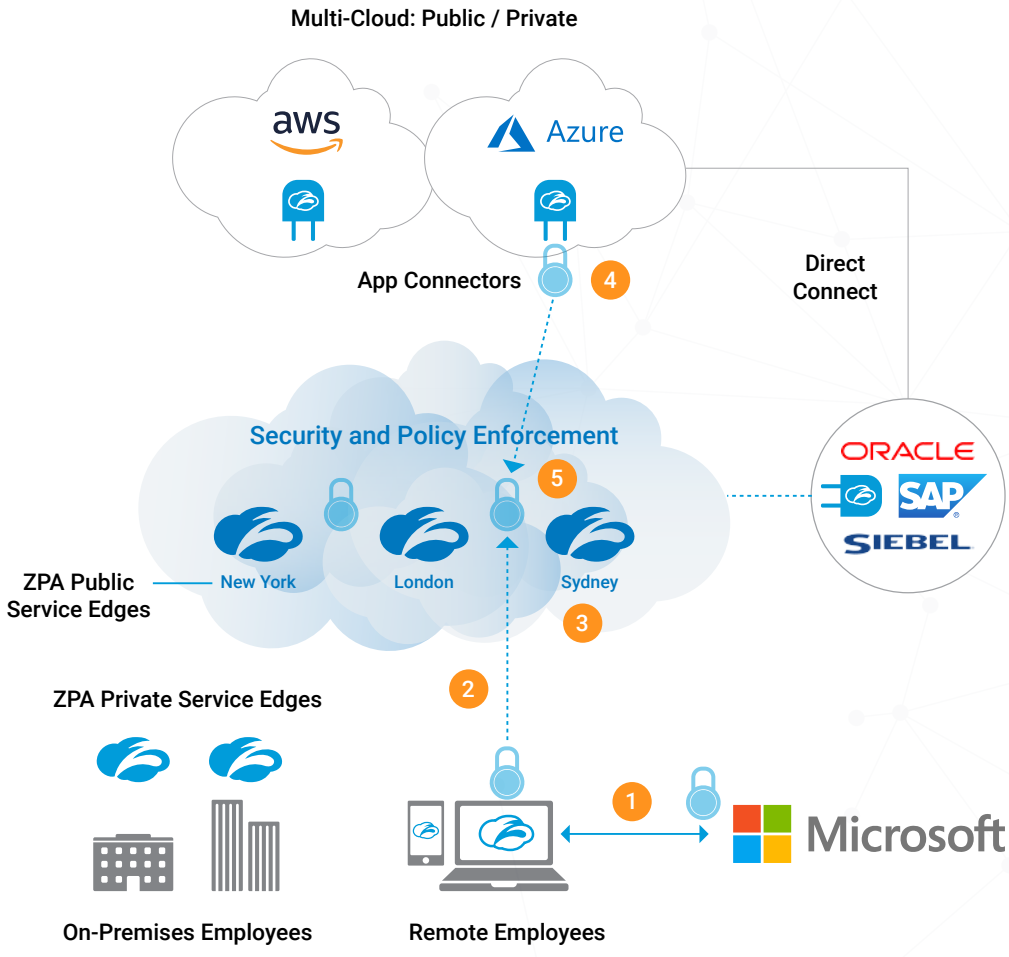
Zscaler Private Access:
Redefine private application access with zero trust network access

Zscaler Private Access (ZPA™) is a cloud service that uses a distributed architecture to provide fast and secure access to private applications running on-prem or in the public cloud. The service provides access based on four key principles:

- Application access should be based on context and should not require network access
- Inside-out connections should be used to make applications invisible to unauthorized users
- Application segmentation should connect users to a specific app and limit lateral movement
- The internet must become the enterprise's new transport network

When a user (employee, third-party contractor, or customer) attempts to access an application, the user's identity and device posture are verified using Zscaler™ Client Connector software (formerly Zscaler App) installed on the user device. Policy is checked, and a ZPA Service Edge determines where the closest application instance exists. ZPA uses the location of the client and determines the closest application to the user according to what a ZPA App Connector (lightweight VM) can see. Lastly, two outbound tunnels, one from the Client Connector on the device and the other from the App Connector, are stitched together by a ZPA Service Edge. All of this takes place automatically and in real time.

A ZPA Service Edge can either be hosted by Zscaler in the cloud (ZPA Public Service Edge) or can be run on-premises on the customer's infrastructure (ZPA Private Service Edge). In either case, they are managed by Zscaler and no appliances are required. Below is a look at the ZPA architecture:



How it works:

1. User authentication with IDP (first time only)
2. Authorized user attempts to access an app; Client Connector tunnel is created
3. The ZPA Service Edge enforces policy and sends dispatch to connectors
4. The App Connector closest to app sends inside-out tunnel to ZPA Service Edge
5. The ZPA Service Edge stitches together the connection between app and user

Empower the enterprise with ZPA

Deliver cloud-like user experiences

With ZPA, employees, contractors, and customers have a completely seamless experience because ZPA:

- Provides a consistent access experience whether users are remote or on-premises
- Integrates with popular identity providers (Azure AD, Okta, Ping, etc.) for single sign-on
- Uses browser access for BYOD or thirty-party users accessing web applications, so there's no need for an endpoint agent

Improve visibility into all user and application activity

ZPA provides the intelligence admins need to understand who is accessing applications, including:

- Discovering applications running in your public cloud and applying granular access controls
- Giving you the ability to view real-time user activity and the health of applications, servers, and connectors
- Automatically streaming user audit logs to your SIEM provider

Define granular policies based on specific user and application

ZPA delivers a central platform that gives IT control over application access by:

- Using policies hosted in the Zscaler cloud to determine which users can access apps
- Defining and managing policies for users, user groups, applications, and application groups
- Segmenting access by user and app as a more granular alternative to network segmentation

Ensure secure access to all public and private cloud environments

ZPA supports access to apps across the data center and public cloud (Azure, AWS, and GCP) environments by:

- Providing secure and consistent access regardless of where an app is running
- Removing the need for the VPN gateway security stack or backhauling traffic to the data center before going out to the cloud
- Accelerating app migration by deploying a ZPA App Connector in just five minutes

Accelerate M&As and divestitures

ZPA removes networking as a barrier to acquiring new IP or selling parts of the business, offering the following benefits:

- Reduces infrastructure setup times from eight months to two weeks
- Eliminates the need to purchase additional equipment (e.g., firewalls, routers, and, switches)
- Leverages a single security platform for all acquired or divested assets
- Supports multiple identity providers and delivers a seamless user experience across entities

	ZPA Professional Edition	ZPA Business Edition	ZPA Transformation Edition
Core			
• ZPA platform: Global coverage (150+ data centers), high availability and low latency • Authentication: SAML authentication and SCIM provisioning support • Secure private application access to all TCP and UDP- based apps • Zscaler Client Connector: Agents for Windows, MacOS, iOS, and Android • Enterprise darknet with DDoS protection • Applications and server discovery • Standard device posture enforcement	✓	✓	✓
Business capabilities			
• Browser Access (client-less secure access to browser-based apps)	✓	✓	✓
• ZPA user portal	✓		
• Log streaming service			
• Continuous health monitoring for all apps			
• Continuous App Connector monitoring			
Transformation capabilities			
• Multiple identity provider support			✓
• Double encryption with customer-provided PKI			
ZTNA components			
• Microsegmentation by application segment (user-to-app)	Up to 10	Up to 100	Unlimited
• ZPA App Connectors	Pair/1,000 users (max:10)	Pair/500 users (max: 100)	Pair/300 users (max: 300)
• ZPA Private Service Edge for on-premises ZTNA		Pair/10k users (max: 5)	Pair/5K users (max: 10)
• Server licenses for microsegmentation (server-to-server), requires Cloud Connector		1 server/500 seats	1 server/100 seats
• Microsegmentation for workload (app-to-app), requires Edgewise service			1 server/100 seats
• Zscaler B2B Pro platform – ZTNA for customers			1 TB/m/50k users (max: 4 TB)

About Zscaler

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multitenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at zscaler.com or follow us on Twitter @zscaler.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com