DATA SHEET

Zscaler Private Access™

Securing access to your private applications with our zero trust network access (ZTNA) service

Enterprises are in the midst of digital transformation. Private apps that once ran solely in the datacenter are moving to private cloud and users are now accessing those apps remotely from personal devices. IT must ensure security while delivering a seamless user experience.

This migration delivers benefits in scale, simplicity, productivity, and more, but it extends the security perimeter to the internet, which breaks the traditional DMZ approach. At the same time, the number of unmanaged user devices connecting to internal applications has continued to rise, forcing IT to find the right balance between the need for access to sensitive applications from unmanaged devices and the need to minimize risk.

To find that balance, IT has often looked to incumbent remote access technologies, finding that they generally fall short, meeting neither users' nor IT's needs.

The traditional DMZ is no longer effective in a cloud-first world

The traditional DMZ approach worked well for data center applications. It provided an additional layer of security for the internal LAN, allowing IT to expose only external facing services to the internet and place all other internal services behind a firewall. But with applications moving to cloud, the perimeter has been extended to the internet, which the DMZ was not built to secure. Moving the DMZ to the cloud—often referred to as the "virtual DMZ"—is recommended by some cloud service providers, but it's expensive, difficult to architect, and complex to implement. It starts with a traditional VPN gateway stack hosted in the data center, and requires architecting and implementing a virtual network (VNET) specific to each cloud provider (often involving NIC, additional network access variables, and more) and a VPN appliance to connect both the internal and virtual networks. The complexity of this method slows the adoption of public cloud, drives up appliance-related costs, and frustrates users attempting to access public cloud applications.

Zscaler Private Access: Redefine private application access with zero trust

Zscaler Private Access (ZPA™) is a cloud service that provides zero trust, secure remote access to internal applications running on cloud or data center. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity versus extending the network to them.

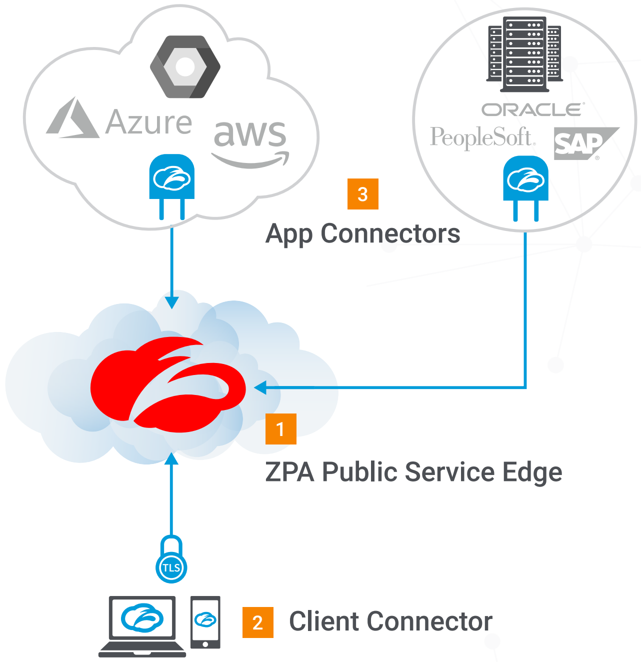
Zero trust access based off four key tenets:

- Application access no longer requires access to the network, or use of VPN.
- Inside-out connections ensure apps are invisible to unauthorized users.
- App segmentation, not network segmentation, connects users to a specific app and limit lateral movement.
- The internet becomes the new secure network via end-to-end encrypted TLS tunnels.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT admin within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, a piece of software called Zscaler Client Connector (formerly Zscaler App) is installed. Client Connector ensures the user's device posture and extends a secure micro-tunnel out to the Zscaler cloud when a user attempts to access an internal application.

Adjacent to an application running in a public cloud or data center, ZPA places a small piece of software called App Connector, deployed as a VM, which is used to extend a micro-tunnel out to the Zscaler cloud. The App Connector establishes an outbound connection to the cloud, and does not receive any inbound connection requests, thereby preventing DDoS attacks. Within the Zscaler cloud, a ZPA Public Service Edge approves access and stitches together the user-to-application connection. ZPA is 100 percent software defined, so it requires no appliances and allows users to benefit from the cloud and mobility while maintaining the security of their applications.

Below is a look at the architecture of the ZPA service.



Zero Trust Network Architecture

1 ZPA Public Service Edge

- Brokers a secure connection between a Client Connector and an App Connector
- Hosted in cloud
- Used for authentication
- Customizable by admins

2 Client Connector

- Mobile client installed on devices
- Requests access to an app

3 App Connector

- Sits in front of apps in Azure, AWS, and other public cloud services
- Listens for access requests to apps
- No inbound connections

Empowering the enterprise with ZPA

Deliver a cloud-like user experience

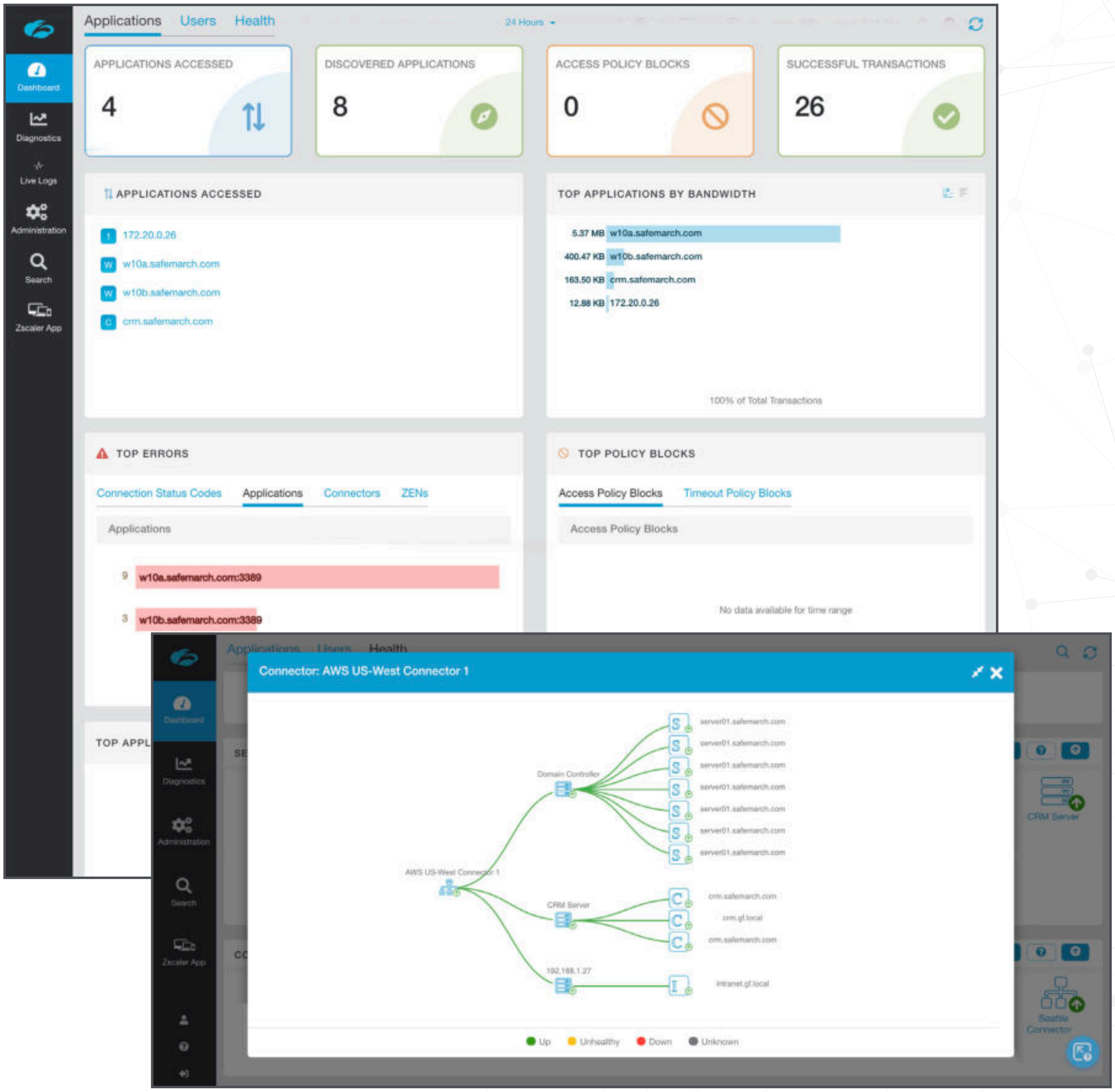
Users are playing a larger role in determining which technologies are deployed in the enterprise. With ZPA, users no longer have to think about which app they are accessing. It just works.

- Consistent user experience for both public cloud and data center applications
- The service integrates with Okta and other single sign-on providers for faster access
- Browser access is available for all web apps, allowing for connectivity without Client Connector
- Admins can customize re-authentication timeframes to ensure the best experience for remote users

Improve visibility into all user and application activity

ZPA provides the intelligence admins need to understand who is accessing applications and take action when necessary, all from within the admin UI.

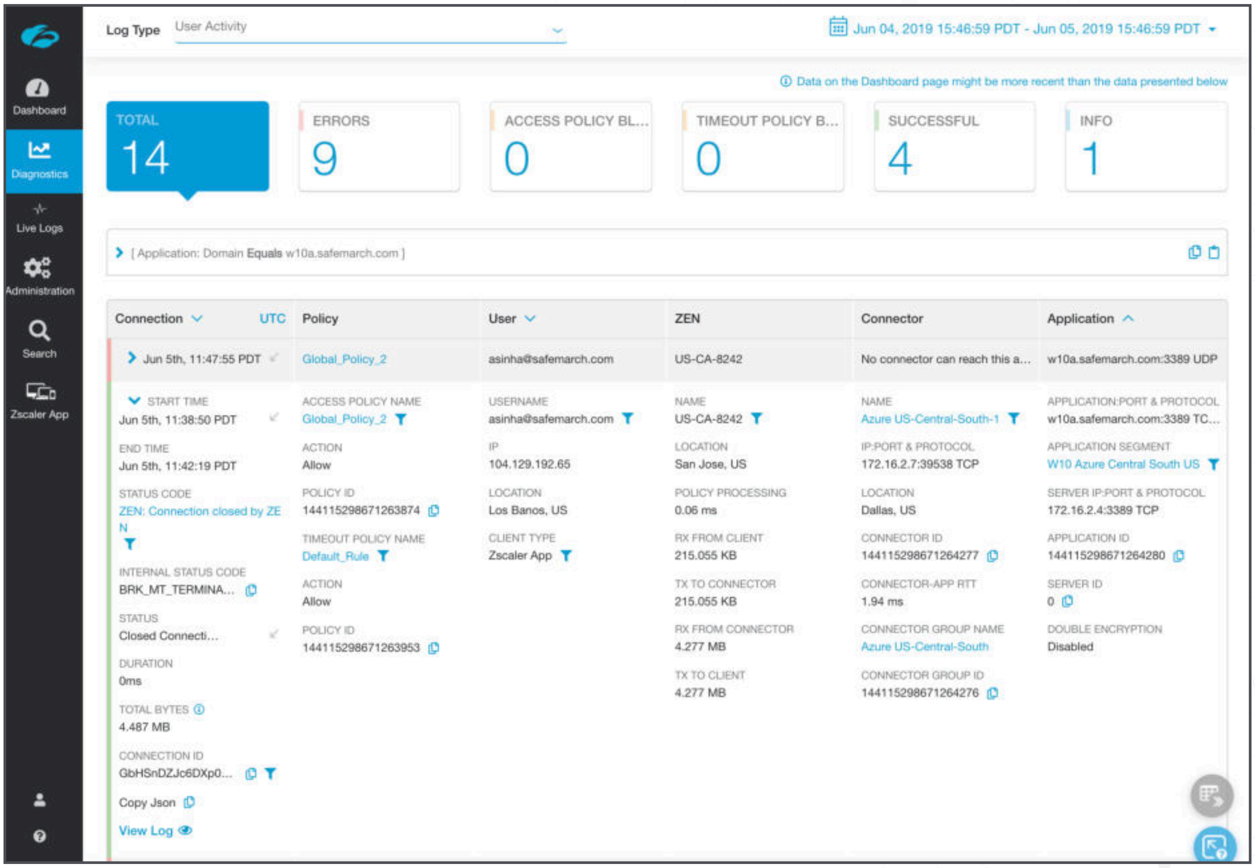
- Discover unknown applications running in your public cloud and apply granular access controls
- Displays user and app data as names, not anonymous IP addresses
- View past and real-time user activity
- View the health of applications, servers, and connectors in your environment
- Automatically stream user audit logs to your SIEM provider
- Visibility into all devices connecting into Zscaler
- App Connector provides visibility into environment health



Define granular policies based on specific user and application

ZPA delivers a central platform that gives IT control over applications and the users authorized to access them.

- Global policies hosted in the Zscaler cloud determine which users can access which applications
- Admins create and manage policies for users, user groups, applications, and application groups
- IT can segment access by applications with no need to segment by network or use ACLs



Log Type: User Activity

Jun 04, 2019 15:46:59 PDT - Jun 05, 2019 15:46:59 PDT

Data on the Dashboard page might be more recent than the data presented below

TOTAL	ERRORS	ACCESS POLICY BL...	TIMEOUT POLICY B...	SUCCESSFUL	INFO
14	9	0	0	4	1

[Application: Domain Equals w10a.safemarch.com]

Connection UTC	Policy	User	ZEN	Connector	Application
Jun 5th, 11:47:55 PDT	Global_Policy_2	asinha@safemarch.com	US-CA-8242	No connector can reach this a...	w10a.safemarch.com:3389 UDP
START TIME Jun 5th, 11:38:50 PDT END TIME Jun 5th, 11:42:19 PDT STATUS CODE ZEN: Connection closed by ZEN INTERNAL STATUS CODE BRK_MT_TERMINA... STATUS Closed Connecti... DURATION 0ms TOTAL BYTES 4.487 MB CONNECTION ID GbHSnDZJc6DXp0... Copy Json View Log	ACCESS POLICY NAME Global_Policy_2 ACTION Allow POLICY ID 144115298671263874 TIMEOUT POLICY NAME Default_Rule ACTION Allow POLICY ID 144115298671263953	USERNAME asinha@safemarch.com IP 104.129.192.65 LOCATION Los Banos, US CLIENT TYPE Zscaler App	NAME US-CA-8242 LOCATION San Jose, US POLICY PROCESSING 0.06 ms RX FROM CLIENT 215.055 KB TX TO CONNECTOR 215.055 KB RX FROM CONNECTOR 4.277 MB TX TO CLIENT 4.277 MB	NAME Azure US-Central-South-1 IP:PORT & PROTOCOL 172.16.2.7:39538 TCP LOCATION Dallas, US CONNECTOR ID 144115298671264277 CONNECTOR-APP RTT 1.94 ms CONNECTOR GROUP NAME Azure US-Central-South CONNECTOR GROUP ID 144115298671264276	APPLICATION:PORT & PROTOCOL w10a.safemarch.com:3389 TC... APPLICATION SEGMENT W10 Azure Central South US SERVER IP:PORT & PROTOCOL 172.16.2.4:3389 TCP APPLICATION ID 144115298671264280 SERVER ID 0 DOUBLE ENCRYPTION Disabled

Ensure secure access to all public and private cloud environments

Accessing apps across both datacenter and public cloud (Azure, AWS and GCP) is now fast, less complex and secure.

- ZPA provides secure and consistent access regardless of where the apps is running
- Removes the need for the VPN gateway stack or connecting to a virtual DMZ for secure access to public clouds
- Drastically reduces the complexity of network and security architectures, accelerating cloud adoption
- Accelerates app migration by simply routing user traffic to a new connector once an app is moved
- Simplifies network security for cloud adoption through partnerships with both Microsoft (Azure) and Amazon (AWS)

Accelerate mergers and acquisitions

Mergers and acquisitions can take months or even years to implement. ZPA reduces the network complexity and cost often experienced by IT architects and admins during an M&A.

- ZPA standardizes security for all current and newly acquired assets
- Eliminates the need to consolidate multiple networks or IP addresses
- Can speed M&A timeframes through simply ZPA software deployment
- Places no employees—existing or acquired—on the network
- Requires no changes to current infrastructure

Zscaler Private Access is available in three product suites:

SUITES	BROWSER ONLY	PROFESSIONAL	BUSINESS
ZPA Platform — Global data centers, high availability, SAML authentication, etc.	✓	✓	✓
Global visibility for users and applications — Single pane of glass shows which users are accessing private, internal apps	✓	✓	✓
Secure private application access to web apps — Allows secure access to all web-based applications without exposing network or apps to the Internet	✓	✓	✓
Secure private application access to internal apps with Client Connector — Allows secure access to internal applications (whether public/private/hybrid cloud or data center environments) without exposing network or apps to the Internet		✓	✓
Includes ZPA App Connectors* — Lightweight VM deployed in data center, cloud, and hybrid environments to enable secure connectivity to applications through ZPA	✓	✓	✓
Multiple identity provider support — Enables simultaneous support of multiple IDP services	✓	✓	✓
Application and server discovery — Wildcard policy shows application and server locations as they are requested by users	✓	✓	✓
Enterprise DarkNet with DDoS protection for apps — Applications are only visible to users that are authorized to connect to them	✓	✓	✓
ZPA User Portal — A centralized portal that visually displays applications the user can access	✓	✓	✓
Microsegmentation by application (up to 5 application segments)* — Granular access control by user or group for up to five specific application definitions, each of which may contain multiple hosts and/or ports	✓	✓	
Microsegmentation by application (up to 6,000 application segments)* — Granular access control for up to 6,000 defined applications and segments			✓
Client Connector — Agent for Windows, Mac, IOS, and Android — Lightweight application used to provide access to Zscaler Internet Access and Zscaler Private Access		✓	✓
Device posture enforcement — Checks device fingerprint and certificate, as well as other postures		✓	✓
Continuous health monitoring — Application health is continuously monitored to ensure that ports are available and users can connect to the app			✓
Real-time user transaction view — Instantaneous logs for end-user support			✓
Log Streaming Service — Automatically streams logs to SIEM provider	$	$	✓
Double Encryption with customer provided PKI — Allow for use of customer-provided certificates. Provides encryption to microtunnel using customer's PKI		$	$

Note: An application segment is any number of FDQNs/IP addresses on a standard set of ports.
**Additional can be added, ($) Feature can be purchased separately*

To learn more about Zscaler Private Access visit zscaler.com/products/zscaler-private-access
Experience ZPA with a free 7 day test-drive zscaler.com/zpa-interactive

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