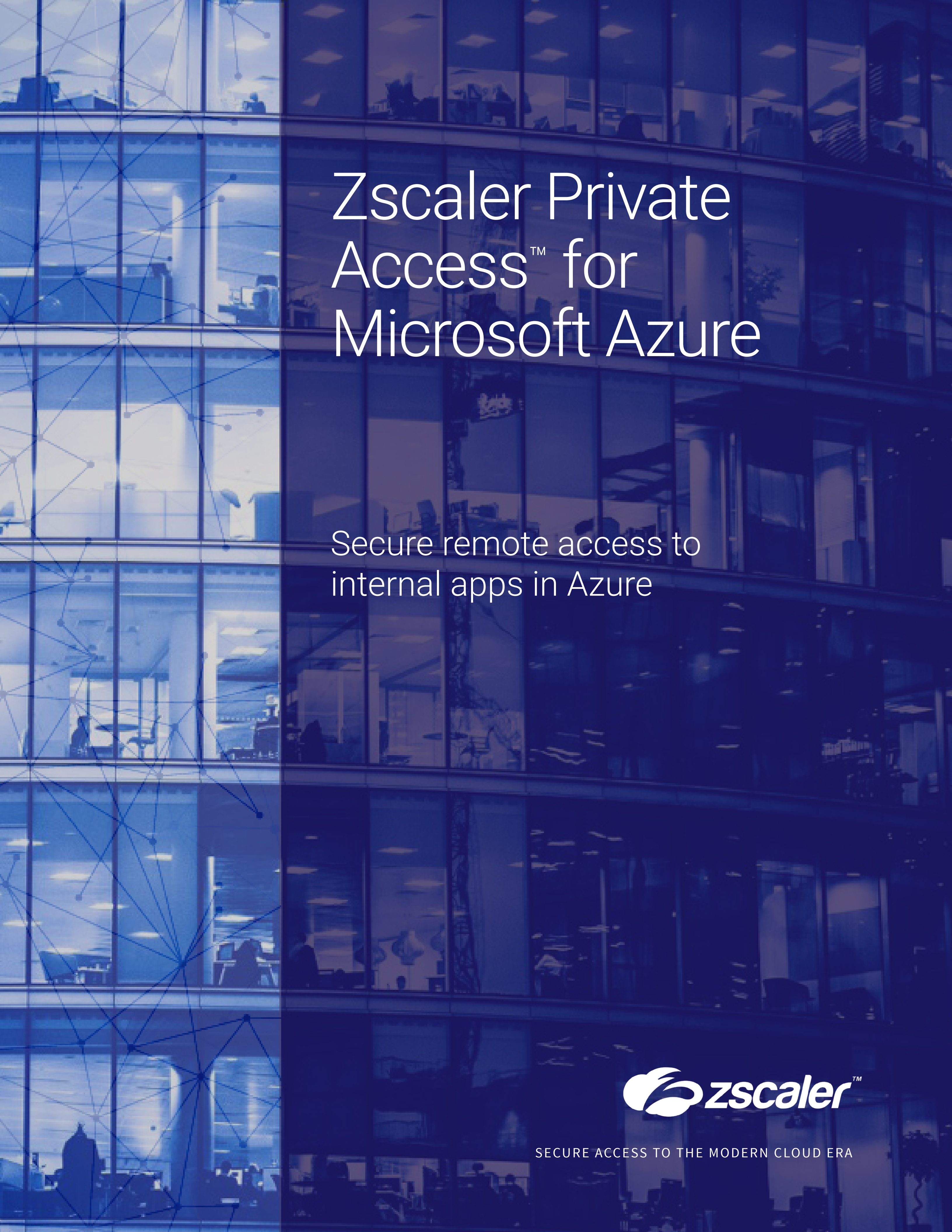


Zscaler Private Access™ for Microsoft Azure

Secure remote access to internal apps in Azure

SECURE ACCESS TO THE MODERN CLOUD ERA

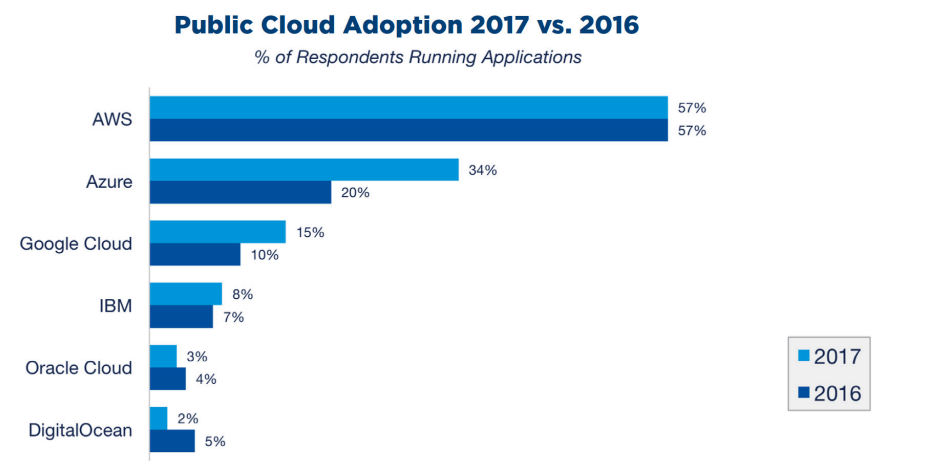
Why enterprises are moving to Azure

Microsoft Azure has become an integral part of global IT transformation. With Azure, enterprises can leverage a global, highly flexible, interconnected Microsoft network, helping them to reduce costs and complexity by running on infrastructure as a service. The Azure cloud empowers enterprises by giving them agility, which enables them to scale elastically and remain in front of changing business demands.

Enterprises are realizing these benefits in greater numbers, and are actively pursuing application transformation initiatives centered around migrating internal applications to Azure. This migration has led to the rapid growth of Azure within the enterprise, with 43 percent of enterprises now running applications on Azure.

Azure is great for users, too, making it easier for mobile users to access applications and services, regardless of their location or time zone. In addition to maximize user productivity, the convenience of the cloud has led to a change in the status quo in terms of user expectation. Remote users, having experienced seamless access to cloud applications, now expect to enjoy a “cloud-like” experience for all applications, including internally managed applications hosted in the Azure cloud.

For enterprises and their users to realize the benefits of moving applications to the cloud, the time has come to rethink remote access.



Source: RightScale 2017 State of the Cloud Report

The use of Microsoft Azure surged within the enterprise in 2017, according to the RightScale 2017 State of the Cloud report.

Applications have moved to cloud. Why does remote access still rely on the data center?

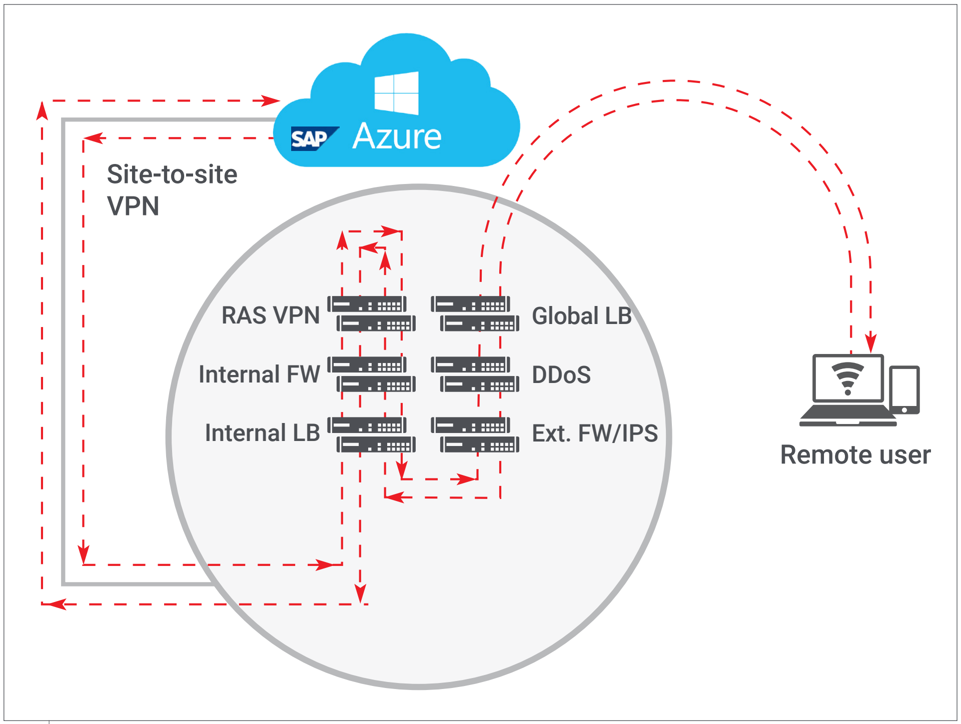
In the early days of security, the focus was on protecting the data and internal applications running within the data center. Security architects determined that the best way to ensure that protection was to build a secure perimeter around the network. And thus, the castle-and-moat architecture that many security teams are familiar with today was born.

From a networking perspective, hosting internal applications within a single data center was a natural fit with the castle-and-moat security architecture. It meant that all traffic from remote users or branch offices would be backhauled to that data center in order to access applications. In many cases, this data center was located in another part of the world.

Now, applications that once resided in the data center are being migrated to the Azure cloud. This breaks the idea of a secure perimeter, as the apps and data that need protecting now reside outside the perimeter. The hub-and-spoke strategy of routing traffic to a central data center becomes inefficient with apps running in Azure. Yet, today's remote access solutions are still reliant on routing traffic to the data center first. But, given the lack of viable alternatives, enterprises continue to use the remote access VPN.

Since the 1990s, there's been only one way to provide remote access to internal applications: the remote access virtual private network (VPN). But with internal apps moving to cloud providers like Azure, while being accessed by an ever-increasing number of remote workers, it no longer makes sense to route traffic through the data center.

> “DMZs and legacy VPNs were designed for the networks of the 1990s and have become obsolete because they lack the agility needed to protect digital businesses.”
>
> *Gartner*
> September 2016



Internet-bound traffic from remote users takes a slow, circuitous path as it's routed through the data center security stack before it can head out to the cloud or open internet, then goes back through the stack on its return trip.

Challenges of the remote access VPN

Poor user experience

Users attempting to access applications running within the Azure cloud are forced to log in to a remote access VPN. Their traffic is then routed through the data center, instead of going directly to Azure.

High cost and complexity

Remote access VPNs require multiple gateway appliances. This makes it difficult to scale across multiple geographies, as teams would have to replicate gateways across each data center. Remote access VPNs hinder the value of cloud, such as its elasticity, simplicity, and cost savings.

Risk of attack

Remote access VPNs place remote users on the corporate network. This can expose the network to malware or other security attacks that stem from untrusted user devices. Lateral movement makes it easier for attacks to spread to multiple apps.

Direct-to-cloud access with Zscaler Private Access

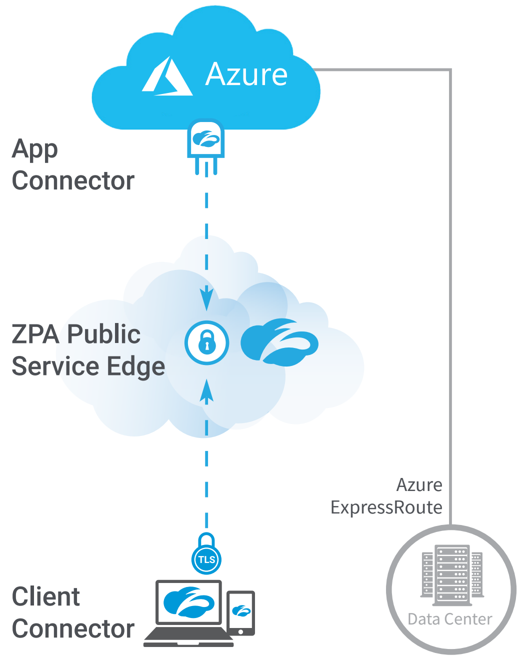
Zscaler Private Access (ZPA™) is a revolutionary service from Zscaler that uses the Zscaler™ cloud to provide secure remote access to internal applications. ZPA enables enterprises to break free from the remote access VPN-driven mindset that is centered around the data center to one of a more modern, cloud-based approach.

Key to its value is ZPA's ability to give remote users the seamless experience they want when accessing internal applications, while giving enterprises the security they need, and the simplicity to make network transformation a success.

App Connector: Sits in front of apps (inside-out connections)

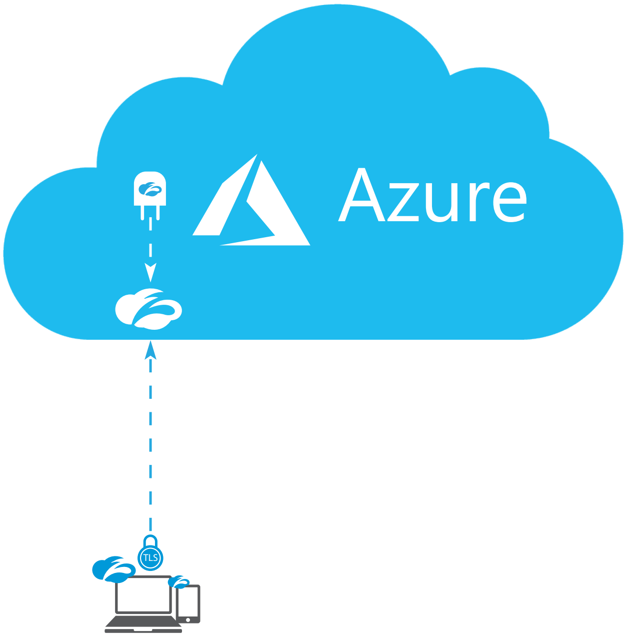
ZPA Public Service Edge: Secure user-to-app connection

Zscaler Client Connector (formerly Zscaler App): Requests access to an app



Zscaler Private Access (ZPA) for Azure

Now, enterprises can combine the benefits of the Azure cloud with the enhanced security and software-defined perimeter delivered by ZPA. Using ZPA eliminates the need for remote access VPN appliances—and the pitfalls associated with them. The ZPA solution delivers a direct-to-cloud experience for all users, taking them quickly and seamlessly to the app that runs within Azure, rather than routing them through a remote access VPN gateway.



Fast access to apps in Azure for remote users

The joint solution enables Zscaler to leverage Microsoft's global footprint to provide faster direct-to-cloud access to applications within Azure for remote users. ZPA Public Service Edge, a component of the ZPA solution, run on Azure's network, comprised of hundreds of data centers and global load balancers. The ZPA Public Service Edge is used to broker a connection between a mobile user and an application, and then routes that traffic. App Connector, which sits in front of an application, also runs with Azure, providing an inside-out connection to the ZPA Public Service Edge.

The combination of ZPA and Azure ensures that user traffic always traverses the optimal path based on the location of the user. Because remote users access the application nearest to them, the user experience improves and so does productivity.

Along with fast performance, users get a seamless experience. With a VPN, users have to log in each time they want access to an application. But with Client Connector, which is installed on the user's mobile device, authenticated users only log in once. So users get connected more quickly to their applications in Azure.

Zscaler Private Access, along with Azure's cloud-based security approach, enables enterprises to determine who has access to which internal applications, even as they are migrated from the data center to Azure. The joint solution is built upon the four key tenets of Zscaler Private Access.

1 | **Users are not on the network –** Users are never given access to the corporate network. Access is application specific, with no need to define policy by IP address or ACL.

2 | **Applications are invisible –** Internal IP addresses are never exposed to the internet. Internal applications are on a corporate "dark-net" and are completely invisible to users, unless users are authorized to access them.

3 | **The internet becomes the new secure network –** Zscaler Private Access leverages the internet for dynamic, app-specific, TLS-based end-to-end encryption. All data remains private and customers can use their own PKI.

4 | **Policies provide application-level segmentation –** There is no user-to-network access. Users have direct access only to specific applications, and each application session has its own micro-tunnel.

Why ZPA for Azure?

A better experience for remote users

- Faster access to apps on Azure
- No more VPN client for each login session
- Seamless experience for apps within Azure or the data center

Less complexity for administrators

- Easy to implement in an hour; no need to set up VPN gateways
- Application segmentation, not network segmentation
- Integrates with Azure AD
- Integrates with single sign-on (SSO) providers, such as Okta
- Works alongside Azure ExpressRoute

Secure remote access to internal apps on Azure

- Users are never on the network
- Policy-based access to specific applications on Azure
- No lateral access to additional internal applications
- Visibility into all apps running within Azure
- Visibility into user activity taking place

Increased business value

- No need to purchase hardware results in cost savings
- Increase in remote user productivity
- Service model converts security to a simple, predictable operating expense

Getting started with Zscaler Private Access and Azure

> “Zscaler helps to simplify the enterprise journey to public Azure Cloud and Hybrid environments…”
>
> *Yousef Khalidi*
> VP, Microsoft
> Azure Networking

ZPA and Azure have redefined the way internal applications are being accessed in a way that was built to enable cloud adoption and a mobile workforce. With this new solution, security—often viewed as an inhibitor of change—becomes the mechanism that accelerates the migration of internal applications to Azure.

For more information or to see a live demo, please contact Zscaler by emailing **zpa@zscaler.com** or visit **zscaler.com/zpa-for-azure**.

SECURE ACCESS TO THE MODERN CLOUD ERA