Deliver a productive and secure work-from-home experience

Keep your employees safe, secure, and productive using the cloud.

zscaler™

Just about every organization has been talking for years about the best ways to secure a remote workforce, but during these unprecedented times, many organizations find themselves being forced into it—immediately. What happens when you're suddenly faced with the need to have all your employees work from home?

Six requirements for a productive and secure at-home workforce

The key to business resilience is protecting your employees' health while empowering them to be as productive and secure at home as they are in the office. To achieve this resilience, there are some key requirements your remote access solution should provide.

1. **All applications:**
   Secure access to all external (internet, SaaS), and internal (data center, Azure, AWS) applications

2. **Cloud identity access management:**
   Optimized for integrations across devices, internal as well as external SaaS applications

3. **Fast user experience:**
   Productive collaboration using tools like Microsoft Teams and Zoom

4. **Security and compliance:**
   Cyberthreat protection and data loss prevention across users

5. **Deployable in days:**
   Agility and simplicity for rapid deployment

6. **Visibility and troubleshooting:**
   Visibility and tools required to diagnose user issues when off-network

Challenges supporting a work-from-home program with a traditional IT infrastructure

Inability to scale quickly

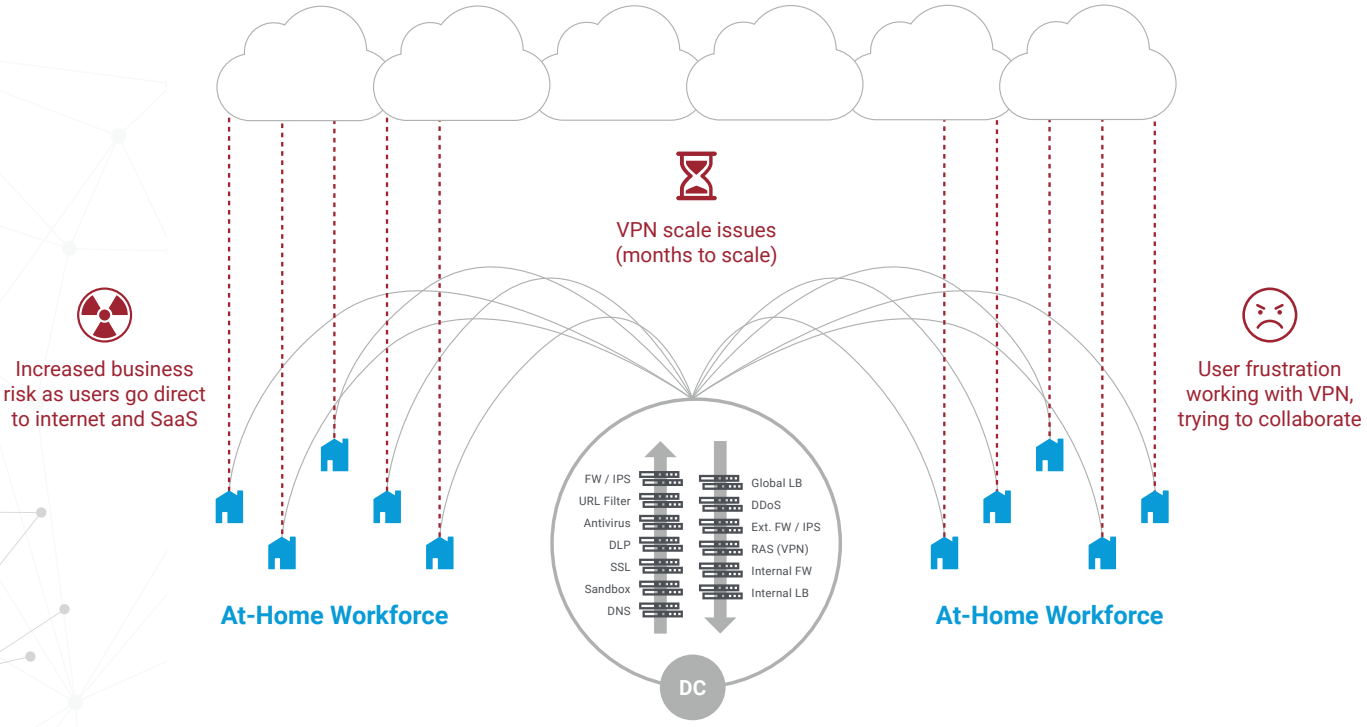
Procuring, configuring, and racking and stacking additional VPN and gateway appliances to accommodate a large at-home workforce can take weeks or even months with disruptions in the hardware supply chain. Such delays affect employee productivity, which, in turn, impacts business performance. Spinning up VMs of single-tenant appliances as a workaround will not only increase complexity, but will increase your risk as every firewall exposed to the internet is an attack surface and has been the entry point for some of the largest ransomware attacks.

Increased risk exposure

While VPN is needed to access internal applications in the data center, it's not required to access internet and SaaS applications. Users seeking a fast at-home experience will directly access these applications without the proper security controls in place. Cybercriminals are well aware of this and have been busy launching new ransomware, sophisticated social engineering campaigns, and targeted attacks.

Poor user experience

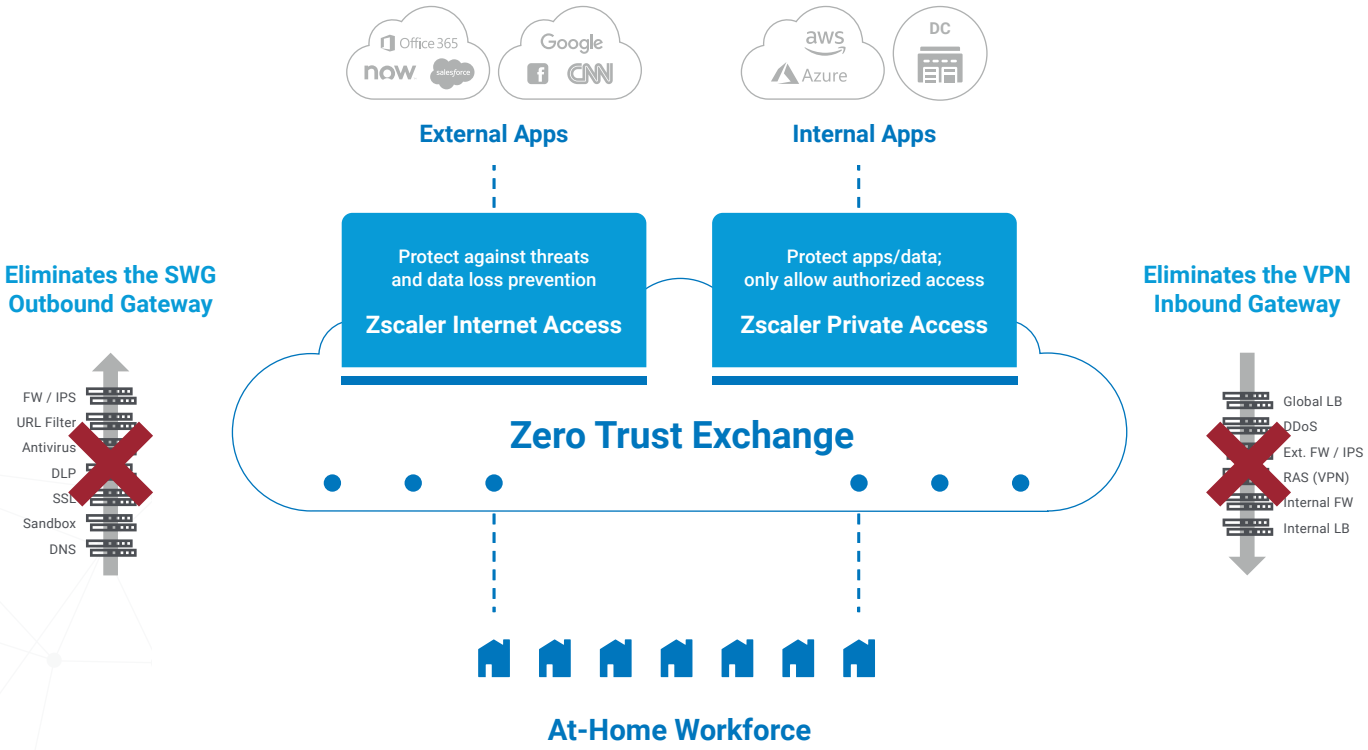
Applications like Office 365 and Zoom play a critical role in facilitating collaboration and driving productivity across a distributed workforce. The challenge is that these and other SaaS applications were designed to be accessed directly. Backhauling traffic through a VPN connection to a centralized internet gateway induces latency that is frustrating and, worse, inhibits users' ability to collaborate.



A fast, secure, work-from-home experience requires a purpose-built security cloud

Organizations have been moving applications and infrastructure to the cloud specifically for its agility, a critical advantage as organizations need to move quickly and efficiently at all times. When unforeseen events that threaten to disrupt business occur, this need becomes even more acute.

As a multitenant platform, Zscaler™ was built from the ground up to enable customers to move securely to the modern world—the world in which the cloud is the new data center and the internet the new network. Zscaler platform services were developed to ensure that business would be able to operate under any conditions, at any scale, anywhere in the world—home or office—and on any device. We have more than 150 globally distributed data centers to bring security close to our customers, and we continue to increase cloud capacity every day.



- **Cloud-native, multitenant architecture** that scales dynamically
- **Globally distributed** across 150+ data centers on six continents
- **Hundreds of peering partnerships** in all major internet exchanges
- **Proxy-based architecture** for full inspection of encrypted traffic at scale
- **Cloud receives 175K+** unique security updates daily, every 15 minutes and on demand with 40+ external threat feeds
- **Cloud processes 120B+ transactions** a day and we apply AI and ML models to identify and block threats as they emerge
- **Protections are pushed to every user** when a threat is detected anywhere in the cloud

How Zscaler can make work-from-home successful and secure

Enables secure access to all internal apps (DC, AWS, Azure) and external apps (SaaS, internet)

For a productive work-from-home experience, your employees need the same level of security and unencumbered access to their applications as they have in the office. The challenge is that while VPN is required to access internal apps, users will turn off VPN when they experience any issues – sluggish performance or dropped VPN connections – and access the internet and SaaS applications without proper security controls in place. You can avoid that risk. Zscaler provides a seamless experience for remote users with no need to log in and out; instead, access is continuous regardless of changes to network connectivity, and security is enforced instantly in the cloud.

Eliminates VPN and provides better security and user experience

Zscaler provides a modern approach to secure application access without the performance implications of backhauling traffic through VPNs, which can quickly become overwhelmed by surges in usage. With Zscaler, users connect locally to their apps through the Zscaler cloud, which is distributed across 150+ data centers worldwide. Users are protected by comprehensive security and policy enforcement no matter where they connect. And once Zscaler is in place, you not only eliminate the high cost of scaling your inbound VPN gateway infrastructure, but you can begin to phase it out.

Integrates with cloud identity and access management (IAM) for conditional access

Moving your enterprise's applications and data to the cloud means you need greater control over which employees can access those cloud resources. Cloud identity and access management (IAM) solutions centralize identity and authentication services, which gives your IT teams greater control over your cloud environment and its security and enabling them to track which users are accessing what applications, and when. Zscaler has deep integrations with leading IAM vendors, including Azure AD, Okta, and Ping to enforce contextual access policies.

> "ZPA has been a key enabler in DB Schenker's business continuity plan, which results in the fact that our users do not wish to go back to traditional VPN connections."

DB SCHENKER

Gerold Nagel
SVP, Global Infrastructure Services

Gets employees up and running in days—not weeks or months

Zscaler is a 100% cloud service that's fast and easy to deploy because there's no need to install, configure, or manage appliances. Access is based on business policies hosted in the Zscaler cloud, and user traffic is forwarded locally to Zscaler through Zscaler Client Connector (formerly Zscaler App), a lightweight app that can easily be distributed through MDM systems such as Microsoft Intune; for web apps, users only need a browser for access.

Zscaler integrates with identity providers to authenticate users and apply contextual access rather than relying on ACLs or IP addresses. App Connectors, which are small VMs, front-end internal apps and use inside-out microtunnels to connect a user to an authorized app. Zscaler handles all routing and load balancing so you don't need to worry about scaling your infrastructure.

Keeps your employees and data safe

Cybercriminals have been busy launching new malware, sophisticated social engineering campaigns, targeted attacks, and more, and they are well aware that there are many users working from home that are usually on a corporate network behind a security perimeter. By moving security to a globally distributed cloud, Zscaler brings the full internet security stack (advanced threat protection, SSL inspection, data loss prevention, sandboxing, remote browser isolation, and CASB) close to the user for a fast and secure experience. No matter where users connect, their security policy follows them.

Provides visibility and quick troubleshooting to diagnose user issues

The ability to monitor network activity becomes a different kind of challenge when all your employees are working from home, many of them on unmanaged devices, and your network is the internet. In addition to real-time visibility into users and applications, you need to be able to see exactly what is going on at every point between a user's device and an application's front door to quickly pinpoint the source of any issues causing performance problems, so you can take corrective action.

> "I shared with my NOV leadership team that all 27,500 users could start working remotely because of Zscaler. They were stunned!"

Alex Philips
CIO, National Oilwell Varco

The Zscaler Cloud Security Platform

Zscaler services are 100% cloud-delivered and provide fast, secure, and reliable access to the internet and cloud apps, as well as private apps in the data center or public and private clouds. Access is based on software-defined business policies that follow users no matter where they connect or what devices they're using.

> "One of the things we are providing is an app-by-app type of approach to giving folks what they need, and not having to over-provision access. With the combo of ZIA and ZPA, we're much more flexible with what we can provide and since we're running all our traffic through it, we know it can scale."

Mike Towers
CSO, Takeda Pharmaceuticals

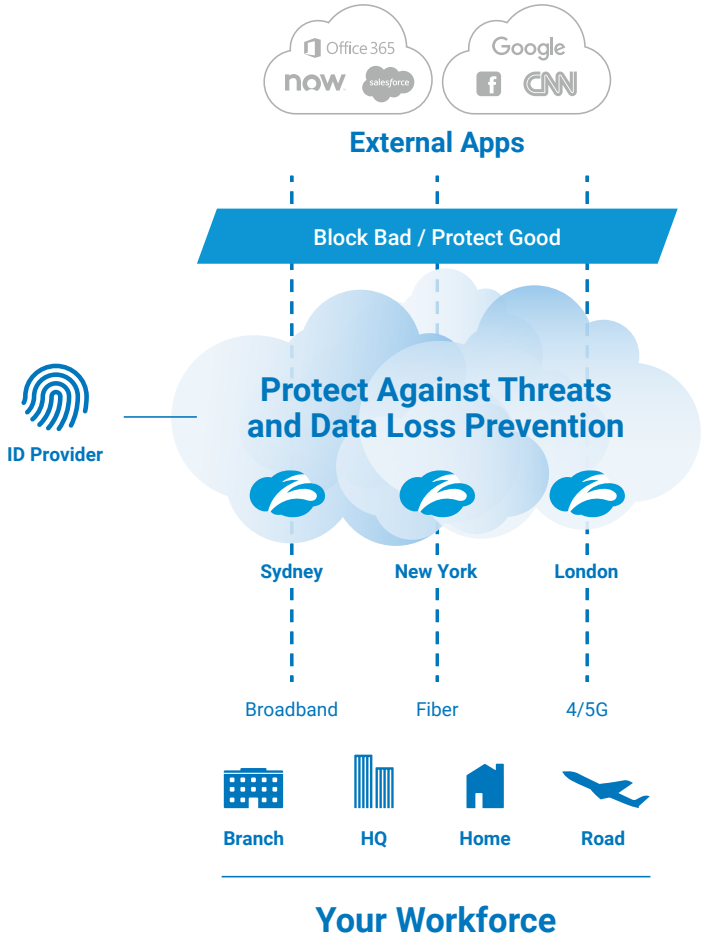
Zscaler Internet Access™ (ZIA™) and Zscaler Private Access™ (ZPA™) make up the Zscaler Cloud Security Platform, moving the outbound and inbound security gateways to the cloud. By making Zscaler your first hop to the internet, every connection is secured and policies are enforced no matter where users connect or where applications are hosted.

Zscaler Internet Access: Your security stack as a service

Zscaler Internet Access (ZIA) delivers the entire outbound security stack as a service from the cloud, eliminating the cost and complexity of traditional secure web gateway approaches. By moving security to a globally distributed cloud, Zscaler brings the internet gateway closer to the user for a faster experience. Organizations can easily scale protection to all offices or users, regardless of location, and minimize network and appliance infrastructure.

Your remote user traffic is forwarded to the Zscaler cloud via our lightweight Client Connector or PAC file. Zscaler Internet Access sits between your users and the internet, inspecting every byte of traffic inline across multiple security techniques, even within SSL. You get full protection from web and internet threats. And with a cloud platform that supports **cloud sandboxing**, **next-generation firewall**, **data loss prevention (DLP)**, **browser isolation**, and **CASB**, you can start with the services you need today and activate others as your needs grow.

To learn more, read the ZIA **data sheet** or watch this **video**.

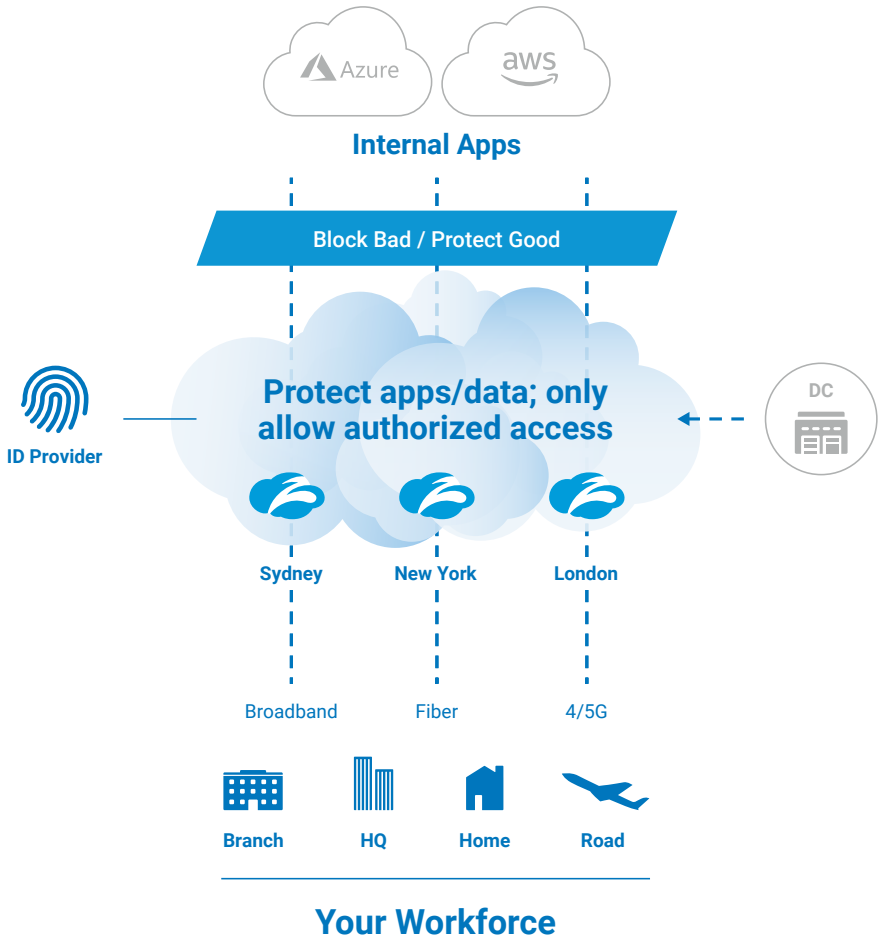


Zscaler Private Access: A scalable alternative to VPN

Zscaler Private Access (ZPA) provides users with fast and secure access to internally managed apps in the data center and public clouds. For users, ZPA offers a seamless experience, requiring no backhauling or tedious logins. There's no need to fire up a VPN for application access; you just go to the application and it works. The ZPA architecture provides key security benefits, too. IP addresses are never exposed, so DDoS attacks are impossible. And, because users are never placed on the network, ZPA reduces the risk of lateral movement and the spread of malware.

How does it work? ZPA creates a secure segment of one between a named user and a named app, ensuring that only authorized users have access to specific private applications. Access is based on business policies that you define in the Zscaler Admin console. ZPA provides a fast and seamless user experience. Instead of logging in to their VPN client (and continuing to do that every time they start a session), users simply open up Zscaler App on their laptop, mobile phone, or tablet, for fast, local connections.

To learn more, watch this whiteboard **video** and download the ZPA **data sheet**.



Getting started with Zscaler is fast and simple

Zscaler services are 100% software-based and can be deployed in days.

Deploy Zscaler App Connectors, which are small VMs that sit in front of your private applications in the data center or in public or private clouds.

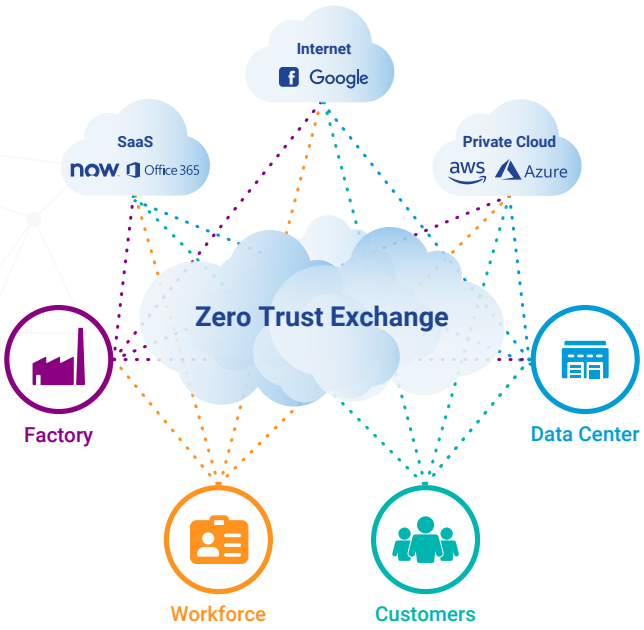
Install Zscaler Client Connector, a lightweight app, which can easily be distributed through your mobile device management (MDM) solution. Client Connector ensures the user's device posture and extends a secure microtunnel to the Zscaler cloud.

Configure policy in the Zscaler Admin console. You set access policies once and they follow users no matter where they connect.

Protect your employees. Protect your business.

As organizations have been moving applications and infrastructure to the cloud and users have been moving off the network, Zscaler has been providing always-on, cloud-delivered security. Today, more than 400 of the Forbes Global 2000 organizations rely on Zscaler to deliver a fast user experience while securing every connection between their users, applications, and devices, regardless of network.

Once you've enabled a productive and secure work-from-home experience, you can begin to think more broadly about your WAN infrastructure and network security. In the modern cloud and mobile world, the network is no longer the center of gravity, so why continue to invest in a network-based security infrastructure?



The Zscaler cloud operates as a zero trust exchange, enabling secure, any-to-any connectivity.

Learn more about Zscaler services and for **enabling your work-from-home initiatives—securely.**

www.zscaler.com/business-continuity

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