Deliver a Secure, Productive Educate-from-anywhere Experience

Keep your faculty and researchers safe, secure and productive from wherever they are working using the Zscaler Zero Trust Exchange

zscaler™

Every organization has had to rethink how they can ensure employees are secure and productive, whether they are working on premise, at home or at a coffee shop - and universities are no different. Zscaler is helping reshape how higher education institutions are providing fast, secure, and reliable access for their users to their applications, regardless of location.

Six requirements for productive and a secure Educate-from-Anywhere Experience

The key to organizational resilience is protecting your staff while empowering them to be as productive and secure at home as they are on campus networks. To achieve this resilience, there are some key requirements your remote access solution should provide.

1. **Application access:**
   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 and seamless user experience when using tools like Microsoft Teams and Zoom

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

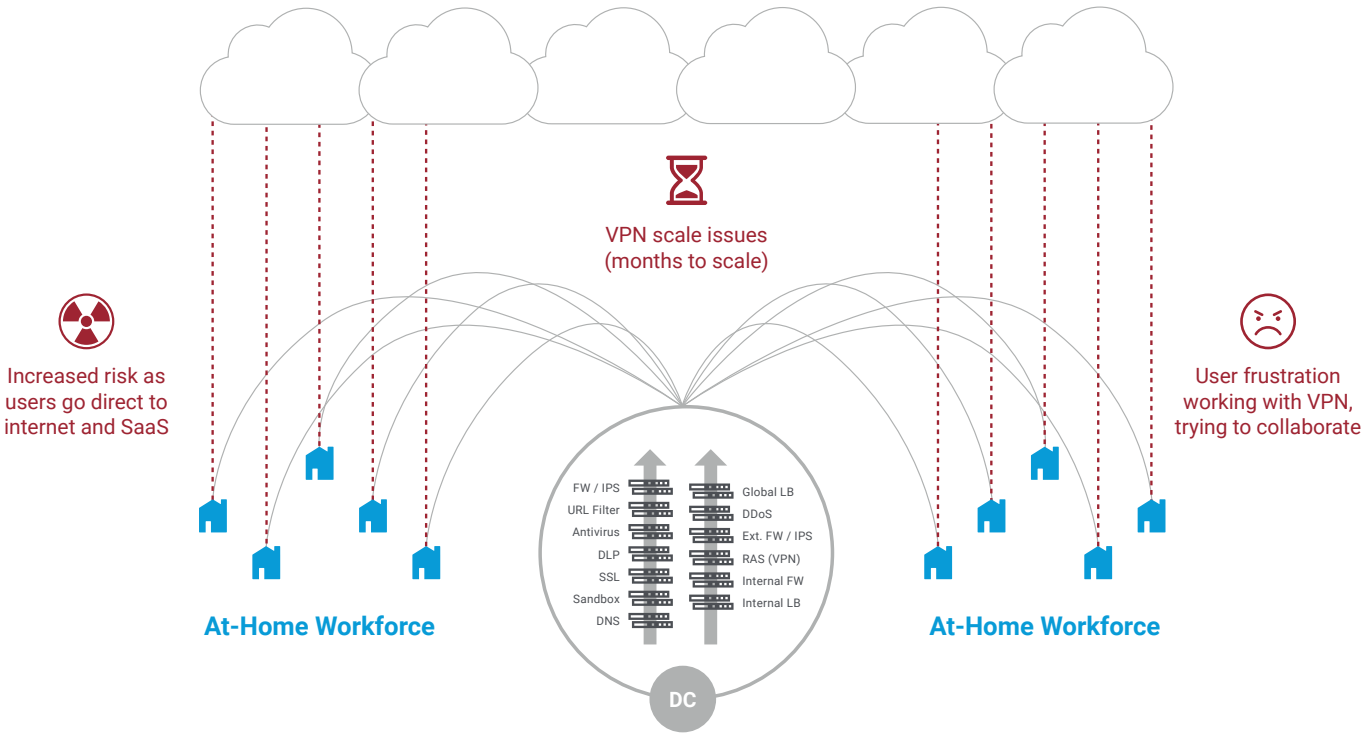
Procuring, configuring, and racking and stacking additional VPN and gateway appliances to accommodate a large at-home workforce can take weeks or even months with disruptions in the hardware supply chain. Such delays affect user productivity, which, in turn, impacts organizational performance. Spinning 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

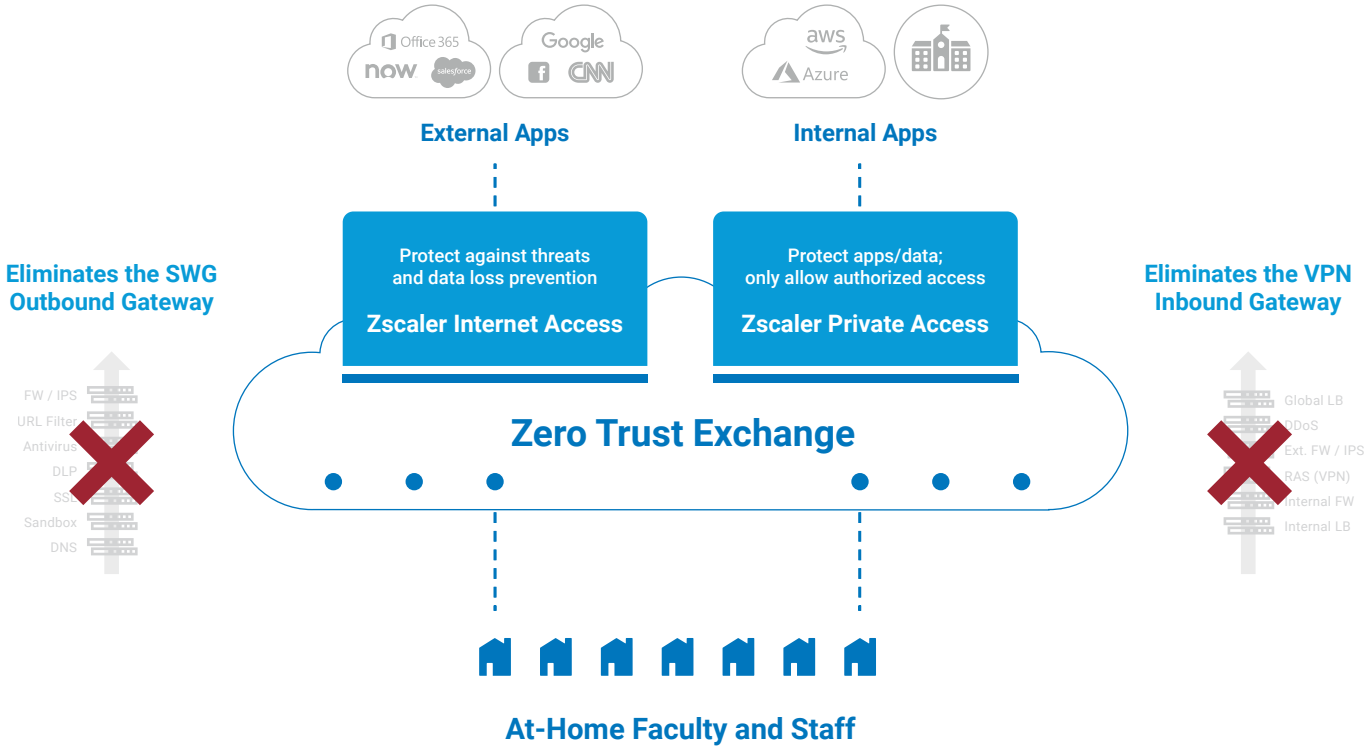
Applications like Office 365 and Zoom play a critical role in facilitating collaboration and driving productivity across a distributed workforce. The challenge is that these and other SaaS applications were designed to be accessed directly. Backhauling traffic through a VPN connection to a centralized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



A fast, secure, Educate-from-Anywhere experience requires purpose-built security for the cloud

Organizations have been moving applications and infrastructure to the cloud specifically for its agility, facilitating the need to move quickly and efficiently at all times. When unforeseen events that threaten to disrupt campus life 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 organizations would be able to operate under any conditions, at any scale, anywhere in the world—home or on campus—and on any device. We have more than 150 globally distributed data centers to bring security close to our customers and their users, 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 160B 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 Educate-from-anywhere successful and secure

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

For a productive work-from-anywhere experience, your staff needs the same level of security and unencumbered access to their applications as they have on campus. 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.

> "Technology trends such as the COVID-19 campus, remote proctoring and faculty information systems are increasingly going to be the norm for institutions and they will need to adapt accordingly."
>
> Gartner

https://emtemp.gcom.cloud/ngw/globalassets/en/information-technology/documents/trends/742584-top-technology-trends-impacting-higher-education-in-2021.pdf

Gets staff 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 administration 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 faculty members 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 campus 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 your entire staff is 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 leadership team that all 27,500 users could start working remotely because of Zscaler. They were stunned!"
>
> **Zscaler Customer**

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 administration policies that follow users no matter where they connect or what devices they're using.

> "Increases in virtual delivery and remote work due to the pandemic have highlighted the vigilance required to maintain safe and reliable environments. 2020 incidents, such as the Blackbaud data breach and SolarWinds attack, are reminders of the unknown vulnerabilities and widespread security threats institutions face on a daily basis. Environments with an average or below average security posture (which includes many higher education institutions) are increasingly the target of malicious attackers."
>
> Gartner

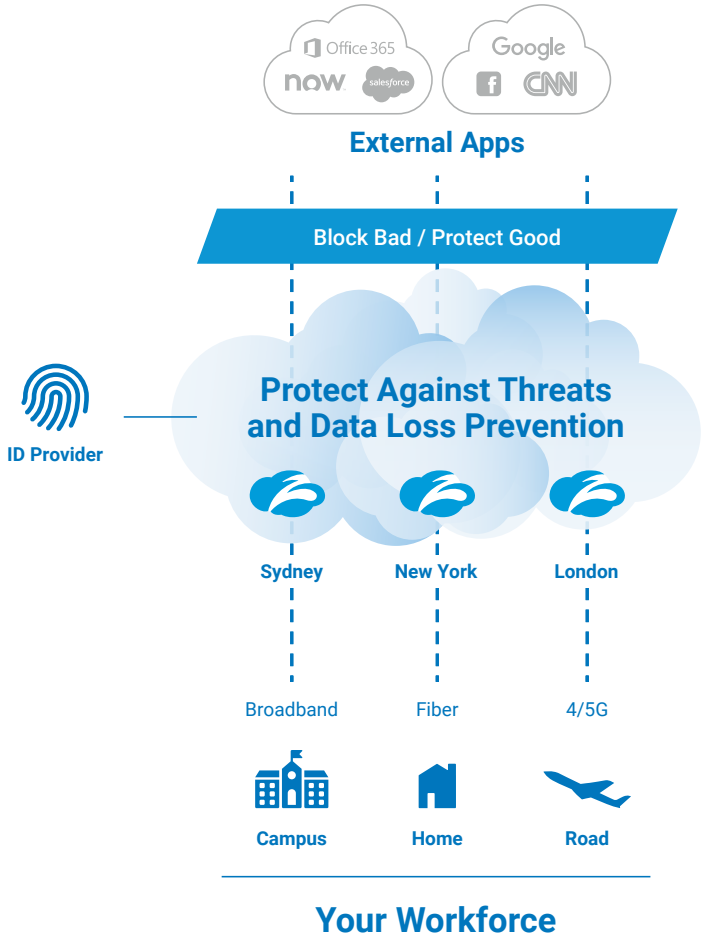
Zscaler Internet Access™ (ZIA™) and Zscaler Private Access™ (ZPA™) make up the Zscaler Cloud Security Platform, moving the outbound and inbound security gateways to the cloud. By making Zscaler your first hop to the internet, every connection is secured and policies are enforced no matter where users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