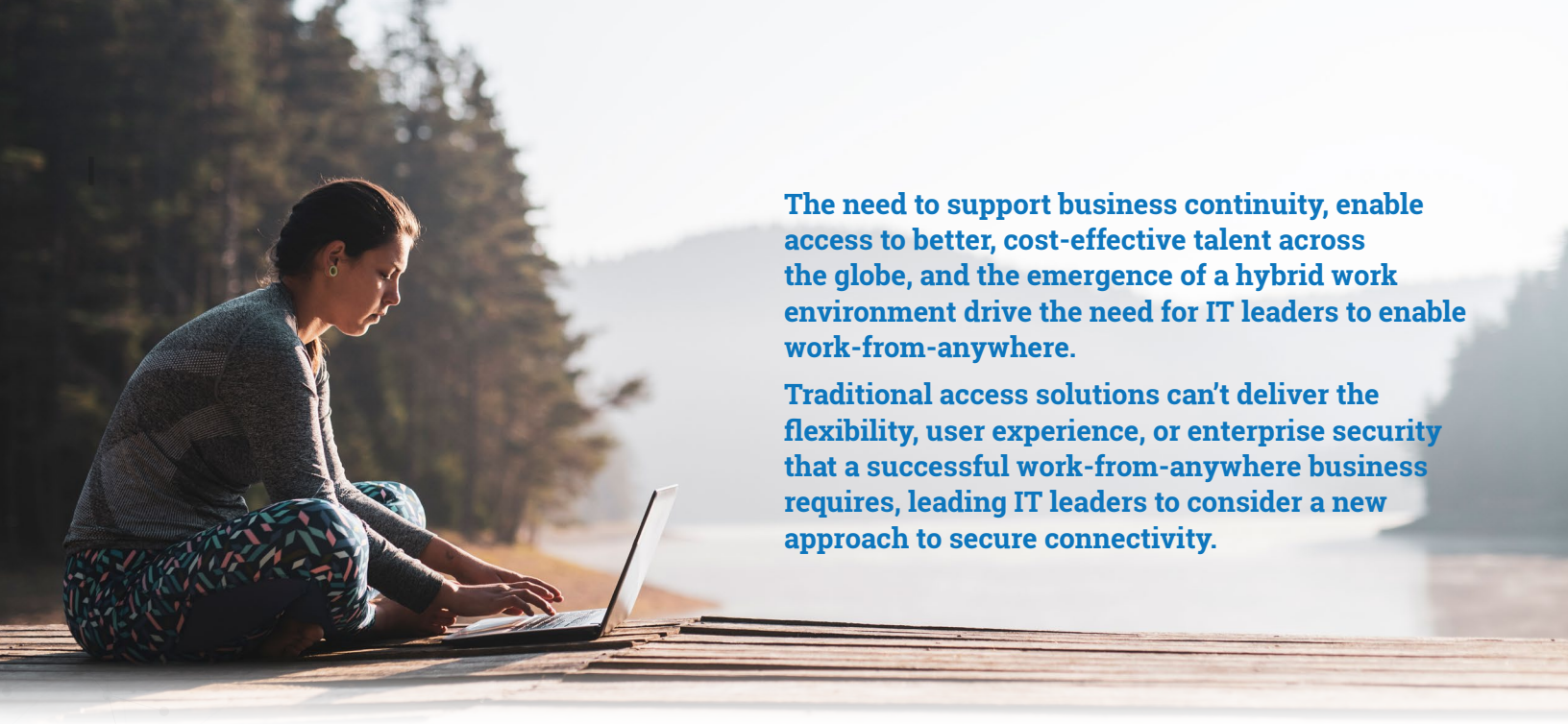
The IT Leader's Guide to Securing Work from Anywhere

Work is no longer a place, it's what people do. Make work-from-anywhere simple for users and secure for IT.

zscaler™ | CS CYBERSHERPA Security by Design



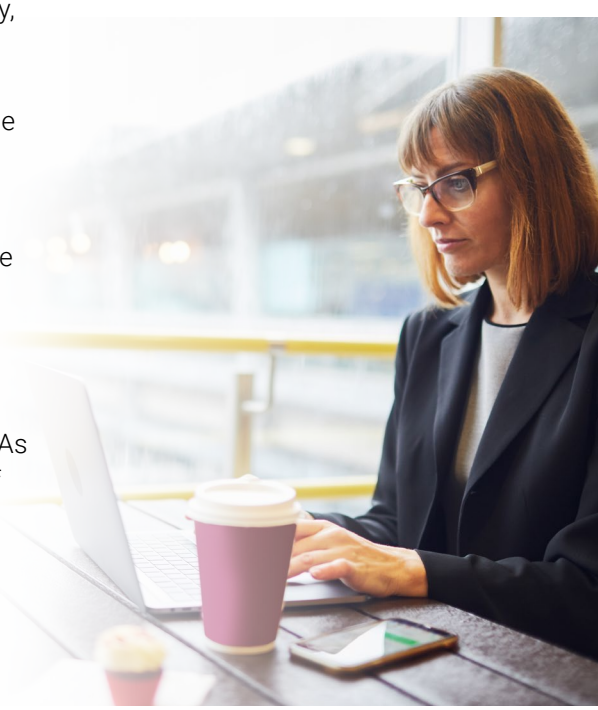
The need to support business continuity, enable access to better, cost-effective talent across the globe, and the emergence of a hybrid work environment drive the need for IT leaders to enable work-from-anywhere.

Traditional access solutions can't deliver the flexibility, user experience, or enterprise security that a successful work-from-anywhere business requires, leading IT leaders to consider a new approach to secure connectivity.

Meet Mary, the hybrid worker

Mary is a sales representative who typically spent half of her time working on the road and half in the office. Her company has just announced their flexible back-to-the-office plan. Mary, along with a subset of her coworkers, will work from home Monday, Wednesday, Friday and come into the office on Tuesday, Thursday.

It's Monday morning, and Mary begins her day at home by grabbing her morning coffee and cracking open her computer. She needs access to SAP, so the first thing she does is log in to her company's VPN and waits. Knowing this will take a while, Mary jumps on Facebook and sees an ad saying, "Win a Free iPad." Feeling lucky, she clicks the ad and signs up for her "prize". Finally, the VPN connects, and by now, Mary's coffee is cold. The slow experience frustrates Mary and the various VPN disconnects throughout the day make it hard for her to stay productive. She even had to log an IT support ticket. "Tomorrow work will be better," she thinks, knowing that she'll at least be at the office.



The alarm wakes Mary up on Tuesday morning and she gets ready to go into the office. She swaps the sweatpants she's been wearing all year and dusts off her favorite pair of slacks. Mary arrives at the office, opens up her laptop, connects to the corporate network, and gets straight to work. Mary wonders when her new iPad will arrive;however, little does she know that yesterday's ad contained dangerous ransomware that she has now brought onto the corporate network. As a result, the network perimeter has been compromised, and it's only a matter of time before IT finds out.

This is what IT is up against today.How can businesses enable employees like Mary—not to mention the partners, suppliers, and customers who also need access to critical business data—to productively work from any location, while protecting data from ransomware, over privileged access, and data leakage?

Securing work-from-anywhere: what's required

IT leaders are under pressure as they are asked to securely enable this modern work environment and make the business successful from anywhere. As IT leaders prioritize this initiative, a number of challenges materialize:

77% of businesses will allow for hybrid work, but enabling access to all apps, from a mix of devices and unmanaged networks, feels impossible.

The workforce needs access when at home, on the road, or at the office and are connected using a mix of corporate laptops, personal smartphones and for some, even RF Scanners. They're accessing business apps that no longer reside solely in the datacenter, but across a hybrid cloud environment. SaaS applications, like M365, and private applications, like SAP, are among the most common business-critical apps in the world, and IT needs to ensure users have fast, secure, and reliable access to all apps from all devices, over any network.

IT must ensure data remains secure - but every user, app and device is connected over an external channel and threats are rising.

Reducing these business risks, while enabling access from anywhere proves difficult. Historically, legacy networking and security have been intertwined, meaning that accessing applications requires access to the network - and inherently trusting users. IT needs to find a way to simultaneously allow secure work from anywhere while enabling better cyber and data protection without extending network access.

IT has performance blind spots into user traffic since traffic is no longer on the network - but user experience is now a top priority.

Traditional network solutions lack the visibility needed to pinpoint the source of poor user experience and resolve IT support issues. The absence of these important visibility and performance insights impedes IT's ability to maintain users' productivity and happiness, creating greater tension between IT and the users.

Zero trust is the new standard for the work-from-anywhere business

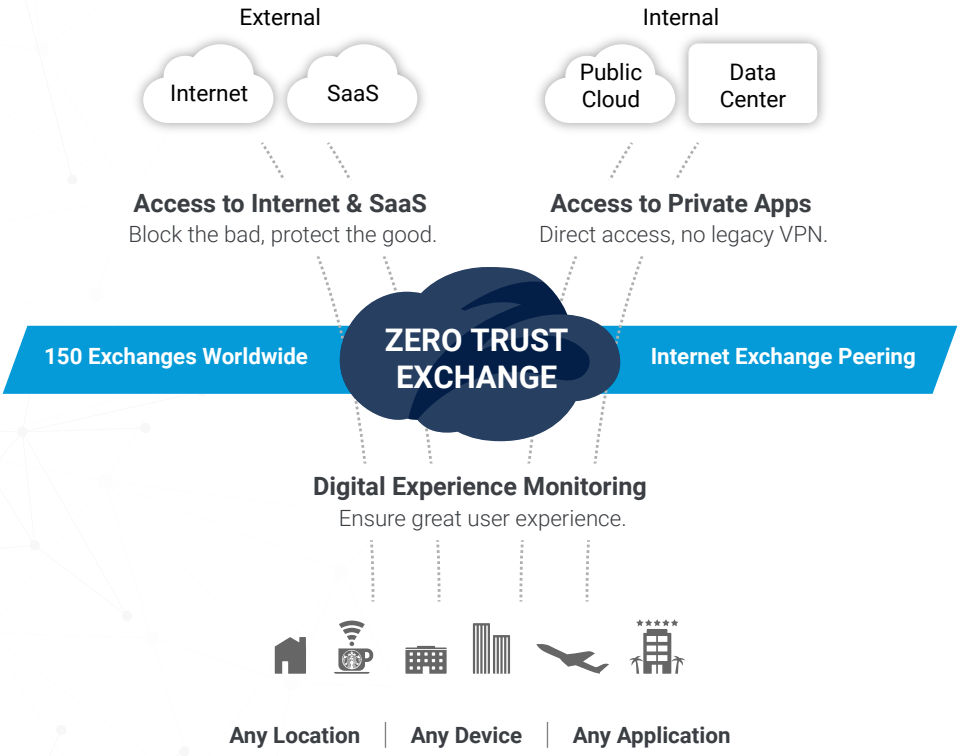
IT leaders have found that a successful work from anywhere environment must rely on zero trust. Based on the principle of least privilege access, zero trust assumes that no entity (user or application) should be inherently trusted, instead access should be granted based on identity and policy. Users, devices, applications, and content all contribute to policy formulation.

Therefore, the Zscaler Zero Trust Exchange is used to connect any user, on any device, from anywhere, to any application securely over the internet. The Zero Trust Exchange helps IT leaders embrace a cloud-delivered approach to enabling zero trust and delivering fast, seamless, and secure access across their entire business ecosystem—regardless of a worker's location. Zscaler's zero trust platform enables simple, secure work-from-anywhere in these five main areas:

- **Access to apps is now universal** – IT gets the versatility to provide fast, reliable access to all external and internal apps—from any location, device, or network with 150 global PoPs.
- **Support of any device** – Users can access apps from any common devices used for work, including laptops, smartphones, tablets, RF Scanner, etc.
- **Prevent compromise, lateral movement, and data loss** – Enforce business policies that follow the user and allow for identical security everywhere—without placing users on-network or allowing data to flow to the internet or an unauthorized device.
- **Restore visibility into user traffic through digital experience monitoring** – Digital experience monitoring enables IT to track each individual users experience and determine app, network, and device performance.
- **Pinpoint issues to resolve IT support tickets faster** – Strengthen the relationship between IT and users by keeping users productive and happy with an optimized access experience.

"Zscaler was able to adapt quickly and increase capacity to more than satisfy our needs. As employee feedback from around the world has come in, I'm hearing exactly what I had hoped–it feels normal."

- Alex Philips, CIO, National Oilwell Varco (NOV)



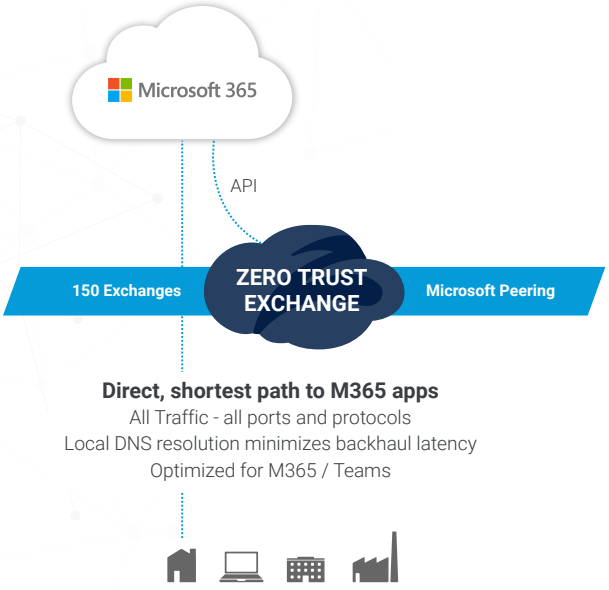
The Zscaler Zero Trust Exchange provides secure, seamless access to the internet and cloud apps **(Zscaler Internet Access™)** or private apps in the data center or public and private clouds **(Zscaler Private Access™)**. Access is based on software-defined business policies that follow users regardless of connection location or device.. IT teams are also empowered through enriched insight and control of business app performance, network performance, and device performance with **Zscaler Digital Experience™**. With more than 150 globally distributed data centers, zero trust security is brought as close to the user as possible, providing fast, local connections to users everywhere.

Lead your work-from-anywhere business to success with these key use cases

It is possible for IT to deliver both the experience their users want and the security the business requires with the right technology. While work-from-anywhere has created urgency for businesses to evolve, IT can start today by developing a plan towards success. IT teams tend to begin by focusing on the following areas:

Fast, direct access to SaaS applications such as M365

The modern workforce needs fast access to SaaS apps like Microsoft Teams and Zoom to remain productive and collaborative. Slow, backhauled traffic to these applications may prompt users to bypass security controls and proceed directly to the Internet. Enable fast, direct access to SaaS and collaboration apps without compromising security.



Direct, shortest path to M365 apps
All Traffic - all ports and protocols
Local DNS resolution minimizes backhaul latency
Optimized for M365 / Teams

Faster file throughput-
TCP optimizations

Threat protection
Protect against phishing, ransomware, zero-days, CVEs

Data protection
CASB to prevent file oversharing
Enforce tenant restrictions

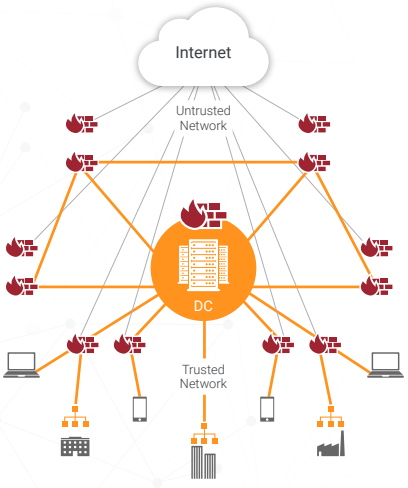
Easy to deploy and manage
One-click configuration
Automated IP address changes

Trusted by 2,000+ enterprises

Secure remote access without VPN or VDI

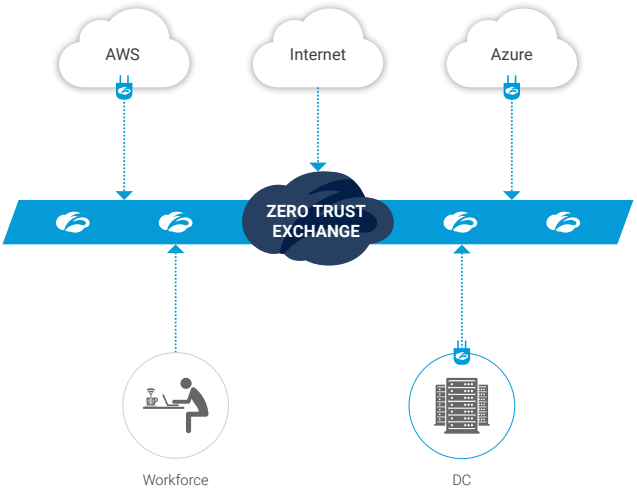
67% of IT leaders are currently looking to replace their traditional VPN. Keep your remote workforce as productive as they would be in the office by enabling seamless zero trust access to your crown-jewel and collaboration apps.

Remote Access Solution (VPN)



Slow - traffic is backhauled
Security risk - lateral threat movement / attack surface
Expensive to scale and maintain

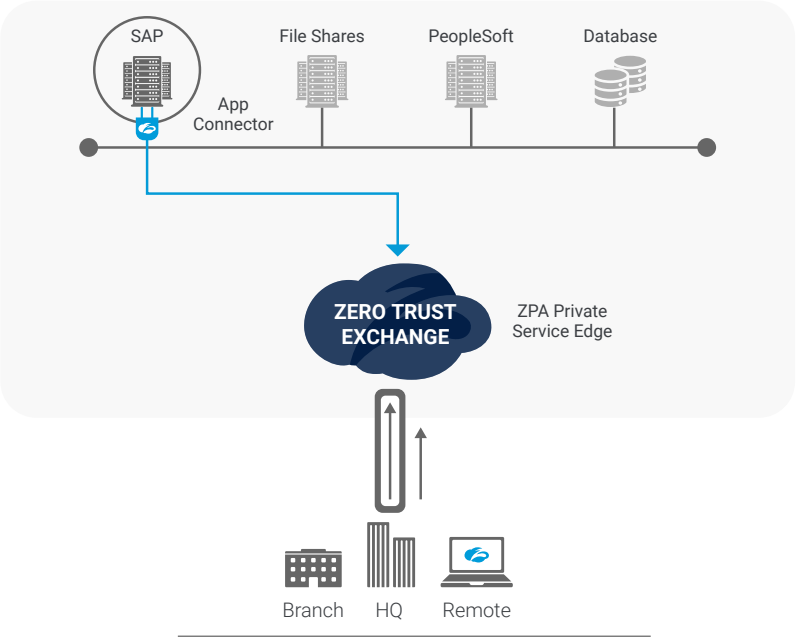
Zero Trust App Access



Direct and fast access
App access just works - no VPN on/off headaches
More secure - no attack surface/lateral threat movement

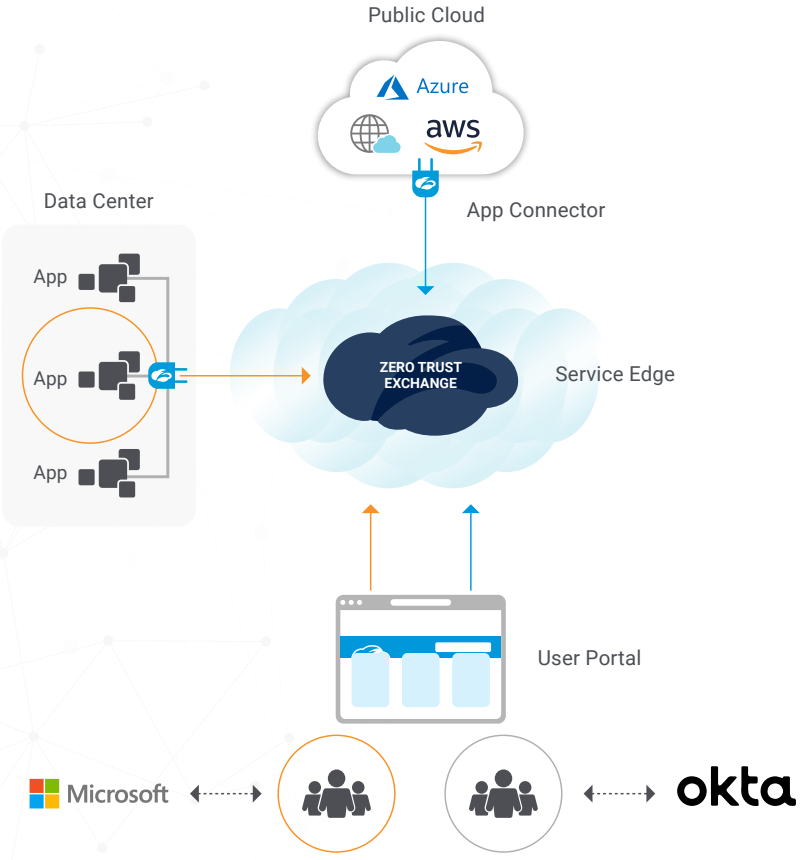
Zero trust access for hybrid and in-office employees

Bring users back to the office securely by keeping them off the corporate network. Enable least-privilege access for on-premise users while still enabling the fast, direct access they need to keep the business running.



On-premises Workforce

Connecting a user to an app (not a network) reducing the risk of something bad happening)

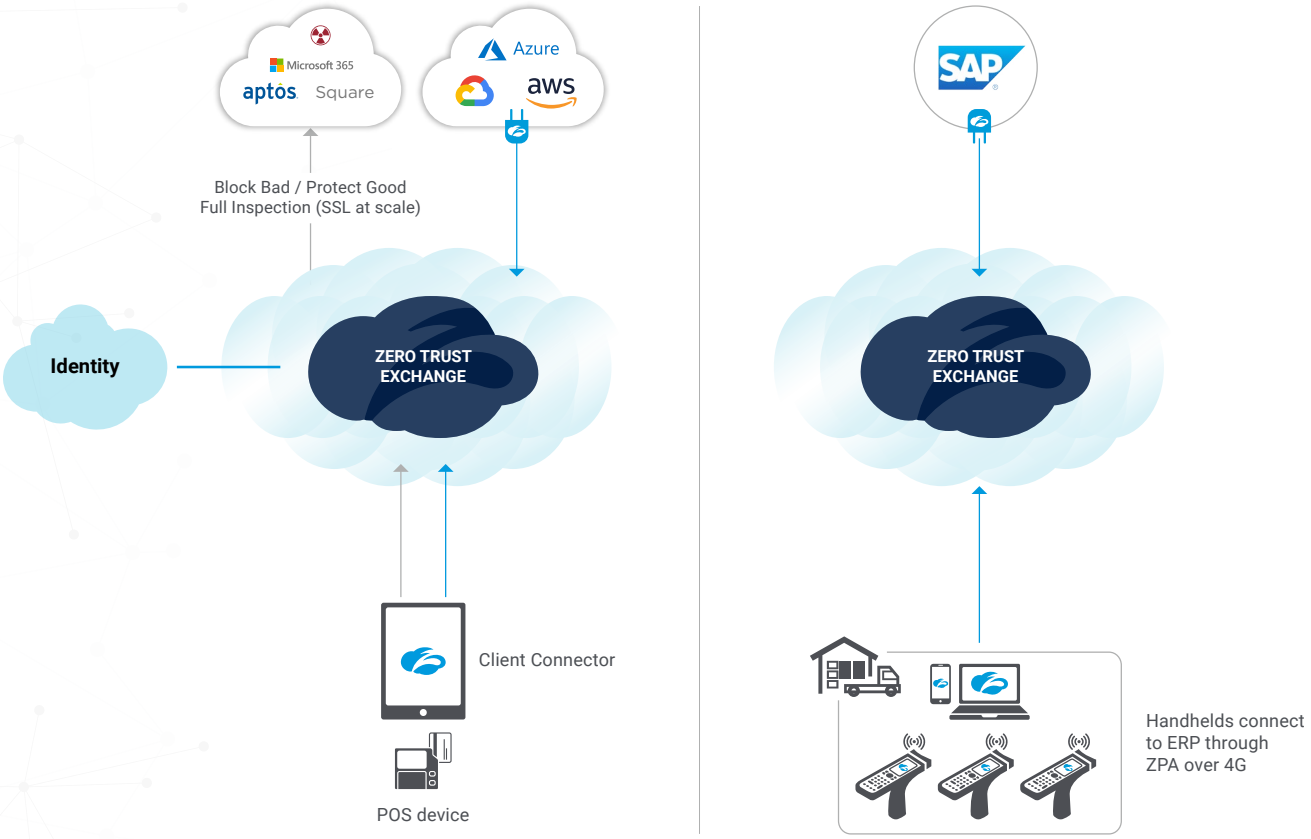


Eliminate risk of B2B access

Supporting the modern workplace includes suppliers, vendors, partners, and most importantly, customers who directly impact revenue. Therefore, it's imperative to business success that each of these unique users can securely access applications without associating risk to the organization.

Zero trust access from handheld & POS systems

The use of mobile and handheld devices is increasing, especially as goods and services are expected to be served quicker. Don't let these devices be a means of exposure to the business. Enable them to access business-critical apps seamlessly for smooth operations, while not incurring risk.



Learn how Zscaler has helped hundreds of companies secure their mobile workforce and adapt to work from anywhere. Visit **zscaler.com/solutions/work-from-home** or request a meeting with our team by emailing **sales@zscaler.com.**

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Contact Cybersherpa
contact@cybersherpa.ch
+41 21 561 3648