



Zscaler™ Zero Trust Exchange at a Glance

Zscaler Zero Trust Exchange™ Benefits:

✔ Reduces IT cost and complexity

Simple to manage and deploy without the need for VPNs or complex firewalls

✔ Delivers a great user experience

Intelligently manages and optimizes direct connections to cloud applications

✔ Eliminates the internet attack surface

Applications sit behind the exchange, preventing discovery and targeted attacks

✔ Prevents the lateral movement of threats

Connects users to apps directly without network access, so threats are isolated

The cloud and mobility are empowering digital transformation—all to make business more agile and competitive. Employees, customers, and partners are leveraging SaaS applications, such as Microsoft 365, as well as the public cloud to deploy their own applications. The users accessing these services are increasing mobile and may be on any device in any location. The result of these changes is that business is happening everywhere—and more likely off the corporate network than on it.

A legacy hub-and-spoke network and castle-and-moat security model, which worked well in the past, does not work anymore. Offices and branches are connected by expensive MPLS WAN links to a couple of central locations such as the data center. Users outside the office typically VPN into this network to access applications, an approach that is expensive, slow and adds operational complexity. The cloud and mobile world requires a new approach to networking, a new approach to security.

The Zscaler Zero Trust Exchange is a modern approach that enables fast, secure, connections and allows your employees to work from anywhere, using the internet as the corporate network. The Zero Trust Exchange runs across 150 data centers worldwide, ensuring that the service is close to your users, co-located with the cloud providers and applications they are accessing, such as Microsoft 365 and AWS. It guarantees the shortest path between your users and their destinations, providing comprehensive security and an amazing user experience.



Zero Trust Exchange Key Capabilities



Secure work-from-anywhere

Employees can safely and seamlessly work from anywhere without having to worry about the network or whether or not they need to turn on a VPN.



Ensure a great user experience

By enabling you to understand the experience of every employee for every application, zero trust allows you to consistently deliver a great user experience.



Prevent cyberthreats

Enable full SSL decryption and cyberthreat protection, not just for users, but also for cloud workloads, servers, and SaaS applications.



Simplify user and branch connectivity

Transform legacy hub-and-spoke networks by allowing branches that rely on expensive MPLS links or connecting users over VPN links to enable secure direct connectivity over the internet to any destination, regardless of where the user connects.



Zero attack surface

Adversaries can't attack what they can't see, which is why the Zscaler architecture hides source identities by obfuscating their IP addresses. Because Zscaler removes an attack vector that traditional offerings expose, it helps to prevent targeting.



Secure cloud connectivity

Workloads securely connect to other workloads using zero trust and machine learning instead of relying on extending a traditional site-to-site VPN to the cloud, and thus the same risks of lateral movement.



Data loss prevention

Inspects your traffic inline, encrypted or not, and ensures your SaaS and public cloud applications are secure, giving you the protection and visibility you need.

To learn more about the Zscaler Zero Trust Exchange, go to [zscaler.com/products/zero-trust-exchange](https://www.zscaler.com/products/zero-trust-exchange) >

