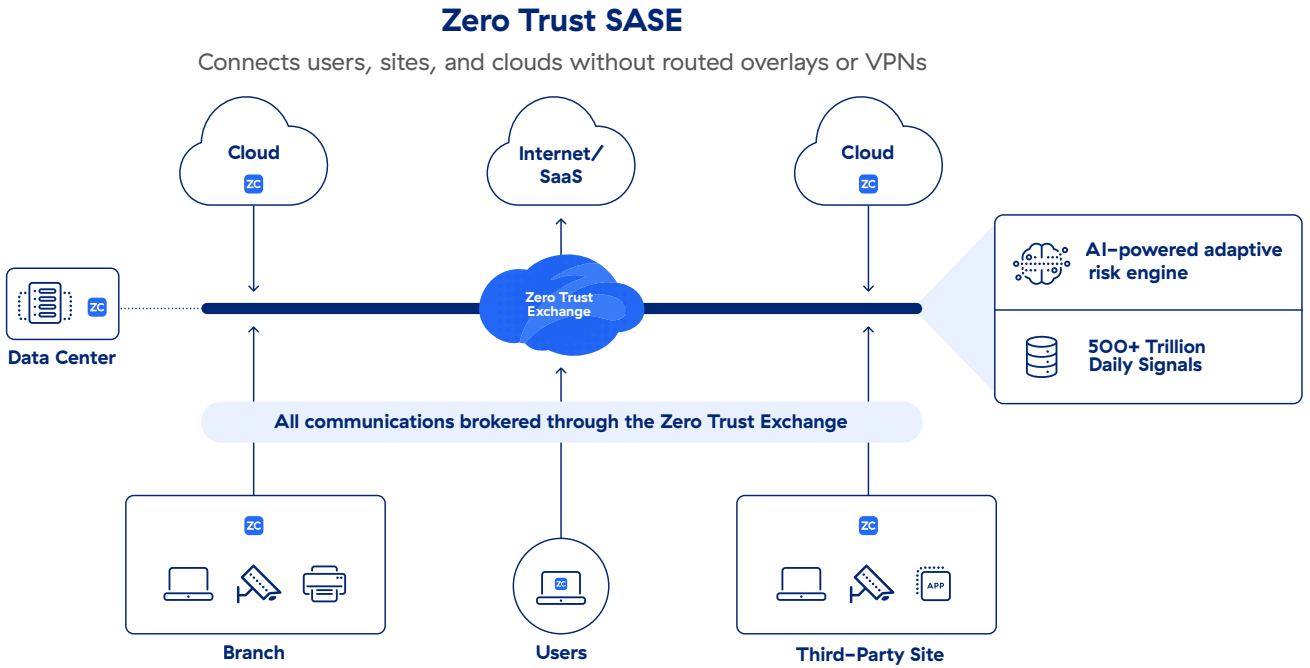
Zero Trust SASE at a Glance

Zero Trust SASE benefits:

Reduces IT cost and complexity
Easy to deploy and manage as an automated, cloud-delivered service that scales

Delivers a great user experience
Brings security and policy close to the user to eliminate unnecessary blackhaul

Reduces risk
Inline inspection of encrypted traffic at scale for threat protection and data loss prevention



Modern digital business models are allowing new levels of customer, stakeholder and employee engagement by delivering globally available access to applications and services that is consistent, no matter where they connect or what devices they are using.

The notion of network security when your users and applications are distributed is no longer viable in a digital world. Gartner developed a new model of networking and security that matches the requirements of the digital enterprise known as secure access service edge (SASE).

Zscaler's AI powered cloud security platform is a SASE service built from the ground up for performance and scalability. As a globally distributed platform, Zscaler ensures that users are always a short hop to their applications, and through peering with hundreds of partners in major internet exchanges around the world, Zscaler provides optimal performance and reliability for your users, workloads, business partners and locations.

Key Capabilities

A cloud-first architecture

Zero Trust SASE architecture helps accelerate cloud adoption by removing network and security friction through a consolidation and simplification of IT services. Without the need for device management and separate services, Zscaler offers a frictionless and transparent experience for users and standardization across locations for the IT team.

Full inline SSL inspection at scale

With the majority of traffic encrypted today, you need an AI powered proxy-based architecture that can scale for effective threat protection and data loss prevention.

Application peering and optimization

Zscaler globally peers at the edge with leading application and service providers and optimizes traffic routing to provide the best user experience.

Zero trust networking

Zero Trust SD-WAN securely connects your branches, factories and data centers through the Zero Trust Exchange — without routed overlays or implicit trust. Authenticated users gain access to only the apps for which they are authorized, without bringing them onto the network.

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 and avoids exposing the corporate network to the internet.

Cloud Delivered Security and Networking

Security Service Edge (SSE)

Cyber Threat Protection
(SWG, FWaaS, DNS Security, Sandbox, Browser Isolation)

Data Protection
(CASB, DLP)

Zero Trust User-App Access (ZTNA)

Digital Experience Management

Zero Trust Networking

Zero Trust SD-WAN

Workload Communications

To learn more about Zero Trust SASE, go to zscaler.com/capabilities/secure-access-service-edge to discover the future of network security— without the network.

zscaler™ | Experience your world, secured.™

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**.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.com