

Zscaler Zero Trust SASE

AT-A-GLANCE

Zero Trust SASE Benefits

REDUCED COST & COMPLEXITY

Consolidate multiple point products into one integrated platform with a unified policy engine and admin console to reduce operational friction and cost.

SUPERIOR SECURITY

Eliminate your attack surface and prevent lateral threat movement with true Zero Trust. Replace legacy firewalls with adaptive access and AI-powered security for all traffic.

BETTER USER EXPERIENCE

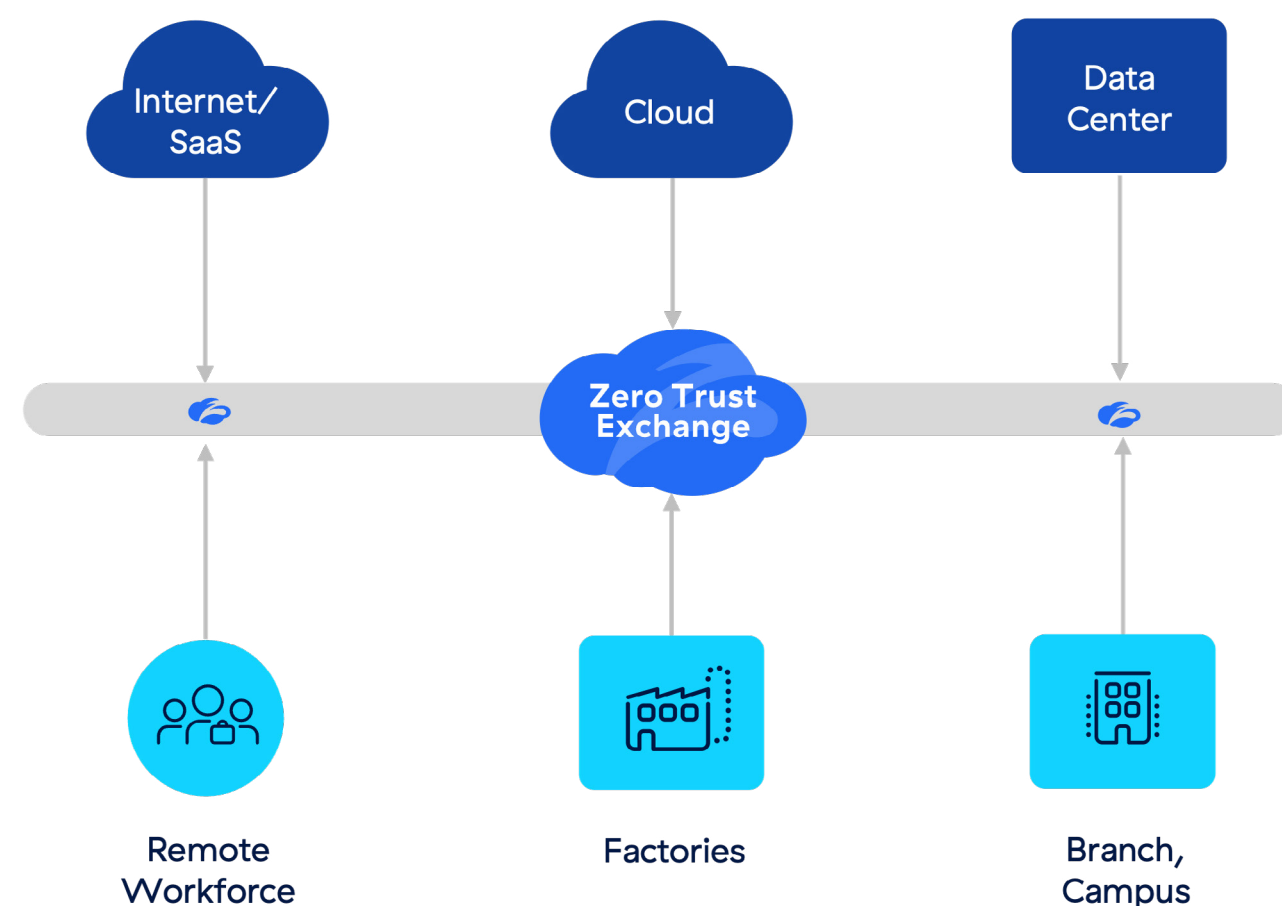
Optimize user experience across all locations—from HQ to coffee shops—by accelerating cloud migration and eliminating unnecessary traffic backhaul.

IMPROVED BUSINESS AGILITY

Scale rapidly without legacy network constraints. Accelerate M&A integration to realize value within days by connecting users directly to cross-org business apps.

Zscaler Zero Trust SASE: Unified Branch, SSE, and AI Security

Zscaler Zero Trust SASE™ is a cloud-native platform that securely connects users and branches to cloud applications. By eliminating the attack surface and preventing lateral movement, Zscaler offers the market's only true Zero Trust SASE solution, replacing legacy firewall-based approaches.



Security Service Edge (SSE)

- Cyberthreat Protection
- Data Security
- Zero Trust Access
- AI Security

Zero Trust Networking

- Zero Trust Branch
- Zero Trust Cloud
- Digital Experience
- Zscaler Cellular

Why Zscaler Zero Trust SASE

- ✓ Best-in-class cyber threat protection and data security powered by the world's largest AI security cloud
- ✓ Cloud-native platform delivered from 160+ global data centers with sovereignty controls
- ✓ Differentiated zero trust architecture that shrinks attack surface and eliminates lateral movement risk



Zero Trust SASE: Key Capabilities

Zero Trust SASE Platform

Powered by Zscaler's Zero Trust Exchange — the world's largest AI security cloud that processes over 500 billion daily transactions—Zero Trust SASE securely connects users, IoT/OT devices, AI agents and cloud apps.

- **No Attack Surface:** Prevents exposure and breaches from AI-driven threats.
- **No Implicit Trust:** Stops lateral movement and minimizes blast radius.
- **Zero Trust Everywhere:** Unified protection for users, IoT/OT, and workloads across all locations.
- **AI-Powered Security:** Uses the industry's largest dataset for adaptive access and threat protection.
- **Digital Experience:** AI-driven troubleshooting and telemetry for optimized performance.

Security Service Edge (SSE) Capabilities

Zscaler's SSE delivers comprehensive protection through a unified proxy architecture, ensuring consistent security for the web, cloud services, and private applications. Key capabilities include:

- **Secure Web Gateway (ZIA):** Full proxy inspection with AI-driven malware prevention, advanced sandboxing, and dynamic bandwidth control.
- **Zero Trust Network Access (ZPA):** Identity-based Zero Trust adaptive access that hides apps from the internet, replacing legacy VPNs and preventing lateral movement.
- **Data Security:** Visibility and protection across all data loss channels, integrating advanced AI Classification, CASB, and Data Security Posture Management (DSPM) with proven inline DLP.

Zero Trust Branch

Zscaler Zero Trust Branch securely connects sites using a zero trust architecture, eliminating complex routing and firewalls while preventing lateral movement for users and IoT/OT devices. Key capabilities include:

- **High-Performance Connectivity:** Scalable throughput from 2 Gbps to 40 Gbps.
- **Agentless Segmentation:** Native microsegmentation for IoT/OT to block lateral movement.
- **Visibility :** Automated asset discovery and traffic profiling without extra hardware or agents.

Advanced AI Security

Zscaler provides a complete AI security framework that enables safe GenAI adoption while protecting against emerging AI-native threats.

- **AI Asset Management:** Comprehensive visibility into your AI footprint across Gen AI apps, LLMs, models, MCP servers and pipelines, to help pinpoint exposure and vulnerabilities.
- **AI Access Security:** Enforce the safe use of AI applications with granular access controls and DLP protection, to ensure compliance with corporate policies.
- **Model Security (SPLX):** Integration of advanced AI red teaming and threat inspection to secure internal AI application lifecycles.



Zscaler Zero Trust SASE: Feature Overview

THREAT PROTECTION	Full proxy inspection with AI-driven malware prevention and advanced sandboxing across web, SaaS, and private applications. Includes real-time threat prevention, AI-powered phishing detection, and Zero Trust Browser
ADAPTIVE ACCESS	Dynamic, identity-based access control leveraging a real-time risk score from AI and third-party signals. The Adaptive Access Engine dynamically adjusts access, including forcing step-up authentication or browser isolation. It uses User Entity Behavior Analytics (UEBA) to detect anomalies like impossible travel and bulk uploads.
IN-LINE ON-PREMISES SECURITY CONTROLS	Zero Trust Branch replaces complex, routable SD-WAN and eliminates legacy VPNs and firewalls. It provides agentless microsegmentation for unmanaged IoT and OT devices to block lateral movement within the branch and factory.
SECURING PRIVATE APPLICATIONS	Secure Private Access (ZPA) hides private applications (including APIs and workloads) from the internet by brokering every connection through the Zero Trust Exchange and enforcing identity-based Zero Trust controls. Employing a lightweight App Connector with no inbound open ports, it shrinks the attack surface and prevents breaches. AppProtection inspects payloads with OWASP Top-10 and custom signatures.
SAAS CONTROL AND VISIBILITY	Unified visibility and control via a cloud proxy (inline) and API integrations (out-of-band CASB) ensures granular controls to allow, block, or isolate access to specific sanctioned/unsanctioned apps. It provides comprehensive risk assessment for over 90,000 SaaS apps, including plugins and code.
DATA SECURITY	Zero Trust SASE delivers a unified approach to data security, scaling visibility and protection across all data loss channels. By integrating Advanced AI Classification and Data Security Posture Management (DSPM) with proven inline DLP, Zscaler provides comprehensive control over all data, everywhere.
AI SECURITY	Complete AI security framework with inline inspection for AI apps. AI Guard & Prompt Inspection prevent data leakage via prompt inputs and file uploads. Offers full AI lifecycle security (AI-SPM, AI Red Teaming, AI Guardrails) and unified AI asset inventory.

SD-WAN

Zero Trust SD-WAN replaces complex, routable SD-WAN with a zero trust overlay. Features include intelligent app-aware traffic steering, support for routing protocols like BGP and OSPF, centralized visibility and management, and zero-touch provisioning for ZT Branch appliances.

COFFEE SHOP NETWORKING

Zero Trust SASE delivers a simplified, consistent experience for users regardless of location, minimizing networking complexity and ensuring a fast, consistent experience anywhere. Zscaler's "Cafe-like branch" concept is a disruptive approach that eliminates branch firewalls and network routing complexity.

UNIFIED PLATFORM

A single, cloud-native Zero Trust Exchange platform provides a unified proxy architecture for security across web, SaaS, and private applications. It uses a unified policy engine and admin console across all services (security and networking) to simplify workflows and reduce operational friction.

ENTERPRISE INTEGRATION

Zscaler's Zero Trust SASE features robust API-driven integrations with 150+ technology partners (SIEM, SOAR, EDR, ITSM).. Nanolog Streaming Service (NSS) pushes logs to any receiver for seamless ecosystem collaboration.

DIGITAL EXPERIENCE

Integrated Digital Experience (ZDX) monitoring provides AI-powered root cause analysis across apps, ZIA/ZPA, ISPs, and devices.

SOVEREIGNTY CONTROLS

Provides granular organizational control over the data plane, control plane, and management plane to meet specific regional sovereignty requirements. Enables control over traffic routing, inspection, and the hosting location of logs and the management plane.

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.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform 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 SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at zscaler.com or follow us on X @zscaler.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288

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

zscaler.com



**Zero Trust
Everywhere**