Simplifying Governance and Compliance with Zscaler Zero Trust Cloud

Reduce scope. Enforce controls. Automate evidence.

SOLUTION BRIEF

The rules you answer to keep changing. Multicloud, SaaS, and now AI have multiplied the places your data can go and the ways it can move. Regulators are paying attention: enterprises sent 93% more data to AI tools in 2025 than the year prior[1], and GDPR fines alone totaled €1.2B in 2025, €7.1B cumulative by January 2026[2]. It's no surprise the audit scope is constantly expanding and evidence requests are getting harder to respond to. Zscaler's Zero Trust Cloud helps you turn compliance from an episodic scramble into a continuous, automated state you can rely on day to day.

The Challenge: Achieving and maintaining compliance is harder now

Most compliance regulations were written for a network perimeter that doesn't exist anymore. Multiple workload types, identity providers and inconsistent roles across hybrid cloud environments create gaps auditors find. Flat networks and VPN adjacency broaden what's "in scope." Controls vary from one cloud or tool to the next, so enforcement is fragmented and evidence collection is manual and error-prone. Encrypted data, east—west traffic, and shadow IT mask data movement. And without unified logging and centralized governance, proving posture is time-consuming even when you're doing the right things.

Traditional network security stacks don't help enough. Appliance and virtual-firewall sprawl increases the scope of the regulated environment and allows unauthorized lateral movement. Backhauling adds latency, obscures ownership, and breaks uniform policy across clouds. The result is more busy work, higher costs, and a slower path to "audit ready." Solving this problem requires rethinking compliance at an architectural level, not just short term fixes.

[1] Zscaler 2026 AI Threat Report

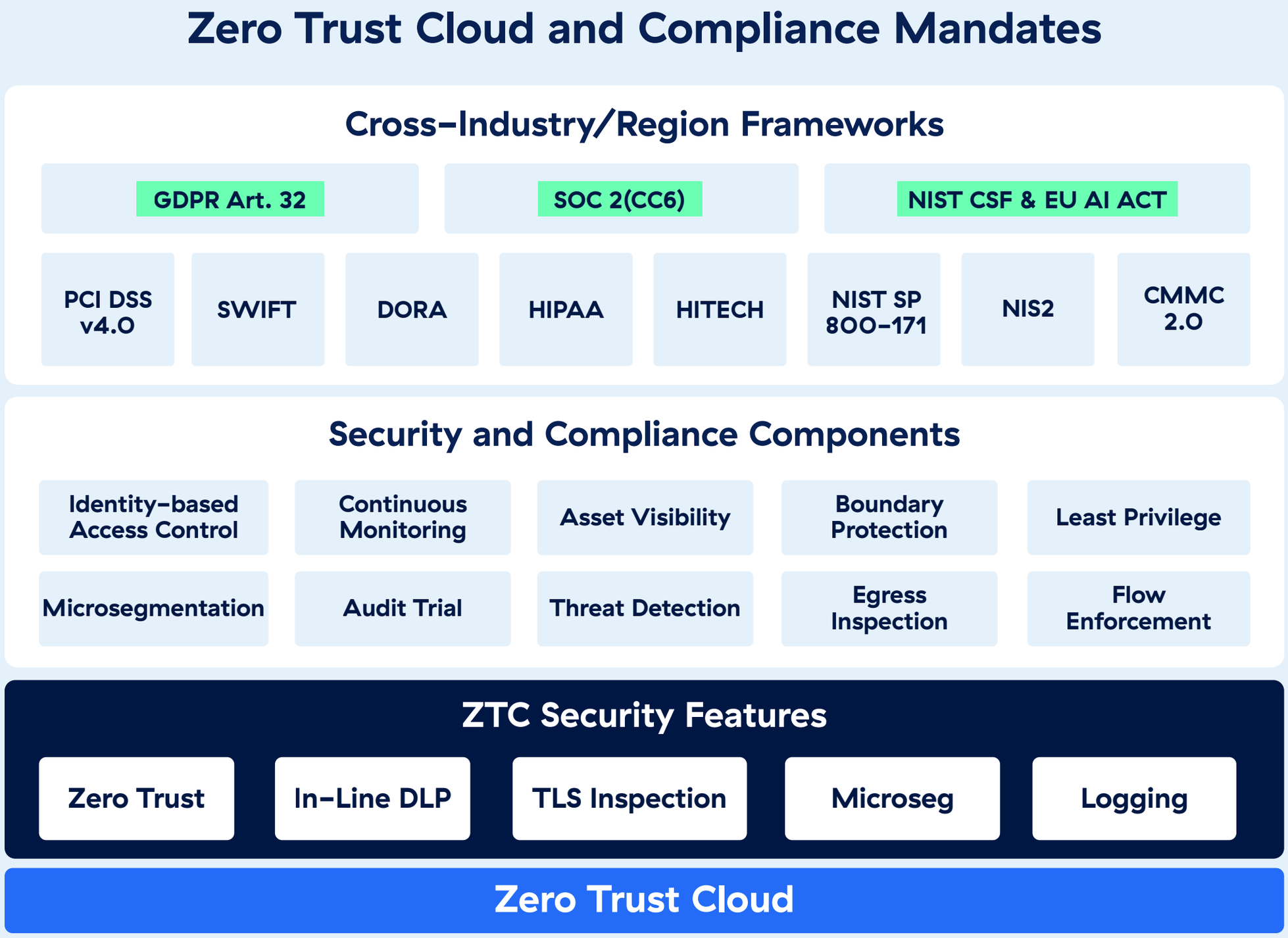
[2] DLA Piper GDPR Fines and Data Breach Survey: January 2026

[3] IBM 2025 Cost of a Data Breach Report

The Solution: Rethinking compliance with a Zero Trust approach

Data security and compliance are two sides of the same coin—one enforces, the other verifies. Zscaler—the pioneer of zero-trust security—helps simplify compliance by reimagining network security with zero trust principles from the ground-up. The results speak for themselves—organizations that have deployed zero trust architecture save $1.76M on average per breach compared to peers who have not.[3]

Zero Trust Cloud is a unified Zero Trust platform that provides secure connectivity for workloads across public and private clouds, fundamentally reducing the attack surface and preventing lateral movement. Instead of exposing networks, it makes apps invisible and connects identities directly to applications. Every connection applies least-privilege access based on identity and context. Traffic is inspected bidirectionally at cloud scale, with TLS decryption governed by privacy controls and inline DLP to detect and prevent data loss or exfiltration. App-to-app and in-app microsegmentation stops lateral movement and dramatically reduces audit scope. And all of it is automatically logged in one place—immutable, consistent, and ready for auditors.



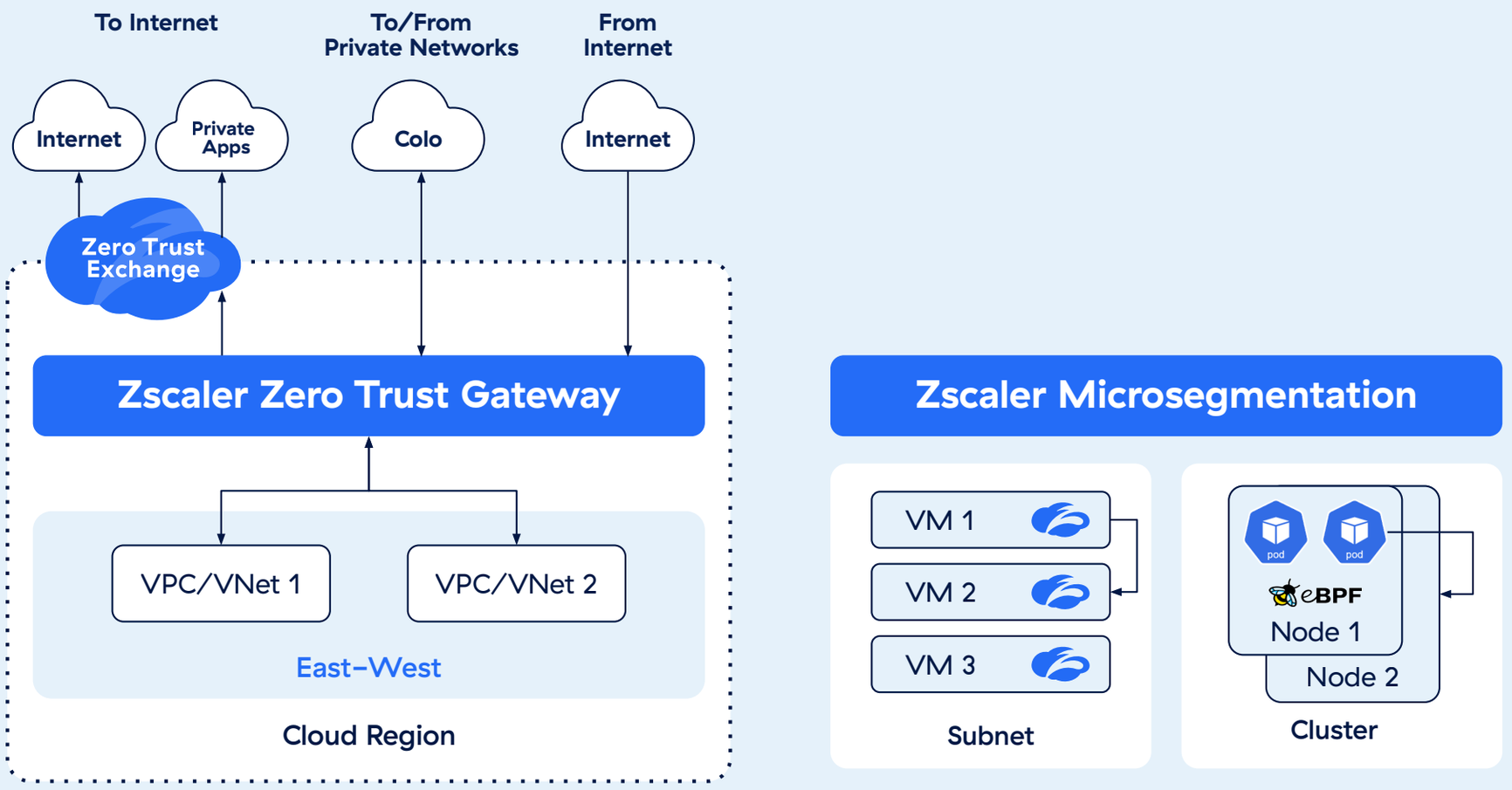
This approach supports your efforts across key frameworks like PCI DSS, HIPAA/HITECH, SOC 2, NIST 800-171/CMMC, NIS2, SWIFT/DORA, GDPR Article 32, and many more. Typical mappings include identity-based access control, boundary protection and monitoring, data loss prevention, segmentation for scope reduction, and audit and accountability through unified logs. (We don't imply certification; we help you implement and demonstrate the necessary controls).

How it fits into your architecture

Picture Internet/SaaS, public clouds (AWS, Azure, GCP), private apps in your data center or colo, and workloads talking east—west. Zero Trust Cloud (consisting of two components: Zero Trust Gateway and Microsegmentation) sits in the middle as a proxy-based service. It secures ingress, egress, and east—west flows without putting users "on the network" or exposing apps to the internet. Controls like least privilege, TLS inspection with inline DLP, microsegmentation, and unified logging apply everywhere—consistently—so you can reduce scope, enforce guardrails, and automatically generate the evidence you need.

©2026 Zscaler, Inc. All rights reserved.

Secure All Traffic Paths of your Workload Using Zero Trust Cloud

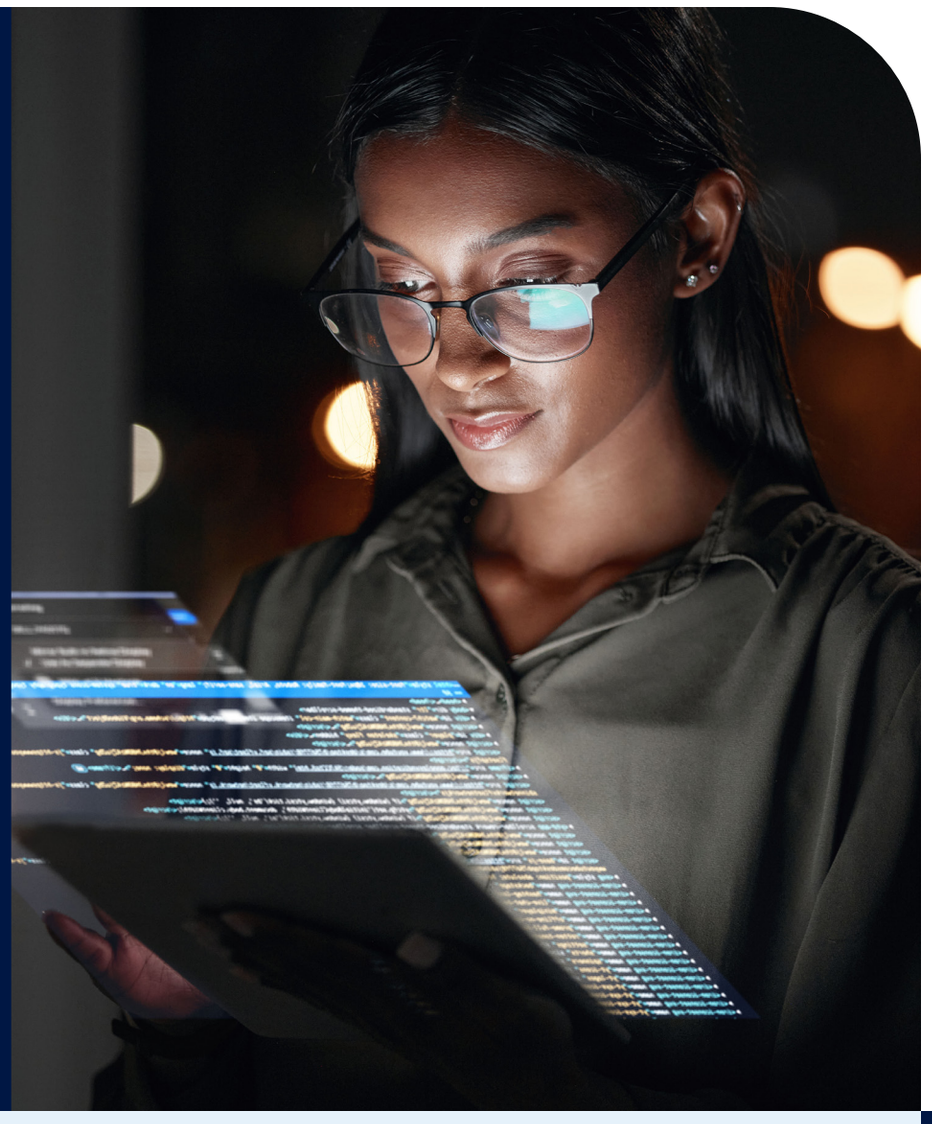


Benefits: What you get out of it

You shrink audit scope by removing inbound exposure and segmenting app-to-app flows. Evidence stops being a manual project; unified, tamper-evident logs and framework-aligned reports streamline audits. Inline protection prevents sensitive data from leaving—without waiting for an after-the-fact investigation. Policy stays consistent across ingress, egress, and east—west in AWS, Azure, GCP, and on-prem. And because one platform replaces virtual-firewall sprawl and per-cloud silos, you lower both risk and operational cost.

Zero Trust Cloud Compliance Benefits

- Boundary control and microsegmentation
- Unified visibility and automated policy enforcement
- Advanced threat detection through TLS inspection, in-line DLP
- Identity-correlated audit and continuous evidence



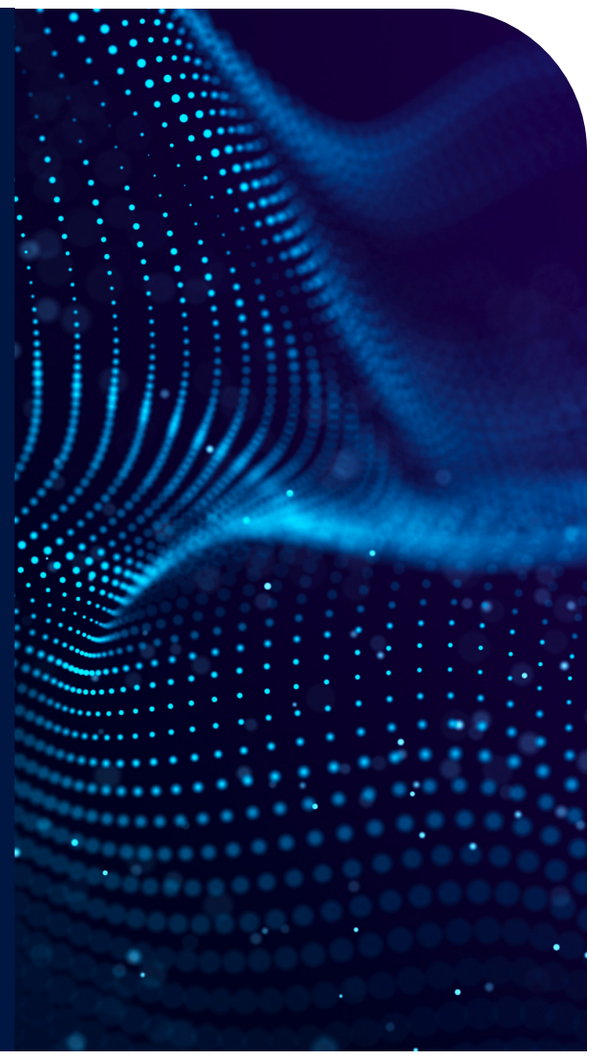
©2026 Zscaler, Inc. All rights reserved.

Why Zscaler: A single platform to enforce data security and continuous compliance

Zscaler pioneered zero trust data security at cloud scale. Our zero-exposure architecture and granular microsegmentation minimize your regulatory footprint. Bidirectional TLS inspection covers all traffic paths. Advanced inline DLP protects sensitive information in real time. Automatic logs from multicloud workloads simplify evidence collection without per-cloud silos. These unified, immutable logs feed directly into your SIEM and GRC systems, giving you verifiable proof for audits without duplication or rework. And a proxy-based, hybrid-cloud-ready design delivers the security, performance and consistency your teams expect—every day, everywhere. One platform that delivers Zero Trust data security, enforces compliance across all frameworks simultaneously, and proves posture without any extra work.

Proof in practice

- A global financial services firm unified egress inspection and standardized rules across business units to support PCI and SWIFT, using centralized logs to accelerate audits.
- A large health insurer deployed TLS inspection and inline DLP to safeguard PHI under HIPAA/HITECH while microsegmentation reduced scope.
- A major pharma retailer consolidated per-cloud tools, establishing repeatable, auditable architectures that support PCI DSS 4.0.



Zscaler supports your compliance efforts. Your audit team remains the authority for exact framework language and evidence requirements; our role is to help you enforce the right controls everywhere and prove it without the scramble.

Learn more by visiting the Zscaler Compliance Center or the Zero Trust Cloud page.

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 Twitter **@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**

zscaler™

Act Fast.
Stay Secure.