Provide Secure, Reliable, and Seamless Access to the Internet, Apps and Data

zscaler™

DATASHEET

The Challenges of Securing the Hybrid Workforce

Organizations today face significant challenges as they navigate the complexities of a rapidly evolving digital landscape and strive to find the right balance of productivity, agility, and security:

- Traditional firewalls and VPNs create critical blind spots, exposing systems to sophisticated cyber threats
- Siloed tools and multiple point products complicate operations, consume budget and resources with no guarantee of scalability
- Unexpected disruptions prevent ensuring business continuity for the hybrid workforce while leveraging distributed infrastructure

Combined with increasing cybersecurity demands and cost pressures, leaders are further challenged to balance operational resilience, risk management, and employee productivity. Meanwhile, hybrid workers expect seamless, reliable access to resources, yet legacy architectures introduce latency and poor user experiences. To stay competitive, businesses must enhance visibility to secure data, streamline operations, and evolve architectures to prioritize agility, scalability, and user experience.

Secure, reliable and high-performance access to the internet, SaaS and private apps for any user, anywhere

As the world's largest cloud security platform, Zscaler offers a cloud-native approach to security enforcing context-aware security policies, blocking lateral movement, and proactively detecting threats in real time, minimizing business risk and protecting critical resources.

Zscaler delivers a comprehensive, AI-powered solution that ensures secure, reliable, and high-performance access to the internet, SaaS applications, and private resources for any user—employees, contractors, or third parties—on any device, from any location.

The solution consolidates point products into a unified platform, eliminating costly hardware and reducing operational complexity. Advanced AI capabilities provide real-time visibility, root cause analysis, and proactive policy enforcement to optimize digital experiences for users.

Key Benefits

Minimize Business Risk

Apply zero trust principles and AI-powered security solutions to reduce the attack surface, prevent compromise, halt lateral movement, and stop data loss.

- Block known threats on all ports and protocols with a cloud-native proxy architecture that delivers full inspection and blocks threats using AI-powered security controls backed by the world's largest security cloud.
- Stop unknown and evasive threats with inline cloud sandboxing and a Zero Trust Browser that isolates suspicious web traffic.
- Reduce the attack surface by eliminating exploitable hardware, hiding applications from the internet, and using granular AI-powered user-to-app segmentation.

Improve End-User Productivity

Enable fast, secure, and seamless access to apps for employees and third parties anywhere, with the visibility and control to optimize digital experiences.

- Zscaler's 160 global datacenters enforce policies and broker access at the edge without backhauling, thus eliminating latency and delivering better performance than VPNs and legacy firewalls.
- Achieve end-to-end visibility across all locations, users, devices, and applications to optimize performance and drive collaboration, with insights into network performance—benchmarking ISP and last-mile connectivity, monitoring Wi-Fi trends, and Zero Trust environments—alongside application response times and device health metrics like CPU, memory, and disk usage.
- Leverage unified insights and use AI to pinpoint root causes in minutes, empowering network operations, support, and security teams to deliver seamless user experiences everywhere.
- Ensure resilience with business continuity capabilities that keep users productive while protecting organizations across blackouts, brownouts, and even rare black swan failure events.

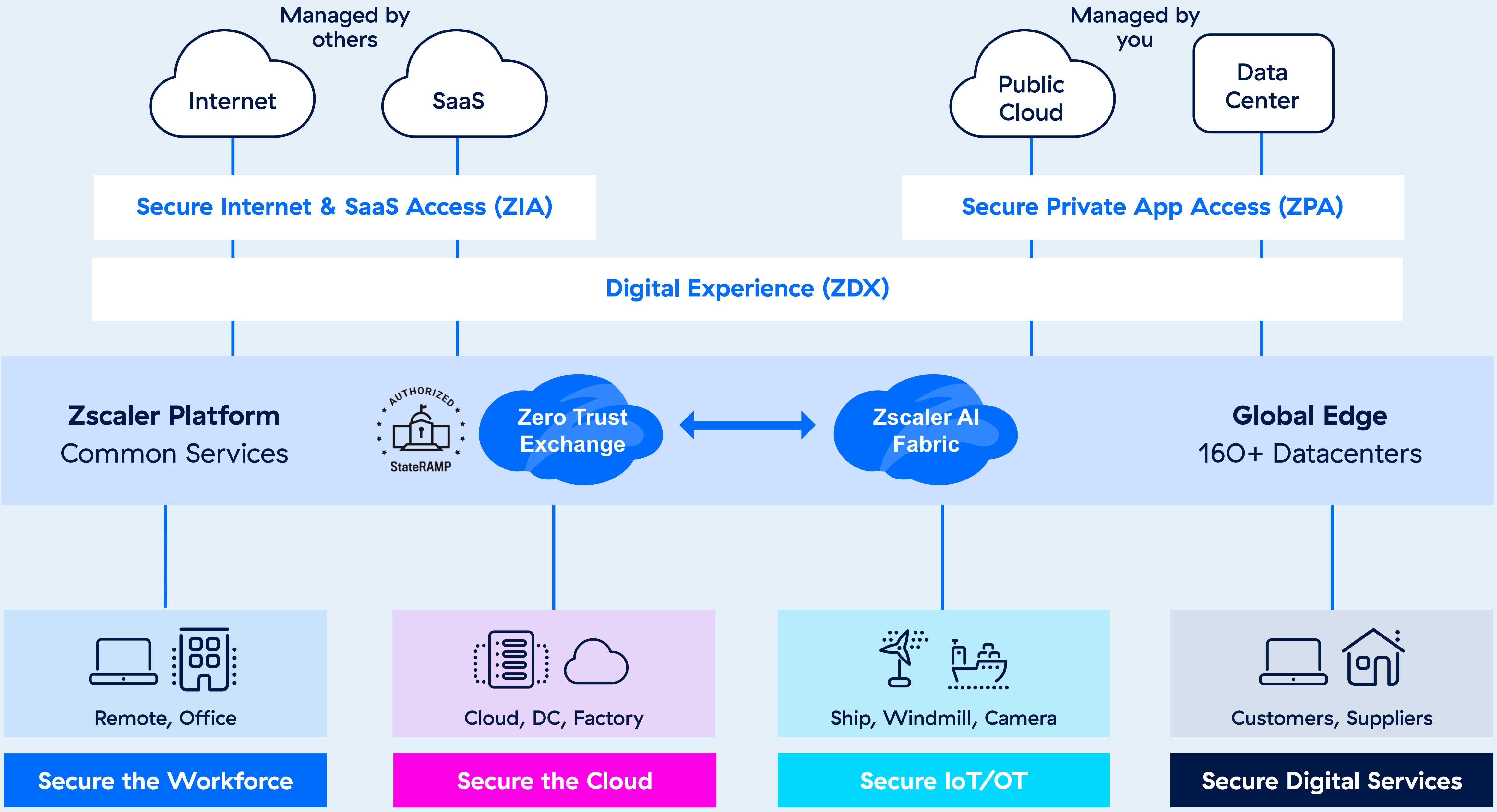
Lower Cost and Complexity

Eliminate capex and overhead from legacy technology like VPNs and firewalls, and simplify your network with fast, secure, direct-to-cloud access. Advanced AI capabilities provide real-time visibility, root cause analysis, and proactive policy enforcement to optimize digital experiences for users.

- Build one set of access policies that is managed centrally and enforced globally by Zscaler's distributed cloud-native infrastructure.
- Eliminate siloed point products to reduce hardware and operational costs.
- Consolidate visibility into a single pane view with a user-friendly unified console, and generative AI-powered copilot for administrative ease of use.

Empower Your Organization with a Zero Trust Architecture

Zscaler's Zero Trust Exchange is the world's largest security cloud platform that delivers comprehensive security for users, devices, workloads and applications. The platform is built on the principle of least-privileged access to establish trust based on user identity and context—including location, device, application, and content—and then creates secure, direct user-to-app, app-to-app, and machine-to-machine connections.



Managed by others

Internet

SaaS

Managed by you

Public Cloud

Data Center

Secure Internet & SaaS Access (ZIA)

Secure Private App Access (ZPA)

Digital Experience (ZDX)

Zscaler Platform
Common Services

AUTHORIZED StateRAMP

Zero Trust Exchange

Zscaler AI Fabric

Global Edge
160+ Datacenters

Remote, Office

Cloud, DC, Factory

Ship, Windmill, Camera

Customers, Suppliers

Secure the Workforce

- User to App Segmentation
- Secure BYOD
- No VDI, No VPN

Secure the Cloud

- Workload Segmentation
- Secure SaaS Data
- Secure Cloud Data

Secure IoT/OT

- Discovery and Control
- Privileged Access
- Device Segmentation

Secure Digital Services

- App Portal Access
- Site-to-Site Communications
- Guest WiFi

Use Cases

Secure Internet and SaaS Access and Replace Secure Web Gateway (SWG)

Legacy SWG appliances cannot keep pace with the modern distributed workforce's need for fast, scalable, and remote-friendly solutions. With our industry-leading AI-powered, cloud-native secure web gateway, you can secure internet and SaaS access from any location without hindering performance with inline inspection of all ports, protocols, and encrypted traffic to block advanced threats. AI-powered threat intelligence helps stop known and unknown threats in real time using inline sandboxing and machine learning.

Provide Secure Application Access and Replace VPN

VPNs have several weaknesses that introduce significant security risk including granting implicit trust, increasing the risk of lateral movement for attackers after they gain network access. VPNs also put your organization on attackers' radar: public IP addresses broadcast their existence along with any vulnerabilities that threat actors can easily exploit. With Zscaler you can connect specific users directly to authorized apps without exposing applications to the public internet. Zscaler Private Access provides zero trust network access (ZTNA) for secure, fast, and scalable access to private applications without the friction, risk, or inefficiency of legacy VPNs.

Secure Third-Party Application Access and Replace VDI

Traditional approaches to providing access to business partners and vendors rely on legacy solutions like VPNs that often over-permission access and increase risk, or VDI that is prohibitively expensive and difficult to manage. With Zscaler you can provide third-party vendors, contractors, or partners with secure, limited access to specific applications and resources on managed or unmanaged devices without compromising security.

Enable Secure Mergers and Acquisitions (M&A)

M&A activities often lead to mismatched infrastructure, making it challenging to unify IT assets across organizations, some of which include legacy solutions that create prolonged timelines to integrate access and create secure connectivity across entities. Traditional perimeter-based tools also fail to dynamically support rapidly changing business needs during M&A. But Zscaler accelerates time-to-productivity with seamless and secure connectivity between newly acquired users, systems, and applications during M&A activities, without introducing security risks.

Ensure Highly Performant User Experience

Hybrid workforces depend on a reliable application experience, yet poor connectivity and infrastructure issues degrade productivity. Network Operations teams often lack visibility into network performance across ISP, Wi-Fi, and home-office environments, making it difficult to identify and resolve problems. These limitations don't exist with Zscaler: you can deliver consistently fast and seamless digital experiences for users by maximizing application performance and minimizing friction.

Solution Capabilities

Zscaler Internet Access: Secure Internet & SaaS Access

Protect your users from evolving attacks with comprehensive zero trust threat protection at the speed and scale of the cloud. Inspect 100% of TLS/SSL-encrypted traffic inline to protect against advanced threats and data loss. Gain industry-leading protection with Zero Trust Firewall, Cloud Sandbox, and Zero Trust Browser that replace other point solutions with a unified platform that's powered by AI-driven threat detection.

- **Stay safe from ransomware and other threats:** Minimize the attack surface, stop compromise, eliminate lateral movement, and prevent data loss.
- **Reduce costs and complexity:** Simplify your network with fast, secure, direct-to-cloud access that removes the need for edge and branch firewalls.
- **Protect data:** Prevent loss of data from users, SaaS apps, and the public cloud due to accidental exposure, theft, or double extortion ransomware.
- **Secure your hybrid workforce:** Empower employees, customers, and third parties to securely access web apps and cloud services from anywhere, on any device—with a great digital experience.

"Zscaler provides modern architecture that has less of a surface area for attack. It really is a platform that allows us flexibility as we move forward and the ability to create simplicity in our network environment and simplicity gives us the ability to move quickly."
—Ryan Winn, Chief Information Security Officer, AdventHealth

Zscaler Private Access: Secure Access to Private Apps

Enable fast, reliable connectivity with the world's most deployed zero trust network access (ZTNA) solution.

- **Replace vulnerable VPN solutions:** Reduce the attack surface and eliminate lateral movement by connecting users directly to applications—not the network, elevating your security posture.
- **Prevent private app compromise:** Minimize the risk of app compromise and data loss with full inline inspection of private app traffic and data loss prevention.
- **Empower your hybrid workforce:** Seamlessly extend lightning-fast access to private apps across remote users, HQ, branch offices, and third parties.
- **Reduce cost and complexity:** Offer secure, optimized access, without costly and complex point products, through a unified, cloud native ZTNA platform for users, workloads, and IoT/OT.
- **Enable privileged remote access:** Secure user connectivity to servers, jump hosts and bastion hosts, or desktops using Remote Desktop Protocol (RDP), Secure Shell (SSH), or Virtual Network Computing (VNC) from the end user's modern browser without installing Zscaler Client Connector or any browser plugins.

"For a workforce that's nearly 100% remote, ZPA offers a seamless experience, provides vastly improved protection, and reduces the support burden."
—Anthony Cunha, CISO, Mercury Financial

Zscaler Digital Experience:
Proactively monitor and optimize the user experience

Ensure users everywhere get great performance, from device to ISP to cloud proxy to app and back, with no need for VPNs, firewalls, or siloed management tools. See from the end user's perspective to optimize performance and rapidly fix app, network, and device issues.

- **Get end-to-end visibility:** Gather metrics from users' devices, over multiple networks, to apps and services—even those not in your control.
- **Reduce help desk tickets:** Detect and fix IT issues. with AI-powered root cause analysis, before they affect users.
- **Consolidate multiple monitoring tools:** Simplify your monitoring stack with a single end-to-end view, reducing costs and effort.
- **Turn the lights on in minutes:** Simply enable ZDX once you've installed Client Connector. There's nothing else to deploy.

"Using ZDX we can rule out our network in minutes and focus the CSR's attention on their internet connectivity issue."
—Peeyush Patel, CIO and CISO, Careem

Zscaler Risk360:
Visualize and remediate cybersecurity risk with actionable insights

Provides guidance on top cyber risk drivers, recommended investigative workflows, trend and peer comparisons, and actionable CISO board slides. The model spans across the four stages of attack — external attack surface, compromise, lateral propagation, and data loss — and all the entities in your environment, including assets, applications, and users.

- **Unified dashboard:** Replace multiple tools and spreadsheets with an interactive, data-driven dashboard that provides a holistic view of risk.
- **Expansive correlation:** Leverage our cloud native platform for correlated risk views of your workforce with Zscaler data.
- **Deeper risk insights:** Turn data insights into actionable, policy-driven mitigation recommendations to improve your risk score and ultimately your risk posture.
- **Financial risk summary:** Map risk directly to your potential financial exposure for better decision-making and prioritized remediation.

"With Risk360, we gain a more comprehensive picture of cyber risks and actionable ways to remediate them. It is an invaluable tool for risk management, providing us with both a broad and deep view into risk exposure and how it could potentially affect the bottom line."
—Debashis Singh, CIO, Persistent Systems Ltd.

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**.

zscaler™

Zero Trust Everywhere