DATA SHEET

Zscaler Internet Access

AI-powered protection for all users, all apps, all locations

Zscaler Internet Access™ defines safe, fast internet and SaaS access with the industry's most comprehensive zero trust platform.

Legacy network security has become ineffective in a cloud- and mobile-first world

Legacy hub-and-spoke architectures were effective when users were located primarily at headquarters or in a branch office, applications resided solely in the corporate data center, and your attack surface was limited to what your organization sanctioned. Today, we live in a drastically different world, with a threat landscape in which ransomware, encrypted threats, supply chain attacks, and other advanced threats break through legacy network defenses. It's time to find a cloud native security solution that holistically reduces risk and complexity while enabling flexibility to help drive business initiatives forward.

Zscaler Internet Access

Securing today's cloud- and mobile-first enterprise requires a fundamentally different approach built on zero trust. Zscaler Internet Access, part of the Zscaler Zero Trust Exchange™, is the world's most deployed security service edge (SSE) platform, built on a decade of secure web gateway leadership.

Benefits:

- **Prevent cyberthreats and data loss with AI:** Protect your organization against advanced threats with a suite of AI-powered cyberthreat and data protection services, enriched by real-time updates sourced from 500 trillion daily threat signals from the world's largest security cloud.
- **Get an unmatched user experience:** Get the world's fastest internet and SaaS experience (up to 40% faster than legacy security architectures) to boost productivity and increase business agility.
- **Modernize your security architecture:** Realize 139% ROI with Zscaler by replacing 90% of your costly, complex, and slow appliances with a fully cloud-native zero trust platform.

Delivered as a scalable SaaS platform from the world's largest security cloud, it eliminates legacy network security solutions to stop advanced attacks and prevent data loss with a comprehensive zero trust approach, offering:

Best-in-class, consistent security for today's hybrid workforce: When you move security to the cloud, all users, apps, devices, and locations get always-on threat protection based on identity and context. Your security policy goes everywhere your users go.

Lightning-fast access with zero infrastructure: Direct-to-cloud architecture ensures a fast, seamless user experience. This eliminates backhauling, improves performance and user experience, and simplifies network administration—with no physical infrastructure, ever.

AI-powered protection from the world's largest security cloud: Inline inspection of all internet and SaaS traffic, including SSL decryption, with a suite of AI-powered cloud security services to stop ransomware, phishing, zero-day malware, and advanced attacks based on threat intelligence from 500 trillion daily signals.

Simplified management: Using a cloud native security solution infused with AI, no hardware to manage, streamlined workflows, and business-focused policy creation frees up valuable time for your team to focus on strategic goals.

Integrated, AI-powered security and data protection services

Zscaler Internet Access includes a comprehensive suite of AI-powered security and data protection services to help you stop cyberattacks and data loss. As a fully cloud-delivered SaaS solution, you can add new capabilities without any additional hardware or lengthy deployment cycles. The modules available as part of Zscaler Internet Access are:

- **Cloud Secure Web Gateway (SWG):** Deliver a safe, fast web experience that eliminates ransomware, malware, and other advanced attacks with real-time, AI-powered analysis and URL filtering.
- **Cloud Access Security Broker (CASB):** Secure cloud apps with integrated CASB to protect data, stop threats, and ensure compliance across your SaaS and IaaS environments.
- **Cloud Data Loss Prevention (DLP):** Protect data in motion with full inline inspection and advanced measures like exact data match (EDM), optical character recognition (OCR), and machine learning.

Gartner

Zscaler named a Leader in the 2024 Gartner® Magic Quadrant™ for Security Service Edge*

See More →

*Gartner Magic Quadrant for Security Service Edge, 10 April 2023, Charlie Winckless, et al.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.

- **Zscaler Firewall & cloud IPS:** Extend industry-leading protection to all ports and protocols, and replace edge and branch firewalls with a cloud native platform.
- **Zscaler Sandbox:** Stop never-before-seen and elusive malware across web and file transfer protocols with AI-driven quarantine, sharing consistent and global protection across all users in real time.
- **AI-Powered Cloud Browser Isolation:** Make web-based attacks obsolete and prevent data loss by creating a virtual air gap between users, the web, and SaaS.
- **Digital Experience Monitoring:** Reduce IT operational overhead and speed up ticket resolution with a unified view of application, cloud path, and endpoint performance metrics for analysis and troubleshooting.
- **Zero Trust Branch Connectivity:** Reduce risk and complexity with non-routable branch and data center connectivity for users, servers, and IOT/OT devices.
- **DNS Security:** Optimize DNS security and performance for all users, devices, and applications, on all ports and protocols, anywhere in the world.

Zscaler Internet Access for Users and Workloads

Eliminate risk for cloud workloads accessing any internet or SaaS destination with Zscaler Internet Access. By removing the need for workloads to access the internet through legacy, network-centric tools such as VPNs, firewalls (including virtual firewalls), or WAN technologies, you can prevent compromise and stop lateral movement without requiring a patchwork of security tools. By applying ZIA's comprehensive suite of security and data protection capabilities to workloads, you can unify zero trust security for your users and workloads with a single, integrated platform.

By pairing ZIA with Zscaler Private Access, you can extend protection to your private apps and workloads, whether they reside in the public cloud or a private data center.

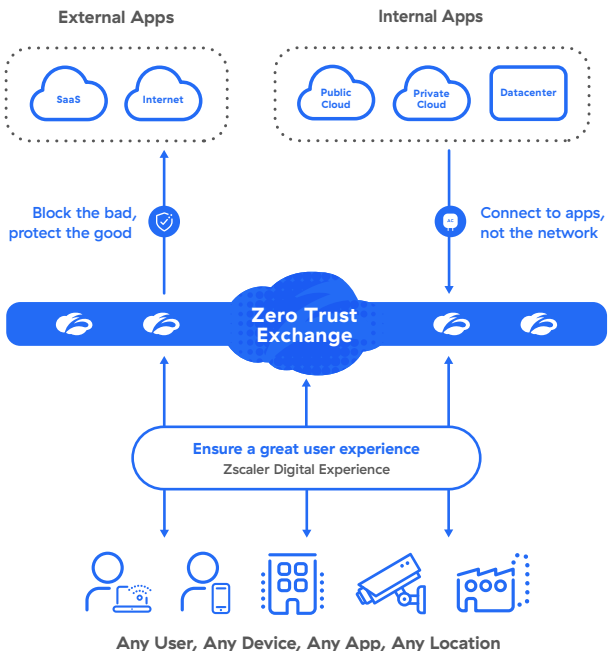

Figure 1: The Zero Trust Exchange

Use cases

Cyberthreat and ransomware protection

Move from legacy network security to Zscaler's revolutionary zero trust architecture that prevents compromise, eliminates the attack surface, stops lateral movement, and keeps data safe.

Learn More →

Secure hybrid workforce

Empower employees, partners, customers, and suppliers to securely access web applications and cloud services from anywhere, on any device—and ensure a great digital experience.

Learn More →

Data protection

Stop data loss from users, SaaS apps, and public cloud infrastructure from accidental exposure, data theft, or double-extortion ransomware.

Learn More →

Infrastructure modernization

Eliminate costly, complex networks with fast, secure, direct-to-cloud access that removes the need for edge and branch firewalls.

Learn More →

The Zscaler Zero Trust Exchange Ecosystem

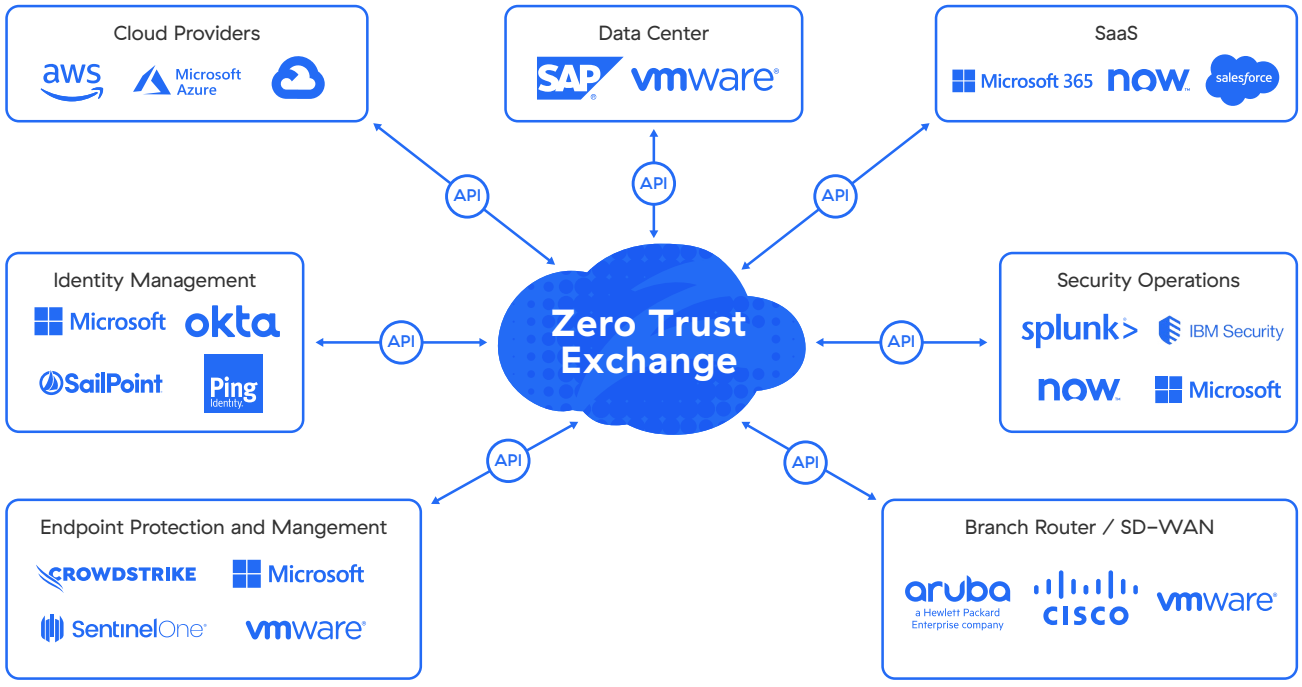

Figure 2: Zscaler Internet Access partner ecosystem

TABLE 1: ZSCALER INTERNET ACCESS FEATURES AND CAPABILITIES	
FEATURE	**DETAILS**
Capabilities	
URL filtering	Allow, block, caution, or isolate user access to specified web categories or destinations to stop web-based threats and ensure compliance with organizational policies.
SSL inspection	Get unlimited TLS/SSL traffic inspection to identify threats and data loss hiding in encrypted traffic. Specify which web categories or apps to inspect based on privacy or regulatory requirements.
DNS security	Identify and route suspicious command-and-control connections to Zscaler threat detection engines for full content inspection.
File control	Block or allow file download/upload to applications based on app, user, or user group.
Bandwidth control	Enforce bandwidth policies and prioritize business-critical applications over recreational traffic.
Advanced threat protection	Stop advanced cyberattacks like malware, ransomware, supply chain attacks, phishing, and more with proprietary advanced threat protection. Set granular policies based on your organization's risk tolerance.
Inline data protection (data in motion)	Use forward proxy and SSL inspection capabilities to control the flow of sensitive information to risky web destinations and cloud apps in real time, stopping internal and external threats to data. Advanced inline protection is provided whether an app is sanctioned or unmanaged without requiring network device logs.
Out-of-band data protection (data at rest)	Use API integrations to scan SaaS apps, cloud platforms, and their contents to identify sensitive data at rest and remediate automatically by revoking risky or external shares, for example.
Intrusion prevention	Get complete threat protection from botnets, advanced threats, and zero-days, along with contextual information about the user, app, and threat. Cloud and web IPS works seamlessly across Firewall, Sandbox, DLP, and CASB.
Dynamic, risk-based access and security policy	Automatically adapt security and access policy to user, device, application, and content risk.
Traffic Capture	Seamless Packet Capture: easily capture decrypted traffic via specific criteria within Zscaler policy engines, supporting efficient security forensics without requiring additional appliances.
Malware analysis	Detect, prevent, and quarantine unknown threats hiding in malicious payloads inline with advanced AI/ML to stop patient-zero attacks.
DNS filtering	Control and block DNS requests against known and malicious destinations.
Web isolation	Make web-based threats obsolete by delivering active content as a benign stream of pixels to the end user's browser.
Correlated threat insights	Speed investigation and response times with contextualized and correlated alerts with insights into threat score, affected asset, severity, and more.
Application isolation	Allow safe, agentless unmanaged device access to SaaS, cloud, and private apps with granular control over user actions like copy/paste, upload/download, and print to stop sensitive data loss.
Digital experience monitoring	Get a unified view of application, cloud path, and endpoint performance metrics for analysis and troubleshooting.
Zero Trust Branch Connectivity	Modernize branch connectivity through the Zero Trust Exchange, eliminating the attack surface and preventing lateral movement.
Workload-to-internet communication protection	Prevent compromise and stop lateral movement for workload-to-internet communications. Includes SSL inspection, IPS, URL filtering, and data protection for all communication.
IoT Device Visibility	Gain a complete view of all IoT devices, servers, and unmanaged user devices across your business, with automated discovery, continuous monitoring, and AI/ML classification with industry-leading auto-labeling capabilities

FEATURE	DETAILS
Platform features	
Flexible connectivity options	• **Zscaler Client Connector (ZCC):** Forward traffic to the Zero Trust Exchange via a lightweight agent that supports Windows, macOS, iOS, iPadOS, Android, and Linux. • **GRE or IPsec tunnels:** Use GRE and/or IPsec tunnels to send traffic to the Zero Trust Exchange for devices without ZCC. • **Browser isolation:** Seamlessly connect any BYOD or unmanaged devices with integrated Cloud Browser Isolation. • **Proxy chaining:** Zscaler supports forwarding traffic from one proxy server to another, but this is not recommended in production environments. • **PAC files:** Send traffic to the Zero Trust Exchange with PAC files for devices without ZCC.
Cloud-delivered deployment	100% cloud-native platform delivered as a SaaS service. For unique use cases, private and virtual service edges are available.
Data privacy and retention	When logging data, content is never written to the disk and there are granular controls to determine where exactly logging takes place. Use role-based access control (RBAC) to provide read-only access, username anonymization/obfuscation, and separate access rights by department or function, in accordance with key compliance regulations. Data is retained for a rolling period of six months or less, depending on the product. You can purchase additional storage that retains data for as long as desired.
Key compliance certifications	Certifications include: • FedRAMP • ISO 27001 • SOC 2 Type II • SOC 3 • NIST 800-63C See the full list of our compliance certifications here.
Granular API support	We maintain REST API integrations with numerous identity, networking, and security vendors. For example, you can share logs between Zscaler and your cloud-based or on-prem SIEM (e.g. Splunk). Learn more
Direct peering	Direct peering with major internet and SaaS providers and public cloud destinations ensures the fastest traffic path possible.
Service level agreements (SLAs)	
Availability	99.999%, measured by transactions lost
Proxy latency	< 100 ms, including when threat and DLP scanning is on
Virus capture	100% of known viruses and malware
Supported platforms & systems	
Client Connector	Support for: • iOS 9 or later • Android 5 or later • Windows 7 and later • Mac OS X 10.10 and later • CentOS 8 • Ubuntu 20.04 Learn more
Branch Connector	Support for: • VMware vCenter or vSphere Hypervisor • Centos • Redhat

Zscaler Internet Access Editions

	Capabilities	Essentials	Business	Transformation	Unlimited
Platform Services		Content Filtering, Inline AV, SSL Inspection, Nanolog streaming	(+) SSL Private Certificate	(+) Cloud NSS, NSS Log recovery, Extended DC Access IPSec Tunnel, Contextual Alerts, ZIA Virtual Pvt Service Edge (8)	(+) Source IP Anchoring, Test Environment, Priority categorization, ZIA Virtual Pvt Service Edge (32) Server & IoT Protection (1 GB/10u)
Threat Protection	**Advanced Threat Protection (incl. AI-powered phishing & C2 detection)** Protection against known and unknown threats (URL, AV, Botnet/C2, Phishing)	✓	✓	✓	✓
	Cloud Sandbox Zero Day Attack prevention by analyzing suspicious files with AI-powered quarantine	Add-on	Add-on	✓	✓
	Isolation – Cyber Threat Protection Zero Day Attack protection from suspicious web content. AI-powered risk-based Isolation	Add-on	Add-on	Isolation for Cyber Protection: Std (100MB/user/mo.)	Isolation for Cyber Protection: Std (1.5GB/user/mo.)
	Correlated Threat Insights Speed investigations and response time with contextual threat intelligence	–	✓	✓	✓
	Dynamic Risk-Based Policy Automatically adapts and recommends security policies based on various risk factors	–	–	✓	✓
	Integrated Deception Boost your zero trust security posture by proactively luring, detecting, and intercepting active attackers	–	–	Standard[1]	Standard[1]
Network Transformation	**DNS Resolution & Filtering** Trusted DNS Resolver for geocentric and optimal DNS resolution	Up to 64 rules	Up to 64 rules	✓	✓
	DNS Tunnel Detection Detect and prevent DNS-based attacks and data exfiltration through DNS tunnels	–	–	✓	✓
	Bandwidth Control Traffic control and bandwidth prioritization, rate limiting for web traffic		✓	✓	✓
	Cloud Firewall Work-from-anywhere protection for all users and traffic(both web and non-web) with infinite SSL inspection	Network, Application Services, Locations, FQDNs up to 10 rules	Network, Application Services, Locations, FQDNs up to 10 rules	(+) work-from-anywhere users + locations, deep packet application inspection	(+) work-from-anywhere users + locations, deep packet application inspection
	Protection for unauthenticated traffic Protect networks with fully automated carrier-grade security with limitations	0.5 GB /user/mo.	1 GB /user/mo.	1.5 GB /user/mo.	2 GB /user/mo.

	Capabilities	Essentials	Business	Transformation	Unlimited
Protect Data and Prevent Data Loss	**Cloud App Control + Tenancy Restrictions** Find and control use of risky or unsanctioned apps (Shadow IT)	✓	✓	✓	✓
	Isolation – Data protection (SaaS) Prevent data loss from SaaS apps to BYOD or unmanaged endpoints (clientless)	Add-on	Add-on	Add-on	Isolation for Data Protection (SaaS): Std. (100MB/user/mo.)
	DLP, CASB, Inline Web Essentials, SaaS API (1-app) Prevent the loss of sensitive data to the internet. Scan 1 SaaS App for risky sharing of sensitive data or malware	–	Data Protection Std (DLP and CASB Essentials)	(+) SaaS API Retro Scan	✓
	SaaS API, SaaS Supply Chain Security, Unmanaged Devices, Classification, Incident Management Benefits of Standard Data Protection plus: Control BYOD risks by streaming data as pixels, scan multiple SaaS apps for risky sharing/malware, customize DLP with EDM, IDM, OCR, and tools for incident management and workflow automation	Add-on	Add-on	Add-on	✓
Digital experience monitoring	Monitor digital experiences from the end user to optimize performance and rapidly fix offending application, network and device issues	–	Standard	Standard	Standard
Premium Support Plus		Add-on	Add-on	Add-on	✓

Licensing model

All Zscaler Internet Access editions are priced per user. For certain products inside of your edition, pricing may vary outside of user count. For more information on pricing, talk to your Zscaler account team.

Part of the holistic Zero Trust Exchange

The Zero Trust Exchange enables fast, secure connections and allows your employees to work from anywhere using the internet as the corporate network. Based on the zero trust principle of least-privileged access, it provides comprehensive security using context-based identity and policy enforcement.

> "When ransomware attacks happen to other companies, thousands of systems in their environment are crippled, in addition to having serious impacts with having to pay a ransom. When this kind of event hits the news, I get worried calls from executives, and it warms my heart to tell them, 'We're fine.'."
>
> **Ken Athanasiou,** VIP & CISO, AutoNation

zscaler™ | Experience your world, secured.™

About Zscaler

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 SSE-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