Zscaler Internet Access

KI-gestützter Schutz für alle User, alle Anwendungen, alle Standorte

DATENBLATT

Zscaler Internet Access™ gewährleistet sicheren und schnellen Zugriff auf Internet und SaaS-Anwendungen mit der branchenweit funktionsreichsten Zero-Trust-Plattform.

Herkömmliche Netzwerksicherheit ist in einer cloudzentrierten Mobile-first-Welt nicht mehr zeitgemäß

Herkömmliche Hub-and-Spoke-Architekturen waren effektiv, als sich die User hauptsächlich in der Zentrale oder in einer Zweigstelle befanden, die Anwendungen ausschließlich im Rechenzentrum des Unternehmens ausgeführt wurden und die Angriffsfläche auf klar definierte, vom Unternehmen verwaltete Bereiche beschränkt war. Heute leben wir in einer völlig anderen Welt mit einer Bedrohungslandschaft, in der Ransomware, verschlüsselte Bedrohungen, Angriffe auf die Lieferkette und andere komplexe Bedrohungen die herkömmlichen Verteidigungsmechanismen der Netzwerke durchbrechen. Es ist an der Zeit, eine Cloud-native Sicherheitslösung zu implementieren, die Risiken und Komplexität ganzheitlich reduziert und gleichzeitig Flexibilität bietet, um Geschäftsinitiativen voranzutreiben.

Zscaler Internet Access

Der Schutz heutiger Cloud- und mobilorientierter Unternehmen erfordert einen grundlegend anderen Ansatz, der auf Zero Trust basiert. Zscaler Internet Access wird als Modul der Zscaler Zero Trust Exchange bereitgestellt, ist die weltweit am häufigsten eingesetzte SSE-Plattform (Security Service Edge) und baut auf jahrelanger Erfahrung im Bereich Secure Web Gateway auf.

Die Lösung wird als skalierbare SaaS-Plattform über die weltweit größte Security Cloud bereitgestellt und ersetzt Legacy-Netzwerksicherheitslösungen mit dem Ziel, komplexe Bedrohungen abzuwehren und Datenverluste zu verhindern. Möglich macht dies ein umfassender Zero-Trust-Ansatz, der folgende Vorteile beinhaltet:

Erstklassige, konsistente Sicherheit für die hybriden Arbeitskräfte von heute: Wenn Sie die Sicherheit in die Cloud verlagern, erhalten alle User, Anwendungen, Geräte und Standorte stets einen identitäts- und kontextbasierten Schutz vor Bedrohungen. Ihre Sicherheitsrichtlinie gilt überall dort, wo Ihre User arbeiten.

Blitzschneller Zugriff ohne zusätzliche Infrastruktur: Die Direct-to-Cloud-Architektur sorgt für eine schnelle, nahtlose User Experience. Dies macht Backhauling überflüssig, verbessert die Performance sowie die User Experience und vereinfacht die Netzwerkverwaltung — ganz ohne physische Infrastruktur.

KI-gestützter Schutz über die weltweit größte Security Cloud: Die Inline-Überprüfung des gesamten Internet- und SaaS-Traffics, einschließlich SSL-Entschlüsselung, mit einer Reihe von KI-gestützten Cloud-Sicherheitsservices stoppt Ransomware, Phishing, Zero-Day-Malware und Advanced Threats anhand von Bedrohungsinformationen aus 500 Billionen Signalen pro Tag.

Vereinfachtes Management: Mit einer Cloud-nativen Sicherheitslösung mit KI, ohne zu verwaltende Hardware, mit optimierten Workflows und geschäftsorientierter Richtlinienerstellung gewinnt Ihr Team wertvolle Zeit, um sich auf strategische Ziele zu konzentrieren.

Integrierte, KI-gestützte Services für Sicherheit und Data Protection

Zscaler Internet Access beinhaltet eine umfassende Suite KI-gestützter Services für Sicherheit und Data Protection zum Schutz vor Cyberangriffen und Datenverlust. Da es sich um eine vollständig in der Cloud bereitgestellte SaaS-Lösung handelt, können neue Funktionen ohne zusätzliche Hardware oder langwierige Bereitstellungszyklen hinzufügt werden. Folgende Module sind als Teil von Zscaler Internet Access verfügbar:

- **Cloud-SWG (Secure Web Gateway):** Eine sichere, schnelle Web-Erfahrung dient zur Abwehr von Ransomware, Malware und anderen Advanced Threats mithilfe von KI-gestützter Echtzeitanalyse und URL-Filterung.

- **Cloud Access Security Broker (CASB):** Ein integrierter CASB zur Sicherung von Daten, Abwehr von Bedrohungen und Gewährleistung der Compliance in allen SaaS- und IaaS-Umgebungen sorgt für den Schutz von cloudbasierten Anwendungen.

- **Cloud Data Loss Prevention (DLP):** Mithilfe einer vollständigen Inline-Überprüfung und erweiterten Funktionen wie Exact Data Match (EDM), Optical Character Recognition (OCR) und maschinellem Lernen können Daten bei der Übertragung geschützt werden.

- **Zscaler Firewall und Cloud IPS:** Der branchenführende Schutz wird auf alle Ports und Protokolle erweitert und Edge- sowie Zweigstellen-Firewalls werden durch eine Cloud-native Plattform ersetzt.

- **Zscaler Sandbox:** Stoppen Sie neuartige und schwer erkennbare Malware in Web- und Dateiübertragungsprotokollen mit KI-gesteuerter Quarantäne und gewährleisten Sie konsistenten und globalen Echtzeit-Schutz für alle User.

- **KI-gestützter Zero-Trust-Browser:** Webbasierte Angriffe und Datenverluste gehören dank virtueller Air Gaps zwischen Usern, Internet und SaaS der Vergangenheit an.

VORTEILE:

- **Vorbeugung von Cyberbedrohungen und Datenverlusten mit KI:** Schützen Sie Ihr Unternehmen vor fortschrittlichen Bedrohungen mit einer Reihe von KI-gestützten Services für Data Protection und zum Schutz vor Cyberbedrohungen, die mit Echtzeit-Updates aus 500 Billionen Bedrohungssignalen pro Tag aus der weltweit größten Security Cloud angereichert werden.

- **Unvergleichliche User Experience:** Nutzen Sie die weltweit schnellste Internet- und SaaS-Erfahrung (bis zu 40 % schneller als herkömmliche Sicherheitsarchitekturen), um die Produktivität zu steigern und die Flexibilität Ihres Unternehmens zu erhöhen.

- **Weniger Kosten und Komplexität:** Erzielen Sie mit Zscaler einen ROI von 139 %, indem Sie 90 % Ihrer kostspieligen, komplexen und langsamen Appliances durch eine vollständig Cloud-native Zero-Trust-Plattform ersetzen.

- **Sicherheit für die hybride Belegschaft:** Mitarbeiter, Kunden und externe User können sicher sowie standort- und. geräteunabhängig auf webbasierte Anwendungen und Cloud-Services zugreifen — und so von einer hervorragenden digitalen Erfahrung profitieren.

- **Einheitliche SecOps- und NetOps-Bemühungen:** Erzielen Sie schnellere, gemeinsame Sicherheitsergebnisse mit geteilten Tools wie Echtzeit-Einblicke in den Traffic, API-First-Integrationen und granulare RBAC.

- **Vollständige Daten- und Inhaltssouveränität:** Setzen Sie Compliance für sicheren und lokalen Zugriff ohne Leistungseinbußen durch, indem Sie Egress NAT, geolokalisierte Inhalte und länderspezifische Datenprotokollierung nutzen.

- **Sichere KI in Ihrer Umgebung:** Ermöglichen Sie die sichere Nutzung von Microsoft Copilot und anderen KI-Anwendungen.

- **Schützen von Entwicklerumgebungen im großen Maßstab:** Automatisieren Sie die SSL/TLS-Überprüfung für mehr als 30 Entwickler-Tools, während Sie Code und unbekannte oder große Dateien mit sofortigen KI-gestützten Urteilen in einer Sandbox isolieren – und das alles, ohne Innovationen auszubremsen.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

- **Digital Experience Monitoring:** Eine einheitliche Ansicht der Performancemetriken von Anwendungen, Cloud-Pfaden und Endgeräten für Analyse und Fehlerbehebung ermöglicht die Verringerung des Betriebsaufwands für die IT und eine beschleunigte Problemlösung.

- **Zero-Trust-Konnektivität für Zweigstellen:** Mit nicht routingfähigen Verbindungen zwischen Zweigstellen und Rechenzentren sowie Usern, Servern und IOT-/Betriebstechnologiegeräten reduzieren Sie Risiken und Komplexität.

- **DNS-Sicherheit:** Profitieren Sie von optimierter DNS-Sicherheit und Performance für alle User, Geräte und Anwendungen, auf allen Ports und Protokollen weltweit.

Zscaler Internet Access für User und Workloads

Zscaler Internet Access reduziert die Risiken, die durch den Zugriff von Cloud-Workloads auf Internet- oder SaaS-Ziele entstehen. Da Workloads nicht mehr über herkömmliche, netzwerkzentrierte Tools wie VPNs, Firewalls (einschließlich virtueller Firewalls) oder WAN-Technologien auf das Internet zugreifen müssen, können Sicherheitslücken behoben und laterale Bewegungen verhindert werden, ohne dass ein Sammelsurium unterschiedlicher Sicherheitstools erforderlich ist. Durch die Anwendung der umfassenden Suite an Funktionen für Sicherheit und Data Protection von ZIA auf Workloads kann allen Usern und Workloads mit einer zentralen, integrierten Plattform konsistente Zero-Trust-Sicherheit bereitgestellt werden.

Durch die Kombination von ZIA mit Zscaler Private Access können Sie den Schutz auf Ihre privaten Anwendungen und Workloads ausweiten, unabhängig davon, ob sie sich in der öffentlichen Cloud oder in einem privaten Rechenzentrum befinden.

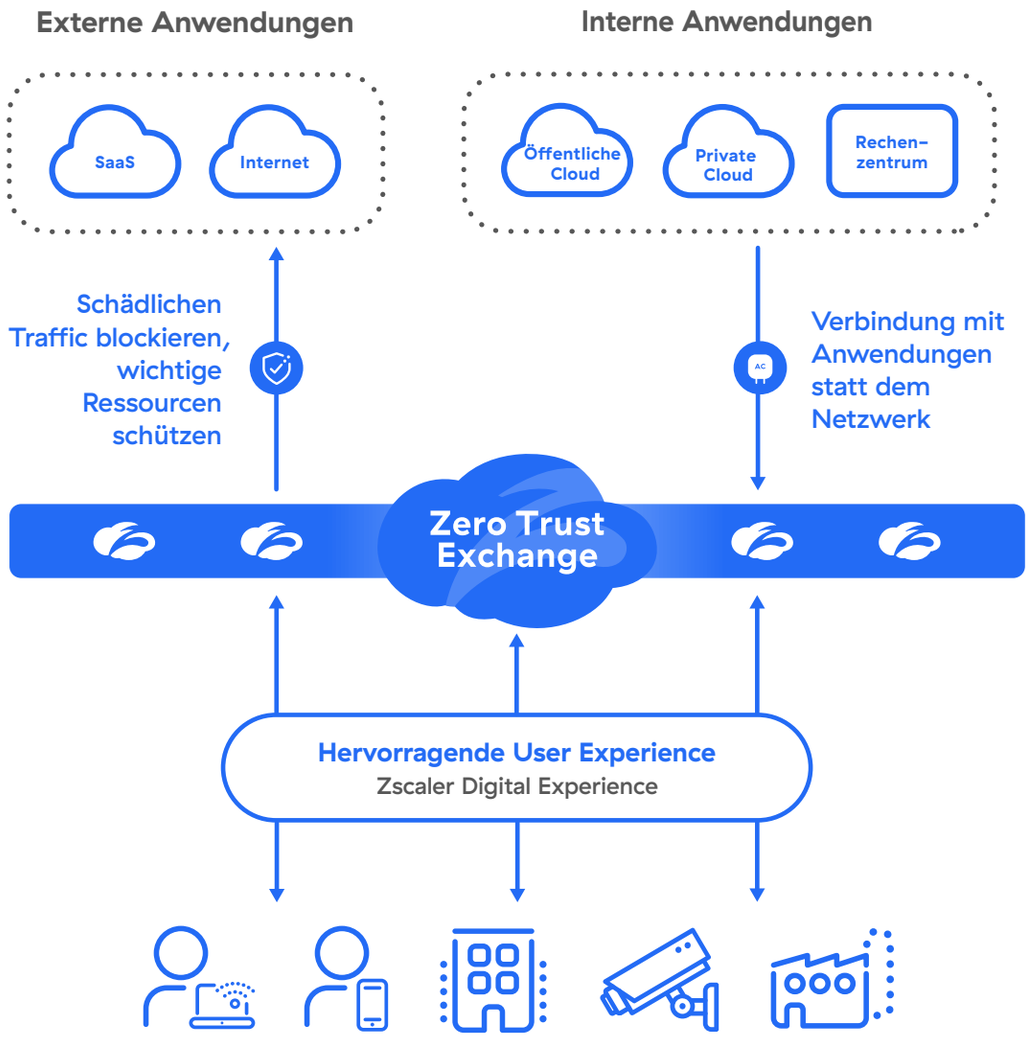


Abbildung 1: Die Zero Trust Exchange

* Gartner, Magic Quadrant for Security Service Edge, 15. April 2024, Charlie Winckless et al.

Gartner unterstützt keine Anbieter, Produkte oder Dienstleistungen, die in seinen Forschungspublikationen aufgeführt sind, und empfiehlt Technologieanwendern nicht, nur Anbieter mit den höchsten Bewertungen auszuwählen. Publikationen von Gartner spiegeln die Ansichten von Gartners Forschungsunternehmen wider und sollten nicht als Tatsachenfeststellungen interpretiert werden. Gartner übernimmt keinerlei ausdrückliche oder stillschweigende Gewähr in Bezug auf diese Studie, insbesondere in Bezug auf Angaben zur Marktgängigkeit oder Eignung für einen bestimmten Zweck.

GARTNER ist eine eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. und/oder den mit ihm verbundenen Unternehmen innerhalb und außerhalb der USA; MAGIC QUADRANT ist eine eingetragene Marke von Gartner, Inc. und/oder seinen Tochtergesellschaften. Sie werden hierin mit Genehmigung verwendet. Alle Rechte vorbehalten.

Gartner

Zscaler wurde als ein Leader im Gartner® Magic Quadrant™ für Security Service Edge 2024 gewürdigt.

MEHR DAZU

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Anwendungsfälle

SCHUTZ VOR CYBERBEDROHUNGEN UND RANSOMWARE

Wechseln Sie von herkömmlicher Netzwerksicherheit zur revolutionären Zero-Trust-Architektur von Zscaler, die Kompromittierungen verhindert, die Angriffsfläche eliminiert, laterale Bewegungen stoppt und Datensicherheit gewährleistet.

Mehr erfahren

SCHUTZ FÜR HYBRIDE MITARBEITER

Mitarbeiter, Partner, Kunden und Lieferanten können sicher sowie orts- und geräteunabhängig auf webbasierte Anwendungen und Cloud-Services zugreifen — und so von einer hervorragenden digitalen Erfahrung profitieren.

Mehr erfahren

DATA PROTECTION

Daten von Usern, in SaaS-Anwendungen und öffentlichen Cloud-Infrastrukturen müssen vor versehentlicher Offenlegung, Diebstahl und Ransomware-Angriffen mit Doppelerpressung geschützt werden.

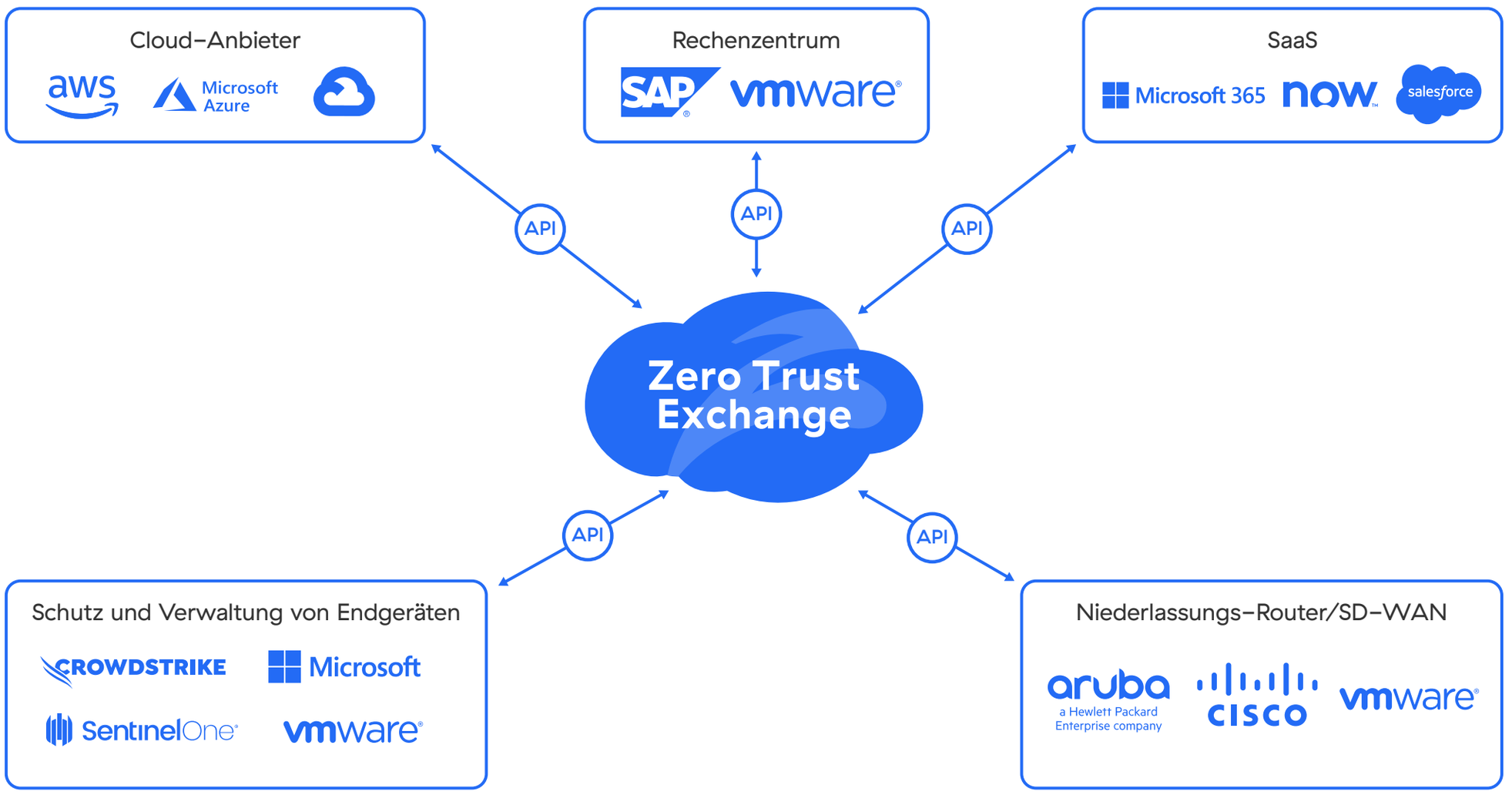
Mehr erfahren

MODERNISIERUNG DER INFRASTRUKTUR

Kostspielige, komplexe Netzwerke sind dank schnellem, zuverlässigen und sicherem Direktzugriff auf die Cloud nicht mehr erforderlich. Auch Edge- und Zweigstellen-Firewalls werden nicht länger benötigt.

Mehr erfahren

Das Ökosystem der Zscaler Zero Trust Exchange



©2025 Zscaler, Inc. Alle Rechte vorbehalten.

TABELLE 1: FUNKTIONEN VON ZSCALER INTERNET ACCESS	
FUNKTION	**DETAILS**
FUNKTIONEN	
URL-Filterung	Der User-Zugriff kann auf bestimmte Webkategorien oder -ziele zugelassen, blockiert, mit Warnmeldungen versehen oder eingeschränkt werden, um webbasierte Bedrohungen zu verhindern und die Einhaltung von Unternehmensrichtlinien zu gewährleisten.
SSL-Inspektion	TLS/SSL-Traffic wird lückenlos überprüft, um Bedrohungen und Datenverluste im verschlüsselten Traffic zu erkennen. Basierend auf Datenschutzanforderungen oder behördlichen Auflagen kann angegeben werden, welche Webkategorien oder Anwendungen geprüft werden sollen. Integrieren Sie Überprüfungen in das Entwicklertool, um die Workflows der Entwickler abzusichern.
DNS-Sicherheit	Identifizieren Sie verdächtige Command-and-Control-Verbindungen und leiten Sie diese zur vollständigen Inhaltsprüfung an Zscaler weiter.
Dedizierte IP	Gewähren Sie Zugriff auf Anwendungen, die IP-Adressen auf eine Allow-List setzen, mithilfe von IP-Adressen, die exklusiv Ihrem Unternehmen zugewiesen sind. Dies ermöglicht auch eine einfache Umstellung von Legacy-Architekturen auf Zero Trust.
Dateikontrolle	Dateidownloads/-uploads in Anwendungen können nach User oder Usergruppe blockiert oder zugelassen werden.
Bring Your Own IP	Sorgen Sie für Konsistenz und Kontrolle über Ihre Netzwerkidentität und stellen Sie für Drittanbieter-Anwendungen oder externe Infrastrukturen sicher, dass der Traffic ausschließlich von Ihrem Unternehmen ausgeht.
Bandbreitenkontrolle	Setzen Sie Bandbreitenrichtlinien durch und priorisieren Sie geschäftskritische Anwendungen gegenüber privatem Traffic.
Länderbezogene Protokollierung	Speichern und verwalten Sie Protokolle innerhalb der Grenzen eines bestimmten Landes, um die Anforderungen der Datensouveränität zu erfüllen, die vorschreiben, dass Daten von Bürgern gemäß den lokalen Gesetzen verarbeitet werden müssen.
Advanced Threat Protection	Komplexe Cyberangriffe wie unter anderem Malware, Ransomware, Supply-Chain-Angriffe oder Phishing können mit proprietärer Advanced Threat Protection abgewehrt werden. Auf Grundlage der Risikotoleranz des jeweiligen Unternehmens lassen sich granulare Richtlinien festlegen.
Inline-Data Protection (für Datenübertragungen)	Mithilfe von Weiterleitungsproxy und SSL-Überprüfung können Unternehmen in Echtzeit kontrollieren, ob vertrauliche Informationen an riskante Webziele oder cloudbasierte Anwendungen übertragen werden. So lassen sich interne und externe Bedrohungen der Datensicherheit beheben. Erweiterter Inline-Schutz wird für genehmigte und inoffiziell genutzte Anwendungen gleichermaßen bereitgestellt. Netzwerkgeräteprotokolle sind dazu nicht erforderlich.
Out-of-Band-Data Protection (Ruhende Daten)	Mithilfe von API-Integrationen können SaaS-Anwendungen, Cloud-Plattformen und deren Inhalte gescannt werden, um ruhende vertrauliche Daten zu identifizieren. Probleme werden automatisch behoben, indem beispielsweise riskante oder externe Freigaben widerrufen werden.
Eindringschutz	Erhalten Sie vollständigen Schutz vor Bedrohungen wie Botnets, komplexe Bedrohungen und Zero-Day-Angriffen sowie kontextbezogene Informationen zu Usern, Anwendungen und Bedrohungen. Cloud- und Web-IPS lässt sich nahtlos mit Firewall, Sandbox, DLP und CASB verwenden. Setzen Sie mithilfe von Cloud Custom IPS maßgeschneiderte Bedrohungssignaturen ein, um gezielte Angriffe zu erkennen und zu stoppen.
Dynamische, risikobasierte Zugriffs- und Sicherheitsrichtlinien	Sicherheits- und Zugriffsrichtlinien lassen sich automatisch an von Usern, Geräten, Anwendungen und Inhalten ausgehende Risiken anpassen.
Traffic-Erfassung	Nahtlose Paketerfassung: Einfaches Erfassen von entschlüsseltem Traffic über spezifische Kriterien innerhalb der Zscaler-Richtlinien-Engines — für eine effiziente Sicherheitsforensik ohne zusätzliche Appliances

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Malware-Analyse	Unbekannte Bedrohungen, die sich in schädlichen Payloads verbergen, lassen sich zur Verhinderung von Patient-Zero-Angriffen mit fortschrittlichen KI/ML-Funktionen erkennen, abwehren und unter Quarantäne stellen.
DNS-Filterung	Kontrollieren und blockieren Sie DNS-Anfragen an bekannte schädliche Ziele.
Zero-Trust-Browser (Web-Isolierung)	Durch die Übertragung aktiver Inhalte als harmlose Pixel an den Browser des Endusers gehören webbasierte Bedrohungen der Vergangenheit an.
Korrelierte Bedrohungsinformationen	Durch Kontextualisierung und Korrelation von Warnmeldungen mit Informationen zu Bedrohungseinstufung, betroffenen Ressourcen, Schweregrad usw. können Sicherheitsvorfälle schneller untersucht und behoben werden.
Anwendungsisolierung	Durch granulare Kontrolle von Useraktionen wie Kopieren/Einfügen, Hochladen/Herunterladen und Drucken lässt sich sicherer agentenloser Zugriff über nicht verwaltete Geräte auf SaaS-, cloudbasierte und private Anwendungen realisieren und der Verlust sensibler Daten verhindern.
Digital Experience Monitoring (ZDX)	Eine einheitliche Ansicht der Performancemetriken von Anwendungen, Cloud-Pfaden und Endgeräten ermöglicht optimierte Analyse und Fehlerbehebung.
Zero-Trust-Konnektivität für Zweigstellen	Mithilfe der Zero Trust Exchange minimieren Sie die Angriffsfläche, unterbinden die laterale Ausbreitung von Bedrohungen und modernisieren die Zweigstellenkonnektivität.
Schutz der Kommunikation zwischen Workloads und Internet	Beugt Infektionen vor und verhindert laterale Bewegungen bei der Kommunikation zwischen Workloads und Internet. Umfasst SSL-Überprüfung, IPS, URL-Filterung und Data Protection für die gesamte Kommunikation.
Transparenz über alle IoT-Geräte	Dank automatischer Erkennung, kontinuierlichem Monitoring und KI/ML-Klassifizierung mit branchenführenden automatischen Kennzeichnungsfunktionen erhalten Sie einen vollständigen Überblick über alle IoT-Geräte, Server und nicht verwalteten User-Geräte in Ihrem Unternehmen.
Rollenbasierte Zugriffskontrolle (Role Based Access Control, RBAC)	Legen Sie genau definierte Berechtigungen fest, um zu kontrollieren, welche Administratoren Richtlinien und Analyseberichte innerhalb der Zscaler-Plattform bearbeiten und anzeigen können, um Konflikte zu vermeiden und die Governance zu verbessern.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

FUNKTION	DETAILS
FUNKTIONEN DER PLATTFORM	
Flexible Konnektivitätsoptionen	• Zscaler Client Connector (ZCC): Leiten Sie Traffic über einen schlanken Agent an die Zero Trust Exchange weiter, der Windows, macOS, iOS, iPadOS, Android und Linux unterstützt. • GRE- oder IPsec-Tunnel: Verwenden Sie GRE- und/oder IPsec-Tunnel, um den Traffic von Geräten ohne ZCC an die Zero Trust Exchange zu senden. • Browser-Isolierung: Verbinden Sie nahtlos alle BYOD- oder nicht verwalteten Geräte mit integrierter Zero-Trust-Browser-Isolierung. • Proxy-Verkettung: Zscaler unterstützt die Weiterleitung von Traffic von einem Proxyserver zu einem anderen; dies wird jedoch in Produktionsumgebungen nicht empfohlen. • PAC-Dateien: Senden Sie den Traffic von Geräten ohne ZCC mit PAC-Dateien an die Zero Trust Exchange.
Cloudbasierte Bereitstellung	Die zu 100 % Cloud-native Plattform wird als SaaS-Service bereitgestellt. Für die Business-Continuity-Planung und andere spezielle Anwendungsfälle stehen private und virtuelle Service Edges zur Verfügung.
Datenschutz und Datenspeicherung	Beim Protokollieren von Daten werden Inhalte niemals auf einen Datenträger geschrieben. Mithilfe granularer Kontrollen lässt sich bestimmen, wo genau die Protokollierung stattfindet. Unternehmen können die rollenbasierte Zugriffskontrolle (Role Based Access Control, RBAC) einsetzen, um schreibgeschützten Zugriff, Anonymisierung/Verschleierung von Usernamen und nach Abteilungen oder Funktionen festgelegte Zugriffsberechtigungen gemäß den wichtigsten Compliance-Bestimmungen bereitzustellen. Die Daten werden je nach Produkt maximal sechs Monate lang aufbewahrt. Sie haben die Möglichkeit, zusätzlichen Speicherplatz zu erwerben, um Daten länger zu speichern.
Die wichtigsten Compliance-Zertifizierungen	Zu den Zertifizierungen gehören: • FedRAMP • ISO 27001 • SOC 2 Typ II • SOC 3 • NIST 800-63C Die vollständige Liste unserer Compliance-Zertifizierungen finden Sie hier.
Granulare API-Unterstützung	Wir stellen REST-API-Integrationen mit zahlreichen Identitäts-, Netzwerk- und Sicherheitsanbietern bereit. Beispielsweise können Sie Protokolle zwischen Zscaler und cloudbasierten oder On-Premise-SIEM-Lösungen (z. B. Splunk) teilen. Mehr erfahren
Direktes Peering	Direktes Peering mit großen Internet- und SaaSS-Anbietern sowie Zielen in öffentlichen Clouds stellt die schnellstmögliche Übertragung des Traffics sicher.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

FUNKTION	DETAILS
SERVICE LEVEL AGREEMENTS (SLAS)	
Verfügbarkeit	99,999 %, gemessen an verlorenen Transaktionen
Proxy-Latenz	< 100 ms, auch wenn Bedrohungs- und DLP-Scans aktiviert sind
Virenerfassung	100 % der bekannten Viren und Malware
UNTERSTÜTZTE PLATTFORMEN UND SYSTEME	
Client Connector	Unterstützung für: • iOS 9 oder höher • Android 8 oder höher • Windows 8 oder höher • Mac OSX 10.14 oder höher • CentOS 9 • Ubuntu 20.04 Mehr erfahren
Branch Connector	Unterstützung für: • VMware vCenter oder vSphere Hypervisor • CentOS • Redhat

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Zscaler Internet Access: Mehrere Optionen für den Einstieg

	ESSENTIALS-PLATTFORM Beginnen Sie Ihre Zero-Trust-Transformation mit sicherem, zuverlässigem Internetzugang und eingeschränktem Private Access mit weiteren Innovationen von Zscaler.	ZSCALER PLATTFORM Komplette SASE/SSE-Lösung, einschließlich uneingeschränkte Nutzung von Internet Access, Private Access und Data Protection.
PLATTFORM-SERVICES		
Traffic Forwarding – Client Connector, GRE, PAC, Proxy Chaining, IPsec	ja	ja
Mehrere Identitätsanbieter (IdP), API-Zugriff, Device Posture	ja	ja
Authentifizierung — SAML, Secure LDAP, Kerberos	ja	ja
ZS-Testumgebung	–	–
Zugang zu öffentlichen Zscaler-Rechenzentren	ja	ja
Zugang zu öffentlichen Premium-Rechenzentren von Zscaler (Australien, Neuseeland, Dubai (unreguliert), Südamerika, Afrika, Südkorea, Taiwan und Festlandchina)	–	ja
China-Prämie/Regulierter RZ-Zugang im Nahen Osten	–	–
INTERNET ACCESS		
Inhaltsfilterung	ja	ja
Dateityp-Kontrolle	ja	ja
TLS/SSL-Überprüfung	ja	ja
Private SSL-Zertifikate	ja	ja
Bandbreitenübersicht (Dashboard)	ja	ja
Streamen zu On-Premises SIEM (Nanolog Streaming Service mit Live-Verwaltung.)	ja	ja
Cloud NSS (für >500 User)	ja	ja
Source IP Anchoring	–	ja
ZIA Private Service Edge – Virtuelle Appliance	–	ja
Hardware: ZIA Private Service Edge — 3 Instanzen, 5 Instanzen	–	–

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

SCHUTZ VOR CYBERBEDROHUNGEN		
Cyberthreat Protection Standard: Advanced Threat Protection, Sandbox Standard, Zero Trust Firewall Standard, Zero Trust Browser Standard	ja	ja
Antivirus und Antispyware inline	ja	ja
Sandbox Advanced	–	–
Zero Trust Firewall Advanced	–	–
Zero Trust Browser Advanced (1,5 GB Traffic/User/Monat, für alle Zero-Trust-Browser-User)	–	–
Zero Trust Browser Unlimited (keine Beschränkungen der Traffic-Nutzung)	–	–
PRIVATE ACCESS (ZPA)		
Sicherer Zugriff auf private Unternehmensanwendungen: Log-Streaming, Quell-IP-Verankerung, mehrere IdPs, Zustandsüberwachung	1 User pro 20 Abonnenten (Min.: 500 Abonnenten)	ja
App Connectors	So viele wie erforderlich (bis zur max. Anz. für das System)	So viele wie erforderlich (bis zur max. Anz. für das System)
DATA PROTECTION		
Standardversion Data Protection: Cloud-App-Kontrolle, Shadow-IT-Bericht, Mandantenbeschränkung, Inline-Web (Monitormodus), SaaS-API (1 App), GenAI Security	ja	ja
Inline-Web und Gen AI DLP, alle Apps (Internet und Private Access)	–	ja
RISIKOMANAGEMENT		
Standardversion Risk Management: Deception Standard	–	ja
ZERO TRUST FÜR WORKLOADS		
Standardversion Zero Trust für Workloads: Stateful Filtering, DNS, TLS-Inspektion	1 GB monatlicher Workload-Traffic pro abonniertem User	2 GB monatlicher Workload-Traffic pro abonniertem User
DIGITAL EXPERIENCE (ZDX)		
ZDX Standard: Pre-Set	ja	–
ZDX Standard	–	ja
SUPPORT		
Standard-Support	ja	ja
Support Plus	–	–

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

LIZENZMODELL

Bei allen Editions von Zscaler Internet Access gilt der Preis pro User. Für bestimmte Produkte innerhalb Ihrer Plattformedition können die Preise unabhängig von der Useranzahl variieren. Weitere Informationen zu den Preisen erhalten Sie von Ihrem Zscaler-Account-Team.

Teil der ganzheitlichen Zero Trust Exchange

Mithilfe der Zero Trust Exchange können Mitarbeiter über schnelle und sichere Verbindungen standortunabhängig auf Anwendungen zugreifen, sodass das Internet effektiv als Unternehmensnetzwerk fungiert. Die Plattform beruht auf dem Zero-Trust-Prinzip der minimalen Rechtevergabe und gewährleistet mithilfe kontextbasierter Identitäts- und Richtliniendurchsetzung umfassende Sicherheit.

Zscaler bietet mit seiner Lösung wirklich alles, was wir von einer Zero-Trust-Plattform erwarten: skalierbare SSL-Trafficüberprüfung sowie weitere Funktionen zur Bedrohungsprävention und für die Data Protection.

NITIN NEGI
Senior Manager for Cybersecurity Engineering and Operations, Micron Technology

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, resilienter und sicherer arbeiten können. Die Plattform Zscaler Zero Trust Exchange™ schützt unzählige Kunden mit standortunabhängig sicheren Verbindungen zwischen Usern, Geräten und Anwendungen vor Cyberangriffen und Datenverlusten. Die in 160 Rechenzentren auf der ganzen Welt verfügbare SSE-basierte Zero Trust Exchange™ ist die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen finden Sie auf **zscaler.com/de**. Folgen Sie uns gerne auch auf Twitter: **@zscaler**.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™ sowie weitere unter **zscaler.com/de/legal/trademarks** aufgeführte Marken sind entweder (i) eingetragene Handelsmarken bzw. Dienstleistungsmarken oder (ii) Handelsmarken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

+1 408 533 0288 **Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA** **zscaler.com/de**

Zero Trust Everywhere