DATENBLATT

Zscaler Internet Access

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

Zscaler Internet Access™ bietet mit der umfassendsten Zero-Trust-Plattform der Branche sicheren, schnellen Internet- und SaaS-Zugriff.

Veraltete Netzwerksicherheit ist in einer Cloud- und Mobile-first-Welt wirkungslos. Herkömmliche Hub-and-Spoke-Architekturen waren effektiv, als sich die User hauptsächlich in der Zentrale oder in Zweigstellen befanden, die Anwendungen ausschließlich im Rechenzentrum des Unternehmens untergebracht waren und die Angriffsfläche auf von der Organisation 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 fortschrittliche Bedrohungen die bestehenden Abwehrmechanismen des Netzwerks durchbrechen. Es ist an der Zeit, eine cloudnative Sicherheitslösung zu finden, die Risiken und Komplexität ganzheitlich reduziert und gleichzeitig Flexibilität bietet, um Geschäftsinitiativen voranzutreiben.

Zscaler Internet Access

Der Schutz der Cloud- und Mobile-first-Unternehmen von heute erfordert einen grundlegend anderen Ansatz, der auf Zero Trust basiert. Zscaler Internet Access, Teil der Zscaler Zero Trust Exchange, ist die weltweit am häufigsten eingesetzte SSE-Plattform (Security Service Edge) und baut auf jahrelanger Erfahrung im Bereich Secure Web Gateway auf.

Vorteile:

- **Vorbeugung von Cyberbedrohungen und Datenverlusten mit KI:** Schützen Sie Ihr Unternehmen vor fortschrittlichen Bedrohungen mit einer Reihe von KI-gestützten Services zum Schutz vor Cyberbedrohungen und Daten, 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.
- **Modernisierte Sicherheitsarchitektur:** Erzielen Sie mit Zscaler einen ROI von 139 %, indem Sie 90 % Ihrer kostspieligen, komplexen und langsamen Appliances durch eine vollständig cloudnative Zero-Trust-Plattform ersetzen.

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 cloudnativen 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.

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

Integrierte, KI-gestützte Sicherheits- und Data Protection Services

Zscaler Internet Access beinhaltet eine umfassende Suite KI-gestützter Sicherheits- und Data Protection Services 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 erweiterter Funktionen wie Exact Data Match (EDM), Optical Character Recognition (OCR) und maschinellem Lernen können Sie Daten während der Übertragung schützen.

- **Zscaler Firewall und Cloud IPS:** Der branchenführende Schutz wird auf alle Ports und Protokolle erweitert und Edge- sowie Zweigstellen-Firewalls werden durch eine cloudnative Plattform ersetzt.
- **Zscaler Sandbox:** Mit KI-gesteuerten Quarantänemaßnahmen wehren Sie neuartige und komplexe Malware in Web- und Dateiübertragungsprotokollen ab. So profitieren alle User von konsistentem und globalem Echtzeitschutz.
- **KI-gestützte Cloud-Browser-Isolierung:** Webbasierte Angriffe und Datenverluste gehören dank virtueller Air Gaps zwischen Usern, Internet und SaaS der Vergangenheit an.
- **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 Sicherheits- und Data Protection-Funktionen 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.

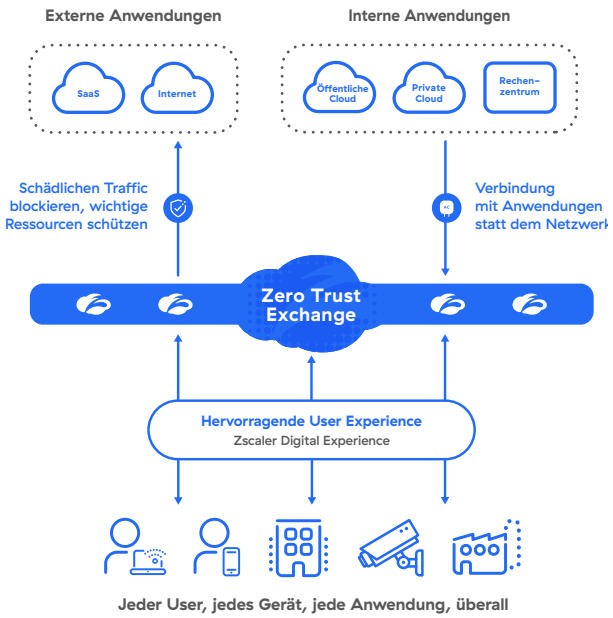

Abbildung 1: Die Zero Trust Exchange

Anwendungsfälle

Schutz vor Cyberbedrohungen und Ransomware

Wenn Unternehmen von ihrer veralteten Netzwerksicherheit auf die revolutionäre Zero-Trust-Architektur von Zscaler umsteigen, können sie Sicherheitslücken schließen, die Angriffsfläche minimieren, laterale Ausbreitung verhindern und ihre Daten schützen

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 profitieren so von einer hervorragenden digitalen Erfahrung.

Mehr erfahren →

Data Protectio

Verhindern Sie Datenverluste von Usern, SaaS-Anwendungen und öffentlichen Cloud-Infrastrukturen durch versehentliche Exposition, Datendiebstahl oder Ransomware mit Doppelerpressung.

Mehr erfahren →

Modernisierung der Infrastruktur

Kostspielige, komplexe Netzwerke sind dank schnellem, 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

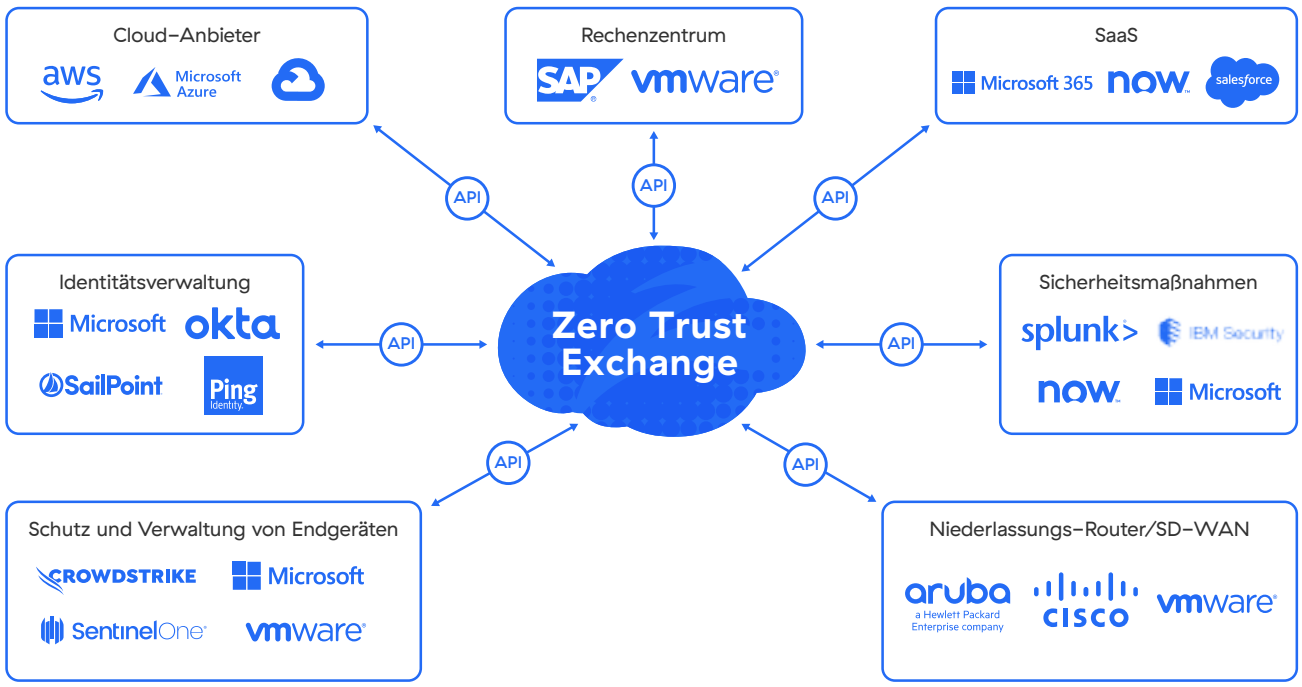

Abbildung 2: Das Partner-Ökosystem von Zscaler Internet Access

TABELLE 1: FUNKTIONEN VON ZSCALER INTERNET ACCESS	
FUNKTION	**DETAILS**
Funktionen	
URL-Filterung	Der User-Zugriff kann für 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 uneingeschränkt überprüft, um Bedrohungen und Datenverluste im verschlüsselten Traffic zu erkennen. Legen Sie fest, welche Webkategorien oder Anwendungen aufgrund von Datenschutzanforderungen oder behördlichen Auflagen geprüft werden sollen.
DNS-Sicherheit	Identifizieren Sie verdächtige Command-and-Control-Verbindungen und leiten Sie diese zur vollständigen Inhaltsprüfung an Zscaler weiter.
Dateikontrolle	Dateidownloads/-uploads in Anwendungen können nach User oder Usergruppe blockiert oder zugelassen werden.
Bandbreitenkontrolle	Setzen Sie Bandbreitenrichtlinien durch und priorisieren Sie geschäftskritische Anwendungen gegenüber privatem Traffic.
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 der jeweiligen Organisation lassen sich granulare Richtlinien festlegen.
Inline-Data Protection (für Datenübertragungen)	Mithilfe von Weiterleitungsproxy und SSL-Überprüfung können Organisationen 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 (für 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, Advanced Threats 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.
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
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.
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 Sie Sicherheitsvorfälle schneller untersuchen und beheben.
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	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 einer Kompromittierung 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.

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:** Mit integrierter Cloud Browser Isolation lassen sich alle BYOD- und nicht verwalteten Geräte nahtlos verbinden. • **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 % cloudnative Plattform wird als SaaS-Service bereitgestellt. Für besondere Anwendungsfälle sind Private und Virtual Service Edges verfügbar.
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. Sie 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 Eine 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 SaaS-Anbietern sowie Zielen in öffentlichen Clouds gewährleistet die schnellstmögliche Übertragung des Traffics.
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 5 oder höher • Windows 7 oder höher • Mac OSX 10.10 oder höher • CentOS 8 • Ubuntu 20.04 Mehr erfahren
Branch Connector	Unterstützung für: • VMware vCenter oder vSphere Hypervisor • CentOS • Redhat

Editionen von Zscaler Internet Access

	Funktionen	Essentials	Business	Transformation	Unbegrenzt
Plattform-Services		Inhaltsfilterung, Inline-AV, SSL-Überprüfung, Nanolog-Streaming	(+) Private SSL-Zertifikate	(+) Cloud NSS, NSS-Protokoll-wiederherstellung, erweiterter DC-Zugang, IPSec-Tunnel, kontextbezogene Alarme, ZIA Virtual Private Service Edge (8)	(+) Quell-IP-Verankerung, Testumgebung, Prioritätskategorisierung, ZIA Virtual Private Service Edge (32), Server- & IoT-Schutz (1 GB/10 User)
Threat Protection	**Advanced Threat Protection (inkl. KI-gestützter Phishing- & C2-Erkennung** Schutz vor bekannten und unbekannten Bedrohungen (URL, AV, Botnet/C2, Phishing)	ja	ja	ja	ja
	Cloud Sandbox Schutz vor Zero-Day-Angriffen durch Analyse verdächtiger Dateien mit KI-gestützter Quarantäne	Add-on	Add-on	ja	ja
	Isolierung — Schutz vor Cyberbedrohungen Schutz vor Zero-Day-Angriffen durch verdächtige Webinhalte. KI-gestützte risikobasierte Isolierung	Add-on	Add-on	Isolierung für Cyberschutz: Standard (100 MB/User/Monat)	Isolierung für Cyberschutz: Standard (1,5 GB/User/Monat)
	Korrelierte Bedrohungsinformationen Schnellere Untersuchungen und kürzere Reaktionszeiten durch kontextbezogene Bedrohungsdaten	–	ja	ja	ja
	Dynamische risikobasierte Richtlinien Automatische Anpassung und Empfehlung von Sicherheitsrichtlinien auf Grundlage verschiedener Risikofaktoren	–	–	ja	ja
	Integrierte Deception-Technologie Höhere Zero-Trust-Sicherheit durch proaktives Ködern, Erkennen und Abfangen von aktiven Angreifern	–	–	Standard[1]	Standard[1]
Netzwerk-Transformation	**DNS-Auflösung und -Filterung** Trusted DNS Resolver für geozentrische und optimale DNS-Auflösung	Bis zu 64 Regeln	Bis zu 64 Regeln	ja	ja
	DNS Tunnel Detection Erkennung und Unterbindung von DNS-basierten Angriffen und Datenexfiltration durch DNS-Tunnel	–	–	ja	ja
	Bandbreitenübersicht (Dashboard) Traffic-Kontrolle und Bandbreiten-priorisierung, Ratenbegrenzung für Web-Traffic		ja	ja	ja
	Cloud-Firewall Standortunabhängiger Schutz für alle User und den gesamten Traffic (sowohl Web als auch Nicht-Web) mit unbegrenzter SSL-Überprüfung	Netzwerk, Anwendungsservices, Standorte, FQDNs bis zu 10 Regeln	Netzwerk, Anwendungsservices, Standorte, FQDNs bis zu 10 Regeln	(+) Remote-User und -Standorte, Deep Packet Application Inspection	(+) Remote-User und -Standorte, Deep Packet Application Inspection
	Schutz für nicht authentifizierten Traffic Schutz von Netzwerken mit vollautomatischer Sicherheit auf Netzbetreiberniveau mit Einschränkungen	0,5 GB/User/Monat	1 GB/User/Monat	1,5 GB/User/Monat	2 GB/User/Monat

	Funktionen	Essentials	Business	Transformation	Unbegrenzt
Datenschutz und Verhinderung von Datenverlusten	**Cloud App Control + Mandantenbeschränkungen** Erkennen und Kontrollieren der Nutzung von riskanten oder nicht genehmigten Anwendungen (Schatten-IT)	ja	ja	ja	ja
	Isolierung — Data Protection (SaaS) Verhindern von Datenverlusten durch SaaS-Anwendungen auf BYOD- oder nicht verwalteten Endgeräten (ohne Client)	Add-on	Add-on	Add-on	Isolierung für Data Protection (SaaS): Standard (100 MB/User/ Monat)
	DLP, CASB, Inline Web Essentials, SaaS API (1 Anwendung) Kein Verlust vertraulicher Daten über das Internet. Scannen einer SaaS-Anwendung auf riskante Freigabe von sensiblen Daten oder Malware	–	Standard Data Protection (grundlegende DLP- und CASB-Funktionen)	(+) SaaS-API-Retro-Scan	ja
	SaaS-API, SaaS-Sicherheit in der Lieferkette, nicht verwaltete Geräte, Klassifizierung, Incident Management Vorteile Standard Data Protection plus: Kontrolle der BYOD-Risiken durch Streaming von Daten als Pixel, Scannen mehrerer SaaS-Aw. auf riskante Freigaben/Malware, Anp. von DLP mit EDM, IDM, OCR und Tools für Incident Management und Workflow-Automatisierung	Add-on	Add-on	Add-on	ja
Digital Experience Monitoring	Monitoring der digitalen Erfahrungen der User, um die Performance zu optimieren und Probleme mit Anwendungen, Netzwerken und Geräten schnell zu beheben	–	Standard	Standard	Standard
Premium Support Plus		Add-on	Add-on	Add-on	ja

Lizenzmodell
Die Preise für alle Editionen von Zscaler Internet Access werden pro User berechnet. Für bestimmte Produkte innerhalb einer Edition können die Preise unabhängig von der Anzahl der User variieren. Weitere Informationen zu den Preisen erhalten Sie beim Zscaler-Kundenservice.

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.

> „Wenn andere Unternehmen einem Ransomware-Angriff zum Opfer fallen, werden Tausende von Systemen in ihrer IT-Umgebung lahmgelegt — ganz zu schweigen von den schwerwiegenden Folgen einer Lösegeldzahlung. Wenn solche Vorfälle in die Schlagzeilen geraten, bekomme ich besorgte Anrufe aus der Chefetage. Ich bin jedes Mal heilfroh, dass ich dann sagen kann, dass bei uns alles in Ordnung ist.“
>
> **Ken Athanasiou,** VIP & CISO, AutoNation

zscaler™ | Experience your world, secured.™

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, zuverlässiger und sicherer arbeiten können. Die Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an beliebigen Standorten vor Cyberangriffen und Datenverlust. Die SSE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.de** oder folgen Sie uns auf Twitter unter **@zscaler**.

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