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.

Legacy-Netzwerksicherheit ist in einer Cloud- und Mobile-first-Welt unzureichend
Als User noch hauptsächlich in der Zentrale oder in Zweigstellen arbeiteten, sich Anwendungen ausschließlich im Rechenzentrum befanden und Unternehmen die volle Kontrolle über ihre Angriffsfläche hatten, waren herkömmliche Hub-and-Spoke-Architekturen wirkungsvoll. Heute leben wir aber in einer völlig anderen Welt mit einer Bedrohungslandschaft, in der Ransomware, verschlüsselte Bedrohungen, Lieferkettenangriffe und andere komplexe Bedrohungen veraltete Abwehrmechanismen zum Schutz von Netzwerken durchbrechen. Es ist an der Zeit, Cloud-native Sicherheitslösungen einzusetzen, die Risiken und Komplexität ganzheitlich reduzieren und gleichzeitig flexibel genug sind, 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)

Vorteile:

- **Keine Cyberbedrohungen und Datenverluste dank KI:** Mit einer Suite KI-gestützter Services zur Abwehr von Cyberbedrohungen und zum Datenschutz, die mittels Echtzeitupdates aus 300 Billionen täglichen Bedrohungssignalen aus der weltweit größten Security Cloud optimiert werden, ist Ihr Unternehmen stets vor komplexen Bedrohungen geschützt.
- **Erstklassige Anwendererfahrung:** Dank der weltweit schnellsten Internet- und SaaS-Erfahrung (bis zu 40 % schneller als bei herkömmlichen Sicherheitsarchitekturen) lässt sich die Produktivität steigern und die geschäftliche Agilität erhöhen.
- **Modernisierte Sicherheitsarchitektur:** Indem Sie 90 % Ihrer kostspieligen, komplexen und langsamen Appliances durch eine vollständig Cloud-native Zero-Trust-Plattform ersetzen, können Sie einen ROI von 139 % erzielen.

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 hybride Belegschaft von heute: Wenn die Sicherheit in die Cloud verlagert wird, profitieren alle User und Anwendungen an jedem Standort von permanentem identitäts- und kontextbasiertem Bedrohungsschutz. Die Sicherheitsrichtlinien folgen den Usern jederzeit.

Blitzschneller Zugriff ohne Infrastruktur: Eine Direct-to-Cloud-Architektur gewährleistet eine schnelle, nahtlose Anwendererfahrung. So lässt sich Backhauling vermeiden, die Performance und User Experience verbessern sowie die Netzwerkverwaltung vereinfachen — ganz ohne physische Infrastruktur.

KI-gestützter Schutz über die weltweit größte Security Cloud: Die Inline-Überprüfung des gesamten Internet-Traffics, einschließlich SSL-Entschlüsselung, mit einer Reihe KI-gestützter Cloud-Sicherheitsservices stoppt Ransomware, Phishing, Zero-Day-Malware und Advanced Threats anhand von Bedrohungsinformationen aus 300 Billionen Signalen pro Tag.

Vereinfachtes Management: Durch die Verwendung einer Cloud-nativen, KI-gestützten Sicherheitslösung ohne zu verwaltende Hardware, mit optimierten Workflows und geschäftsorientierter Richtlinienerstellung sparen Teams wertvolle Zeit ein, in der Sie sich stattdessen auf strategische Ziele konzentrieren können.

Integrierte, KI-gestützte Sicherheits- und Datenschutzservices

Zscaler Internet Access beinhaltet eine umfassende Suite KI-gestützter Sicherheits- und Datenschutzservices 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 Secure Web Gateway (SWG):** Stellen Sie eine sichere, schnelle Weberfahrung bereit, die Ransomware, Malware und andere Advanced Threats mithilfe von KI-gestützter Echtzeitanalyse und URL-Filterung des einzigen Leaders im Gartner Magic Quadrant 2020 für SWGs abwehrt.
- **Cloud Access Security Broker (CASB):** Mit einem integrierten CASB zur Absicherung von Daten, Abwehr von Bedrohungen und Gewährleistung der Compliance in allen SaaS- und IaaS-Umgebungen schützen Sie Ihre Cloud-basierten 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 Cloud-native 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 Isolation:** 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 Datenschutzfunktionen von ZIA auf Workloads kann allen Usern und Workloads mit einer zentralen, integrierten Plattform konsistente Zero-Trust-Sicherheit bereitgestellt werden.

Wenn Sie ZIA zudem mit Zscaler Private Access kombinieren, können Sie den Schutz auf private Anwendungen und Workloads erweitern — unabhängig davon, ob sie sich in der öffentlichen Cloud oder einem privaten Rechenzentrum befinden.

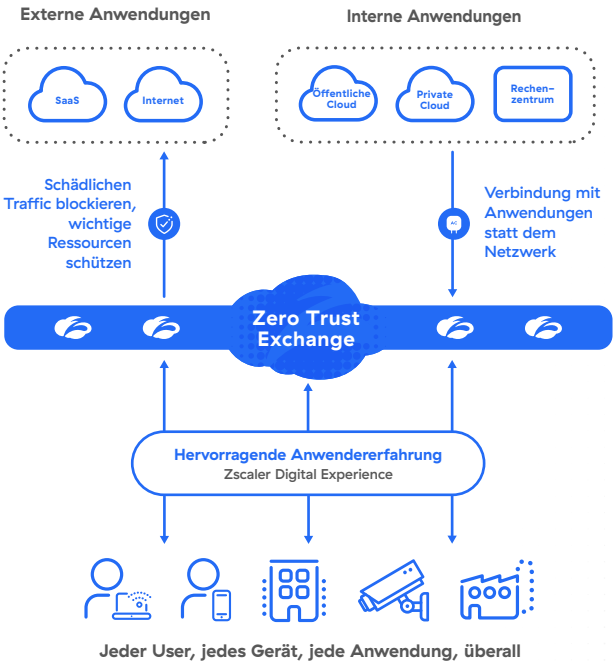

Abbildung 1: Die Zero Trust Exchange

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 ➞

Datenschutz

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, 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

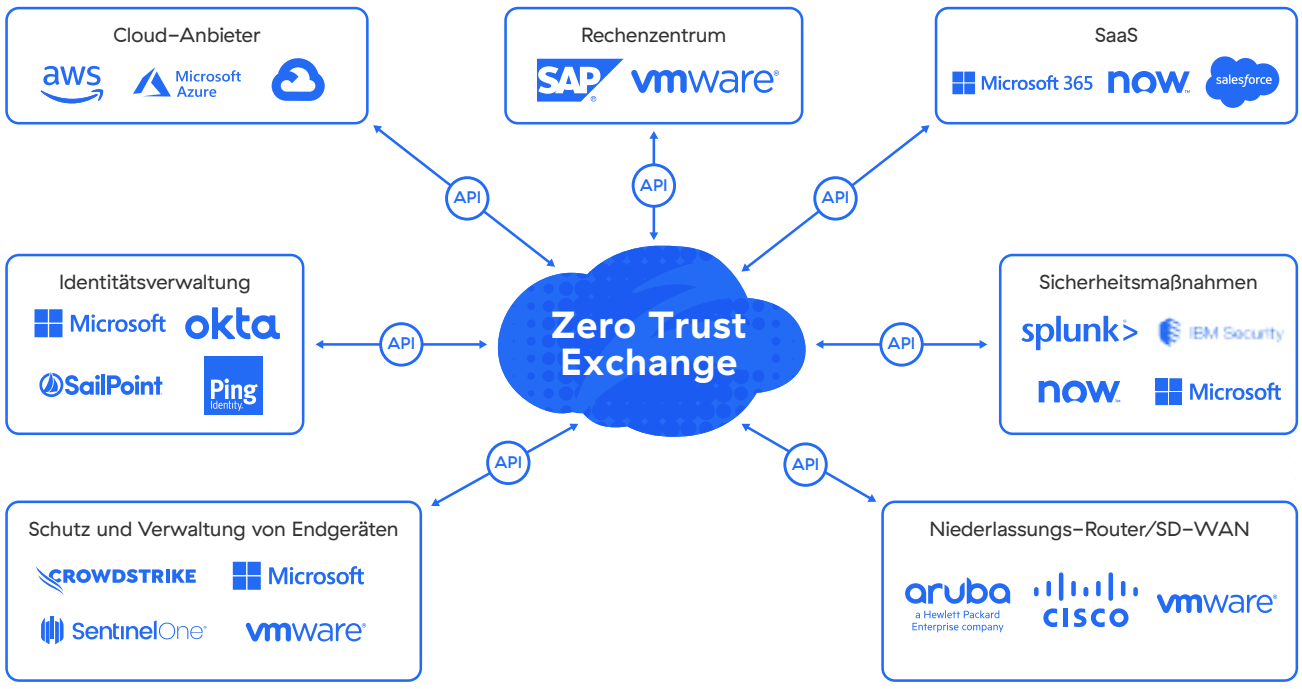

Abbildung 2: Das Partner-Ökosystem von Zscaler Internet Access

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-Datenschutz (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-Datenschutz (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.
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 Datenschutz 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):** Über einen ressourcenschonenden Agent, der Windows, macOS, iOS, iPadOS, Android und Linux unterstützt, wird der Traffic an die Zero Trust Exchange weitergeleitet. • **GRE- oder IPSec-Tunnel:** Bei Geräten ohne ZCC können Sie GRE- und/oder IPSec-Tunnel verwenden, um den Traffic 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-Chaining:** Zscaler unterstützt die Weiterleitung des Traffics von einem Proxyserver zu einem anderen. Dies wird jedoch in Produktionsumgebungen nicht empfohlen. • **PAC-Dateien:** Bei Geräten ohne ZCC wird der Traffic mittels PAC-Dateien an die Zero Trust Exchange gesendet.
Cloudbasierte Bereitstellung	Die zu 100 % Cloud-native 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

	ZIA Essentials Edition	ZIA Business Edition	ZIA Transformation Edition	ZIA Unlimited Edition
Secure Web Gateway	✓	✓	✓	✓
Vollständige TLS/SSL-Überprüfung	✓	✓	✓	✓
URL-Filterung	✓	✓	✓	✓
Transparenz und Kontrolle von Cloud-Anwendungen	✓	✓	✓	✓
Inline-Malware-Schutz	✓	✓	✓	✓
KI-basierte Phishing- und C2-Erkennung	✓	✓	✓	✓
Grundlegende Datenschutzfunktionen (DLP, Transparenz und Warnmeldungen; CASB, 1 Anwendung)	Add-on	✓	✓	✓
Digital Experience Monitoring (Standardversion)	—	✓	✓	✓
Private SSL-Zertifikate	—	✓	✓	✓
Advanced Firewall mit erweiterten Funktionen und IPS	Add-on	Add-on	✓	✓
Erweiterte Sandbox mit KI-gestützter Quarantäne	Add-on	Add-on	✓	✓
Attacker Deception (Standardversion)	Add-on	Add-on	✓[1]	✓[1]
Dynamische, risikobasierte Richtlinien	—	—	✓	✓
Kontextbezogene Warnungen	—	—	✓	✓
KI-gestützte Browser-Isolierung	Add-on	Add-on	✓	✓
Streaming von Cloud-NSS-Logs	—	Add-on	✓	✓
NSS-Log-Wiederherstellung	—	Add-on	✓	✓
Erweiterter RZ-Zugriff	Add-on	Add-on	✓	✓
IPSec-Tunnel	Add-on	Add-on	✓	✓
Data Protection Advanced Plus (Inline-Web, SaaS, E-Mail, erweiterte Klassifizierung, Incident Management)	Add-on	Add-on	Add-on	✓
Source IP Anchoring	Add-on	Add-on	Add-on	✓
Testumgebung	Add-on	Add-on	Add-on	✓
Prioritätseinstufung	Add-on	Add-on	Add-on	✓
ZIA Virtual Private Service Edge	Add-on	Add-on	Add-on	32 Einheiten
Server- und IoT-Schutz	Add-on	Add-on	Add-on	1 GB/10 User
Schutz des Gäste-WLAN	Add-on	Add-on	Add-on	1 GB/4 User
Premium Support Plus	Add-on	Add-on	Add-on	✓
Transparenz über alle IoT-Geräte	Add-on	Add-on	Add-on	Add-on

[1]Mindestens 1000 ZIA-Lizenzen erforderlich

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. Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Benutzern, 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