E-Book

Die wichtigsten Anwendungsfälle für SSE-Datenschutz

Mithilfe von Zscaler SSE Datenpannen
in der modernen Geschäftswelt verhindern

Inhalt

E-Book

Der Durchbruch von SSE

User und Anwendungen von Unternehmen befanden sich in der Vergangenheit On-Premise, was zu einem Siegeszug der Sicherheitsmaßnahmen nach dem Festung-mit-Burggraben-Prinzip führte. Dafür waren allerdings kostspielige Appliances erforderlich, die Netzwerkperimeter bildeten, um die enthaltenen Daten zu schützen.

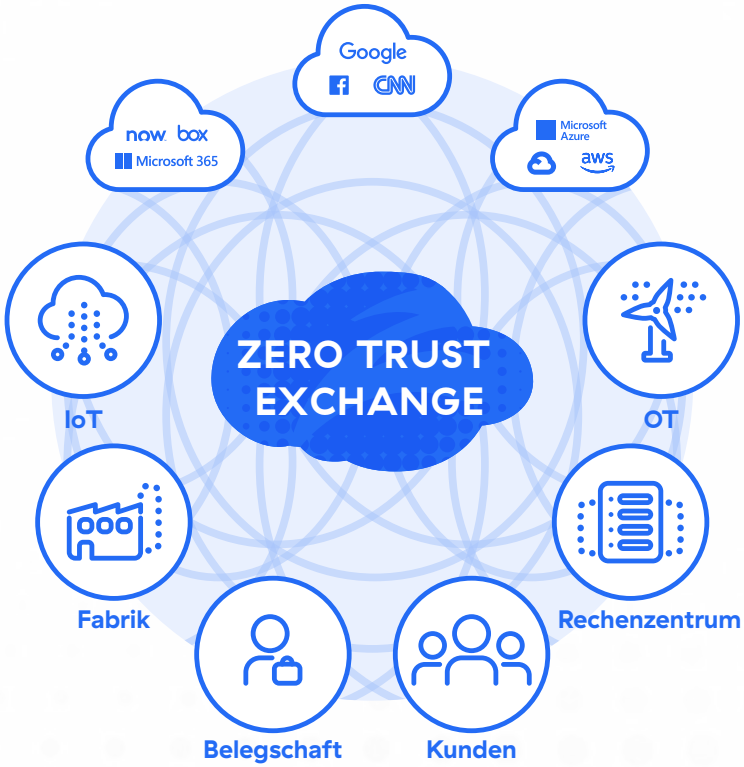
Durch die Cloud, das Web und Remote-Arbeit ist dieses Prinzip überholt. Trotzdem verlassen sich zahlreiche Unternehmen nach wie vor auf veraltete Architekturen. Leider können komplexe Appliance-Stacks modernen Anforderungen an den Datenschutz nicht gerecht werden. Das Backhauling von Traffic führt zu schlechter Performance und beeinträchtigt die Skalierbarkeit ebenso wie die Produktivität der User.

Auch viele moderne Datenschutz-Tools sind unzureichend — insbesondere, wenn sie sich auf Bedrohungen durch Insider konzentrieren und externe Bedrohungen vernachlässigen. Mit anderen Worten: Für den richtigen Datenschutz sind leistungsstarke Sicherheitsvorkehrungen erforderlich.

Security Service Edge (SSE) ist die Lösung für diese Herausforderungen. Der Begriff beschreibt vollständige Plattformen, die durch die Integration von CASB, SWG, ZTNA und weiteren Lösungen die Komplexität reduzieren und moderne Datenschutzlücken schließen. Durch Cloud-basierte Sicherheit an der Edge bietet SSE maximale Performance, Skalierbarkeit und eine optimale Anwendererfahrung.

Die **Zscaler Zero Trust Exchange™** ist die weltweit größte Security Cloud und wurde lange vor SSE entwickelt, um jede Transaktion abzusichern. Sie schiebt sowohl internen als auch externen Bedrohungen des Datenschutzes einen Riegel vor.

Hier werden die häufigsten Anwendungsfälle im Bereich Datenschutz vorgestellt, die Kunden mit der SEE von Zscaler lösen.



Zero-Trust-Sicherheit erreichen

Mit Legacy-Sicherheitstools ist der uneingeschränkte Zugriff auf das gesamte Netzwerk — und auf alle darin enthaltenen Daten und Anwendungen — möglich. So können sich Bedrohungen allerdings lateral zwischen Ressourcen bewegen, wodurch die Auswirkungen von Datenpannen unter Umständen massiv verstärkt werden. Dies verstößt gegen das Zero-Trust-Prinzip der minimalen Zugriffsrechte, wonach autorisierte User nur Zugriff auf die Ressourcen erhalten, die sie benötigen — und ausschließlich in dem Moment, in dem sie sie benötigen.

Zero Trust Exchange

Die Zero Trust Exchange verfolgt einen grundlegend anderen Ansatz und bietet modernen, Zero-Trust-basierten Datenschutz. Als intelligente Schaltzentrale zwischen Usern, SaaS-Anwendungen, privaten Anwendungen, IoT/OT und mehr erweitert Zscaler den sicheren Zugriff nur auf einzelne Ressourcen, wenn dies erforderlich ist, und setzt gleichzeitig Maßnahmen zur Data Loss Prevention (DLP) durch, um mehr Granularität zu erzielen.

Der Zscaler-Vorteil

- Alle IT-Ressourcen werden hinter der Zero Trust Exchange verborgen, um die Angriffsfläche zu minimieren
- User werden direkt mit Anwendungen verbunden, ohne Zugang zum Netzwerk zu erhalten — so können sich Bedrohungen nicht mehr lateral ausbreiten
- Kompromittierungen werden verhindert, da alle Transaktionen zwischen User und Anwendung, von Anwendung zu Anwendung und zwischen Computern geschützt werden

Datenverlust durch verschlüsselten Traffic verhindern

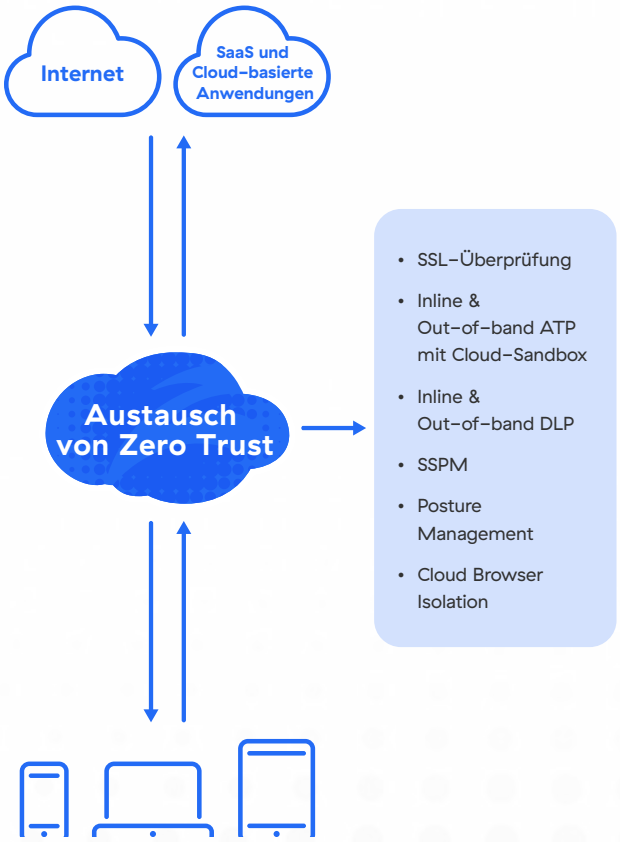
Legacy-Sicherheitsappliances (ob Hardware oder virtuell) werden häufig verwendet, um den Web-Traffic auf Datenverluste zu überprüfen. Appliances verfügen jedoch über feste Kapazitäten, die Usern zur Verfügung gestellt werden, können verschlüsselten Traffic nicht in großem Maßstab bewältigen und bieten daher kaum oder gar keine Möglichkeiten zur SSL-Überprüfung. Da mehr als 95 % des Web-Traffics mittlerweile verschlüsselt sind, ist dies eine gefährliche Schwachstelle.

Eine echte Cloud-Architektur

Die Zscaler Security Service Edge basiert auf der weltweit größten Security Cloud und liefert die erforderliche Performance, um verschlüsselten Traffic für globale Unternehmen mit Hunderttausenden von Usern in großem Maßstab zu überprüfen. Dadurch wird sichergestellt, dass jeder potenzielle Datenverlust, der mittels SSL verborgen wird, erfolgreich in Echtzeit erkannt und behoben werden kann.

Der Zscaler-Vorteil

- Eine Security Service Edge mit einzigartiger Skalierbarkeit und Performance, die täglich über 200 Milliarden Transaktionen verarbeitet
- Eine Plattform, die auf einer bewährten Inline-Architektur basiert und von über 25 % der Forbes Global-2000-Unternehmen genutzt wird
- Eine globale Präsenz von über 150 Rechenzentren, die Sicherheit an der Edge bieten, um eine erstklassige Anwendererfahrung zu gewährleisten



Ransomware mit Doppelerpressung abwehren

Zusätzlich zur Geräteverschlüsselung stehlen Cyberkriminelle über Ransomware für Doppelerpressung Daten und drohen mit deren Offenlegung, wenn das Lösegeld nicht gezahlt wird. Angreifer suchen nach „weichen" Zielen (beispielsweise ungesicherte ruhende Daten und falsch konfigurierte Anwendungen), um Daten zu vervielfältigen und zu exfiltrieren. Leider können Legacy-Sicherheitsappliances dies in unserer Cloud-first-Welt nicht verhindern.

Vollständiger Schutz vor Bedrohungen und Datenschutz

Zscaler bietet einen umfassenden Schutz vor Bedrohungen, um Ransomware bei Upload und ruhenden Daten im gesamten IT-Ökosystem abzuwehren. Darüber hinaus überprüfen DLP und CASB alle Cloud-Datenkanäle, um die Exfiltration zu verhindern, während Posture Management und SSPM Fehlkonfigurationen bei Cloud-basierten Anwendungen aufdecken, durch die Daten offengelegt werden.

Der Zscaler-Vorteil

- Vollständige, skalierbare SSL-Überprüfung zur Echtzeiterkennung von Datenexfiltration und Ransomware bei der Übertragung
- Cloud-Sandboxing-Technologie zum Stoppen von Zero-Day-Ransomware sowohl inline als auch out-of-band
- Die weltweit größte Security Cloud — Bedrohungen werden jederzeit abgewehrt — egal, wo sie auftreten

SaaS-Anwendungen schützen

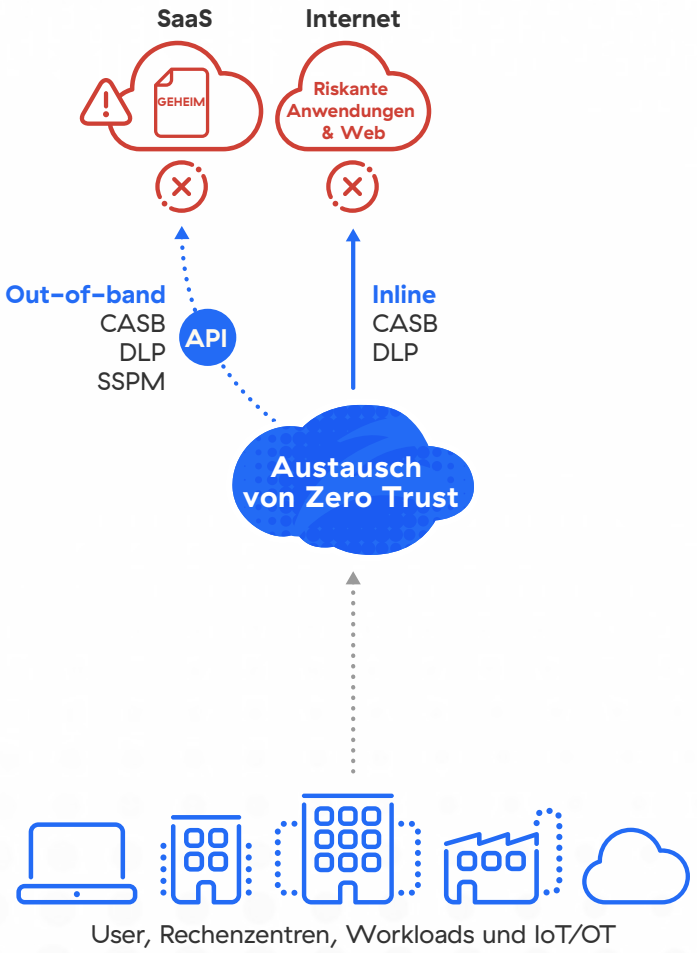
SaaS-Anwendungen sorgen für beispiellose Produktivität und Flexibilität, sind jedoch anfällig für Datenverluste, wenn sie nicht ordnungsgemäß geschützt sind. Dies liegt daran, dass User regelmäßig Daten in inoffiziell genutzte Anwendungen hochladen und ruhende Dateien leicht mit Unbefugten geteilt werden können. Außerdem kann der Sicherheitsstatus von Anwendungen durch Fehlkonfigurationen beeinträchtigt werden, wodurch unter Umständen auch Daten offengelegt werden.

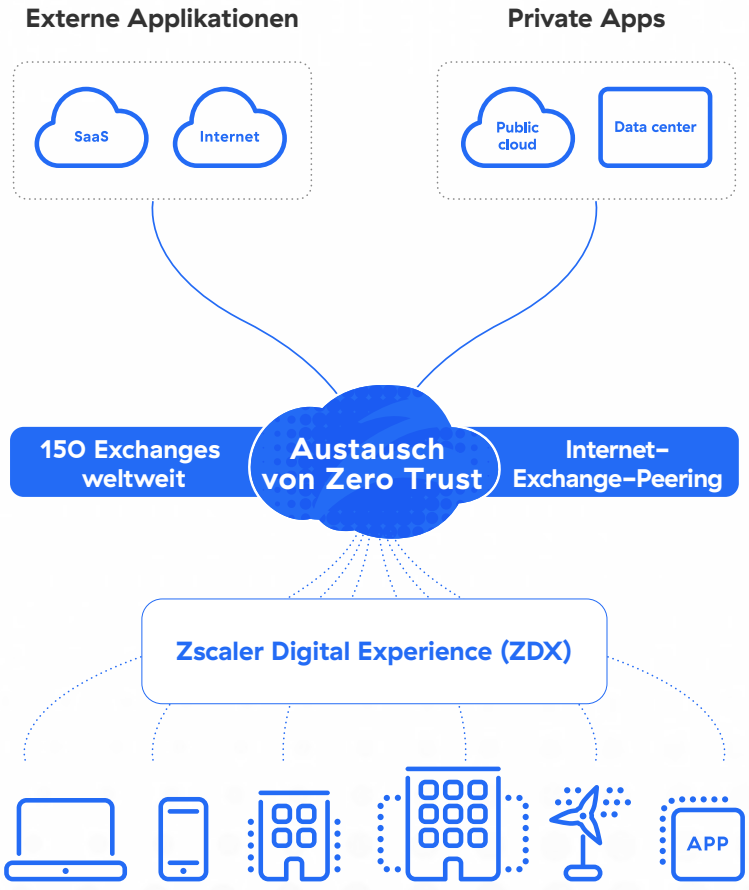
CASB mit DLP

Zscaler ermöglicht die sichere Verwendung von SaaS-Anwendungen: Schatten-IT wird erkannt, Datenuploads in inoffiziell genutzte Cloud-basierte Anwendungen werden kontrolliert und ruhende Daten in genehmigten Cloud-basierten Anwendungen geschützt. Darüber hinaus scannt das SaaS Security Posture Management Anwendungen auf Fehlkonfigurationen, durch die Daten offengelegt werden könnten oder die Compliance gefährdet wird.

Der Zscaler-Vorteil

- Einheitlicher Datenschutz, der alle SaaS- und Cloud-Datenkanäle mit einer einzigen Richtlinie schützt
- Leistungsstarke CASB-Funktionen als Teil der bewährten und integrierten Security Service Edge
- Cloud DLP mit erweiterten Funktionen wie EDM und OCR zum Schutz bestimmter Werte und Bilddaten





Jeder User, jedes Gerät, jede Anwendung, überall

Daten von Remote-Usern schützen

Remote-Arbeit ist aus unserem Alltag nicht mehr wegzudenken, aber Legacy-Sicherheitskonzepte wurden nicht für diese Arbeitsweise entwickelt. Die Nutzung von VPN und das Backhauling des User-Traffics zu Sicherheitsappliances führt zu unzureichender Skalierbarkeit, beeinträchtigt die Produktivität der User und ist nicht für moderne Anwendungsfälle im Bereich Datenschutz konzipiert, die Cloud-first-Unternehmen abdecken müssen.

Cloud-basierte Sicherheit an der Edge

Mit der weltweit größten und am besten bewährten Security Cloud verfügt Zscaler über die Skalierbarkeit und das erforderliche Fachwissen, um Daten zu schützen und gleichzeitig Remote-Arbeit auf der ganzen Welt zu ermöglichen. Zscaler ist in der Lage, SaaS, IaaS, PaaS, das Web und private Anwendungen ohne Backhauling des Traffics zu einer Appliance zu schützen, und gewährleistet so Datenschutz mit maximaler Performance auf der ganzen Welt.

Der Zscaler-Vorteil

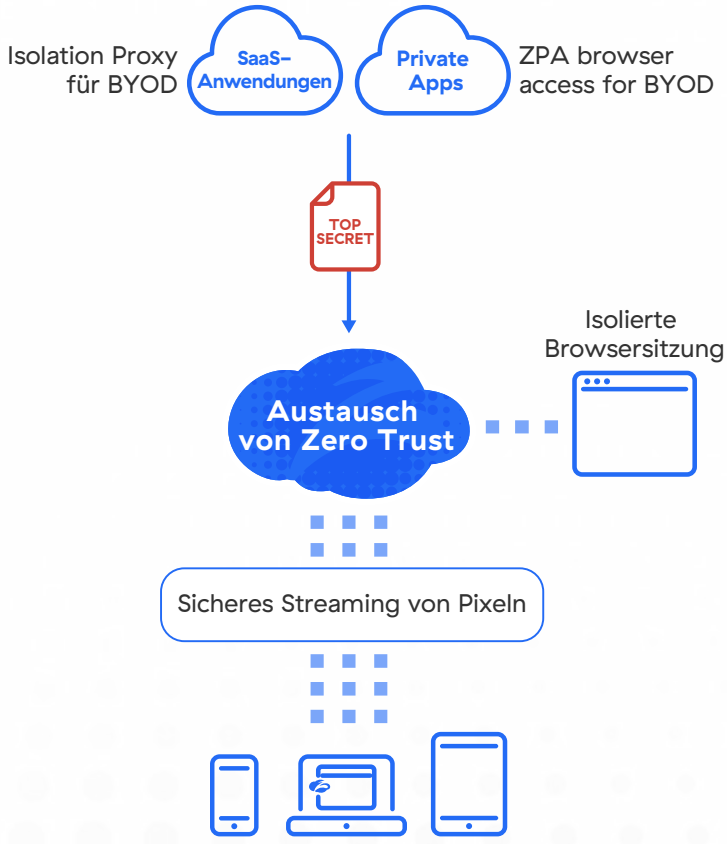
- Die globale Security Cloud mit über 150 Rechenzentren bietet leistungsstarke Datensicherheit an der Edge
- Ein Security-as-a-Service-Angebot macht das Backhauling zu Hardware- und virtuellen Appliances überflüssig
- Unsere Single-Pass-Architektur mit CASB, SWG, ZTNA und mehr bietet effizienten, umfassenden Schutz — überall

BYOD und andere nicht verwaltete Geräte schützen

Private oder nicht verwaltete Endgeräte wie BYOD- und B2B-Geräte müssen oft aus triftigen Gründen auf Unternehmensanwendungen zugreifen — aber die IT verfügt nicht mehr über die nötige Kontrolle, sobald Daten heruntergeladen werden. Das Blockieren dieser Geräte beeinträchtigt die Produktivität, die Installation von Software-Agenten ist in der Regel nicht durchführbar und Reverseproxys funktionieren häufig nicht. Was soll die IT also tun?

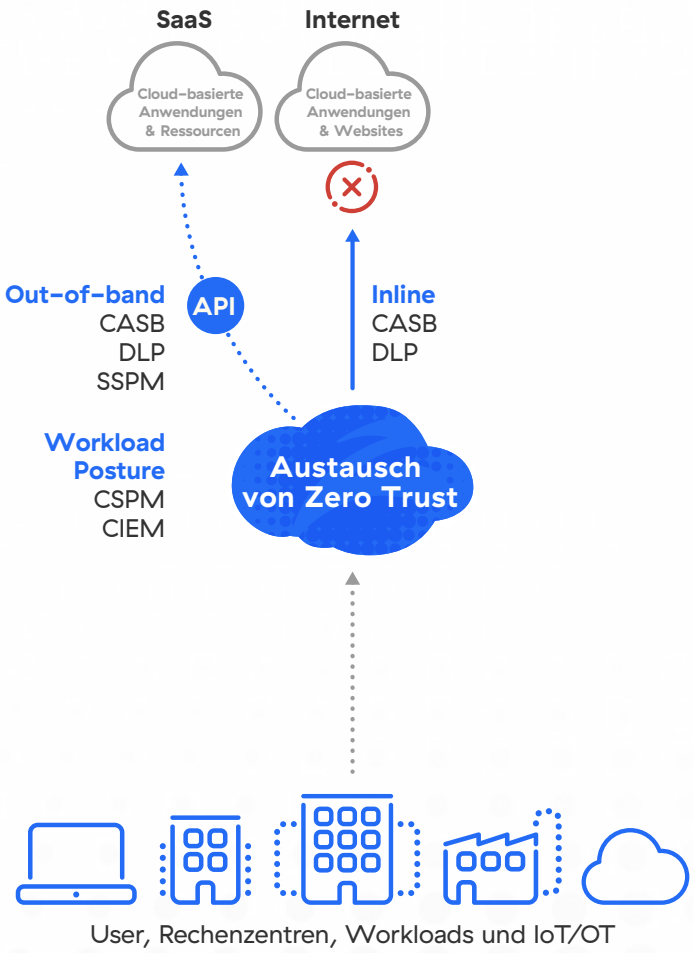
Cloud-Browser-Isolation

Mit agentenloser Browser Isolation virtualisiert Zscaler die Anwendungssitzung eines Users in einer isolierten Umgebung und streamt nur Pixel auf das Endgerät, sodass User keine Daten herunterladen, kopieren, einfügen oder drucken können. Das bedeutet, dass die IT nicht verwalteten Zugriff auf Geräte ermöglichen und gleichzeitig Daten schützen und die Herausforderungen, die Agents und Reverseproxys darstellen, umgehen kann. So lässt sich auch das Hochladen infizierter Dateien über riskante Endgeräte verhindern.



Der Zscaler-Vorteil

- Cloud Browser Isolation basiert auf der weltweit größten Security Cloud mit maximaler Performance
- Isolation Proxy für agentenlose Sicherheit auf jedem Gerät, das auf SaaS-Anwendungen zugreift
- ZPA Browser Access für sicheren Zugriff auf private Anwendungen ohne clientseitige Softwareinstallationen



Gesetzliche Vorschriften einhalten

Daten, die der DSGVO, HIPAA und anderen Vorschriften unterliegen, werden zusammen mit den übrigen vertraulichen Unternehmensinformationen off-Premise verlagert. Legacy-Tools sind jedoch nicht in der Lage, sie zu schützen und die Compliance in der Cloud sicherzustellen. Dies ist von entscheidender Bedeutung, da die Nichteinhaltung von Datenschutzgesetzen wie CCPA und Frameworks wie PCI DSS zu Geldstrafen, dem Vertrauensverlust der Verbraucher und Umsatzeinbußen führen kann.

Lückenlose Compliance sicherstellen

Die Zscaler Security Service Edge wurde mit Blick auf die gesetzlichen Vorschriften konzipiert. Die Lösung bietet vollständige Transparenz und Kontrolle im gesamten IT-Ökosystem und stellt so sicher, dass regulierte Daten geschützt sind, Anwendungen keine Sicherheitsrisiken aufweisen, die die Compliance beeinträchtigen, und Zero-Trust-Prinzipien überall durchgesetzt werden.

Der Zscaler-Vorteil

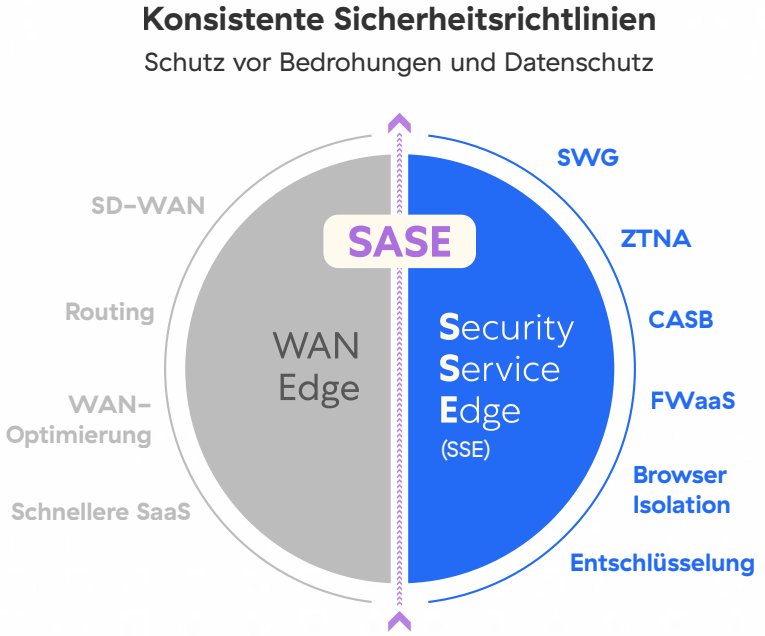
- Cloud DLP mit multimodalen CASB-Funktionen, die regulierte Daten bei der Übertragung und im Ruhezustand schützen
- Einhaltung der Compliance — Zscaler lädt keine Daten zur Überprüfung herunter, auch nicht für Maßnahmen wie Exact Data Match
- Zscaler SSPM und Posture Management zur Ermittlung und Behebung von Fehlkonfigurationen und Berechtigungen, die zu mangelhafter Compliance führen

Einheitlichen, verwaltbaren Datenschutz erzielen

Ein Sammelsurium unzusammenhängender Einzelprodukte mit unterschiedlichen Funktionen zu verwenden, bringt eine Reihe von Herausforderungen mit sich. Insbesondere führt diese Vorgehensweise zu inkonsistentem Datenschutz in einem zunehmend komplexen IT-Ökosystem. Darüber hinaus haben Administratoren, die eine Vielzahl von Einzellösungen überwachen, mit einem erheblichen Verwaltungsaufwand zu kämpfen.

Eine All-in-One-Plattform

Zscaler SSE integriert führende Technologien, die alle Transaktionen und Daten einheitlich und vollständig schützen können, wo immer sie sich befinden. Durch ein umfassendes Cloud-Angebot mit einer Single-Pass-Architektur können Unternehmen darüber hinaus ihre IT-Komplexität reduzieren und gleichzeitig den Verwaltungsaufwand für Administratoren verringern.



Der Zscaler-Vorteil

- Konsistenter Datenschutz für alle SaaS-, Cloud-, Web- und privaten Anwendungen
- Vereinfachte Architektur, die die Anzahl der Einzelprodukte und Appliances reduziert
- Konsolidiertes Management ohne doppelte Richtlinien, wodurch sich Administratoren wieder auf das Wesentliche konzentrieren können

Cloud und Mobilität bieten unzählige Vorteile hinsichtlich Produktivität und Flexibilität. Um diese jedoch ohne Gefährdung der Datensicherheit optimal nutzen zu können, benötigen Unternehmen eine neue Herangehensweise an die Cybersicherheit. Mit der Zscaler Security Service Edge können Unternehmen die digitale Transformation vorantreiben und gleichzeitig ihre Daten schützen — egal, wo sie sich befinden.

- **Kundenreferenzen zu Zscaler SSE aufrufen**
- **Magic Quadrant für Security Service Edge lesen**

zscaler™ | **Experience your world, secured.™**

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

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