3 unverzichtbare Voraussetzungen für zuverlässigen Datenschutz

Besserer CASB und stärkerer DLP? Das geht nur mit dem richtigen Fundament.

In puncto Datenschutz war früher vieles einfacher: Ihre Daten waren im Rechenzentrum sicher aufgehoben, und Ihre Mitarbeiter saßen im Büro an Rechnern, die mit dem Unternehmensnetzwerk verbunden waren. Diese Zeiten sind definitiv vorbei.

Heute sind Ihre Daten über Hunderte von Cloud-Apps verteilt. Und Ihre Mitarbeiter sitzen im Homeoffice – außer Reichweite des Unternehmensnetzwerks und weit weg von Ihren Sicherheitskontrollen. Als ob das noch nicht problematisch genug wäre, wird durch die zunehmende Verschlüsselung des Internet-Traffics die Überwachung erschwert – und Cyberkriminellen die Arbeit leicht gemacht. Dass die Mitarbeiter derweil in ungesicherten Netzwerken mit ungeschützten Geräten unterwegs sind, trägt zur weiteren Verschärfung der Risiken bei.

In dieser schönen neuen Welt kommen Unternehmen nicht ohne eine Datenschutzplattform aus, die speziell für Cloud- und Mobilanwendungen konzipiert wurde und die beschriebenen Voraussetzungen erfüllt.

Das sollten Sie wissen

Der durch CASB und DLP gewährleistete Datenschutz ist nur so gut wie die zugrunde liegende Architektur. Diese Erkenntnis ist der erste Schritt zum Erfolg.

Voraussetzung Nr. 1

Speziell konzipierte SASE-Architektur

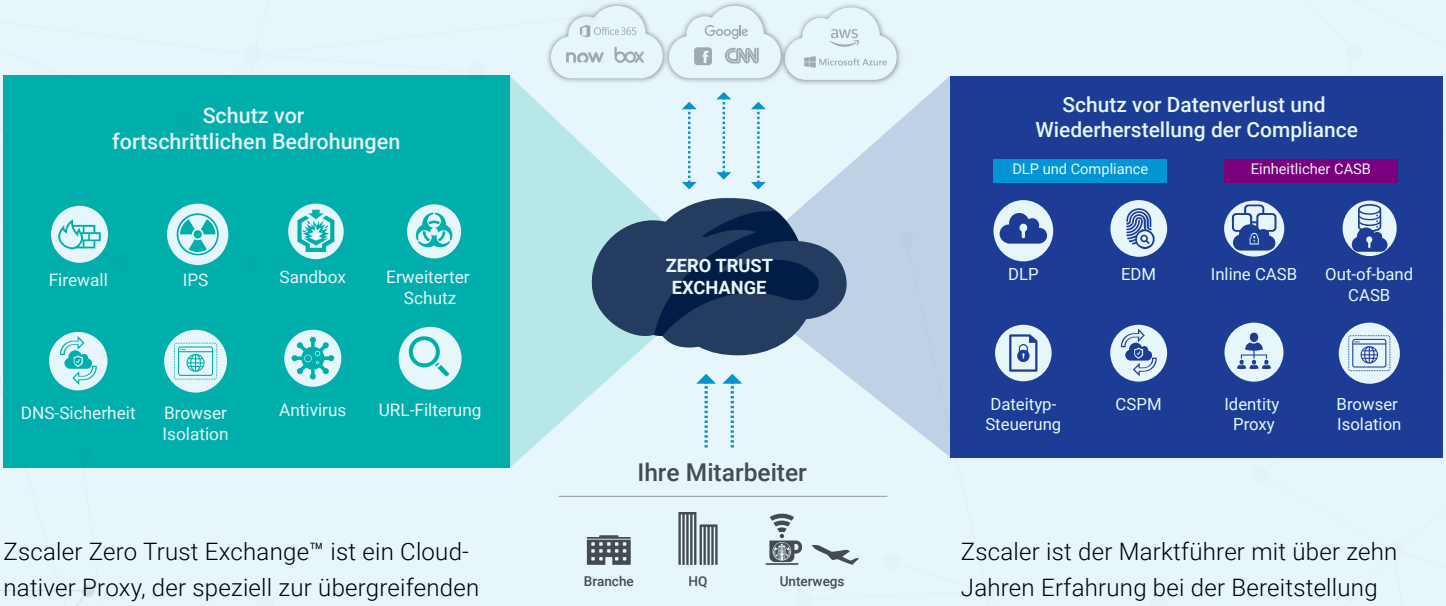
Angesichts der Cloud und der zunehmenden Mobilität können hardwarebasierte Sicherheitslösungen naturgemäß nicht überall sein. Mit Verlassen des Unternehmensnetzwerks verlieren Sie Ihre User aus dem Blick, und schon sind Ihre Daten in Gefahr. Zur lückenlosen Bereitstellung von CASB- (Cloud Access Security Broker) und DLP-Funktionen (Data Loss Protection) ist zudem vollumfängliche SSL-Überprüfung erforderlich. Hardwarebasierte Lösungen können das nicht leisten.

Eine speziell konzipierte SASE-Cloud-Plattform ist die erste Voraussetzung zur standortunabhängigen Gewährleistung jederzeit verfügbarer sicherer Hochleistungsverbindungen. SASE kombiniert alle CASB-, DLP- und Sicherheitsfunktionen in einer dezentralen Cloud-Plattform, die für weniger Komplexität, besseren Datenschutz und mehr Geschwindigkeit für die User sorgt.

Das sollten Sie wissen

Der Aufbau einer SSL-übergreifend skalierbaren, unternehmenstauglichen Inline-Datenschutzarchitektur ist alles andere als einfach. Deshalb sollten Sie Ihren Traffic nur einem Anbieter mit ausgewiesener Erfahrung und unternehmenstauglichen SLAs anvertrauen.

Die Zscaler™-Lösung



Zscaler Zero Trust Exchange™ ist ein Cloud-nativer Proxy, der speziell zur übergreifenden Datensicherung und SSL-Überprüfung für 150 Rechenzentren konzipiert wurde. Jeder User erhält eine schnelle und sichere Verbindung. Dank unserer unbegrenzten SSL-Kapazität werden sämtliche Daten bei allen User-Verbindungen innerhalb und außerhalb des Netzwerks gesichert.

Zscaler ist der Marktführer mit über zehn Jahren Erfahrung bei der Bereitstellung von Lösungen für die Inline-Überprüfung. Durch die Integration von DLP, CASB und allen weiteren Sicherheitslösungen profitieren Unternehmen zudem von vereinfachter Richtlinienverwaltung und einer einheitlichen Plattform für Datenschutz und Bedrohungsabwehr.

Voraussetzung Nr. 2

Zuverlässige Kontextinformationen

Zur richtigen Klassifizierung der vorliegenden Daten benötigen Sie Kontextinformationen. Die Qualität Ihrer Entscheidungsfindung hängt von der Qualität dieser Informationen ab.

Früher war das kein Problem: Die User griffen über einen Exchange-Server auf E-Mails zu; bestenfalls hatten Sie vielleicht noch ein paar Dateiserver. Alle Informationen, die Sie für eine fundierte Entscheidungsfindung brauchten, standen buchstäblich auf Abruf bereit.

Heute sind Ihre Daten in Hunderten von Kanälen unterwegs – von Cloud-Apps über öffentliche Clouds bis hin zu Filesharing-Plattformen, und die benötigten Kontextinformationen sind in SSL-Verschlüsselungen verborgen.

Das sollten Sie wissen

Kontext ist das Lebenselixier Ihres CASB und DLP. Sie brauchen eine Plattform mit der leistungsstärksten Klassifizierungsengine, die bei jeder Cloud-Transaktion – innerhalb oder außerhalb des Netzwerks sowie in SSL – die meisten Attribute erkennt.

Die Zscaler™-Lösung

Beim Thema Kontext ist Zscaler unübertroffener Spitzenreiter.

Zscaler Zero Trust Exchange und die Client-Connector-App unterstützen den lückenlosen Schutz Ihrer Daten bei allen Verbindungen innerhalb oder außerhalb des Netzwerks. Durch transparenten Einblick in den gesamten SSL-Traffic erhalten Sie wertvolle Kontextinformationen.

Branchenspezifische und benutzerdefinierte Wörterbücher sowie zukunftsweisende Techniken wie Exact Data Match (EDM) Fingerprinting unterstützen die Klassifizierung von Daten in gängigen Branchenformaten (PCI, HIPAA) und unternehmensspezifischen Definitionen.

Kontext von einer Firewall oder einem Proxy	**172.16.1.12** Source IP | **64.81.2.24** Destination IP | **TCP/443** Destination Port **SSL** Protokoll | **HTTPS** Protokoll	Traditionelle Inline-Ansätze bieten keinen ausreichenden Einblick in den Kontext.
Zusätzlicher Kontext, den Sie mit vollständiger SSL-Entschlüsselung erhalten	**JohnDoe** User | **prodmgmt** Gruppe | **HQ** Standort **upload** App-Funktion | **jumpshare** Anwendung | **PowerPoint** Dateityp **file sharing** URL-Kategorie | **"Confidential"** Inhalt	Die Entschlüsselung aller SSL-Daten ohne Einschränkung stellt den benötigen Kontext dar, um bessere Schutzentscheidungen zu treffen.

Voraussetzung Nr. 3

Einheitliche Plattform zum Schutz sämtlicher Kanäle

Zum wirksamen Schutz Ihrer Daten vor versehentlicher Offenlegung und böswilliger Exfiltration ist eine kanalübergreifende Überwachung erforderlich. Ihre Daten sind angreifbar und potenziellen Bedrohungen ausgesetzt, wenn diese nicht gewährleistet ist.

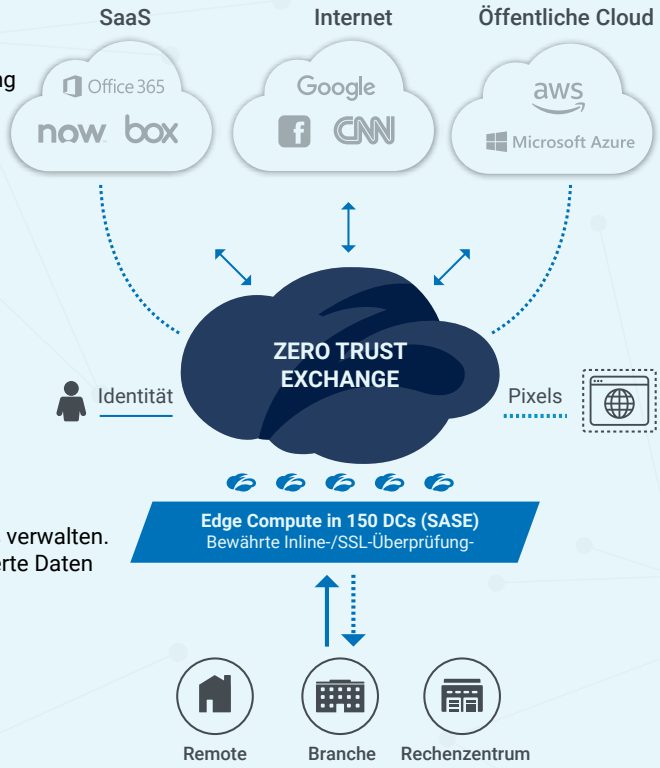
Wenn sich nicht alle CASB- und DLP-Funktionen über eine einheitliche Plattform verwalten lassen, machen Sie sich die Arbeit unnötig schwer. Ohne eine einheitliche Plattformansicht verlieren Sie schnell den Überblick. Die Folge sind widersprüchliche Richtlinien, Sicherheitslücken und kostspielige Konfigurationsfehler.

Das sollten Sie wissen

Eine einheitliche Plattform für alle wichtigen Datenkanäle – bei der Übertragung, im Ruhezustand, Endgeräte und Cloud-Anbieter – trägt signifikant zur Stärkung Ihrer Richtlinien und Vereinfachung Ihrer Workflows bei.

Die Zscaler™-Lösung

Alle Cloud-Dienste von Zscaler sind in eine speziell konzipierte Inline-Cloud-Architektur integriert. Durch ihr reibungsloses Zusammenwirken werden Richtlinien vereinheitlich und Mechanismen zum kanalübergreifenden Schutz Ihrer Daten optimiert.



Daten im Ruhezustand

User verwalten und Bedrohung Aufdeckung in Microsoft 365 und SaaS

- DLP
- Bedrohung Verhinderung
- Historische Daten-Scans
- Sharing-Anfälligkeit

Anbieter

Behebung von Fehlkonfigurationen in öffentlichen Clouds und SaaS (CSPM)

Daten-in-motion

Unbefugte und Shadow-Apps verwalten. Industrie und benutzerdefinierte Daten einordnen und verwalten

- Dateityp-Steuerung
- Cloud App Control
- Cloud DLP
- Exact Data Match
- Microsoft 365-Überprüfung

Endpoints

Verhindert unkontrollierten / BYOD-Zugriff und Schutz vor Datenverlusten

- Identitäts-Proxy
- Browser Isolation

Das funktioniert so:

Bei der Übertragung: Unternehmenstaugliche Inline-Überprüfung ist eine unverzichtbare Voraussetzung für zuverlässigen Datenschutz in Echtzeit. Die Inline-Cloud von Zscaler wurde speziell zu diesem Zweck konzipiert und ermöglicht die Überwachung der User auch außerhalb des Netzwerks und in SSL. So können unternehmenskritische Daten schnell klassifiziert und ihre Übertragung verhindert werden. Nicht genehmigte Cloud-Apps werden einfach gesperrt.

Im Ruhezustand: Behalten Sie den Überblick über die Cloud-Apps, mit denen Ihre User arbeiten. Mit dem Out-of-Band CASB von Zscaler haben Sie dem unzulässigen Dateiaustausch über Microsoft-365-Apps wie SharePoint und OneDrive schnell einen Riegel vorgeschoben. Unterstützt wird auch das Scannen von Datei-Repositories auf DLP- und Malware-Bedrohungen.

Endgeräte: In diesem Kanal geht es darum, den Zugriff auf Ihre Daten ausschließlich auf befugte User einzuschränken. Zugriffskontrollen für private Endgeräte der User ermöglichen schnelle SAML/SSO-Lookups zur Verhinderung unbefugter Zugriffe auf Microsoft-365-Ressourcen. Zscaler Cloud Browser Isolation verhindert die Offenlegung von Daten auf nicht geschützten privaten Endgeräten, indem Daten ausschließlich als Pixel ausgegeben werden. So kann z. B. ein Auftragnehmer die jeweils benötigten Daten anzeigen und mit ihnen interagieren. Hingegen ist kein Speichern, Herunterladen oder Kopieren der Daten möglich. Dadurch wird sichergestellt, dass nach Schließen der jeweiligen Session keine Daten auf dem Gerät verbleiben.

Anbieter: Die versehentliche Fehlkonfiguration von Cloud-Anwendungen zählt zu den häufigsten Ursachen von Datenschutzverletzungen und ist für die betroffenen Unternehmen mit einem hohen Zeit- und Kostenaufwand verbunden. Zscaler Cloud Security Posture Management (CSPM) erkennt und behebt Fehlkonfigurationen von Anwendungen in SaaS, IaaS und PaaS, sodass das Risiko von Datenverlusten minimiert und die Compliance gewährleistet wird.

Fazit

Die zunehmende Beliebtheit von Cloud- und Mobilanwendungen hat den Geschäftsalltag von Unternehmen und Mitarbeitern gleichermaßen verändert. Daten werden heute anders verarbeitet und müssen daher auch anders geschützt werden. Herkömmliche Sicherheitsanwendungen sind dieser Aufgabe einfach nicht mehr gewachsen. Stattdessen brauchen Sie eine Cloud-native, SASE-basierte Sicherheitsplattform, die Ihre Daten an jedem Punkt schützen kann. Sie brauchen Zscaler.

Erleben Sie unseren Inline-CASB/DLP in Aktion
youtube.com/watch?v=R88TlNEMgGE

Erleben Sie unseren Out-of-Band CASB in Aktion
youtube.com/watch?v=1KtoW-IXgMs

Kontaktieren Sie uns oder buchen Sie eine Vorführung
zscaler.com/company/contact

Über Zscaler
Zscaler unterstützt Unternehmen bei der digitalen Transformation mit Zero Trust Exchange, einer SASE-basierten Plattform zur Einrichtung schneller und sicherer Verbindungen zwischen Usern, Geräten und Anwendungen in jedem beliebigen Netzwerk.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134, USA
+1 408 533 0288
www.zscaler.com