Überdenken Sie die Sicherheit für eine sich weiterentwickelnde Belegschaft

IT-Abteilungen befinden sich in der wenig beneidenswerten Situation, Beschäftigte absichern zu müssen, die überall arbeiten – in der Firmenzentrale, in einer Niederlassung, zu Hause oder praktisch an jedem beliebigen Ort. Da VPNs mit einer größeren Remote-Belegschaft zu kämpfen haben und sich Benutzer direkt mit ihren Cloud-Applikationen verbinden, werden immer mehr Geschäfte abseits von Sicherheitsrichtlinien und -kontrollen abgewickelt. Dies weckt die Aufmerksamkeit von Cyberkriminellen, die ihre Angriffe gegen die wachsende Remote-Belegschaft richten. All dies setzt Ihr Unternehmen einem noch größeren Risiko aus und zwingt Sie dazu, nach einer einfachen, effektiven Lösung für diese Sicherheitsprobleme zu suchen.

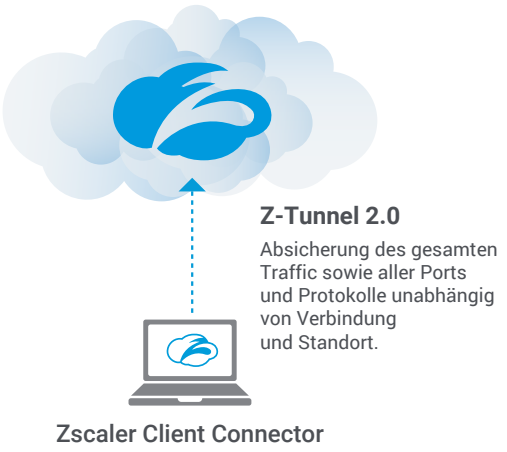
Mithilfe der Leistungsfähigkeit und Flexibilität von Zscaler Internet Access™ (ZIA™) können Organisationen ihre sich weiterentwickelnde Belegschaft unabhängig von deren Arbeitsort und Gerät vollständig absichern. Mit Cloud Firewall, Cloud Sandbox und Cloud DLP, die den Verbindungen der Benutzer folgen, können IT-Abteilungen schnelle direkte Internetverbindungen bereitstellen, ohne das Risiko zu erhöhen. Sie erhalten hermetischen Schutz vor Verstößen und Exfiltration und geben Ihren Benutzern gleichzeitig die Freiheit, wo und wie auch immer zu arbeiten, und das alles zu einem Bruchteil der Kosten herkömmlicher Ansätze.

Ihre Benutzer fordern mehr Flexibilität, um überall und ganz nach Belieben arbeiten zu können. Das Problem ist, dass die auf Ihre Benutzer abzielenden Bedrohungen zunehmen, wenn Benutzer Ihr Netzwerk verlassen und Ihre Richtlinien umgehen. Ihr Netzwerk und Ihre Sicherheit kosten mehr, als sie wert sind. Es bedarf eines besseren Ansatzes für die Zukunft der Konnektivität.

Wie Sie Ihre ortsunabhängig arbeitende Remote-Belegschaft absichern

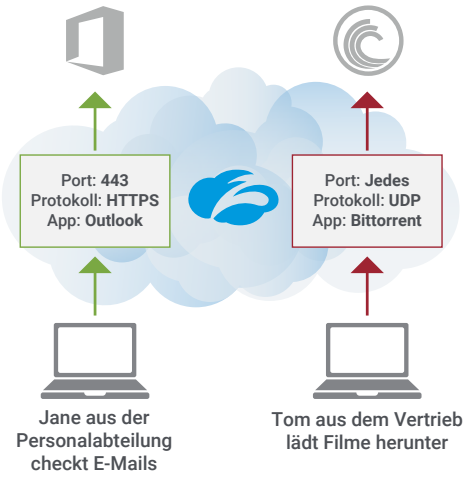
Es beginnt mit Zscaler Client Connector und Z-Tunnel 2.0

Alles beginnt mit dem Zscaler Client Connector (ehemals bekannt als Zscaler App). Bevor das Gerät des Benutzers mit dem Internet verbunden wird, stellt der Client Connector eine sichere Verbindung zur Zscaler-Cloud her. Über die neue Zscaler-Architektur Z-Tunnel 2.0, die als Proxy fungiert, werden der gesamte Traffic sowie alle Ports und Protokolle zur Überprüfung an Zscaler geleitet. Der Client Connector ist der Grundstein für schnelle, sichere Benutzerverbindungen an jedem Standort.



Kontrolle von Verbindungen außerhalb des Netzwerks mit Advanced Cloud Firewall

Selbst wenn Ihre Benutzer außerhalb des Netzwerks arbeiten, müssen ihnen Ihre Unternehmensrichtlinien folgen. Hier kommt die Advanced Cloud Firewall ins Spiel. Durch Kombinieren von Advanced Cloud Firewall und Z-Tunnel 2.0 können Sie die Verbindungen Ihrer Benutzer vollständig kontrollieren und absichern und das Risiko ohne VPN, Backhauling oder kostspielige Appliances reduzieren. Von der Blockierung von BitTorrent, über das Kontrollieren von FTP-, RDP- oder SIP-Verbindungen bis hin zur Definition von Benutzergruppen für den Zugriff auf Ring Central, Zoom and andere Applikationen, deckt die Advanced Cloud Firewall von Zscaler alles ab. Sie können endlich eine einzige, konsistente Richtlinie überall dort einsetzen, wo Ihre Benutzer Verbindungen herstellen möchten – jetzt und in Zukunft.

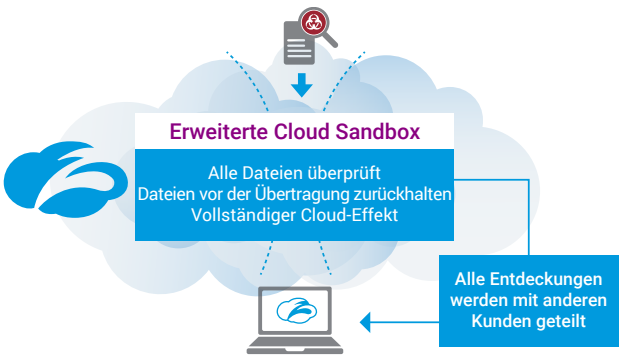


Durchsetzung von Unternehmensrichtlinien außerhalb des Netzwerks mit der Cloud Firewall

> „Wir stellten fest, dass eine Menge P2P-Traffic über unser Netzwerk lief, der an Klienten ging, die wir nicht kannten. Wir konnten das komplette Paket der Firewall-Überprüfung von Zscaler einsetzen, um diesen P2P-Traffic zu unterbinden, und auf diese Weise BitTorrent und andere P2P-File-Sharing-Services stoppen."
>
> **- Jeff Johnson, Director of Security Operations, AutoNation**

Reduzierung des Risikos von Remote-Benutzern mit Advanced Cloud Sandbox

Wenn sich Ihre Benutzer außerhalb des Netzwerks und von Ihrem Gateway entfernt aufhalten, sind sie am meisten gefährdet. Ransomware und unbekannte schädliche Dateien schlagen zu, wenn Sie es am wenigsten erwarten. Deshalb benötigen Sie eine fortschrittliche Cloud Sandbox und die ZIA Proxy-Architektur. Sie können alle Benutzer durch Inline-Zero-Day-Schutz abschirmen und sogar die Übertragung von unbekannten Dateien verzögern, bis diese als unbedenklich bestätigt werden. Sie erhalten volle Abdeckung für alle Dateitypen, die Ihre Benutzer herunterladen könnten, sowie wertvolle Bedrohungsinformationen von anderen Zscaler-Organisationen. Noch besser: Dank unbegrenzter SSL-Überprüfung können Sie jedes Byte des Traffic untersuchen und mehr Bedrohungen dort finden, wo sie sich verstecken.



Nach Einsatz von Zscaler und Cloud Sandbox konnte NOV eine 35-fache Verringerung von infizierten Geräten verzeichnen.

Umfassende Kontrolle von Datenexfiltration mit Cloud DLP

Ihre Benutzer haben das Netzwerk verlassen, das muss jedoch nicht bedeuten, dass sie Ihre sensiblen Daten mitnehmen. Mit Zscaler Cloud DLP können Sie den absichtlichen oder versehentlichen Verlust vertraulicher Daten verhindern, unabhängig davon, wo sich Ihre Benutzer verbinden. Mit vollständiger SSL-Überprüfung eliminieren Sie Schwachstellen in Ihrem verschlüsselten Traffic und erhalten besseren Einblick in Ihre Compliance-Bemühungen. Und mithilfe von Zscalers Exact Data Match können Sie Fingerabdrücke nehmen und Sie mit persönlich identifizierbaren Informationen (PII) abgleichen, um diese vor Exfiltration zu schützen.

Sichern Sie alle vertraulichen Daten über alle Verbindungen hinweg und innerhalb von SSL

> „Sofort einsetzbare DLP-Verzeichnisse sind extrem unkompliziert und waren genau das, was wir brauchten. Die Bereitstellung für Benutzergruppen war so einfach, dass der komplette DLP-Einsatz zu einer trivialen Aufgabe wurde."
>
> **- Brad Moldenhauer Director of Information Security, Steptoe & Johnson LLP**

Zusammenfassung

Wie uns die jüngsten Ereignisse gelehrt haben, müssen sich Organisationen auf eine Vielzahl von Möglichkeiten vorbereiten, einschließlich auf das Arbeiten der gesamten Belegschaft außerhalb des Firmensitzes. Diese Abwanderung aus dem Büro bedeutet auch ein Verlassen der dort vorhandenen Sicherheitsrichtlinien und -kontrollen. Organisationen benötigen eine neue Methode, um ihre Mitarbeiter und die Anwendungen, auf die sie zugreifen, unabhängig vom Arbeitsort und ohne Beeinträchtigung der Nutzererfahrung abzusichern.

Zscaler hat bereits Tausende von Organisationen dabei unterstützt, diese neue Realität des Arbeitens von überall aus sicher umzusetzen. Lassen Sie uns Ihnen zeigen, wie Sie die nötige Flexibilität erreichen können, um der Belegschaft von heute – und der zukünftigen – ein erfolgreiches Arbeiten zu ermöglichen.

Über Zscaler

Zscaler versetzt weltführende Organisation in die Lage, ihre Netzwerke und Applikationen sicher für eine mobile und Cloud-orientierte Welt zu transformieren. Seine Vorzeigedienste, Zscaler Internet Access™ und Zscaler Private Access™, stellen schnelle, sichere Verbindungen zwischen Benutzern und Anwendungen, unabhängig von Gerät, Standort oder Netzwerk, her. Die Dienste von Zscaler werden zu 100% in der Cloud bereitgestellt und bieten eine Einfachheit, Hochsicherheit und Nutzererfahrung, mit der herkömmliche Appliances oder Hybridlösungen nicht konkurrieren können. Zscaler betreibt eine in mehr als 185 Ländern genutzte mandantenfähige, verteilte Cloud-Sicherheitsplattform, die Tausende von Kunden vor Cyberangriffen und Datenverlust schützt. Weitere Informationen finden Sie unter zscaler.com, oder folgen Sie uns auf Twitter @zscaler.

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