E-Book

# 4 Gründe, warum Firewalls und VPNs für Unternehmen ein Sicherheitsrisiko bedeuten

# Die Lösungen von gestern sind die Probleme von heute

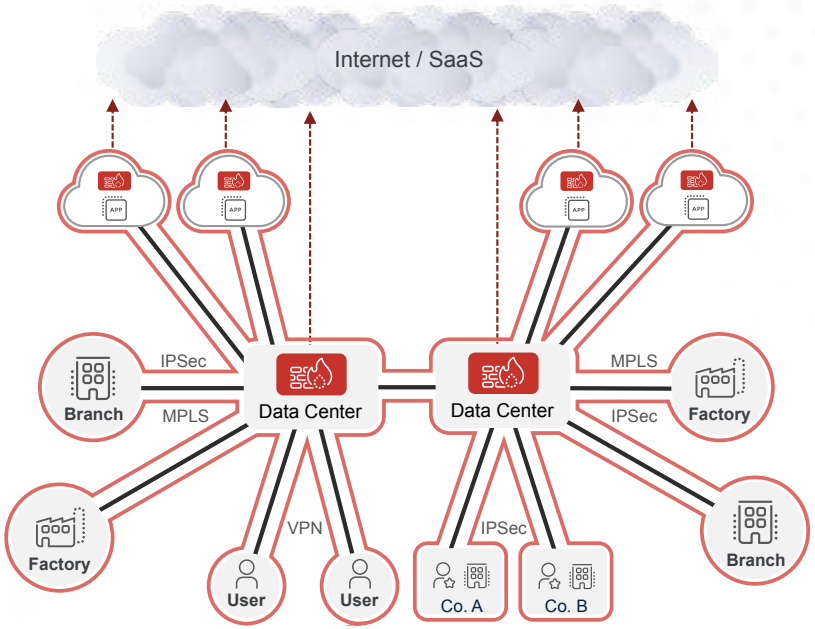
Firewalls und VPNs setzen Unternehmen der Gefahr von Sicherheitsverletzungen aus. Das mag kontraintuitiv erscheinen, da beide seit Jahrzehnten bevorzugte Sicherheitstools sind — aber genau darin liegt das Problem. Sie wurden für eine Zeit entworfen, in der ganz andere Arbeitsbedingungen herrschten als heute. Damals befanden sich User und Anwendungen vor Ort (sei es am Hauptstandort oder in einer Niederlassung), und die Sicherheitsbemühungen konzentrierten sich auf die Errichtung eines Perimeters um das Netzwerk, das sie verband. Mit anderen Worten: Ein Hub-and-Spoke-Netzwerk wurde durch ein Sicherheitsmodell nach dem Prinzip „Festung mit Burggraben" vor Bedrohungen geschützt.

Dieser Ansatz hat mehrere Namen, darunter perimeterbasierte Architektur, netzwerkzentrierte Architektur und traditionelle oder Legacy-Architektur. Unabhängig davon, wie man es nennt, beinhaltet es grundsätzlich den Einsatz von Tools wie Firewalls und VPNs zur Absicherung des Netzwerks; insbesondere durch die Blockierung externer Bedrohungen und den Schutz interner Daten.

Unternehmen haben sich in den letzten Jahren rasant weiterentwickelt, was zum großen Teil auf die COVID-19-Pandemie zurückzuführen ist. Um im Jahr 2020 produktiv zu bleiben, mussten sie ihre digitale Transformation beschleunigen und Cloud-Anwendungen und Remote-Arbeit zur neuen Norm machen. Diese Entwicklung war jedoch nicht mit Firewalls, VPNs und den perimeterbasierten Architekturen kompatibel, die die Tools voraussetzten. Das liegt daran, dass es unmöglich ist, einen Sicherheitsperimeter um ein Netzwerk herum aufzubauen, das sich immer weiter auf externe User, Geräte, Anwendungen und Clouds ausdehnt.

Für Unternehmen, die ihre digitale Transformation mit Legacy-Architektur vorantreiben, entstehen zahlreiche Herausforderungen in Bezug auf Komplexität, Flexibilität, Kosten und Produktivität. Insbesondere erhöht sich dadurch auch das Cyberrisiko und Unternehmen werden auf vier wesentliche Arten Sicherheitsgefahren ausgesetzt, die auf den folgenden Seiten erläutert werden.

**Firewall- und VPN-zentrierte Architektur**



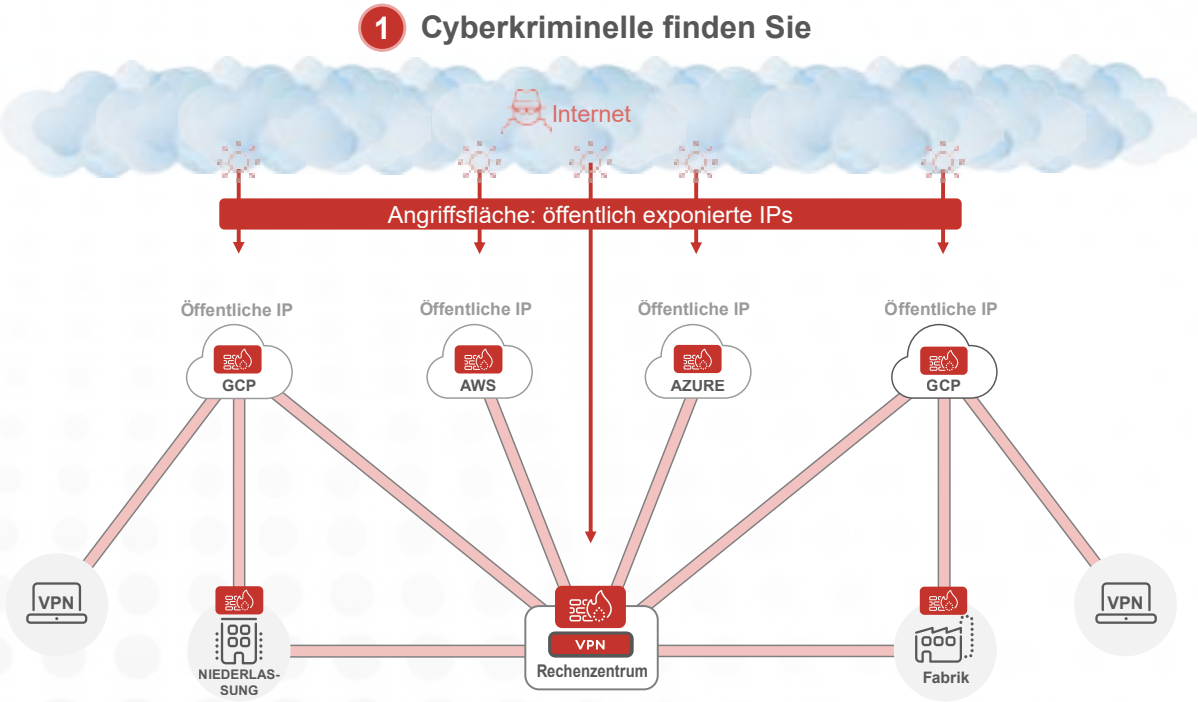

**Ein vertrauenswürdiges Netzwerk vernetzt User, Websites und Apps. Der Schwerpunkt von Bedrohungs- und Datenschutz liegt auf der Absicherung des Netzwerks.**

# #1 Firewalls und VPNs vergrößern die Angriffsfläche

Cyberkriminelle sind ständig auf der Suche nach Zielen, die sie angreifen können, um die Verteidigungslinien von Unternehmen zu durchbrechen und ihre böswilligen Pläne auszuführen. Leider vergrößern perimeterbasierte Architekturen in heutigen Arbeitsumgebungen die Angriffsfläche und unterstützen böswillige Akteure unbeabsichtigt bei ihren Bemühungen, attraktive Ziele zu identifizieren.

Wie bereits erwähnt, erfordert die weitere Nutzung eines Hub-and-Spoke-Netzwerks in der modernen Welt die kontinuierliche Erweiterung dieses Netzwerks auf immer mehr standortunabhängige User, Geräte, cloudbasierte Ressourcen, Zweigstellen und Ähnliches. Das bedeutet im Grunde, dass ein weitläufiges flaches Netzwerk eine wachsende Ansammlung miteinander verbundener Ressourcen ist. Dadurch ergeben sich für Cyberkriminelle viele mögliche Eintrittspunkte (Cloud-Anwendungen, Remote-User usw.) in das Netzwerk. Vereinfacht ausgedrückt, erzeugt ein ständig wachsendes Netzwerk eine immer größer werdende Angriffsfläche.

**Wie Firewall- und VPN-zentrierte Architektur Risiken erhöht**



Unglücklicherweise gehen Probleme in Bezug auf die Angriffsfläche bei perimeterbasierten Architekturen weit über das oben Genannte hinaus. Der Grund sind Firewalls und VPNs. Diese Tools werden als Mittel eingesetzt, um Hub-and-Spoke-Netzwerke mithilfe von Sicherheitsmodellen nach dem Festung-mit-Burggraben-Prinzip zu schützen. Ihre Verwendung hat jedoch unbeabsichtigte Folgen.

Firewalls und VPNs verfügen über öffentliche IP-Adressen, die im öffentlichen Internet auffindbar sind. Dies ist bewusst so konzipiert, damit legitime, autorisierte User über das Internet auf das Netzwerk zugreifen, mit den darin verbundenen Ressourcen interagieren und ihre Aufgaben erledigen können. Allerdings können diese öffentlichen IP-Adressen auch von böswilligen Akteuren gefunden werden, die nach Zielen suchen, die sie angreifen können, um Zugriff auf das Netzwerk zu erhalten.

Mit anderen Worten: Firewalls und VPNs bieten Cyberkriminellen mehr Angriffsvektoren, indem sie die Angriffsfläche der Organisation vergrößern. Ironischerweise bedeutet dies, dass die übliche Strategie, zusätzliche Firewalls und VPNs zur Skalierung und Verbesserung der Sicherheit einzusetzen, das Problem der Angriffsfläche tatsächlich noch verschärft.

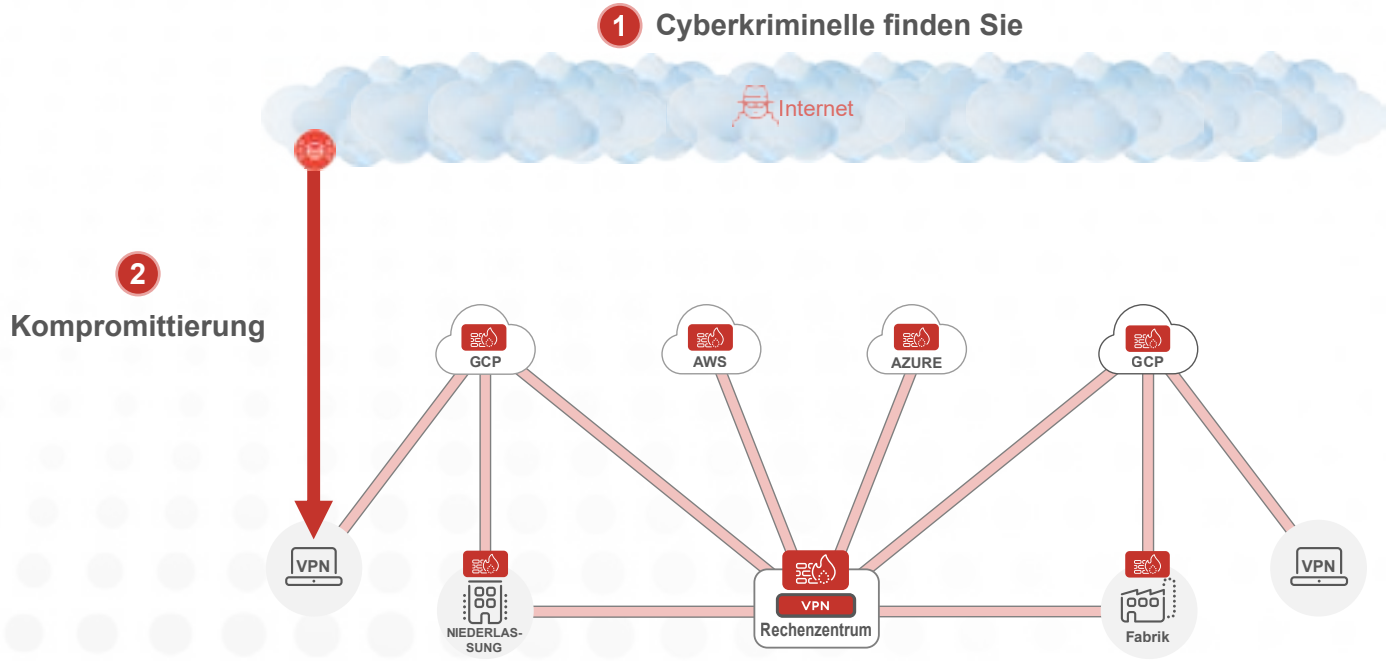
#2

# Firewalls und VPNs können eine Kompromittierung nicht verhindern

Sobald es Cyberkriminellen gelungen ist, ein attraktives Ziel zu identifizieren, starten sie ihre Cyberangriffe, um die Abwehrmechanismen der Organisation zu durchbrechen. Auch in dieser Phase der Angriffskette sind herkömmliche Tools wie Firewalls und VPNs nicht geeignet, um angemessenen Schutz zu bieten.

Um eine Kompromittierung zu verhindern, ist der Einsatz von Inline-Sicherheitsrichtlinien erforderlich, durch die Bedrohungen in Echtzeit gestoppt werden können, bevor sie in die Umgebung eines Unternehmens eindringen und Schaden anrichten können. Dies wiederum bedeutet, dass Unternehmen in der Lage sein müssen, den gesamten Traffic in ihren Betriebsabläufen zu überprüfen, um potenzielle Bedrohungen zu erkennen. Dafür ist die Fähigkeit erforderlich, verschlüsselten Traffic zu überprüfen — und zwar deshalb, weil mit über 95 % der Großteil des Web-Traffics heute verschlüsselt

**Wie Firewall- und VPN-zentrierte Architektur Risiken erhöht**



ist. Doch hier zeigt sich eine weitere entscheidende Schwäche der Firewall- und VPN-basierten Architektur.

Die Überprüfung des verschlüsselten Traffics ist ein ressourcenintensiver Prozess, was bedeutet, dass zu seiner Entschlüsselung, Untersuchung und erneuten Verschlüsselung viel Rechenleistung erforderlich ist. Sicherheitsappliances wie Firewalls haben jedoch Schwierigkeiten, die dafür erforderliche Leistung zu erbringen — unabhängig davon, ob sie als Hardware-Appliances vor Ort oder als virtuelle Appliances in einer Cloud-Instanz bereitgestellt werden.

Das liegt daran, dass Appliances über feste Kapazitäten verfügen, um ein bestimmtes Serviceniveau zu gewährleisten. Sie können nicht unbegrenzt skaliert werden, um den ständig wachsenden Anforderungen eines Unternehmens an die Echtzeit-Überprüfung von Traffic gerecht zu werden — insbesondere in Bezug auf verschlüsselten Traffic. Dies führt dazu, dass Unternehmen, die sich auf herkömmliche Tools und Architekturen verlassen, ihren verschlüsselten Traffic im besten Fall nur unvollständig und im schlimmsten Fall gar nicht überprüfen können.

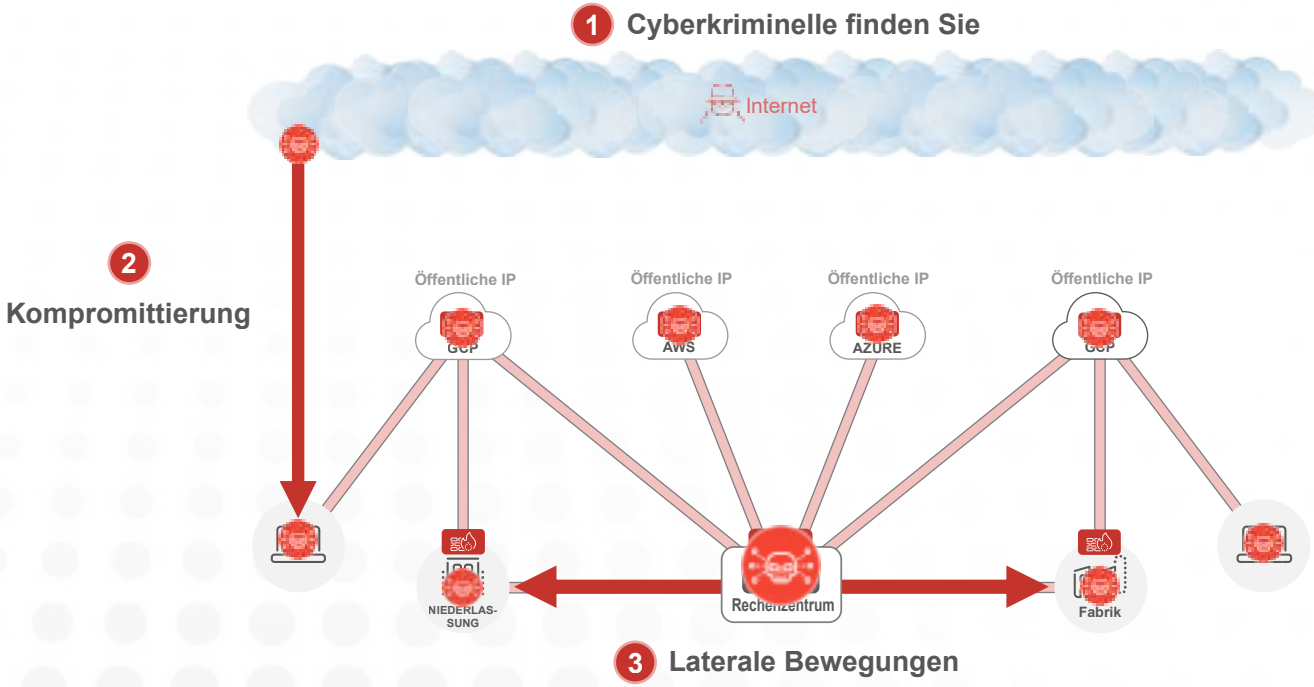
Wenn der verschlüsselte Traffic nicht in großem Umfang untersucht wird, können Bedrohungen die Abwehrmechanismen unbemerkt umgehen und Angreifer ungehindert agieren. Unglücklicherweise sind sich Cyberkriminelle dieser Tatsache mittlerweile bewusst und haben begonnen, verschlüsselten Traffic als bevorzugtes Mittel zur Durchführung ihrer Angriffe zu nutzen. Heutzutage erfolgen etwa **86 %** der Cyberangriffe über verschlüsselten Traffic. Wenn eine Organisation also ihren verschlüsselten Traffic nicht überprüft, kann sie die überwiegende Mehrheit der Bedrohungen nicht davon abhalten, ihre Abwehrsysteme zu durchbrechen. Vereinfacht gesagt, können Firewall- und VPN-Architekturen eine Kompromittierung nicht verhindern.

# #3 Firewalls und VPNs ermöglichen die laterale Ausbreitung von Bedrohungen

Nach der erfolgreichen Kompromittierung und Überwindung der organisationseigenen Abwehrmechanismen durch eine Cyberbedrohung treten die Schwachstellen von Firewalls und VPNs deutlich zutage. Die laterale Bewegung oder Ausbreitung von Bedrohungen bezieht sich auf die Art und Weise, wie Bedrohungen im Netzwerk auf die verschiedenen Ressourcen der Organisation zugreifen können — seien es lokale Anwendungen, Workloads in privaten Clouds oder SaaS-Anwendungsinstanzen. Wenn eine Bedrohung in den Perimeter einer Organisation eindringt, ist selten nur eine einzige Anwendung gefährdet. Um zu verstehen, wie es zur lateralen Bewegung einer Bedrohung kommen kann, hilft ein Blick auf die Analogie des Sicherheitsprinzips „Festung mit Burggraben".

Ein Burggraben dient der Verteidigung einer Festung. Konkret gelingt das, indem Angreifern der Zugang verwehrt wird. Ziel ist dabei der Schutz der Reichtümer und Menschen innerhalb der Anlage.

**Wie Firewall- und VPN-zentrierte Architektur Risiken erhöht**



Wenn es Angreifern jedoch gelingen würde, den Burggraben zu überwinden, wäre damit der primäre Verteidigungsmechanismus hinfällig. In diesem Fall gäbe es nur noch wenig, was Feinde davon abhalten könnte, die gesamte Festung zu plündern.

Die oben beschriebene Schwäche von Festungen und Burggräben spielt auch bei der Verwendung von Firewalls und VPNs eine Rolle. Dies liegt an der Beschaffenheit der stark vernetzten Hub-and-Spoke-Netzwerke, auf die sich einige Unternehmen immer noch verlassen, sowie an der Art und Weise, wie „Festung-mit-Burggraben"-Sicherheitsmodelle Maßnahmen zum Bedrohungsschutz auf die grundsätzliche Abwehr des Netzwerkzugangs ausrichten.

Firewalls sind in dieser Analogie der „Burggraben", VPNs die „Zugbrücke" und das Netzwerk selbst die „Festung". Sobald eine Cyberbedrohung den „Burggraben" überwindet und in die „Festung" eindringt, kann sich der böswillige Akteur problemlos von einer verbundenen Ressource zu einer anderen bewegen und sich so Zutritt zu den verschiedenen „Räumen" in der „Festung" verschaffen.

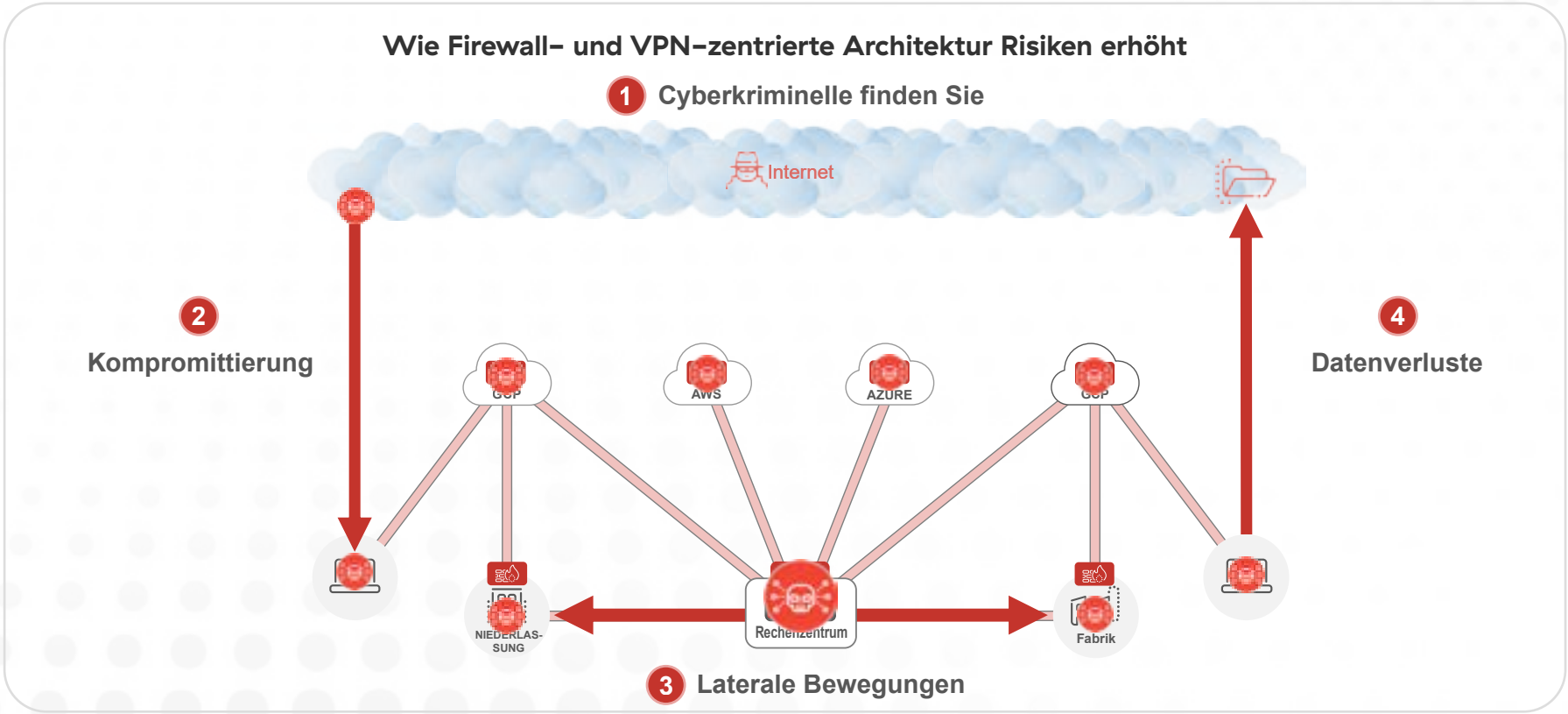
Um es ganz deutlich zu machen: Firewalls und VPNs ermöglichen eine laterale Ausbreitung von Bedrohungen, sodass Cyberkriminelle die Reichweite ihrer Angriffe auf das gesamte Netzwerk ausdehnen können, was wiederum zu massiven Schäden, Betriebsunterbrechungen und Kosten führt. Punktuelle Kompromittierung ist im Endeffekt gleichbedeutend mit flächendeckender Kompromittierung. Zwar wird Netzwerksegmentierung oft als Lösung für dieses Problem dargestellt, diese Taktik läuft aber unweigerlich auf die Anschaffung von immer mehr Firewalls hinaus. Die zugrunde liegenden Probleme in der Architektur veralteter perimeterbasierter Tools werden dadurch nicht gelöst.

# #4 Firewalls und VPNs bewahren nicht vor Datenverlust

In den allermeisten Fällen geht es böswilligen Akteuren nicht einfach um den Nervenkitzel beim Verüben von Cyberangriffen auf Unternehmen.Vielmehr haben sie ein bestimmtes Ziel vor Augen, und dieses Ziel besteht darin, vertrauliche Daten zu stehlen. Das ist deshalb lukrativ, weil sich gestohlene Daten im Dark Web mit erheblichem Gewinn verkaufen oder als Druckmittel in einem Ransomware-Angriff mit Doppelerpressung nutzen lassen, um Lösegeld von einem Unternehmens zu fordern. In jedem Fall können die Auswirkungen für das Unternehmen katastrophal sein.

Sobald Cyberkriminelle also eine Angriffsfläche gefunden, die Abwehrmechanismen kompromittiert und begonnen haben, sich lateral auszubreiten (Aktivitäten, die allesamt durch Firewalls und VPNs erleichtert werden), suchen sie im gesamten Netzwerk nach so vielen Daten wie möglich und dabei insbesondere nach vertraulichen oder regulierten Daten. Im Anschluss folgt natürlich die Datenexfiltration.

Sich auf herkömmliche Tools zu verlassen, um dieses letzte Glied in der Angriffskette zu stoppen, geht wiederum mit erheblichen Risiken einher und ermöglicht Datenverlust.



Heute sind, wie bereits erwähnt, über 95 % des Web-Traffics verschlüsselt. Die Überprüfung des verschlüsselten Traffics erfordert umfangreiche Rechenleistung und statische Appliances sind nicht in der Lage, die erforderliche Skalierung zu gewährleisten, die für die Verarbeitung der enormen Mengen an verschlüsseltem Traffic wachsender Unternehmen nötig ist. Diese Herausforderung (sowohl für Hardware- als auch virtuelle Appliances) ist nicht nur in Bezug auf Gefährdungen, sondern auch auf Datenverlust relevant. Cyberkriminelle sind sich bewusst, dass die Sicherheit in Unternehmen dort, wo Traffic verschlüsselt ist, eher Lücken aufweist, und nutzen diesen Traffic als bevorzugten Weg zur Datenexfiltration.

Aber es liegt nicht nur an der mangelden Skalierbarkeit, dass Tools wie Firewalls nicht in der Lage sind, Datenexfiltration zu stoppen. Bisher gängige Technologien wurden für eine Welt entwickelt, die so nicht mehr existiert; für eine Zeit vor Cloud-Anwendungen und Remote-Mitarbeitern. Daher können sie moderne Übertragungswege, zu denen etwa die integrierte Freigabefunktion in SaaS-Anwendungen wie Google Drive, Box und Microsoft OneDrive zählt, nicht gegen Datenlecks absichern. Auf ähnliche Weise werden Daten durch falsch konfigurierte Cloud-Ressourcen wie AWS S3-Buckets offengelegt, die irrtümlich auf „öffentlich“ eingestellt sind. Eine Behebung ist jedoch mit Firewalls, VPNs oder sogar herkömmlichen Tools zur Verhinderung von Datenverlust (Data Loss Prevention, DLP) nicht möglich.

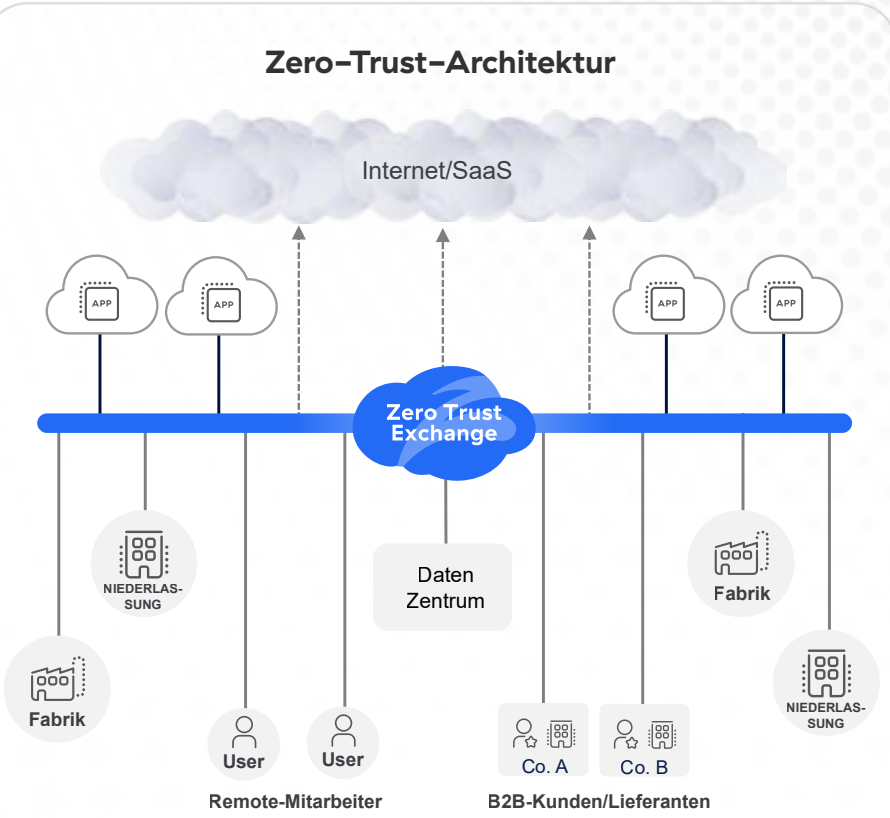
Externe Angreifer sind bestrebt, diese und andere moderne Mittel zu nutzen, um vertrauliche Daten zu stehlen. Dabei darf jedoch nicht vergessen werden, dass sie nicht die einzige Bedrohung für Daten darstellen. Unternehmen müssen sich der Realität stellen, dass böswillige und unvorsichtige Insider auf die oben beschriebene Weise ebenso vertrauliche Daten preisgeben können. Unabhängig vom Täter muss sich die Sicherheitsarchitektur weiterentwickeln, wenn Daten sicher aufbewahrt werden sollen.

# Wie Zero-Trust-Architektur diese Probleme löst

Zero Trust ist nicht nur ein weiteres Tool zur Ergänzung des netzwerkzentrierten Status quo. Ziel des Ansatzes ist es nicht, lediglich die negativen Begleiterscheinungen perimeterbasierter Architekturen zu mindern, während die zugrunde liegenden Ursachen bestehen bleiben. Vielmehr handelt es sich bei Zero Trust um eine eigenständige Architektur, die auf dem Prinzip des Zugriffs mit minimaler Rechtevergabe basiert. Sie unterscheidet sich grundsätzlich von einer standardmäßigen Firewall- und VPN-basierten Architektur.

Mit einer Zero-Trust-Architektur profitieren Unternehmen von einer globalen Security-Cloud, die als intelligente Schaltzentrale fungiert und User, Workloads, IoT/OT-Geräte und B2B-Partner sicher verbindet — ohne dabei das Netzwerk für irgendjemanden oder irgendetwas zu öffnen. Gleichzeitig sollte die Zero-Trust-Cloud umfassende Lösungssuites (z. B. Cyberbedrohung und Datenschutz) bieten, die als Service an der Edge bereitgestellt werden, so nah wie möglich am Enduser.

**Mit Zero Trust werden Sicherheit und Konnektivität erfolgreich vom Netzwerk entkoppelt. Perimeterbasierte Architekturen gehören damit der Vergangenheit an.**




**Unternehmensrichtlinien legen fest, wer per Netzwerkverbindung auf was zugreifen kann. Das Netzwerk ist der Transportweg.**

Mit dieser modernen Architektur können Unternehmen sich gegen die vier Möglichkeiten absichern, durch die Firewalls und VPNs sie angreifbar machen:

- **Minimieren der Angriffsfläche:** Nutzen Sie Zero Trust, um die stetige Ausdehnung des Netzwerks zu kontrollieren, Firewalls, VPNs und ihre öffentlich zugänglichen IP-Adressen abzuschaffen, keine eingehenden Verbindungen zuzulassen und Anwendungen hinter einer Zero-Trust-Cloud zu verstecken.
- **Unterbinden von Kompromittierung:** Überprüfen Sie den gesamten Traffic, einschließlich des verschlüsselten Traffics, mithilfe einer leistungsfähigen Zero-Trust-Cloud in großem Maßstab, um Bedrohungen zu erkennen und Richtlinien in Echtzeit durchzusetzen.
- **Stoppen lateraler Ausbreitung:** Verbinden Sie User, Workloads und Geräte direkt mit Anwendungen statt mit dem gesamten Netzwerk und wahren Sie dabei das Prinzip des Zugriffs mit minimaler Rechtevergabe.
- **Verhindern von Datenverlust:** Stoppen Sie Datenverluste in verschlüsseltem Traffic und auf allen anderen Übertragungswegen, einschließlich ruhender Daten in der Cloud und Daten, die auf Endgeräten der Mitarbeiter genutzt werden.

Eine Zero-Trust-Architektur verringert nicht nur das Risiko von Sicherheitsverletzungen, sondern reduziert auch die Komplexität, steigert die Anwenderproduktivität, senkt Kosten und fördert die Organisationsdynamik. Damit wird eine Vielzahl von Problemen gelöst, die mit Firewall- und VPN-basierten Architekturen einhergehen.

# Zusammenfassung

Wer nach einer Zero-Trust-Lösung sucht, trifft mit der KI-gestützten Zero Trust Exchange von Zscaler die richtige Wahl. Als weltweit größte und am weitesten verbreitete Inline-Security-Cloud sprechen Umfang und Erfolg der Plattform für sich:

**über 150**
Rechenzentren weltweit

**Über 360 Mrd.**
Transaktionen pro Tag abgesichert

**500T+**
Telemetriesignale pro Tag

**>70**
Net Promoter Score

**40 %**
der Fortune 500 sind Kunden von Zscaler

**Marktführer**
im Gartner MQ für SSE

Um mehr zu erfahren, registrieren Sie sich für unser monatliches Webinar „Beginnen Sie hier: Eine Einführung in Zero Trust“. Im Webinar diskutieren wir die Zero-Trust-Architektur aus der Einstiegsperspektive (und geben Ihnen weiterführende Informationen zu Zscaler), um Sie bei den ersten Schritten mit Zero Trust zu unterstützen.

zscaler™ | Experience your world, secured.™

**Über Zscaler**
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die 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 finden Sie auf **zscaler.de** oder auf Twitter unter **@zscaler**.



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