ZTNA – für eine optimale, sichere Anwendererfahrung

Sicherer Anwendungszugriff für alle Mitarbeiter auf jedem Gerät, an jedem Ort, jederzeit.

Your Workforce.
Powered by You.

zscaler™

„Unsere Mitarbeiter wollen gar nicht mehr zurück zu einer klassischen VPN-Verbindung."

– Markus Sontheimer, CIO/CDO Member of the Board of Management, DB Schenker

User haben heute andere Ansprüche

Im Jahr 2020 sitzen die Mitarbeiter nicht mehr tagaus, tagein im Büro. Sie arbeiten im Homeoffice, im Hotel, am Flughafen ... Und sie arbeiten nicht mehr auf BlackBerrys, die von der IT-Abteilung verwaltet und bereitgestellt werden, sondern nach dem BYOD-Prinzip: auf eigenen Smartphones, Tablets und Laptops, die sie sowohl privat als auch geschäftlich nutzen.

Über den Schutz der eigenen Mitarbeiter hinaus ist das Unternehmen auch für den sicheren Zugriff externer Auftragnehmer verantwortlich. Alle diese User müssen gleichermaßen von unterschiedlichen Geräten und Standorten aus auf eine breite Palette privater Apps zugreifen können. Früher wäre es ein Ding der Unmöglichkeit gewesen, diesen Zugriff zu gewährleisten, ohne die Sicherheit zu kompromittieren. Heute ist es machbar.

Herausforderungen einer mobilen Belegschaft

Global verteilte Belegschaften machen die Gewährleistung des sicheren Zugriffs auf private Applikationen zur Herausforderung für IT-Teams. Auch wenn die Belegschaft heute stärker diversifiziert sein mag als vor 15 Jahren, gibt es Gemeinsamkeiten, die alle Mitarbeiter verbinden – z. B. die Notwendigkeit, schnell und zuverlässig auf private Applikationen zuzugreifen, damit im Unternehmen alles rund läuft. Heute sind Belegschaften global verteilt und diversifiziert:

Der Vielreiser

Sam Davis, VP of Sales

„Ich bin viel unterwegs, bestimmt 75 % meiner Arbeitszeit. Dann sitze ich am Flughafen, im Hotel oder am Standort des Kunden und versuche, während der Wartezeiten möglichst viel Arbeit zu erledigen. Mein Arbeitsplatz wechselt also ständig, und ich muss von überall aus schnell auf unsere Unternehmensressourcen zugreifen, um zeitnah auf Kundenanfragen zu reagieren."

Die Präsenzarbeiterin

Danielle Allen, Finance Manager

„Ich arbeite in der Regel vom Büro aus. Ich bearbeite täglich Anfragen von anderen Mitarbeitern, die Fragen zu Zahlungen haben. Das schaffe ich nur, wenn ich jederzeit schnell auf unsere Finanzanwendungen zugreifen kann."

Die Subunternehmerin

Elaina Thalin, Web Development Contractor

„Ich arbeite inzwischen seit ungefähr acht Monaten auf Auftragsbasis für das Unternehmen. Auch wenn ich nicht beim Unternehmen angestellt bin oder dort am Standort arbeite, muss ich im Rahmen meiner Arbeit trotzdem auf einige der privaten Applikationen zugreifen können."

Der Heimarbeiter

Justin Miller, Marketing Manager

„Ich arbeite derzeit von daheim aus, wo wir Familie und Arbeit unter einen Hut bringen. Da darf die Produktivität nicht davon abhängen, wie schnell ich Zugriff auf notwendige Anwendungen habe."

Unabhängig vom User-Typ und Zuständigkeitsbereich müssen Mitarbeiter schnell und sicher von jedem beliebigen Standort aus auf private Applikationen zugreifen können. Die IT benötigt die entsprechende Technologie, um dies zu ermöglichen und gleichzeitig sicherzustellen, dass die Sicherheit nicht auf Kosten der Produktivität der User geht. Deswegen ist VPN heute einfach nicht mehr zeitgemäß.

VPN war gestern – die User von heute brauchen eine bessere Lösung

VPN wurde vor über 30 Jahren entwickelt und wird den Ansprüchen heutiger User einfach nicht mehr gerecht. Sowohl in puncto Sicherheit als auch in Bezug auf die Anwendererfahrung weist diese veraltete Technologie erhebliche Mängel auf.

Hohe Latenz, begrenzte Skalierbarkeit, unbefriedigende Anwendererfahrung
VPNs wurden zur Sicherung des Netzwerkzugangs entwickelt. Entsprechend wird der gesamte User-Traffic erst zum Rechenzentrum zurückgeleitet – und zwar auch dann, wenn die Apps in der öffentlichen Cloud laufen. Dadurch entsteht ein sogenannter Posaunen-Effekt, der wiederum Latenzen verursacht. Zudem sind die User-Kapazitäten von VPN-Appliances begrenzt, und der gleichzeitige Zugriff zu vieler User auf den VPN-Server führt schnell zur Überlastung.

Wiederholte Anmeldungen und unterbrochene Verbindungen
Jede Änderung oder Inaktivität im Netzwerk führt zur Unterbrechung der VPN-Verbindung. Je mobiler die Belegschaft, desto häufiger kommt es zu Ausfällen, die Frust bei den Usern auslösen und Produktivitätseinbußen für das Unternehmen verursachen.

Verunsicherung der Mitarbeiter
Viele User kennen möglicherweise gar nicht den Unterschied zwischen Ihren öffentlichen und privaten Applikationen und sind sich entsprechend auch nicht sicher, wann der Einsatz von VPN angemessen ist und wann nicht. Mit der zunehmenden Migration der Anwendungen in die Cloud wächst auch die Verwirrung: Viele User wissen nicht mehr, wann, wo und wie sie mit VPN arbeiten sollen. Aus Sicht der User ist VPN alles andere als reibungslos oder intuitiv.

Wenn man Tausende von DVD-Spielern miteinander vernetzt, ist das Ergebnis nicht Netflix. Genauso darf auch eine Lösung, die privaten Anwendungszugriff von überall aus ermöglicht, keine Notlösung sein, sondern muss gezielt konzipiert werden. Zuverlässige Verfügbarkeit, hochgradige Skalierbarkeit und Anwenderfreundlichkeit sind ein unverzichtbares Muss. Zur Bewältigung der durch die wachsende Mobilität entstehenden Herausforderungen bezüglich User Experience und Netzwerksicherheit reicht es weder aus, VPN-Appliances im Rechenzentrum nachzurüsten, noch sie zu virtualisieren oder in die Cloud zu verlagern. **Ein neuer Ansatz ist erforderlich.**

„Bis 2023 werden 60 % der Unternehmen ihre Remote-Access-VPNs größtenteils aus dem Betrieb nehmen und stattdessen auf ZTNA umsteigen."

Gartner, Market Guide for Zero Trust Network Access
Steve Riley, Neil MacDonald, Lawrence Orans, April 2019

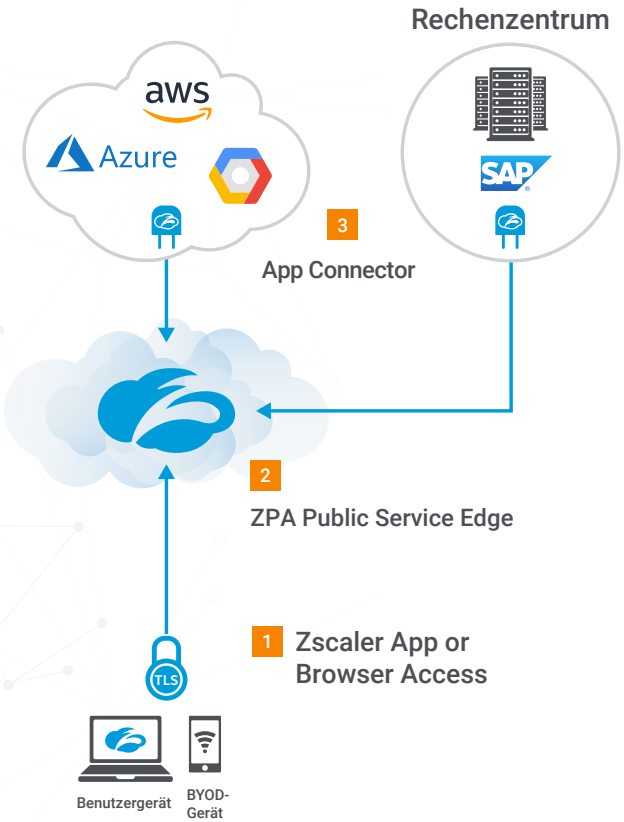
ZTNA steigert die Produktivität der User

Beim Zugriff auf SAP in der öffentlichen Cloud, ein SSH, RDP, firmeneigenes Intranet oder auch eine webbasierte App zur Verwaltung von Arbeitszeitkonten gilt gleichermaßen der Imperativ einer reibungslosen Anwendererfahrung. Deswegen empfiehlt Gartner Unternehmen den Umstieg auf **Zero Trust Network Access (ZTNA)** als bessere Alternative zum Remote-Access-VPN.

ZTNA Services werden zumeist in der Cloud gehostet und gewähren Usern basierend auf Richtlinien Zugriff auf einzelne private Anwendungen. Diese Richtlinien berücksichtigen die Identität und Gruppenzugehörigkeit des Users, Device Posture sowie eine Reihe weiterer Kriterien.

Da viele ZTNA-Services komplett Cloud-basiert sind, werden User mit einem von zahlreichen globalen Einwählknoten verbunden, der dann die sichere Verbindung zur gewünschten privaten Anwendung vermittelt. Dadurch wird höhere Verfügbarkeit und Skalierbarkeit gewährleistet als bei einer VPN-Appliance. Da die User niemals aufs Netzwerk zugreifen, gibt es kein Backhauling von Traffic zum Rechenzentrum mehr. So kann ein reibungsloser Zugriff für den End-User ermöglicht und zugleich das Risiko für das Unternehmen minimiert werden.

ZTNA-Architektur



1 Zscaler App oder Browser Access

- Leitet Traffic zur Authentifizierung an den IDP-Anbieter weiter
- Client Connector leitet Traffic automatisch zum Public Service Edge weiter
- Durch Browser Access muss zum Zugriff auf webbasierte Anwendungen kein Client auf dem Gerät installiert werden

2 ZPA Public Service Edge

- Sichert die User-zu-App-Verbindung
- Setzt alle unternehmensspezifischen Admin-Richtlinien durch

3 App Connector

- Wird privaten Anwendungen in der Cloud und/oder im Rechenzentrum vorgeschaltet
- Reagiert nur auf Anfragen vom ZPA Public Service Edge
- Keine eingehenden Verbindungen. Reagiert nur mit Inside-out-Verbindungen

Sicherheit, die den Ansprüchen der User gerecht wird

Für Unternehmen, die die Produktivität ihrer User fördern wollen, empfiehlt sich ein ZTNA Service.

Das weiß Steve Day, EGM of Infrastructure, Cloud and Workplace bei der National Australia Bank, aus eigener Erfahrung.

Fallstudie der National Australia Bank ansehen

Der nächste Schritt: Testen Sie unseren ZTNA Service.

7-tägige ZTNA Demo starten

Über Zscaler

Zscaler unterstützt weltweit führende Unternehmen bei der sicheren Transformation ihrer Netzwerke und Anwendungen für eine Mobilgerät- und Cloud-orientierte Zukunft. Die Flagship-Services, Zscaler Internet Access™ und Zscaler Private Access™, gewährleisten schnelle, sichere Verbindungen zwischen Usern und Anwendungen unabhängig vom Gerät, Standort oder Netzwerk. Die Services von Zscaler sind komplett Cloud-basiert und bestechen durch überlegene Benutzerfreundlichkeit, Sicherheit und Anwendererfahrung im Vergleich zu herkömmlichen Appliances bzw. hybriden Lösungen. Die mandantenfähige, distribuierte Cloud-Sicherheitsplattform von Zscaler schützt Tausende von Unternehmen in 185 Ländern vor Cyberangriffen und Datenverlusten. Erfahren Sie mehr auf **zscaler.com** oder folgen Sie uns auf Twitter unter**@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134, USA
+1 408.533.0288
www.zscaler.com