paloalto NETWORKS | PRISMA® ACCESS

Sicherer Remotezugriff – leicht gemacht.

Prisma® Access bietet einen einheitlichen Sicherheitsansatz für den Remotezugriff und begeistert Benutzer mit unschlagbarer Leistung.

Die moderne Geschäftswelt ist hybrid. Sowohl die Belegschaft als auch die für den täglichen Geschäftsbetrieb genutzte Infrastruktur von Unternehmen sind stark – häufig über Ländergrenzen hinweg – verteilt.

Hybride Arbeitsmodelle und Infrastrukturen bieten mehr Flexibilität und fördern so potenziell die Produktivität von Mitarbeitenden, da Aufgaben praktisch überall – im Büro, auf Geschäftsreisen, unterwegs oder zu Hause – erledigt werden können. Hybride Infrastrukturen befähigen Unternehmen zudem, von der Agilität, Skalierbarkeit und Resilienz der Cloud zu profitieren, wann und wie sie wollen.

Dazu benötigen sie jedoch Netzwerkverbindungen, die ebenso flexibel sind wie die Arbeitsmodelle, die sie unterstützen sollen. Die Verbindungen müssen außerdem gesichert sein, um Personen, Daten und Ressourcen in weit verteilten Infrastrukturen zu schützen.

Viele herkömmliche Ansätze für Netzwerkverbindungen – wie auch VPNs – bieten modernen Unternehmen nicht die notwendige Leistung, Sicherheit und Verwaltungsfreundlichkeit. Ein besserer Ansatz ist gefragt.

Quelle: Gallup, „The Future of the Office Has Arrived: It's Hybrid", Oktober 2023.

Hybrides Arbeiten ist aus dem modernen Arbeitsalltag nicht mehr wegzudenken, auch wenn einige Unternehmen versuchen, sich diesem Trend durch Präsenzpflicht für ihre Mitarbeitenden zu widersetzen.

2023 haben

5 von 10
hybrid gearbeitet

3 von 10
ausschließlich remote gearbeitet

2 von 10
ausschließlich vor Ort gearbeitet

Eine veraltete Sicherheitslösung

Virtuelle private Netzwerke (VPNs) werden schon seit Jahrzehnten genutzt, um Mitarbeitenden sicheren Remotezugriff auf Daten und Ressourcen zu gewähren.

Als VPNs Mitte der 1990er Jahre erfunden wurden, waren die Anforderungen an den Remotezugriff jedoch noch ganz andere. Nur ein kleiner Bruchteil der Belegschaft benötigte einen derartigen Zugang, da der Großteil der Arbeit im Büro erledigt wurde und sich die dazu erforderlichen Anwendungen und Daten vor Ort, im Rechenzentrum des jeweiligen Büros, befanden. Auf diesem mittlerweile veralteten Arbeitsmodell basieren die Sicherheitsprinzipien von VPNs bis heute.

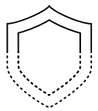
Als die Anzahl der Remotearbeiter während der Coronapandemie schlagartig anstieg, nahm auch die Nutzung von VPNs exponentiell zu und die zahlreichen Einschränkungen der Technologie machten sich plötzlich stärker bemerkbar. Besonders aufreibend war das für die IT- und Sicherheitsprofis, die praktisch über Nacht eine Vielzahl an Mitarbeitenden mit sicheren Verbindungen ausstatten mussten. Da viele Mitarbeitende nun im Rahmen hybrider Arbeitsmodelle zwischen Remote- und Bürostandorten wechseln, besteht diese Belastung weiterhin.

Quelle: ESG, „Ten Considerations for Evaluating Zero Trust Network Access Solutions“, September 2021.

Häufige Einschränkungen

Komplexe Verwaltung und Skalierung

Das Einrichten eines neuen VPN erfordert Hardware-Investitionen und Fachpersonal zur Bereitstellung, Verwaltung und Instandhaltung. Der manuelle Aufwand ist somit groß. Zur Ausweitung der Abdeckung einer VPN-Lösung sind in der Regel Investitionen in zusätzliche Infrastruktur oder mehr Personal erforderlich. Diese Investitionen und der erhebliche Zeitaufwand für den Ausbau und die Pflege der VPN-Lösung führen dazu, dass eine solche Ausweitung hohe Kosten verursacht.



Unzureichende Sicherheit

Herkömmliche VPN-Lösungen prüfen die Zugriffsberechtigung nur am Netzwerkrand. Sobald Benutzern Zugang gewährt wurde, können sie sich frei im Netzwerk bewegen und auf alle darin enthaltenen Anwendungen und Daten zugreifen. Dies ist einer der Gründe dafür, dass Cyberkriminelle seit der Pandemie vermehrt VPN-Schwachstellen ausnutzen, um von der stärkeren Verbreitung von Remote- und Hybridarbeit zu profitieren.

Schlechte Benutzererfahrung

VPN-Lösungen sind nicht immer leicht verständlich oder benutzerfreundlich. Einerseits haben Mitarbeitende, die sich von zu Hause aus mit einem Unternehmensnetzwerk verbinden, nicht unbedingt das nötige Fachwissen, um Probleme selbst zu beheben. Andererseits lässt die Übertragungsgeschwindigkeit von VPNs – aufgrund der Art, wie der Datenverkehr geroutet und gesichert wird – häufig zu wünschen übrig. Das kann zur Folge haben, dass Mitarbeitende das VPN umgehen und damit die unternehmensweit einheitliche Sicherheit aufs Spiel setzen.

Fazit

Der Einsatz von VPN-Lösungen für den Remotezugriff kann in modernen hybriden Organisationen erhebliche negative Auswirkungen haben, von einem größeren Sicherheitsrisiko über Produktivitätsverluste bis hin zu höheren Kosten für die Verwaltung und Skalierung.

Quelle: TechTarget, „Hackers targeting VPN vulnerabilities in ongoing attacks", April 2021.

Hybrides Arbeiten stellt eine Herausforderung für die Netzwerksicherheit dar.

59 % finden Cybersicherheit und -verwaltung nun schwieriger als früher.

41 % nennen die stärkere Nutzung mobiler Arbeitsmodelle als einen Aspekt, der die Cybersicherheit verkompliziert.

Quelle: ESG, „Ten Considerations for Evaluating Zero Trust Network Access Solutions", September 2021

Ein sicherer Ansatz

Aufgrund der wachsenden Unzufriedenheit mit VPNs suchen Unternehmen nach Ansätzen für den Remotezugriff, die leistungsfähiger und sicherer sind und sich zudem leichter bereitstellen und verwalten lassen.

Eine führende Alternative ist der Zero-Trust-Netzwerkzugriff (ZTNA), mit dem Mitarbeitende sicher auf die Anwendungen und Daten zugreifen können, die sie für ihre Arbeit benötigen – unabhängig davon, welche Verbindungsmethode sie von wo aus nutzen.

Ein wichtiger Vorteil von ZTNA gegenüber VPN ist, dass Unternehmen nicht allen Mitarbeitenden Zugang zum gesamten Netzwerk gewähren müssen, sondern die Kernprinzipien von Zero Trust umsetzen können:

- **Zugriff nach dem Least Privilege-Prinzip**: Benutzer erhalten nur Zugriff auf die Anwendungen und Daten, die sie tatsächlich benötigen.

- **Niemandem vertrauen, alles verifizieren**: Bei jedem Benutzerzugriff auf eine Anwendung werden die Identität und Zugriffsrechte überprüft. Diese Überprüfungen laufen kontinuierlich weiter, auch nachdem Benutzer eingangs verifiziert wurden.

Mithilfe von ZTNA sind Unternehmen besser positioniert, Zugriffsrechte im Fall eines Sicherheitsvorfalls einzuschränken und so das unternehmensweite Risiko zu reduzieren.

Laut einer Prognose von Gartner werden 2025 **70 %** der neuen Bereitstellungen für den Remotezugriff auf ZTNA und nicht auf VPN basieren.

Quelle: Pressemitteilung von Gartner, Oktober 2022.

Gestalten Sie Ihren sicheren Remotezugriff zeitgemäß neu

Mit Prisma Access von Palo Alto Networks können Sie den Remotezugriff modernisieren und die Leistungsgrenzen von VPN-Lösungen überwinden. Durch die Bereitstellung eines leistungsstarken sicheren Remotezugriffs reduziert Prisma Access nicht nur Ihre Angriffsfläche, sondern bietet Ihren Mitarbeitenden auch eine hervorragende Anwendungserfahrung.

Prisma Access wurde speziell für die Cloud entwickelt und hilft IT- und Sicherheitsteams dabei, Benutzer, Apps und Daten in Cloud-Umgebungen zu sichern, wodurch sich der Remotezugang schnell und einfach auf so viele Mitarbeiter wie nötig ausdehnen lässt.

Verwandeln Sie hybride und mobile Arbeitsmodelle in einen Wettbewerbsvorteil – mit Prisma Access.

- **Sorgen Sie für einen sicheren Hybridbetrieb und begeistern Sie Ihre Mitarbeiter**
  Bieten Sie kompromisslose Sicherheit, ohne die Produktivität zu beeinträchtigen. Mitarbeitende profitieren von einer konstant guten Leistung von On-Premises-, Cloud- und SaaS-Anwendungen, sicheren direkten Verbindungen zu Anwendungen und der kontinuierlichen Überprüfung des Datenverkehrs auf Bedrohungen.

- **Reduzieren Sie Ihre Angriffsfläche mit granularen Zugriffsrechten und gesichertem Zugang erheblich**
  Prisma Access nutzt das Zero-Trust-Prinzip, um Zugriffsberechtigungen auf Benutzer- und Anwendungsebene zu überprüfen, und reduziert so Ihre Angriffsfläche.

- **Modernisieren Sie die Verwaltung des Remotezugriffs**
  Die manuelle Verwaltung von Zugriffsrechten gehört bald der Vergangenheit an. Revolutionieren Sie die Sicherung und Verwaltung des Remotezugriffs auf Ihre kritischen Systeme und Daten mit einer Lösung, die zur Vereinfachung und Vereinheitlichung von Zugriffsmanagementprozessen entwickelt wurde.

Das Besondere an **Prisma Access**

50 % geringeres Risiko eines Datenlecks

75 % effizientere Verwaltung von Secure Access Service Edge (SASE) sowie effizientere Richtlinienänderungen

107 % Return on Investment (ROI)

Quelle: Forrester, „The Total Economic Impact™ Of Palo Alto Networks Prisma SASE“, November 2023. Im Auftrag von Palo Alto Networks.

KUNDENERFOLG

Better

Schneller und moderner Remotezugriff im großen Umfang

Das US-amerikanische Online-Immobilienfinanzierungsportal Better wollte seinen Sicherheitsansatz für das Netzwerk, die Endpunkte und SecOps modernisieren. Sicherheit hat eine hohe Priorität für das Unternehmen, das einerseits das Vertrauen seiner Kunden gewinnen und andererseits sowohl landesweit gültige als auch von Bundesstaat zu Bundesstaat unterschiedliche gesetzliche Vorgaben beachten muss.

Im Rahmen seiner Modernisierungsbestreben wollte Better den Onlinezugriff für Kunden und Mitarbeiter absichern. Das Unternehmen hatte zwar schon ein VPN, suchte aber nach einer cloudbasierten Lösung, die leichter zu skalieren und zu verwalten sein, Benutzern einen einfacheren Einstieg bieten und gleichzeitig die Datensicherheit verbessern sollte.

Prisma Access weckte das Interesse von Better und wurde mit einem Proof of Concept genauer geprüft. Zu dieser Zeit griff die Coronapandemie immer mehr um sich. Mit Unterstützung von Palo Alto Networks konnte Better innerhalb weniger Tage souverän zur Remotearbeit für die gesamte Belegschaft wechseln.

Lesen Sie den vollständigen Kundenbericht, um mehr über die Modernisierung des Sicherheitsansatzes von Better zu erfahren.

„Mit Prisma Access konnten wir all unseren Mitarbeitern weltweit sicheren Zugang zu unseren Softwarelösungen bereitstellen. Das veränderte alles.“

– **Ali Khan**, Chief Information Security Officer, Better

KUNDENERFOLG

Beam SUNTORY

Bessere Sicherheit und Leistung

Nach einem schwerwiegenden Sicherheitsvorfall beschloss Beam Suntory, der drittgrößte Spirituosenhersteller der Welt, seine Sicherheitsstrategie zu modernisieren.

Das Unternehmen wollte seine veraltete Netzwerk- und Sicherheitsinfrastruktur ersetzen, da diese zahlreiche Unzulänglichkeiten aufwies – von inkonsistentem Schutz über mangelnde Skalierbarkeit bis hin zu Verbindungsunterbrechungen und kostenintensiven Produktivitätsverlusten.

Ursprünglich sollten die Netzwerk- und Sicherheitsanforderungen in zwei verschiedenen Projekten ermittelt und erfüllt werden, doch dann stellte Beam Suntory fest, dass beide Modernisierungsinitiativen mit einer Secure-Access-Service-Edge(SASE)-Architektur konsolidiert werden konnten.

Durch die Implementierung von Prisma SASE hat das Unternehmen sowohl sein Sicherheitsniveau als auch die Zuverlässigkeit und Leistung seines Netzwerks erheblich verbessert. Gleichzeitig wurden auch viele Prozesse vereinfacht, sodass das Management der Netzwerk- und Sicherheitskomponenten nun weniger aufwendig ist.

Und als während der Pandemie mehr Mitarbeiter im Homeoffice arbeiten mussten, vereinfachte Prisma SASE auch diesen Wechsel. Die Benutzer brauchten sich nicht mehr über das Rechenzentrum anzumelden, sondern konnten die erforderlichen Produktivitätstools direkt in der Cloud abrufen.

„Die Lösung hat unseren Geschäftsbetrieb gerettet und sowohl die Leistung als auch das Sicherheitsniveau verbessert.“

– **Qun Wei**, Senior Network Architect, Beam Suntory

Die nächsten Schritte

Mit Prisma Access können hybride und mobile Arbeitsmodelle zum Wettbewerbsvorteil werden. Bieten Sie Ihren Mitarbeitern beispiellose Benutzererfahrungen, während Sie die Angriffsfläche reduzieren und das Zugriffsmanagement langfristig vereinfachen.

1

Entdecken Sie, wie Prisma Access einen sicheren Remotezugriff bereitstellt, von dem Ihre Mitarbeitenden und IT-Teams begeistert sein werden.

2

Entdecken Sie den starken ZTNA-Schutz, den Prisma Access bietet.

3

Kontaktieren Sie uns und fordern Sie eine Demo an, um zu sehen, wie Sie den Remotezugriff für Ihr Unternehmen modernisieren und sicherer gestalten können.

paloalto® NETWORKS | PRISMA® ACCESS