

E-Book



Die 6 überzeugendsten Anwendungsfälle für den vollständigen Austausch des VPN



Einleitung

Veraltete VPN-Infrastrukturen für den Remote-Zugriff sind schon seit Langem eine Sicherheitsschwachstelle. Ihre breit angelegte Netzwerkkonnektivität zieht Angreifer an und lässt nicht autorisierte laterale Bewegungen zu. Die Tatsache, dass der Traffic von Remote-Benutzern per Backhauling durch das VPN und anschließend wieder ins Internet geleitet werden muss, beeinträchtigt das Benutzererlebnis, erhöht die Kosten und erhöht die Komplexität des Routing.

Für Unternehmen, die ihren hybriden Beschäftigten eine zeitgemäßere Form der Konnektivität bieten wollen, ist ZTNA die moderne Alternative zum veralteten Remote-Zugriff per VPN. Aber nicht alle ZTNA-Lösungen können VPN vollständig ersetzen.

Für ein erfolgreiches Upgrade vom veralteten VPN zu ZTNA empfehlen wir, bei der Planung einer vollständigen Migration passende Anwendungsfälle zu ermitteln und zu priorisieren. Mit geschickten Planungen und Investitionen in Technologien können Ihre Teams endlich das VPN vollständig stilllegen.



1. Produktivere Hybrid-Arbeitskräfte

Da die meisten Beschäftigten mittlerweile hybrides Arbeiten bevorzugen, eignen sich veraltete VPN-Lösungen nicht mehr zur Bewältigung der für die Produktivität entscheidenden Sicherheits- und Konnektivitäts Herausforderungen. Ein VPN für den Remote-Zugriff gewährt nur spärliche Einblicke in anwendungsbezogene Aktivitäten und leidet wegen Backhauling unter Latenz- und Leistungsproblemen. Da authentifizierte Benutzer umfassenden Zugriff auf Netzwerkebene erhalten, wird die Angriffsfläche erweitert und dadurch uneingeschränkte laterale Bewegungen ermöglicht. Außerdem sind VPN-Konzentratoren mit nicht gepatchten Schwachstellen ein bedeutender Vektor für Cyberangriffe.

Durch ein Upgrade von veralteten VPN-Lösungen zu einer ZTNA-Lösung wie Netskope One Private Access können Unternehmen die mit VPN verbundenen Sicherheitsrisiken vermeiden. Sie gewähren identitäts- und kontextbewussten Least-Privilege-Zugriff auf private Anwendungen und minimieren nicht autorisierte laterale Bewegungen. Netskope One Private Access bietet Echtzeiteinblicke in die Details zu Anwendungs-Traffic und Benutzeraktivitäten und ermöglicht eine konsequente Richtliniendurchsetzung für Beschäftigte an allen Standorten, unterwegs oder vor Ort. Außerdem kann die Lösung Remote-Arbeitskräften sichere Konnektivität vor der Anmeldung gewähren, das sichere Onboarding neuer Geräte vereinfachen und das Kennwort zurücksetzen. Es wird sichergestellt, dass nur genehmigte Geräte Zugriff auf wichtige interne Ressourcen wie Verzeichnisdienste haben.

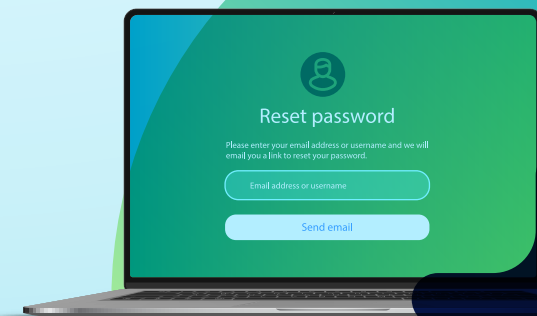
11
Arbeitsstunden
jährlich
verschwenden
Arbeitskräfte für das
Zurücksetzen von
Kennwörtern¹



IMPLEMENTIERUNGSTIPPS:

Eine Bestandsaufnahme der VPN-Bereitstellungen ist eine gute Möglichkeit, um mit dem Infrastruktur-Upgrade zu beginnen. Sie sollte Folgendes umfassen:

- Die Zahl der Instanzen von VPN-Services für den Remote-Zugriff, die Sie derzeit betreiben
- Welcher Anwendungs-Traffic durch diese VPNs für den Remote-Zugriff geleitet wird
- Die Namen der Benutzer mit VPN-Zugriff auf diese Anwendungen



¹Business Reporter, „How much time does your organisation spend on managing passwords?“, 7. September 2022.
<https://www.independent.co.uk/news/business/business-reporter/time-organisation-managing-passwords-b2161856.html>

2. Schnellere Cloud-Migration

Die digitale Transformation hat einen Wendepunkt erreicht: Inzwischen werden mehr Workloads in Public Clouds als in privaten Rechenzentren gehostet. Dementsprechend hat IaaS-Konnektivität für lokal oder remote arbeitende Benutzer höchste Priorität für Unternehmen und ist eines ihrer wichtigsten Anliegen bei der Planung ihrer Cloud-Strategie und -bereitstellung. In einer typischen VPN-Infrastruktur für den Remote-Zugriff wird der Benutzer-Traffic über das private Rechenzentrum und dann in IaaS-Clouds geleitet, die MPLS oder andere Pin-up-Tunnel wie AWS Direct Connect oder Azure ExpressRoute verwenden. Dieses Backhauling beeinträchtigt nicht nur das Benutzererlebnis und erhöht die Infrastrukturkosten, sondern erfordert auch komplexes Netzwerk-Routing.

Als zeitgemäße Alternative zu veralteten VPNs für den Remote-Zugriff sorgt Netskope ohne Hairpinning für eine effiziente Verbindung zur Public Cloud. Diese Verbindung ist sicher, flexibel und hochgradig skalierbar. Netskope One Private Access unterstützt den Schutz von Daten und Ressourcen. Die Zugriffsrechte werden anhand der Benutzeridentität und des Gerätesicherheitsstatus für jede Anwendung einzeln vergeben. Durch Nutzung einer logischen statt einer IP-basierten Konnektivität wird der Cloud- und Netzwerkbetrieb stark vereinfacht. Automatisierung ist jetzt ganz ohne Backhauling möglich.



IMPLEMENTIERUNGSTIPPS:

Wenn Unternehmen ihr VPN für den Remote-Zugriff ersetzen möchten, sollten sie auch Cloud-VPN-Instanzen wie AWS Client VPN oder Azure VPN Gateway berücksichtigen. Sie sollten Automatisierungstools wie Terraform-Module nutzen, um die Bereitstellung, Konfiguration und Skalierung der Publisher von Netskope One Private Access zu automatisieren, die in EC2 und anderen Cloud-Umgebungen ausgeführt werden.



3. Einfacherer Zugriff auf nicht verwaltete Geräte (wenn er sinnvoll ist)

Unternehmen müssen externen Auftragnehmern, Dienstleistungsanbietern und Partnern sicheren Zugriff auf Unternehmensressourcen gewähren. Gleichzeitig erwarten auch die eigenen Beschäftigten nahtlosen Zugriff auf private Ressourcen über ihre persönlichen Geräte. Die Herausforderung besteht darin, nicht verwalteten Geräten den Zugriff zu gestatten, ohne die Ressourcen im Internet oder in der DMZ offenzulegen. Eine speziell entwickelte Client-Software ist vielleicht nicht die richtige Lösung, da viele Benutzer nur ungern Software auf ihren persönlichen Geräten installieren. Wenn nicht verwalteten Geräten per VPN-Zugriff gewährt wird, könnte dies zu übermäßig vielen Zugriffsrechten führen.

Sie können externen Benutzern und Beschäftigten mit BYOD-Geräten sicheren Zugriff auf nicht verwaltete Geräte geben, ohne die mit VPN, DMZ oder frei im Internet zugänglichen Ressourcen verbundenen Risiken in Kauf zu nehmen. Netskope One Private Access unterstützt die Bereitstellung ohne Client für nicht verwaltete Geräte, um sicheren Zero-Trust-Zugriff auf private Anwendungen zu gewähren, die lokal oder in der Cloud gehostet werden.

Die ZTNA-Bereitstellung ohne Client ermöglicht den reibungslosen browsergestützten Zugriff über eine mit Identitätsanbietern (Identity Providers, IdP) integrierte Reverse-Proxy-Architektur zur Authentifizierung der Benutzer, die auf private Anwendungen zugreifen möchten. Unternehmen können mit denselben DLP-Kontrollen wie auf der Plattform Netskope One SSE für granulare Sichtbarkeit und einheitliche Datenschutzrichtlinien auf allen Geräten (verwaltet und nicht verwaltet) sorgen.

Ein durchschnittlicher Arbeitnehmer nutzt bei der Arbeit 2,5 Geräte, auch solche, die nicht dem Unternehmen gehören (persönliche Laptops, Smartphones und Tablets).²



² Zippia. „26 Surprising BYOD Statistics [2023]: BYOD Trends In The Workplace“ Zippia.com. 17. Oktober 2022.
<https://www.zippia.com/advice/byod-statistics/>

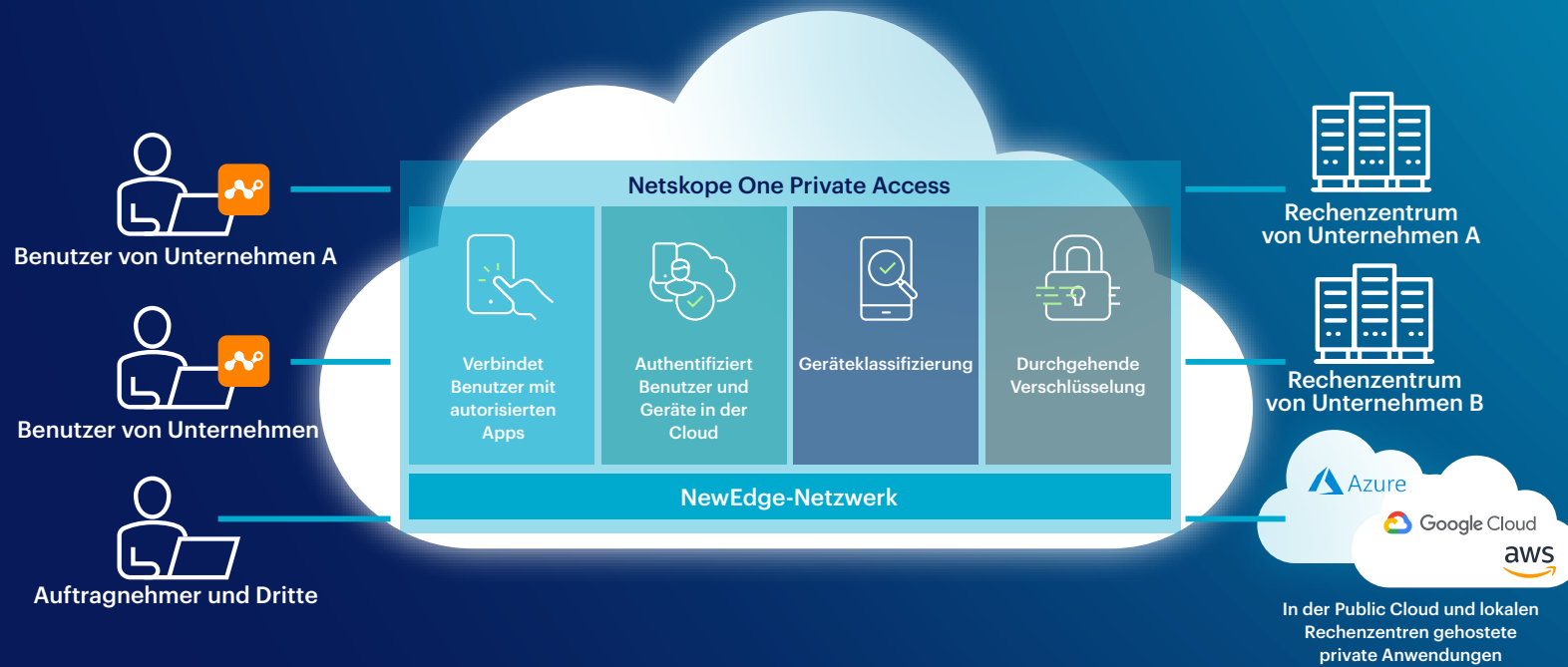
4. Schnellere Integration nach Fusionen und Übernahmen

Fusionen und Übernahmen sind intensive Ereignisse mit hohem Einsatz und kurzen Zeitrahmen. IT-, Netzwerk- und Sicherheitsteams stehen bei Fusionen und Übernahmen vor ganz besonderen Herausforderungen. Der Erfolg bei M&As hängt davon ab, wie schnell die Integration der beiden Unternehmen vonstattengeht.

IT-Operations-Teams stehen vor der Herausforderung, bereits am ersten Tag den Zugriff zu ermöglichen, Benutzer aus beiden Unternehmen mit geschäftskritischen internen Anwendungen zu verbinden und dabei die Sicherheit sensibler Daten zu gewährleisten. Die herkömmliche Methode der Zusammenführung von zwei Netzwerken ist kostspielig, zeitaufwendig und komplex. Oft führt sie zu IP-Konflikten und erfordert eine Umnummerierung von Adressen. Die Firewall-Regeln ermöglichen oft keine granulare Zugriffskontrolle, sodass beide Netzwerke anfällig bleiben.

Netskope One Private Access ist eine zentrale Lösung, die ZTNA/SD-WAN-Funktionen in einen einzigen leichten Endpunkt-Client integriert und für alle relevanten Fälle des Zugriffs auf Anwendungen die vollständige Stilllegung der VPNs für den Remote-Zugriff ermöglicht (nicht nur ihren teilweisen Ersatz). Ein einheitlicher SASE-Client lenkt den Benutzer-Traffic automatisch zu seinen Zielen wie Cloud-Apps, private Apps, IaaS oder Web. Mit Netskope One Private Access können Unternehmen bei Fusionen und Übernahmen schnell einen geschäftlichen Mehrwert erzielen, indem sie Beschäftigte, Auftragnehmer und Berater gleich am ersten Tag mit den nötigen Ressourcen (auch älteren Anwendungen) verbinden. Diese Lösung funktioniert ohne VPN-Einrichtung und Netzwerkzusammenführung. Die Unternehmen können gefahrlos gleich mit der Integration beginnen. Der Zugriff wird anhand adaptiver Vertrauenskriterien gewährt, die die Benutzeridentität, Gerätesicherheit und andere Kontextfaktoren in Betracht ziehen. Durch den selektiven Zugriff auf Anwendungen und Daten reduziert Netskope One Private Access die Gefahr lateraler Bewegungen und die Offenlegung sensibler Informationen.





Bieten Sie von Beginn an Zugriff auf interne Ressourcen, ohne Netzwerke zusammenführen oder VPNs zwischen zwei Standorten und Firewall-Regeln konfigurieren zu müssen.

5. Unterstützung für Remote-Contact-Center

Weltweit arbeiten 1,8 Millionen Menschen in Callcentern, und 52% der Callcenter allein in den USA beschäftigen Remote-Mitarbeiter.³ Sie arbeiten im Kundendienst, für Reisebüros, als Gesundheitsberater und in vielen anderen Funktionen. Zwar führen viele Callcenter ein Upgrade auf cloudbasierte UCaaS (Unified Communication as a Service) durch, doch Unternehmen verlassen sich oft noch auf veraltetes, vor Ort gehostetes VoIP und leiten die Anrufe mit VPNs für den Remote-Zugriff weiter. Für die Remote-Mitarbeiter von Callcentern ist die VoIP-Qualität oft Glückssache, wenn sie sich auf VPNs verlassen. Diese Verbindungen sind oft überlastet und Bildinstabilität und Latenzen bei VoIP-Anrufen daher keine Seltenheit, was für die Gesprächsteilnehmer auf beiden Seiten frustrierend ist.

Bis jetzt haben die meisten cloudbasierten ZTNA-Lösungen keine vor Ort gehosteten VoIP-Systeme unterstützt. Unternehmen mussten deshalb sowohl die ZTNA- als auch die VPN-Infrastruktur behalten.



52 %

der Callcenter allein in den USA beschäftigen Remote-Mitarbeiter.

Netskope One Private Access ist eine zentrale Lösung, die die Vorteile von ZTNA und SD-WAN in sich vereint. Eine dynamische Steuerung des Datenverkehrs und kontextbewusste QoS steigern die Produktivität der Mitarbeiter in Callcentern durch Sprach- und Videoanwendungen mit zuverlässig hoher Qualität. Gleichzeitig wird durch Zero-Trust-Zugriff auf alle internen Ressourcen die Sicherheitslage verbessert.

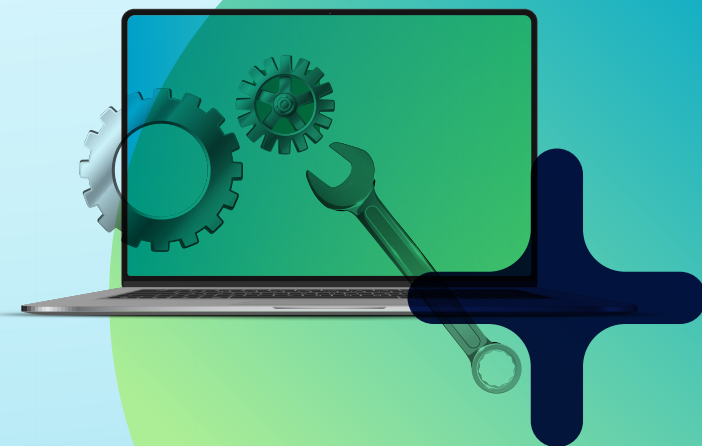


³Quelle: „Call Center Statistics – 2023“ Truelist.com. 1. Januar 2023.
<https://truelist.co/blog/call-center-statistics/#:-:text=The%20number%20of%20people%20working,million%20currently%20to%201.8%20million.>

6. Weitere Nutzung von älteren Anwendungen

Kompatibilitätstests sind ein wichtiger Schritt bei Technologieupgrades. Wenn Unternehmen ZTNA einsetzen, müssen sie die Anwendungen auch auf ihre Kompatibilität prüfen. Dabei entdecken sie in der Regel einige ältere Anwendungen, die mit den meisten aktuellen ZTNA-Lösungen inkompatibel sind. Beispielsweise sind ältere Anwendungen, bei denen der Traffic vom Server initiiert wird, nicht für moderne ZTNA-Lösungen mit ihrer Inside-Out-Konnektivität geeignet, weil dabei der Traffic vom Endpunkt initiiert wird. Diese älteren Systeme sind oft proprietär, weshalb ihre Umgestaltung und Modernisierung Zeit, Ressourcen und eine sorgfältige Planung erfordert (und oft eine Migration zu in der Cloud gehosteten IaaS-Umgebungen erfordert).

Netskope One Private Access ist jedoch eine Lösung für all diese Beispiele veralteter Anwendungen und gewährt sicheren und optimierten Zugriff auf alle privaten Anwendungen über einen einzigen integrierten Client. Unternehmen können dadurch die Lebensdauer dieser veralteten Anwendungen verlängern, Kosten für die Verwaltung unterschiedlicher Lösungen für den Remote-Zugriff reduzieren und schnellen, zuverlässigen Anwendungszugriff unabhängig vom Hosting-Standort gewähren.



Fazit

Auch wenn sie früher einmal der neueste Stand der Technik waren, sind veraltete VPNs für den Remote-Zugriff jetzt eine Herausforderung für Sicherheitsteams, für die sie eine Schwachstelle für Bedrohungen darstellen. Für Infrastruktur- und Betriebsteams sind sie problematisch, weil sie die Netzwerkleistung beeinträchtigen und das Benutzererlebnis beeinträchtigen.

Die meisten ZTNA-Lösungen sind heutzutage aber kein Allheilmittel. Wenn sie nicht alle relevanten Anwendungsfälle abdecken, können Unternehmen ihr VPN nur teilweise ersetzen und müssen eine gemischte Infrastruktur verwalten (veraltetes VPN plus „ein bisschen“ ZTNA), die vielleicht sogar noch komplexer als vorher ist.

Netskope One Private Access soll Unternehmen helfen, die Einführung von ZTNA voranzutreiben. Mit dieser vollständig integrierten Lösung kann der vollständige Austausch der gesamten VPN-Infrastruktur beschleunigt werden. Die Lösung ebnet den Weg für den Austausch aller Arten von VPNs für den Remote-Zugriff auf verschiedenste Anwendungen, verkleinert die digitale Angriffsfläche, verbessert den Sicherheitsstatus durch Zero-Trust-Prinzipien und steigert die Produktivität der Remote-Beschäftigten mit nahtlosem und optimiertem Anwendungszugriff.



Über Netskope One Private Access

Netskope One Private Access ergänzt ZTNA mit SD-WAN-Funktionen und sorgt für sichere, optimierte Verbindungen zu allen privaten Anwendungen, einschließlich vor Ort gehosteter VoIP-, Video- und Remote-Unterstützungslösungen. So können Unternehmen:

- die Konnektivität modernisieren und die Sicherheit erhöhen
- das Benutzererlebnis verbessern
- hochgradig zuverlässigen, optimierten Zugriff auf Sprach- und Videoanwendungen ermöglichen
- die Komplexität und die Betriebskosten reduzieren
- Pläne zur Stilllegung veralteter VPN-Infrastruktur voranbringen, sodass keine separaten Tools für den Remote-Zugriff mehr nötig sind
- eine nie dagewesene Sichtbarkeit und Kontrolle über den Anwendungs-Traffic erreichen

Mit Netskope One Private Access können VPNs für den Remote-Zugriff für alle relevanten Arten des Anwendungszugriffs vollständig stillgelegt (nicht nur teilweise ersetzt) werden. Zugleich wird die Sicherheitslage verbessert und nahtloser, optimierter Zugriff auf Anwendungen ermöglicht.



Über Netskope

Netskope, ein weltweit führender Anbieter von SASE-Lösungen, hilft Organisationen bei der Umsetzung von Zero-Trust-Prinzipien und KI/ML-Innovationen, um ihre Daten zu schützen und gegen Cyberbedrohungen zu verteidigen. Die schnell und einfach nutzbare Plattform Netskope One und ihre patentierte Zero Trust Engine bieten optimierten Zugriff und Echtzeit-Sicherheit für Personen, Geräte und Daten, wo immer sich diese befinden. Tausende Kunden vertrauen Netskope und seinem leistungsstarken NewEdge-Netzwerk, wenn es um die Verringerung von Risiken geht. Sie profitieren von unübertroffenen Einblicken in die Aktivitäten sämtlicher Cloud-, Web- und privaten Anwendungen und können ihre Sicherheitslage und Leistung ohne Kompromisse verbessern. Weitere Informationen finden Sie unter [netskope.com](https://www.netskope.com).

Sie möchten mehr erfahren?

Demo anfordern

