paloalto NETWORKS | PRISMA ACCESS BY PALO ALTO NETWORKS

# Das Sicherheitsniveau hybrider Belegschaften 2021

# Inhalt



Präsentiert von:


Als branchenweit umfassendste cloudbasierte Sicherheitsplattform konsolidiert Prisma Access von Palo Alto Networks mehr Punktlösungen in einem konvergierten Service als jedes andere Angebot auf dem Markt. Als Teil unserer SASE-Lösung (Secure Access Service Edge) revolutioniert Prisma Access die Netzwerksicherheit und versetzt Unternehmen in die Lage, ihre hybriden Belegschaften effektiv zu schützen. Im Gegensatz zu den Plattformen anderer Anbieter sichert Prisma Access den gesamten Anwendungsverkehr durch umfassende, branchenführende Schutzmaßnahmen und sorgt dank einzigartiger SLAs gleichzeitig für ein herausragendes Nutzererlebnis.

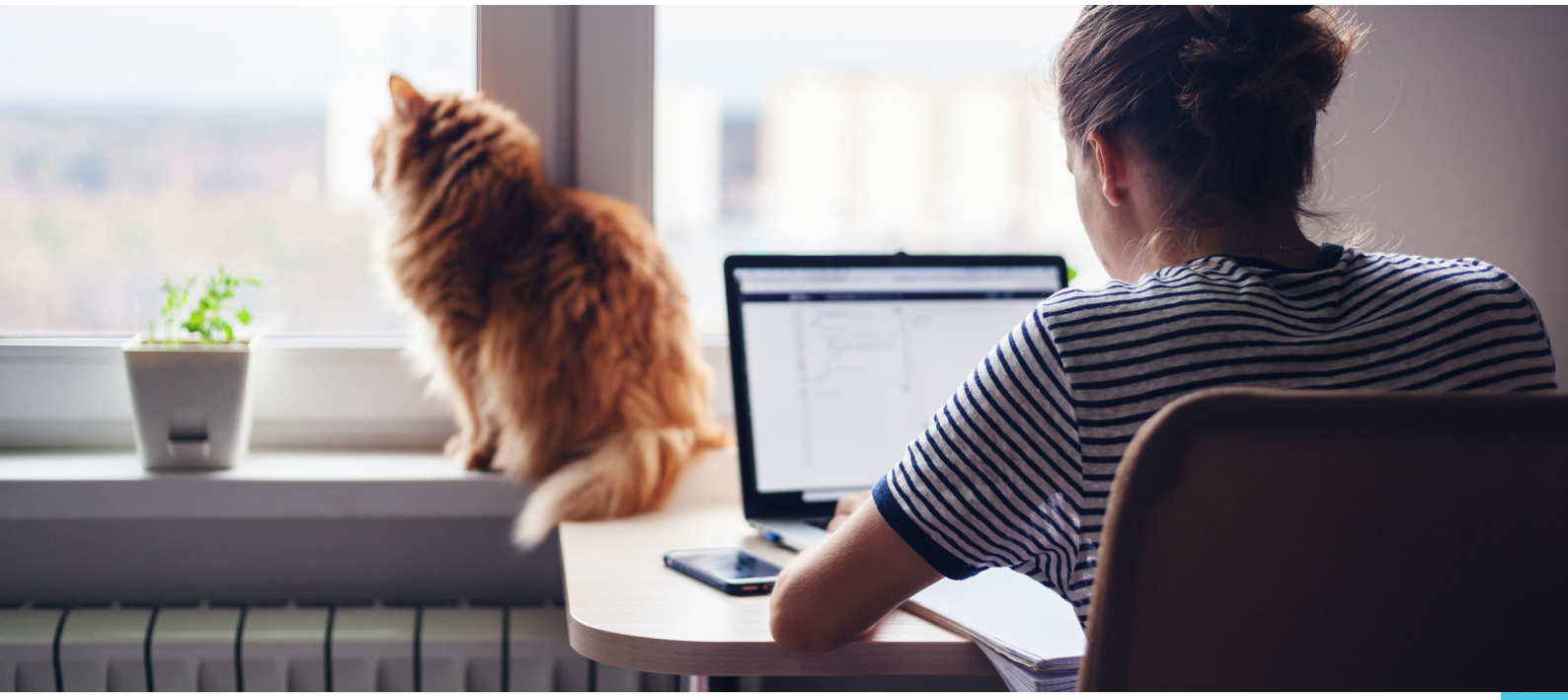
Folgen Sie @PrismaAccess auf Twitter oder schauen Sie unter https://www.paloaltonetworks.com/prisma/access vorbei, um mehr zu erfahren.

# Einleitung: Eine hybride Belegschaft nimmt Gestalt an

Die Covid-19-Pandemie hat uns gezwungen, unsere Arbeitsweisen schlagartig grundlegend zu ändern. Rund um den Erdball wurden die Angestellten der meisten Unternehmen aufgefordert, nach Möglichkeit von zu Hause aus zu arbeiten. Dabei mussten vorhandene Infrastrukturen schnellstmöglich an die neuen Gegebenheiten angepasst oder neue Lösungen implementiert werden, um die Voraussetzungen für ein produktives Arbeiten im Homeoffice zu schaffen.

Inzwischen werden die Kontaktbeschränkungen in verschiedenen Regionen der Welt gelockert, doch gleichzeitig nehmen langfristige hybride Arbeitsweisen Gestalt an. Viele Arbeitnehmer bestehen sogar darauf. Der Umfrage „Global Work-from-Home Experience Survey“ zufolge wollen 76 Prozent der Angestellten weltweit weiterhin zumindest einen Teil der Arbeitswoche außerhalb des Büros verbringen.[1] Gartner konstatiert denselben Trend: „Bis 2022 werden 25 Prozent der Wissensarbeiter das Homeoffice zu ihrem vorrangigen Arbeitsort machen und 45 Prozent der Beschäftigten werden an zwei oder drei Tagen pro Woche von zu Hause aus arbeiten.“[2]

In Unternehmen und Institutionen wird derzeit darüber nachgedacht, wie die Netzwerk- und Sicherheitsarchitekturen weiterentwickelt werden können, um die Produktivitätsvorteile hybrider Arbeitsweisen zu erhalten und gleichzeitig die mit ihnen einhergehenden Sicherheitsrisiken zu reduzieren. Zu Beginn der Pandemie wurde in diesen Unternehmen fieberhaft daran gearbeitet, die erheblich gestiegene Anzahl der mobilen Arbeiter zu unterstützen. Dabei stieß man vielerorts an die Leistungsgrenzen älterer Systeme, die natürlich weder für eine schnelle Skalierung noch für eine derartige Ausweitung des zu schützenden Netzwerks konzipiert worden waren. Nun werden Strategien für die langfristige Unterstützung einer hybriden Belegschaft entwickelt und die Netzwerk- und Sicherheitsarchitekturen modernisiert, um Unternehmensressourcen rund um die Uhr verfügbar zu machen und ein sicheres, optimiertes Nutzererlebnis zu gewährleisten.



# Über die Umfrage

## Ziele

Um besser zu verstehen, wie Unternehmen den durch die Pandemie veranlassten Übergang zu hybriden Belegschaften bewältigen, hat Palo Alto Networks mit „State of Hybrid Work Security 2021“ eine der weltweit größten und umfassendsten Untersuchungen zum Sicherheitsniveau hybrider Belegschaften durchgeführt. Das Ziel dieser Untersuchung war, Antworten auf folgende Fragen zu finden:

Welche Technologien und Tools werden zur Implementierung mobiler Arbeitsmodelle genutzt?

Welche Auswirkungen hatte der sichere Fernzugriff auf die Unterstützung der mobilen Arbeiter?

Wie haben sich Investitionen in Netzwerk- und Sicherheitsarchitekturen bei der Bereitstellung sicherer und effizienter Umgebungen für mobiles Arbeiten bezahlt gemacht?

## Methodik

Befragt wurden 3.000 IT-Profis, die in ihren Unternehmen in den Bereichen Informationssicherheit, Netzwerkbetrieb und/oder Anwendungsentwicklung tätig sind. Die Umfrage wurde von ONR, einem unabhängigen Drittanbieter, im Auftrag von Palo Alto Networks durchgeführt.

Die Zusammensetzung war wie folgt:

**1.250**

aus Nord- und Südamerika

**1.000**

aus Europa

**750**

aus dem asiatisch-pazifischen Raum

Zu den Umfrageteilnehmern gehörten sowohl Führungskräfte (CxOs und Vizepräsidenten) mit Verantwortung für die Technologie als auch Mitglieder der Netzwerk-, Sicherheits- und Betriebsteams. Alle Befragten verfügten über detaillierte Kenntnisse der Netzwerk- und Sicherheitsarchitektur ihres Unternehmens.

# Kurzfassung

## Für viele Unternehmen stellten (und stellen) der Fernzugriff und die durch die Pandemie und die hybriden Arbeitsweisen aufgeworfenen Sicherheitsrisiken erhebliche Herausforderungen dar.


fiel es schwer, sicheren Fernzugriff für die Mitarbeiter im Homeoffice bereitzustellen.

## Viele Manager befürchten, dass ihre Unternehmen nun einem größeren Risiko ausgesetzt sind, weil bei der Umstellung auf mobiles Arbeiten einige Schritte übersprungen wurden.

**48 %**

der untersuchten Unternehmen sind einem größeren Sicherheitsrisiko ausgesetzt, weil die Sicherheit hintangestellt und Sicherheitsrichtlinien nicht konsequent durchgesetzt bzw. den Mitarbeitern mehr Freiräume eingeräumt wurden, als normalerweise üblich ist.

**35 %**

der Befragten stimmten der Aussage zu, dass ihre Mitarbeiter die implementierten Sicherheitsmaßnahmen umgangen oder absichtlich deaktiviert hätten.

**53 %**

der Unternehmen, in denen dem Fernzugriff eine höhere Priorität eingeräumt wurde als der Sicherheit, sind nun erheblichen Sicherheitsrisiken ausgesetzt, da die Missachtung der Richtlinien für akzeptable Nutzung und der Einsatz nicht genehmigter Anwendungen lange stillschweigend geduldet wurden.

## Unternehmen schauen mit sicheren Hybridlösungen für ihre Mitarbeiter nach vorn.


der Befragten erwägen Hybridlösungen für ihre Belegschaft.


der befragten Unternehmensvertreter planen, ihre Sicherheitsmaßnahmen im Verlauf der nächsten 24 Monate ganz oder größtenteils in die Cloud zu verlagern.

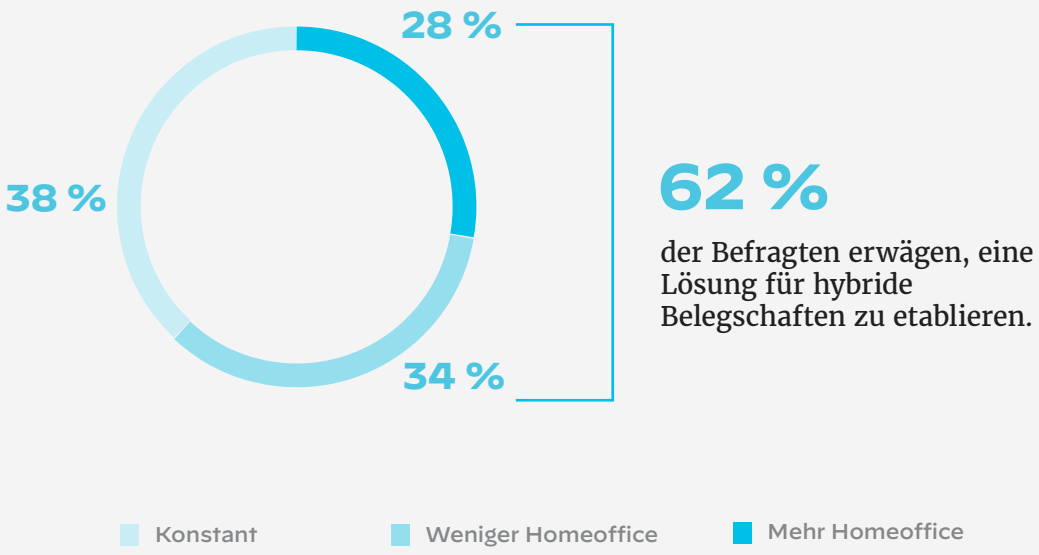
# Hybridarbeit gilt in Firmen als Dauerlösung

Im Rahmen der Planung für die Zeit nach der Pandemie entwerfen Unternehmen momentan Strategien für hybride Belegschaften. Dabei müssen sie die Betriebsprozesse, die Technologieinfrastruktur, die Immobilien, die Mitarbeiterproduktivität und -zufriedenheit sowie die Unternehmenskultur berücksichtigen.

Zum Zeitpunkt der Umfrage lag der Anteil mobiler Arbeiter in zwei Drittel der untersuchten Unternehmen zwischen 25 und 75 Prozent – ähnlich wie auf dem Höhepunkt der Pandemie. Inzwischen ist in einigen Unternehmen ein Teil der Belegschaft ins Büro zurückgekehrt, doch im großen Ganzen unterscheiden die Arbeitsweisen sich nicht wesentlich von dem Muster während der Lockdowns – das mobile Arbeiten herrscht eindeutig vor.

Das optimale Verhältnis zwischen On-Premises- und Telearbeit ist von Firma zu Firma verschieden und wird vielerorts derzeit ermittelt. In den meisten Unternehmen geht man jedoch davon aus, dass es sich in etwa auf dem derzeitigen Niveau einpendeln wird. 44 Prozent der Umfrageteilnehmer gehen davon aus, dass mehr als die Hälfte ihrer Mitarbeiter auch in zwölf Monaten noch mobil arbeiten werden. Aufgrund dessen sind 62 Prozent im Begriff, die Funktionen für den Fernzugriff und somit die Abläufe und das Umfeld für ihre hybride Belegschaft zu perfektionieren. Insgesamt planen 94 Prozent, im Verlauf der nächsten zwölf Monate ein hybrides Arbeitsmodell aufzubauen.

**Unternehmenspläne für die Arbeit im Homeoffice für die nächsten 12 Monate**




Ein Umfrageteilnehmer bemerkte sehr treffend: „Es ist schlicht unmöglich, die Arbeit von zu Hause im kommenden Jahr völlig zu unterbinden. Das wäre einfach zu extrem. Inzwischen sind die Systeme schließlich da und wir haben uns in dieser Richtung entwickelt. Deshalb planen wir, die Homeoffices weiter zu nutzen.“

# Pandemie verschiebt bei den meisten den Fokus der IT-Transformation

Vor der Pandemie liefen in den meisten Unternehmen große Initiativen zur digitalen Transformation, in deren Rahmen auch die Migration in die Cloud und die Modernisierung der Infrastrukturen zur besseren Unterstützung mobiler Mitarbeiter geplant waren. Durch die Pandemie wurden diese Pläne plötzlich mit sehr viel mehr Dringlichkeit umgesetzt. Über Nacht wurde die Unterstützung des mobilen Arbeitens zur obersten Priorität der IT-Teams. Unserer Umfrage zufolge bauten 67 Prozent der Unternehmen die Kapazität ihrer vorhandenen Architekturen für den Fernzugriff aus und implementierten gleichzeitig neue Technologien, um ihre Infrastruktur zu modernisieren. Die anfängliche Kapazitätssteigerung diente jedoch lediglich als Übergangslösung. 64 Prozent planen, die Architektur für den Fernzugriff innerhalb der nächsten 24 Monate grundlegend zu verändern.

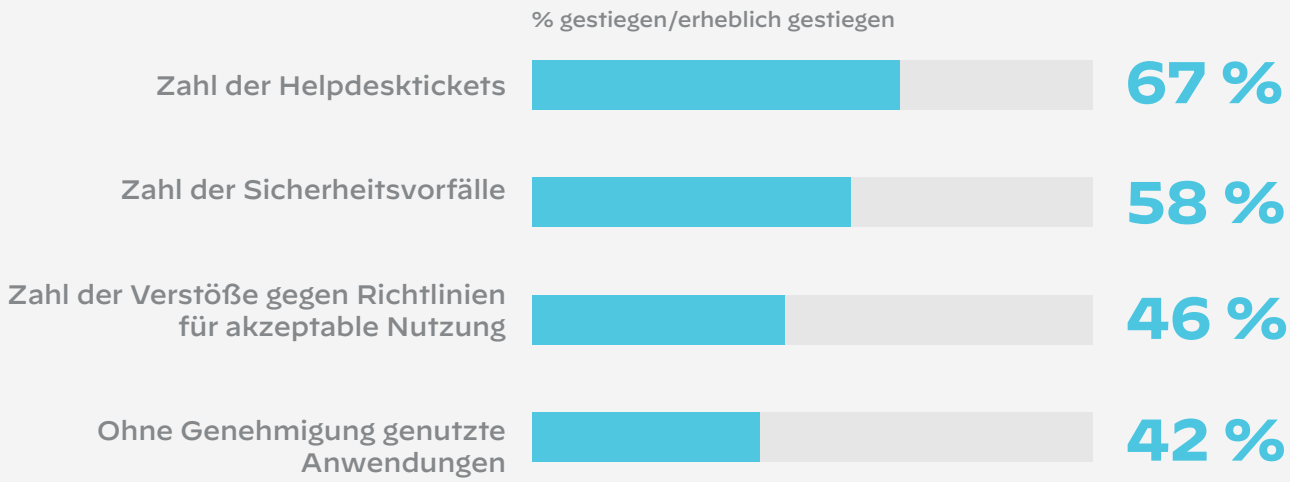
„Unser strategischer Plan (die Migration in die Cloud) bleibt das Langzeitziel. Vielleicht müssen wir die Termine neu stecken, da wir einige Investitionen umdisponieren mussten, um den sofortigen Bedarf an Kapazitäten für den Fernzugriff zu decken."

# Sicherheit ist die größte Herausforderung

Unserer Umfrage zufolge war man Mitte 2021 in den meisten Unternehmen mit dem eigenen Netzwerk zufrieden. Anfängliche Benutzerbeschwerden bezüglich der Leistung und Wirksamkeit der Kollaborationstools waren behoben und der Netzwerk- und Fernzugriff stabilisiert worden. Nur einer Minderheit (zwischen einem Viertel und einem Drittel) fiel es noch immer schwer, Mitarbeitern ein rundum positives Nutzererlebnis zu bieten.

Dennoch sind Unternehmen nach wie vor mit erheblichen Herausforderungen konfrontiert. Für 51 Prozent steht die Sicherheit dabei an erster Stelle, dicht gefolgt von Servicequalität und technischer Komplexität mit 48 bzw. 47 Prozent. Unseren Umfrageteilnehmern zufolge hat der Übergang zum mobilen Arbeiten inmitten der Covid-19-Pandemie die Zahl der Helpdesktickets, Sicherheitsvorfälle, Verstöße gegen Richtlinien für akzeptable Nutzung und ohne Genehmigung genutzten Anwendungen in die Höhe getrieben.

**Auswirkungen von Covid-19 und Homeoffice auf Ihr Netzwerk**



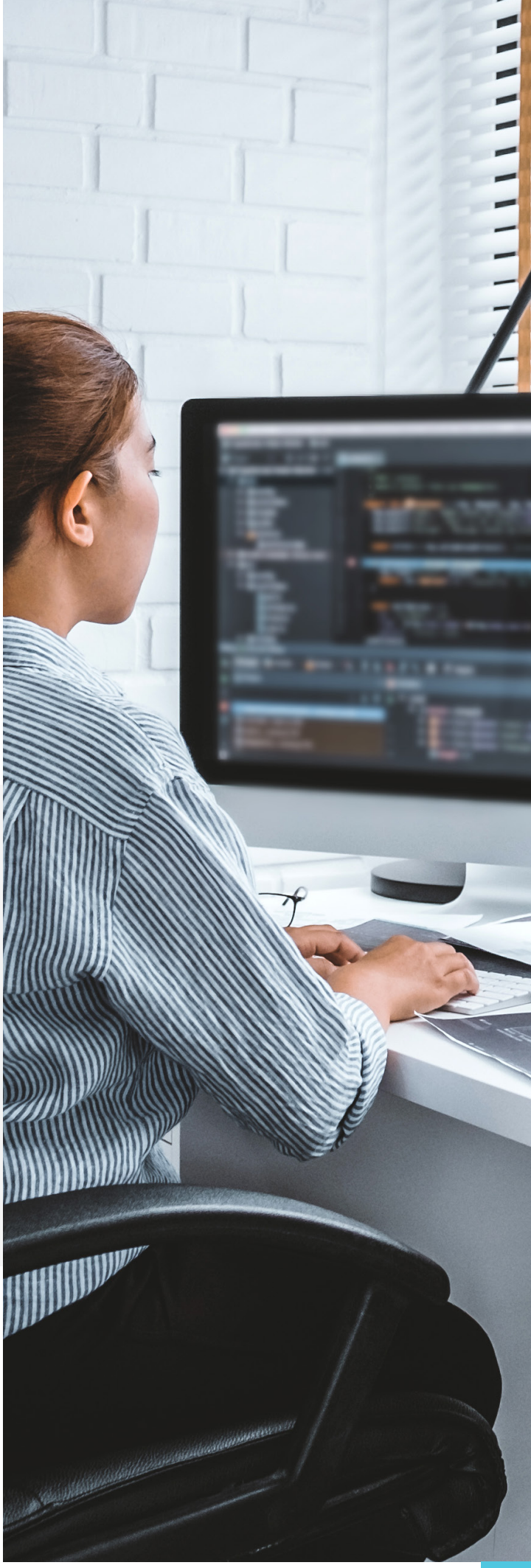

Zudem hat das mobile Arbeiten auch die Problembehebung erschwert. Ein Teilnehmer meinte dazu: „Benutzer können nicht mehr einfach zu jemandem an den Tisch kommen, um ein Problemgerät zu übergeben und es sich später repariert zurückgeben zu lassen.“

# Drei Ansätze für Netzwerkzugang und Sicherheit

Vor dem Hintergrund einer äußerst ungewissen Zukunft und sehr knapper Budgets – insbesondere zu Beginn der Pandemie – waren Unternehmen nicht bereit, in langfristige Lösungen zu investieren. In den von uns untersuchten Unternehmen erwiesen sich sowohl die Verbesserung des Fernzugriffs als auch die Stärkung der dazugehörigen Sicherheitsmaßnahmen als schwierig (59 bzw. 61 Prozent). Investitionen wurden dort getätigt, wo sie am dringlichsten erforderlich waren.

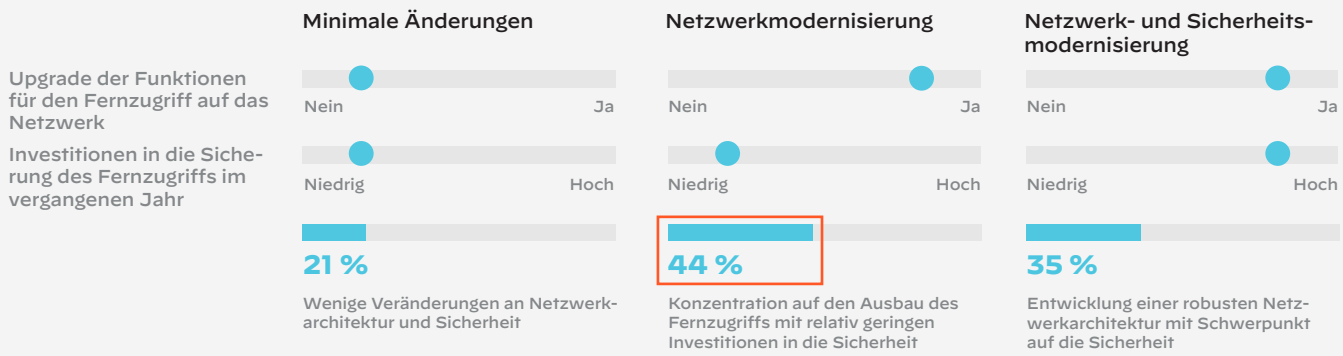

der Unternehmen fiel es schwer, die Kapazitäten für die aufgrund von Covid-19 erforderliche Arbeit im Homeoffice bereitzustellen.


der Unternehmen fiel es schwer, die erforderlichen Sicherheitsmaßnahmen für diese Kapazitäten bereitzustellen.



All dies führte zu drei verschiedenen Ansätzen zum Aufbau der erforderlichen Netzwerk- und Sicherheitskapazitäten:

- **Minimale Änderungen:** 21 Prozent nahmen nur sehr wenige Änderungen an ihrer Netzwerk- und Sicherheitsarchitektur vor.
- **Netzwerkmodernisierung:** 44 Prozent (und damit die größte Gruppe) konzentrierten sich bei ihren Technologieinvestitionen auf die Verbesserung des Fernzugriffs. In dessen Sicherung wurde hingegen relativ wenig investiert.
- **Netzwerk- und Sicherheitsmodernisierung:** 35 Prozent entschieden sich für einen ausgewogeneren Ansatz und investierten sowohl in robustere Funktionen für den Fernzugriff als auch in die dazugehörigen Sicherheitsvorkehrungen.




Jetzt, da hybrides Arbeiten zum neuen Normalzustand wird, treten in den Unternehmen, in denen nur die nötigsten Änderungen und Upgrades vorgenommen wurden, Schwächen in der Netzwerkarchitektur zutage. In 48 Prozent dieser Unternehmen ist man nun der Meinung, dass das Netzwerk das aktuelle Ausmaß der mobilen Arbeit nicht angemessen unterstützen könne und dass die vorhandene Architektur für den Fernzugriff als Dauerlösung ungeeignet sei. Im Gegensatz dazu wird diese Ansicht nur von 21 Prozent der Befragten aus Unternehmen vertreten, in denen das Netzwerk umfassend ausgebaut wurde.  Und wo sowohl Netzwerk als auch Sicherheit modernisiert wurden, berichten nur 14 Prozent der Befragten von andauernden Problemen.

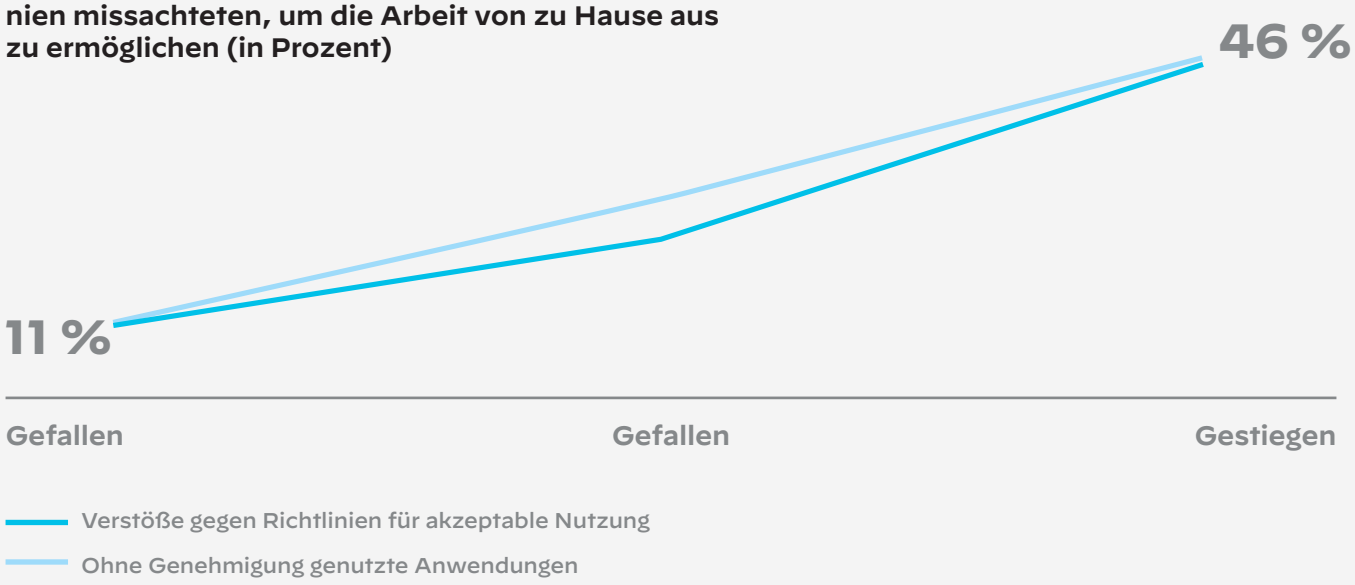
„Als wir zur Arbeit im Homeoffice übergegangen sind, wussten wir nicht, ob die Situation für eine Woche oder für einen Monat anhalten würde. Und es war schwierig, Entscheidungen für längere Zeiträume zu treffen, weil wir ja nicht vorhersagen konnten, ob die Leute sofort ins Büro zurückkehren, sobald dies möglich ist.“

# Sicherheit stand bei vielen hintenan

Die Daten zeigen auch, dass fast die Hälfte der Umfrageteilnehmer sich auf den Ausbau der Netzwerkarchitektur zur Unterstützung des Fernzugriffs konzentrierte, ohne dessen Sicherung die gebührende Aufmerksamkeit zu zollen.

Dabei wirkte sich die Ausweitung der Funktionen und Privilegien auf so viele zusätzliche Mitarbeiter natürlich auch auf die Netzwerksicherheit aus. Eigenen Angaben zufolge sind 48 Prozent der untersuchten Unternehmen seitdem einem größeren Sicherheitsrisiko ausgesetzt, weil Sicherheitsrichtlinien nicht konsequent durchgesetzt oder den Mitarbeitern mehr Freiräume eingeräumt wurden, als zuvor üblich war.

**Anteil der Unternehmen, die ihre Sicherheitsrichtlinien missachteten, um die Arbeit von zu Hause aus zu ermöglichen (in Prozent)**

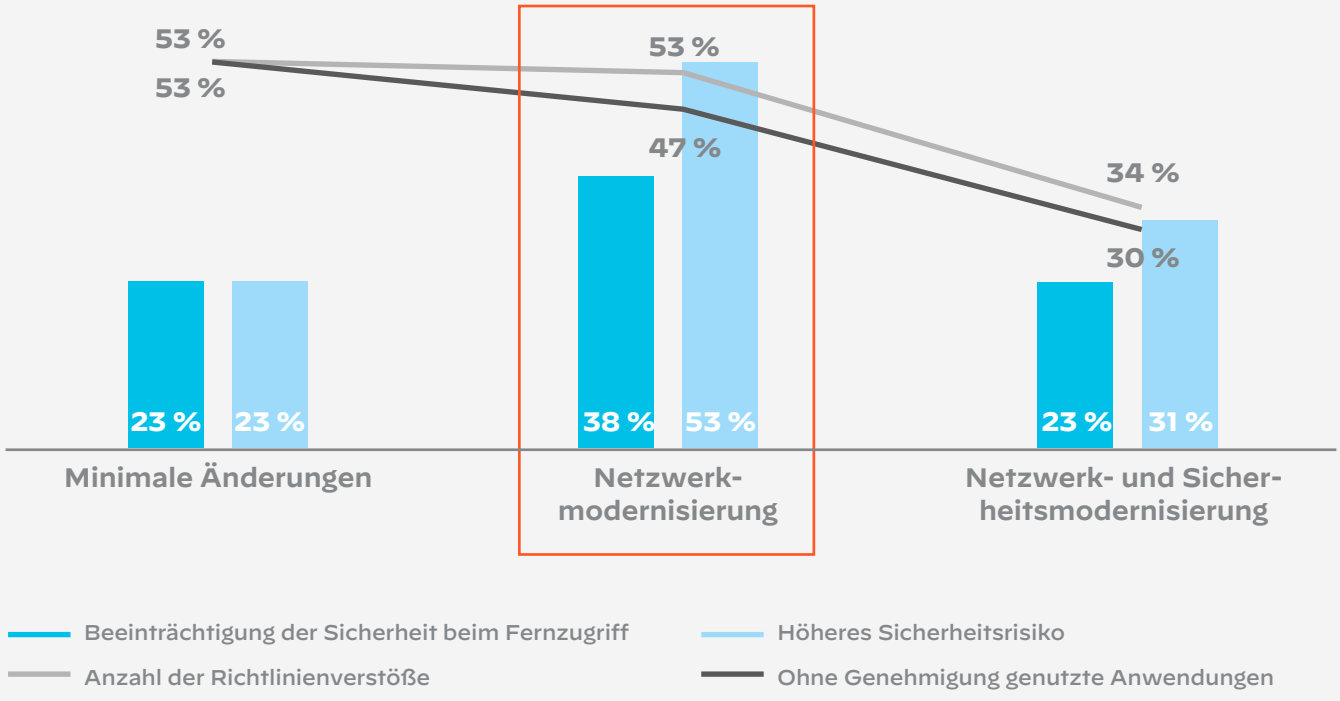



## Mobiles Arbeiten bringt neue Sicherheitsrisiken mit sich

Beim Auf- und Ausbau von Infrastrukturen für den Fernzugriff wurden in vielen Unternehmen nie angemessene Sicherheitsvorkehrungen, -prozesse und -richtlinien für das mobile Arbeiten etabliert. Ein Umfrageteilnehmer brachte dies auf den Punkt: „Wir hatten keine richtige Strategie für das mobile Arbeiten. Als Homeoffice plötzlich zum Thema wurde, entstand eine erhebliche Sicherheitslücke. Schließlich erfordert die Telearbeit eine völlig andere Infrastruktur als die Arbeit in einer Niederlassung.“

Zu den Gründen gehören knappe Budgets, Zeit- und Ressourcenmangel sowie die pandemiebedingte Notwendigkeit, die Anforderungen für mobiles Arbeiten möglichst schnell zu erfüllen. Im Rahmen der Umstellung wurden Sicherheitsbeschränkungen dementsprechend gelockert. Mehr als die Hälfte (53 Prozent) der untersuchten Unternehmen räumten dem Fernzugriff eine höhere Priorität ein als der Sicherheit und sind nun erheblichen Sicherheitsrisiken ausgesetzt, da die Missachtung der Richtlinien für akzeptable Nutzung und der Einsatz nicht genehmigter Anwendungen lange stillschweigend geduldet wurden. Interessanterweise stieg die Anzahl der Sicherheitsvorfälle in Unternehmen mit minimalen Änderungen nur um 23 Prozent. Ihre Sicherheit wurde also ebenfalls geschwächt, aber nicht im gleichen Ausmaß.

**Auswirkungen von Covid-19 und der Umstellung auf mobiles Arbeiten auf verschiedene Aspekte von Unternehmensnetzwerken**
% stimmen zu/voll und ganz zu




Das Phänomen ist hinreichend bekannt: Wenn Sicherheitsmaßnahmen lästig werden – indem sie zum Beispiel Systeme verlangsamen und so die Produktivität oder das Nutzererlebnis beeinträchtigen – finden Mitarbeiter oft kreative Methoden, um sie zu umgehen. Beim mobilen Arbeiten und/oder der Nutzung von cloudbasierten Anwendungen ist dies einfacher als je zuvor. Durch die Ausweitung der Telearbeit können Sicherheitsmaßnahmen einerseits störender und andererseits auch leichter umgangen werden.

An dieser Stelle sollte betont werden, dass man sich in den meisten Unternehmen durchaus bewusst war, welche Risiken man einging. Doch vielerorts fehlten schlicht die finanziellen Mittel für den notwendigen Ausbau der Netzwerksicherheit. Denn ohne konkrete sicherheitsbezogene Metriken lässt sich der ROI von Investitionen in angemessene Sicherheitsmaßnahmen nur schwer nachweisen.

# Konsequenzen ungenügender Sicherheit: Umgehung von Sicherheitsmaßnahmen beim Fernzugriff

Insgesamt stimmten 35 Prozent der Befragten der Aussage zu, dass ihre Mitarbeiter die von ihnen zum Schutz des Fernzugriffs implementierten Sicherheitsmaßnahmen entweder umgangen oder absichtlich deaktiviert hätten. Der Schweregrad dieser Aktivitäten war allerdings sehr unterschiedlich.

Was genau bewog die Benutzer zu diesem riskanten Verhalten? Die Pandemie zwang Angestellte zum plötzlichen Wechsel ins Homeoffice und brachte neue Risikofaktoren mit sich, die die Umgehung von Sicherheitsmaßnahmen begünstigten. Diese waren zwar nicht unbedingt unbekannt, aber vor der Pandemie nicht im selben Ausmaß aufgetreten und/oder nicht gründlich untersucht worden.

Die gestiegene Komplexität, die laxere Durchsetzung von Sicherheitsrichtlinien und ein spontaner, entscheidungsfreudiger (und nicht wie gewohnt bedachter, sorgfältig geplanter) Sicherheitsansatz sind nur einige Beispiele. Von Seiten der Benutzer kamen der Einsatz nicht genehmigter Anwendungen (Schatten-IT) und die geschäftliche Nutzung eigener (statt vom Unternehmen bereitgestellter) Geräte (Bring Your Own Device, BYOD) hinzu.

Überall dort, wo der Sicherheit zu Beginn der Pandemie nicht die notwendige Priorität eingeräumt wurde, sind die Konsequenzen immer noch deutlich spürbar. Die Unternehmen, in denen heute Sicherheitsmaßnahmen massiv umgangen werden, sind nämlich genau die Unternehmen, in denen die Sicherheit bei der Ausweitung der Infrastruktur für den Fernzugriff vernachlässigt wurde. Unter anderem trugen ungeeignete Kollaborationstools, die verstärkte Nutzung von BYOD-Geräten, für die keine angemessenen Sicherheitsmaßnahmen oder -richtlinien vorhanden waren, und der Einsatz ungenehmigter Anwendungen dazu bei, dass die vorhandenen Sicherheitsmaßnahmen von vielen Mitarbeitern umgangen wurden. In vielen Unternehmen dachte man bei der eiligen Suche nach Wegen zur Unterstützung des mobilen Arbeitens nicht daran, welche Konsequenzen die Vernachlässigung der Sicherheit haben würde.

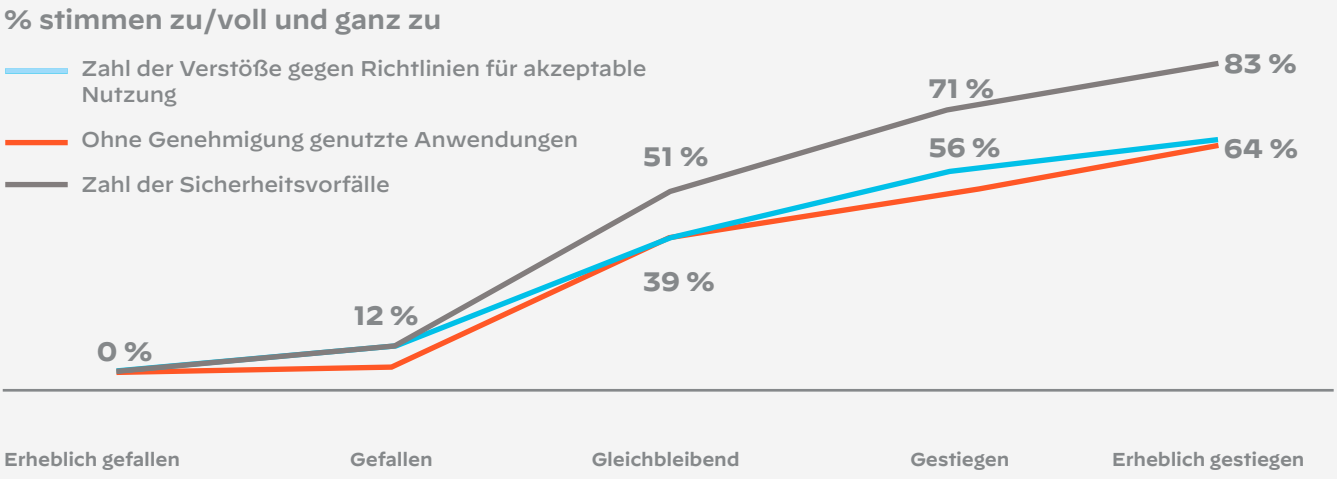
## Riskantes Verhalten der mobilen Arbeiter

- Geschäftliche Nutzung persönlicher Geräte (BYOD)
- Hochladen von Unternehmensdaten zu nicht autorisierten Anwendungen oder Cloud-Diensten
- Umgehung von Sicherheitsmaßnahmen
- Verbindung zu ungesicherten Netzwerken zu Hause oder unterwegs
- Fehlende Weiterbildung zu Cybersicherheitsrisiken
- Kein Melden von Phishing und anderen Bedrohungen
- Weiterleitung vertraulicher Dateien per E-Mail
- Kein Installieren von Sicherheitsupdates auf Geräten

Die Ergebnisse unserer Umfrage bestätigen dies:

- Aus Unternehmen ohne effektive Kollaborationstools haben wir gehört, dass deren Benutzer mit **mehr als achtmal höherer Wahrscheinlichkeit** zugeben, Sicherheitsmaßnahmen häufig zu umgehen. Die Mitarbeiter neigen dazu, nach eigenen Wegen oder nicht genehmigten Anwendungen für eine effizientere Zusammenarbeit zu suchen – wodurch das Sicherheitsrisiko natürlich steigt.
- Auf dem Höhepunkt der Pandemie wurden die BYOD-Richtlinien in vielen Unternehmen gelockert. Unsere Umfrage zeigt, dass 60 Prozent der Unternehmen ihr BYOD-Konzept ausweiteten, damit ihre Mitarbeiter von zu Hause aus arbeiten konnten. Infolgedessen ignorieren, umgehen oder deaktivieren die Mitarbeiter der Unternehmen, in denen die BYOD-Nutzung weitgehend gestattet wurde, nun mit **achtmal höherer Wahrscheinlichkeit** Sicherheitsmaßnahmen als die Mitarbeiter von Unternehmen, die BYOD einschränkten.
- Durch die verstärkte BYOD-Nutzung ist auch die Zahl der Sicherheitsprobleme (Einsatz ungenehmigter Anwendungen und Verstöße gegen Richtlinien für akzeptable Nutzung) und Sicherheitsvorfälle stark gestiegen. In 83 Prozent der Unternehmen, in denen BYOD erheblich ausgeweitet wurde, nahmen sowohl die Sicherheitsvorfälle als auch der Einsatz ungenehmigter Anwendungen zu. Bei 64 Prozent gab es mehr Verstöße gegen Richtlinien für akzeptable Nutzung. Vielleicht vermutete man zu Beginn der Pandemie zwar, dass die verstärkte BYOD-Nutzung die Sicherheitsrisiken vergrößern könnte, war aber nicht auf einen solch rasanten Anstieg vorbereitet.

**Nutzung von Bring Your Own Device (BYOD) seit Covid-19**




„Unsere Sicherheitstechnologie war nicht dafür konfiguriert, uns eine Übersicht über den Fernzugriff zu bieten, weil der größte Teil unserer Belegschaft [vorher] immer im Büro war. Deshalb hatten wir unsere Sicherheitstechnologie auf diesen Bereich und nicht auf den Fernzugriff ausgerichtet."

# Erkenntnisse führen zu neuen Prioritäten bei der Sicherheit

Inzwischen werden die Schwächen der aktuellen Strategien für die Sicherung des mobilen Arbeitens deutlich. In 59 Prozent der untersuchten Unternehmen beruhen diese auf rasch implementierten Punktlösungen. Für 49 Prozent der Befragten führt dieses Flickwerk nicht miteinander verknüpfter Lösungen zu toten Winkeln, die die Priorisierung von Risiken sowie die Bedrohungsprävention erschweren.

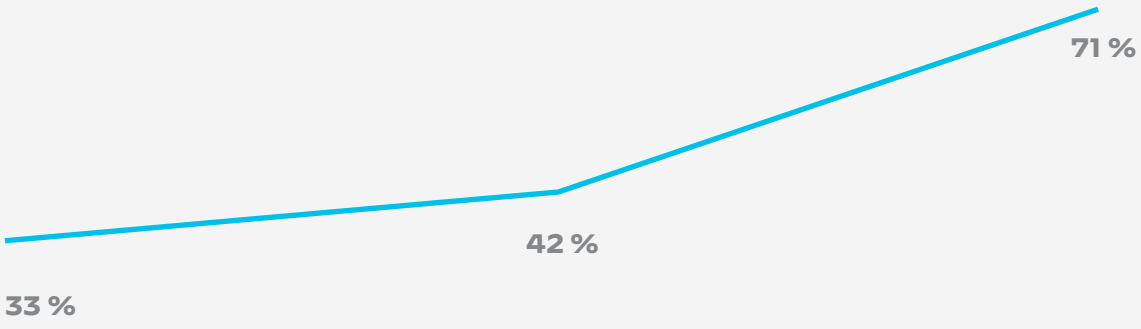
In den meisten Regionen der Welt ist der hastige Übergang zum mobilen Arbeiten inzwischen abgeschlossen. Stattdessen konzentriert man sich in Unternehmen auf die Entwicklung der richtigen Langzeitstrategien und -lösungen für die hybride Belegschaft. 74 Prozent der Umfrageteilnehmer sind der Meinung, dass eine einzige, umfassende Sicherheitslösung ihr Sicherheitsniveau steigern würde. Zudem richten Manager und Entscheidungsträger mit Verantwortung für die Sicherheit ihr Augenmerk auf cloudbasierte Sicherheitsdienste.

## Verlagerung der Sicherheitsdienste in die Cloud

Natürlich gibt es auch Positives zu berichten. In 67 Prozent der untersuchten Unternehmen wurden zu Hochzeiten der Pandemie proaktiv Maßnahmen zum besseren Schutz der mobilen Arbeiter eingeleitet: 41 Prozent verlagerten einige Sicherheitsvorkehrungen in die Cloud und 26 Prozent bauten die Sicherheitslösungen vor Ort als Übergangslösung aus.

Auch die Aussichten für die Zukunft sind gut, denn 71 Prozent der Umfrageteilnehmer planen, ihre Sicherheitsinfrastruktur innerhalb der nächsten 24 Monate größtenteils oder vollständig in die Cloud zu verlagern. Dieser wichtige Trend unterstützt den Übergang zu einer hybriden Belegschaft, denn für mobile Mitarbeiter sind cloudbasierte Sicherheitstechnologien zur Unterstützung der standortunabhängigen Kollaboration unerlässlich.

**Anteil der Unternehmen mit größtenteils oder vollständig cloudbasierter Sicherheit (in Prozent)**



# Konsequenzen umgangener Sicherheitsmaßnahmen

Neben den bereits erörterten Sicherheitsproblemen hat die Umgehung von Sicherheitsmaßnahmen auch die langfristige Effektivität der Netzwerkarchitekturen in Frage gestellt und zu unbefriedigenden Ergebnissen bei hybriden Arbeitsweisen geführt. Unsere Umfrage zeigt, dass dies den Verantwortlichen in Unternehmen mit einem hohen Maß an umgangenen Sicherheitsmaßnahmen mehr Sorgen bereitet als ihren Kollegen in Unternehmen, die diesbezüglich mittelmäßig abschneiden. Umfrageteilnehmer aus Unternehmen mit einem hohen Maß an umgangenen Sicherheitsmaßnahmen:

- haben mit fast viermal höherer Wahrscheinlichkeit Bedenken, dass ihr derzeitiges Netzwerk den aktuellen Anforderungen nicht gewachsen sei.
- sind mit mehr als viermal höherer Wahrscheinlichkeit der Meinung, dass ihre Architektur für den Fernzugriff keine Dauerlösung ist.

Außerdem gestanden die Befragten aus Unternehmen mit einem hohen Maß umgangener Sicherheitsmaßnahmen ein, dass dies sich nicht nur negativ auf die Netzwerke und die Sicherheit auswirke, sondern auch auf das mobile Arbeiten selbst.

- In dieser Gruppe ist die Meinung, dass die Umgehung von Sicherheitsmaßnahmen die Mitarbeiterproduktivität beeinträchtige, doppelt so weit verbreitet wie unter den anderen Umfrageteilnehmern.
- Auch die geschätzte Mitarbeiterzufriedenheit ist in dieser Gruppe mit 60 Prozent am niedrigsten. In Unternehmen mit einem niedrigen Maß umgangener Sicherheitsmaßnahmen liegt diese bei 80 Prozent und bei Unternehmen mit mittlerem Maß bei 70 Prozent.

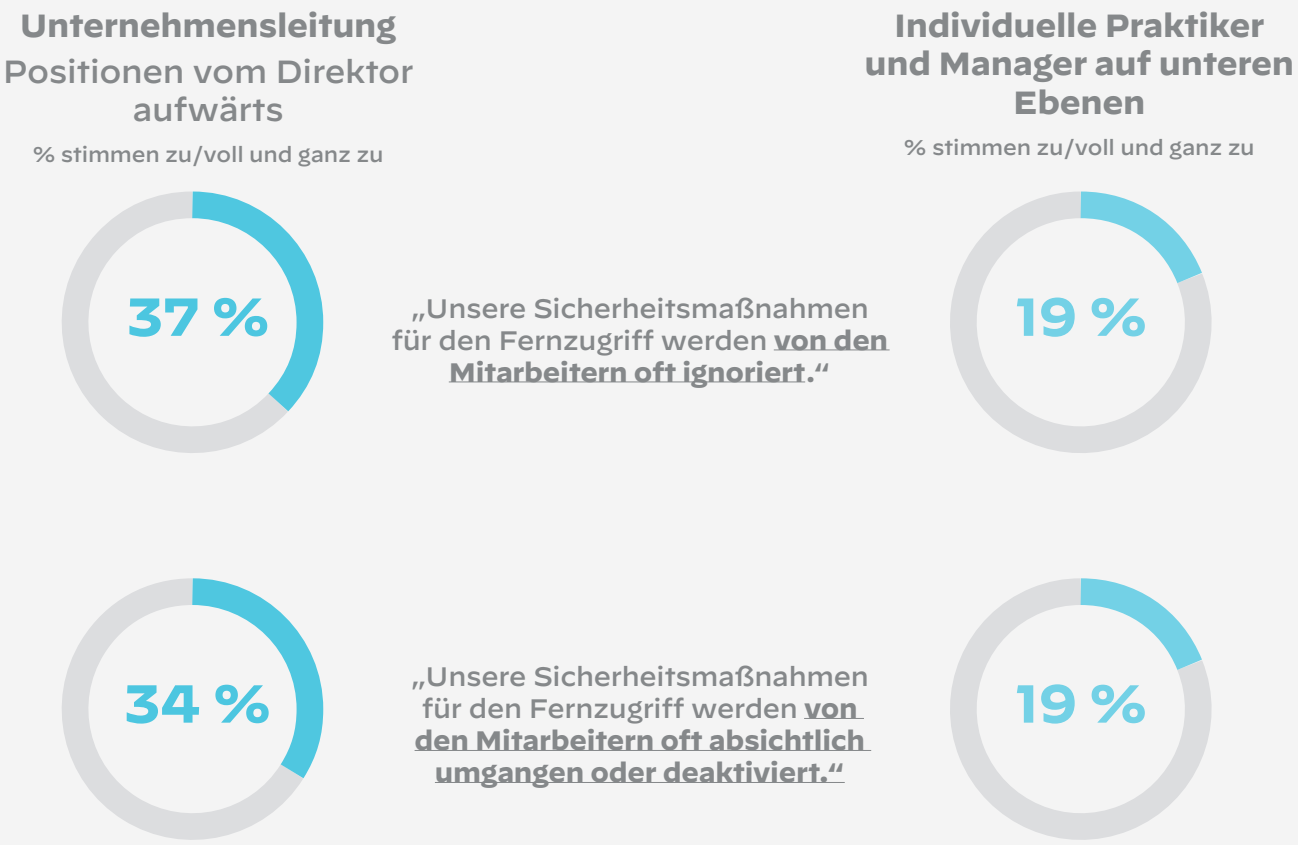
# Perspektiven der Unterneh-mensleitung und der Praktiker

Bei den Fragen zu den Herausforderungen, vor die hybride Arbeitsweisen Unternehmen stellen, gehen die Antworten der Unternehmensleitung (CxOs und Vizepräsidenten) und die der Praktiker (einschließlich der unteren Managementebenen) auseinander. Unsere Umfrage ergab, dass beide Gruppen positive Meinungen zum Nutzererlebnis beim mobilen Arbeiten haben, obwohl die Benutzer sich über ungenügende Konnektivität und mangelnde Kenntnisse der zur Telearbeit genutzten Tools, Technologien und Sicherheitsrichtlinien sowie über fehlende Schulungsangebote beschwert hatten. Etwa 70 Prozent beider Gruppen sind überzeugt, dass ihre Benutzer – unabhängig von deren Arbeitsort – nahtlosen Zugang zu allen Anwendungen hätten und dass ihr Unternehmen ununterbrochene, zuverlässige Konnektivität bereitstelle.

Bezüglich der Stabilität der eigenen Netzwerkinfrastruktur für den Fernzugriff zeigten die Mitglieder der Unternehmensleitung sich jedoch wesentlich besorgter als die Praktiker. 43 Prozent der Führungskräfte, aber nur 13 Prozent der Praktiker, halten die aktuelle Architektur für den Fernzugriff für unzureichend, um die derzeitigen Anforderungen hybrider Arbeitsweisen zu erfüllen, und/oder für nicht zukunftsfähig. Mehr als die Hälfte der Mitglieder der Unternehmensleitung (aber nur 30 Prozent der Praktiker) haben ähnliche Bedenken bezüglich der derzeit genutzten Kollaborationstools.

Woher kommt dieser Unterschied? Praktiker neigen möglicherweise dazu, die Qualität und Wirksamkeit der Lösungen, die sie selbst verwalten, nicht ganz unvoreingenommen und tendenziell zu positiv zu bewerten. Ihre tägliche praktische Erfahrung mit den Tools und der Umgebung vermittelt ihnen jedoch auch ein realistischeres Bild der Architektur für den Fernzugriff und ihrer Leistungsgrenzen, als Manager in gehobenen Führungspositionen und Endbenutzer es haben.

Die Sorgen der Unternehmensleitung könnten auch auf Bedenken über umgangene Sicherheitsmaßnahmen basieren. Mindestens 30 Prozent der Führungskräfte gaben an, dass ihre Mitarbeiter Sicherheitsmaßnahmen ignorierten, umgingen oder deaktivierten. Bei den Praktikern waren nur 19 Prozent dieser Meinung. Die Praktiker sind allerdings möglicherweise nicht in der Lage, das Ausmaß des Problems unternehmensweit einzuschätzen.




Auch bezüglich der Verlagerung der Sicherheitsvorkehrungen in die Cloud mithilfe eines Secure Access Service Edge (SASE) sind die Unternehmensleitung und die Praktiker unterschiedlicher Meinung. Eine große Mehrheit der Praktiker hält diese für nützlich, während 27 Prozent der Vertreter der Führungsriege sich noch an die Idee gewöhnen müssen.

# Aufbau der optimalen Belegschaft

Nun, da die Welt der Zeit nach Covid-19 entgegensieht, denkt man in den meisten Unternehmen darüber nach, wie eine hybride Belegschaft aussehen könnte. Unsere Umfrageergebnisse zeigen, dass die Mehrheit der Unternehmen, in denen sowohl in die Sicherheit als auch in die Netzwerke für den Fernzugriff investiert wurde, eine zu mehr als 50 Prozent hybride Belegschaft anstrebt. In Unternehmen, in denen nur minimale Änderungen vorgenommen oder nur die Netzwerke für den Fernzugriff modernisiert wurden, ist man hingegen weniger zuversichtlich und plant, sich auf eine zu weniger als 50 Prozent hybride Belegschaft zu beschränken.

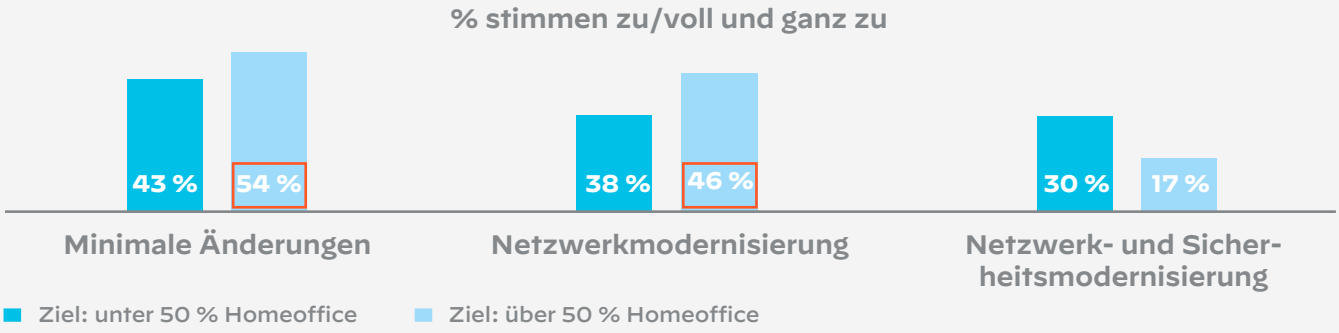
Den Mitarbeitern selbst scheint das mobile Arbeiten zu gefallen, denn in 71 Prozent der Unternehmen ist die Mitarbeiterzufriedenheit seit dem Wechsel ins Homeoffice gestiegen. Daher überrascht es nicht, dass die Mehrheit der Unternehmen ein hybrides Arbeitsmodell beibehalten will. Nur 15 Prozent der Befragten sagten, dass ihr Unternehmen zum traditionellen, bürobasierten Betrieb zurückkehren wolle, und lediglich 6 Prozent erwarten den Wiedereinzug aller Mitarbeiter ins Büro im Laufe des nächsten Jahres. Stattdessen rechnen Umfrageteilnehmer aus 44 Prozent der Unternehmen damit, dass mehr als die Hälfte ihrer Belegschaft auch im kommenden Jahr per Fernzugriff arbeiten wird, und fast alle gehen davon aus, dass ihr Unternehmen weiterhin eine hybride Umgebung unterstützen wird.

Ein Thema, das sich bei der Umfrage herauskristallisiert hat, ist, dass Unternehmen, die eine zu mehr als 50 Prozent hybride Belegschaft anstreben, die Anpassung ihrer Sicherheitsmaßnahmen vorantreiben müssen, um die Umgehung von Sicherheitsmaßnahmen beim Fernzugriff unter Kontrolle zu bekommen. Im Folgenden zitieren wir einige Ergebnisse, die dies bestätigen, insbesondere für Unternehmen, die bislang nur minimale Änderungen vorgenommen oder sich auf die Netzwerkmodernisierung konzentriert haben.

- Wie bereits erwähnt zweifeln fast die Hälfte der Umfrageteilnehmer aus der Führungsriege an der Effektivität der eigenen Kollaborationstools und etwa ein Fünftel der Praktiker teilt diese Bedenken.
- Rund die Hälfte der Befragten aus Unternehmen, die nur minimale Änderungen vorgenommen oder sich auf die Netzwerkmodernisierung konzentriert hatten, berichteten, dass es ihnen schwerfalle, eine effektive und produktive Zusammenarbeit ihrer Mitarbeiter zu unterstützen (54 bzw. 46 Prozent). Im Gegensatz dazu haben nur 17 Prozent der Unternehmen, in denen sowohl das Netzwerk als auch die Sicherheit modernisiert worden war, mit dieser Herausforderung zu kämpfen.

**Ansätze für die Modernisierung von Netzwerk und Sicherheit**

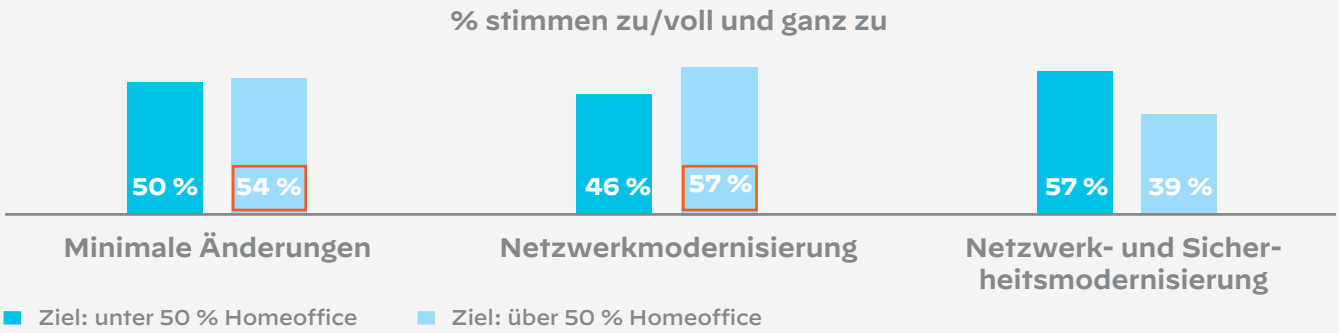
„Die Kollaborationstools meines Unternehmens versetzen unsere mobilen Arbeiter nicht in die Lage, effektiv mit ihren Kollegen zu kommunizieren und zusammenzuarbeiten."




- Auch mangelnde Transparenz aufgrund der Nutzung nicht miteinander verknüpfter Punktlösungen wurde von der Mehrheit der Befragten aus Unternehmen mit minimalen Änderungen (53 Prozent) und auf das Netzwerk beschränkten Investitionen (57 Prozent) als Anlass zu erheblicher Sorge genannt.

**Ansätze für die Modernisierung von Netzwerk und Sicherheit**

„Ich glaube, dass durch die Anzahl an Punktlösungen, die wir zum Schutz unserer mobilen Arbeiter einsetzen, Lücken und tote Winkel entstehen, die es uns erschweren, Risiken zu priorisieren und Bedrohungen zu vermeiden."



# Fazit

In der Nachpandemiezeit gewinnt das Konzept einer hybriden Belegschaft zusehends an Akzeptanz. Daher lautet die entscheidende Frage: In welchem Ausmaß planen Unternehmen, diese Arbeitsweise zu unterstützen, und wie gut sind sie darauf vorbereitet?

Unsere Umfrageergebnisse zeigen, dass Unternehmen, die einen niedrigeren Anteil von Telearbeitern anvisieren, bislang noch wettbewerbsfähig sind. Andererseits müssen diejenigen, die den Ausbau der Unterstützung für hybride Arbeitsweisen planen, einige Herausforderungen bewältigen – insbesondere die Umgehung von Sicherheitsmaßnahmen, ineffektive Kollaborationstools und eine unzureichende Übersicht über ihre gesamte Unternehmensinfrastruktur.

In mehr als drei Viertel der Unternehmen ist man sich bewusst, dass die Netzwerkkonnektivität einen entscheidenden Einfluss auf die Moral der Mitarbeiter hat, und unternimmt erhebliche Anstrengungen, um diese zu gewährleisten. 81 Prozent der befragten Mitglieder der Führungsriege bezeichneten die Infrastruktur für den Fernzugriff als eine ihrer obersten Prioritäten und betonten, dass die Aufrechterhaltung einer umfassenden Sicherheit und Servicequalität sowohl ihre größte Herausforderung als auch ihr wichtigstes Ziel sei. Daher steigern sie die Investitionen in Sicherheitsmaßnahmen für den Fernzugriff und verlagern Sicherheitsdienste in die Cloud.

Durch die Ablösung konventioneller Infrastrukturen für den Fernzugriff durch Cloud-Lösungen können Unternehmen die aktuellen und zukünftigen Anforderungen ihrer hybriden Belegschaft erfüllen und gleichzeitig von erheblichen Vorteilen profitieren, die eine herkömmliche Architektur nicht bieten kann. Darunter:

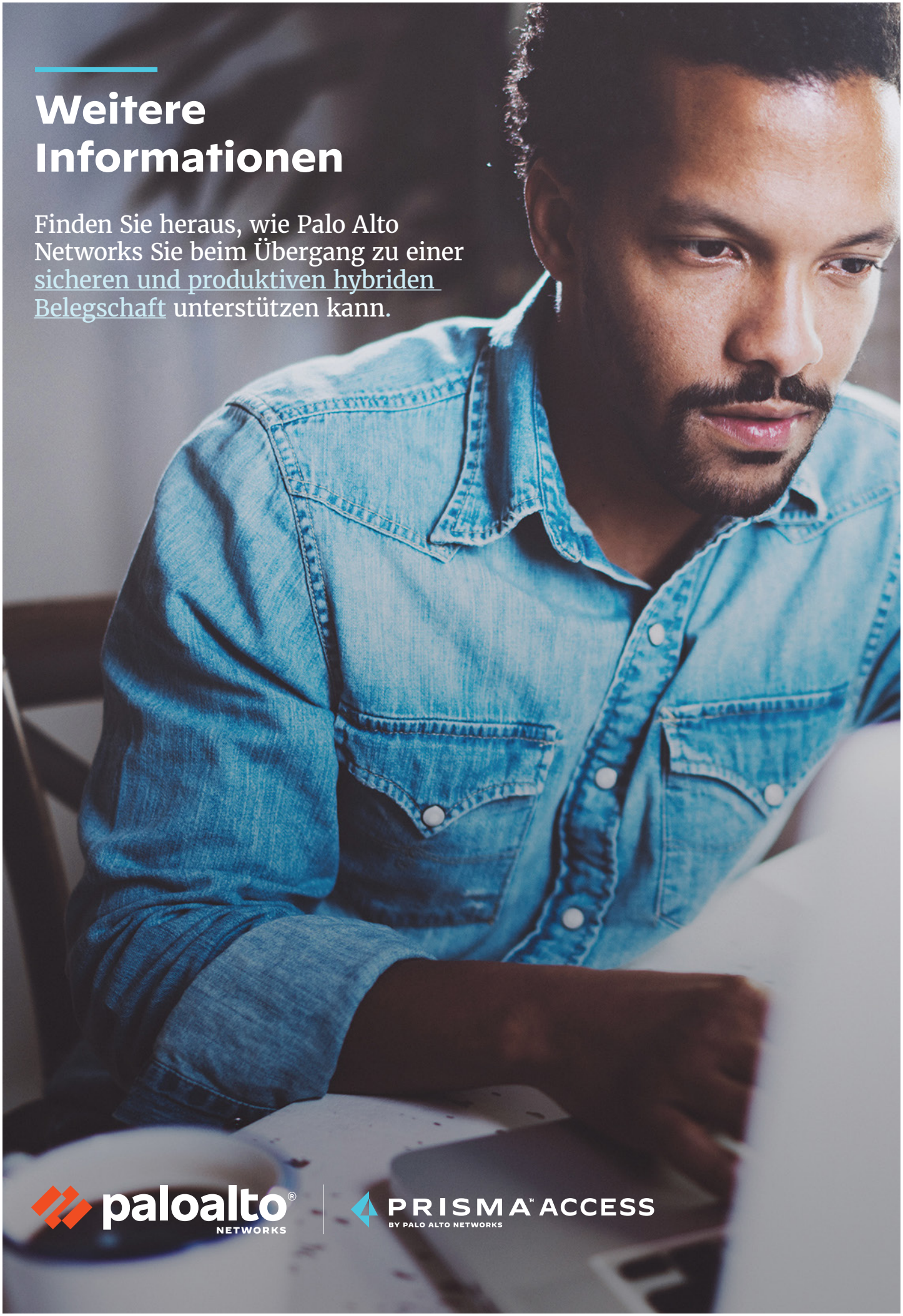
- Übersicht über das Netzwerk, die Anwendungen und den Benutzerdatenverkehr – unabhängig davon, ob Mitarbeiter im Büro, zu Hause oder unterwegs arbeiten
- Kontrolle darüber, worauf Benutzer und Anwendungen zugreifen und was sie weiterleiten
- Sicherheit für die gesamte Netzwerkinfrastruktur und alle Anwendungen, Dienste und Benutzer, sodass Bedrohungen und Schwachstellen schnell behoben werden können
- Einfachere Bereitstellung, sodass Filialen und Homeoffices problemlos in das Netzwerk eingefügt werden können, ohne dass Hardware installiert oder ein Mitglied des IT-Teams sich vor Ort begeben muss

## Steigerung der Investitionen in den sicheren Fernzugriff

**Unternehmen planen, ihre Investitionen in den sicheren Fernzugriff in den nächsten zwölf Monaten zu steigern: 54 Prozent der untersuchten Unternehmen erwarten Ausgaben von über fünf Millionen USD in diesem Bereich. Im Vorjahr waren es nur 31 Prozent.**

Weitere Informationen über das Forschungsunternehmen, das die Feldforschung für diesen Bericht betrieben und die umfangreichen Analysen dafür geliefert hat, finden Sie unter https://www.onrcx.com/.

1. https://globalworkplaceanalytics.com/global-work-from-home-experience-survey
2. https://www.gartner.com/smarterwithgartner/making-hybrid-work-more-permanent-set-some-ground-rules/


Weitere Informationen
Finden Sie heraus, wie Palo Alto Networks Sie beim Übergang zu einer sicheren und produktiven hybriden Belegschaft unterstützen kann.
paloalto NETWORKS
PRISMA ACCESS
BY PALO ALTO NETWORKS