

Leitfaden

# Geheimtipps für eine erfolgreiche SASE-Migration



**verizon**  
business

# Inhalt

**So meistern Sie die Herausforderungen der Migration zu SASE** 3

---

**Herausforderungen bei der Einführung von SASE**

**1. Migration von älteren Umgebungen und Technologien** 5

**2. Wahl des richtigen Anbieters und Zusammenspiel von Netzwerk- und Sicherheitsteams** 6

**3. Erste Schritte bei der Integration mehrerer Technologien** 7

---

**Erarbeiten Sie ein Erfolgskonzept** 8

---

**Beziehen Sie zur richtigen Zeit die richtigen Leute ein** 9

---

**Legen Sie den Projektumfang gemeinsam fest** 10

---

**Erwägen Sie einen schrittweisen Ansatz** 11

---

**Legen Sie realistische Zeitrahmen fest** 12

---

**Finden Sie den richtigen Partner** 13

---

**Wenden Sie sich an uns** 14

---





## So meistern Sie die Herausforderungen der Migration zu SASE

Immer mehr Unternehmen setzen Secure Access Service Edge (SASE) ein, um ihre Netzwerksicherheit zu stärken und den Betrieb zu straffen. Doch der Umstieg auf SASE und die Integration bestehender Ressourcen und Prozesse in eine SASE-Umgebung ist oft ein komplexes Unterfangen. Welche potenziellen Herausforderungen und Probleme erwarten Unternehmen und wie können sie sie meistern? Experten und Expertinnen von Verizon haben hier ihre Geheimtipps dazu zusammengestellt.

Die Netzwerksicherheit muss stets am Puls der Zeit und mehrere Schritte voraus sein, denn Cyberbedrohungen nehmen zu und Angreifer werden immer gewiefter. Hinzu kommt, dass viele Unternehmen inzwischen stark von Multi-Cloud-Umgebungen abhängig sind, sodass Anwendungen und Daten weit verteilt sind und die Angriffsfläche entsprechend größer ist. Auch die Tatsache, dass viele Mitarbeitende hybride, dezentrale Arbeitsmodelle nutzen und nur einen Teil der Woche im Büro verbringen, trägt ihren Teil dazu bei, dass die Netzwerksicherheit wesentlich komplexer ist als früher.

SASE kombiniert Technologien für das softwaredefinierte Wide Area Network

Der Druck auf Sicherheitsteams steigt also unaufhörlich und es wundert daher nicht, dass Unternehmen zunehmend auf SASE umsteigen.

(SD-WAN) mit Secure Service Edge (SSE) und deckt jede Verbindungsart (wie Mobilfunk, das öffentliche Internet sowie private Netzwerke) mit einem vollständig integrierten WAN mit umfassender Sicherheitsinfrastruktur ab. Durch die Integration von Netzwerk und Sicherheit in ein zentrales Framework können Organisationen mit SASE das Richtlinienmanagement vereinfachen und ihr Sicherheitsniveau stärken. In Kombination mit einem Zero-Trust-Ansatz kann SASE zudem das Zugriffsmanagement verbessern und sicherstellen, dass nur autorisierte Benutzer und Geräte Zugang zum Netzwerk erhalten. Außerdem unterstützt SASE moderne, verteilte Cloud-Umgebungen, sodass Unternehmen nicht mehr mit den Einschränkungen der mit traditionellen Netzwerksicherheitsmodellen einhergehenden Hardware- und Konfigurationsverwaltung kämpfen müssen.

Mit SASE können Unternehmen zu einem ganzheitlicheren Sicherheitsansatz wechseln und somit ihren Betrieb straffen. Sie können sich besser vor modernen Cyberbedrohungen schützen und ihren hybrid arbeitenden Teams einen sichereren Zugriff auf das Unternehmensnetzwerk bieten. Doch der Umstieg auf SASE ist nicht ohne Herausforderungen, von der komplexen Integration mehrerer Technologien bis zur Ausarbeitung und Einführung neuer Geschäftsprozesse.

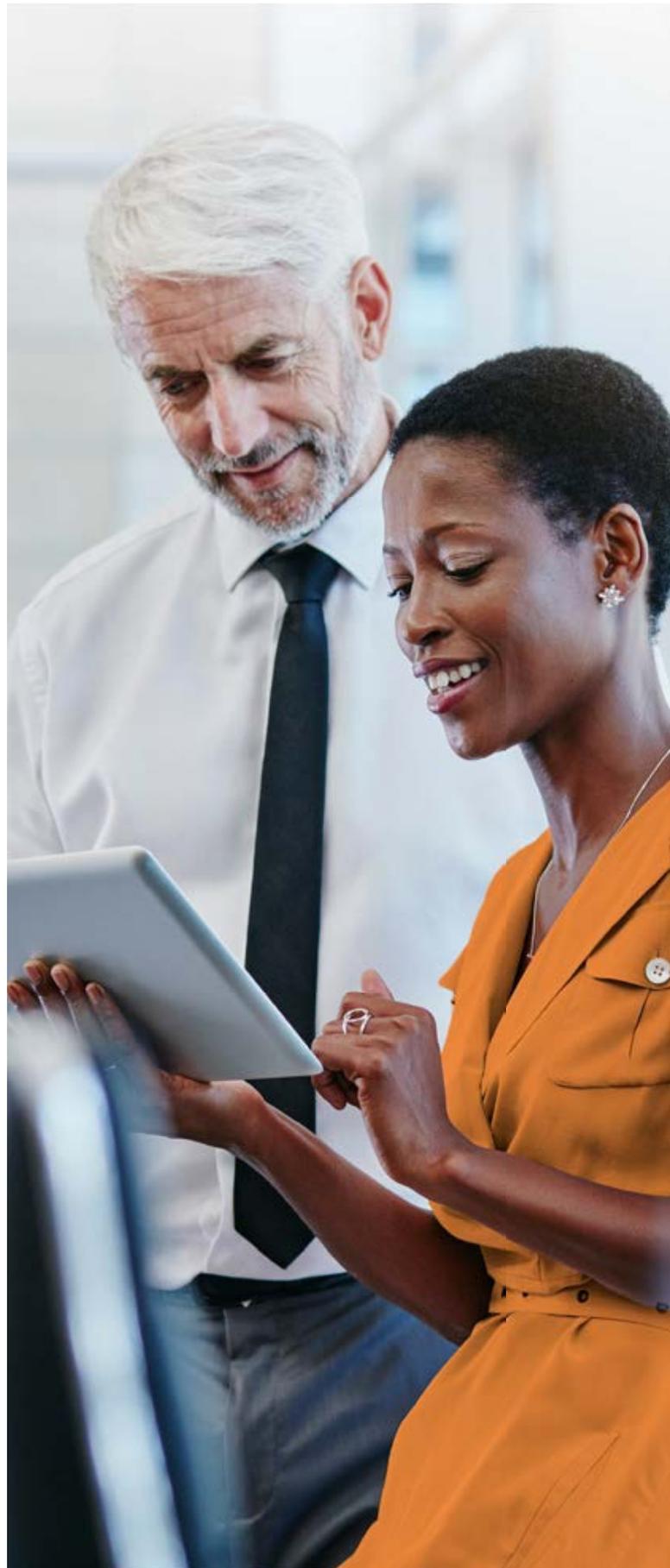


# Herausforderungen bei der Einführung von SASE

## 1 Migration von älteren Umgebungen und Technologien

In Gesprächen mit Verizon erwähnen viele Kunden zwei Beweggründe für die Migration zu SASE: Verträge mit ihren aktuellen Anbietern und die Nutzungsdauer ihrer vorhandenen Technologien. Viele professionelle Tätigkeiten können heute nur mit technologischer Unterstützung erledigt werden – und das bedeutet, dass jedes umfassende technische Upgrade veralteter IT-Infrastrukturen erhebliche Auswirkungen auf Geschäftsprozesse und deren Nutzer haben wird. Es bedarf daher einer sorgfältigen Planung von Umstellungen und Upgrades, damit der laufende Betrieb so wenig wie möglich beeinträchtigt wird.

Jeff Paterson, einer der Lösungsarchitekten bei Verizon UK, unterstützt große, globale Unternehmenskunden, und meint zu solchen Migrationen: „Es geht nicht nur darum, alte Architektur durch eine brandneue SD-WAN- oder SASE-Umgebung zu ersetzen. Die Integration ist immer eine Herausforderung. Sie sollten SD-WAN- und SSE-Technologien wählen, die sich bereits bei der Integration mit älteren Hybrid-Umgebungen – und der nativen Integration mit CSP/Cloud-Umgebungen – bewährt haben. Das ist extrem wichtig, wenn Sie sich den Umstieg auf eine ganzheitliche SASE-Lösung vereinfachen wollen.“



## 2 Wahl des richtigen Anbieters und Zusammenspiel von Netzwerk- und Sicherheitsteams

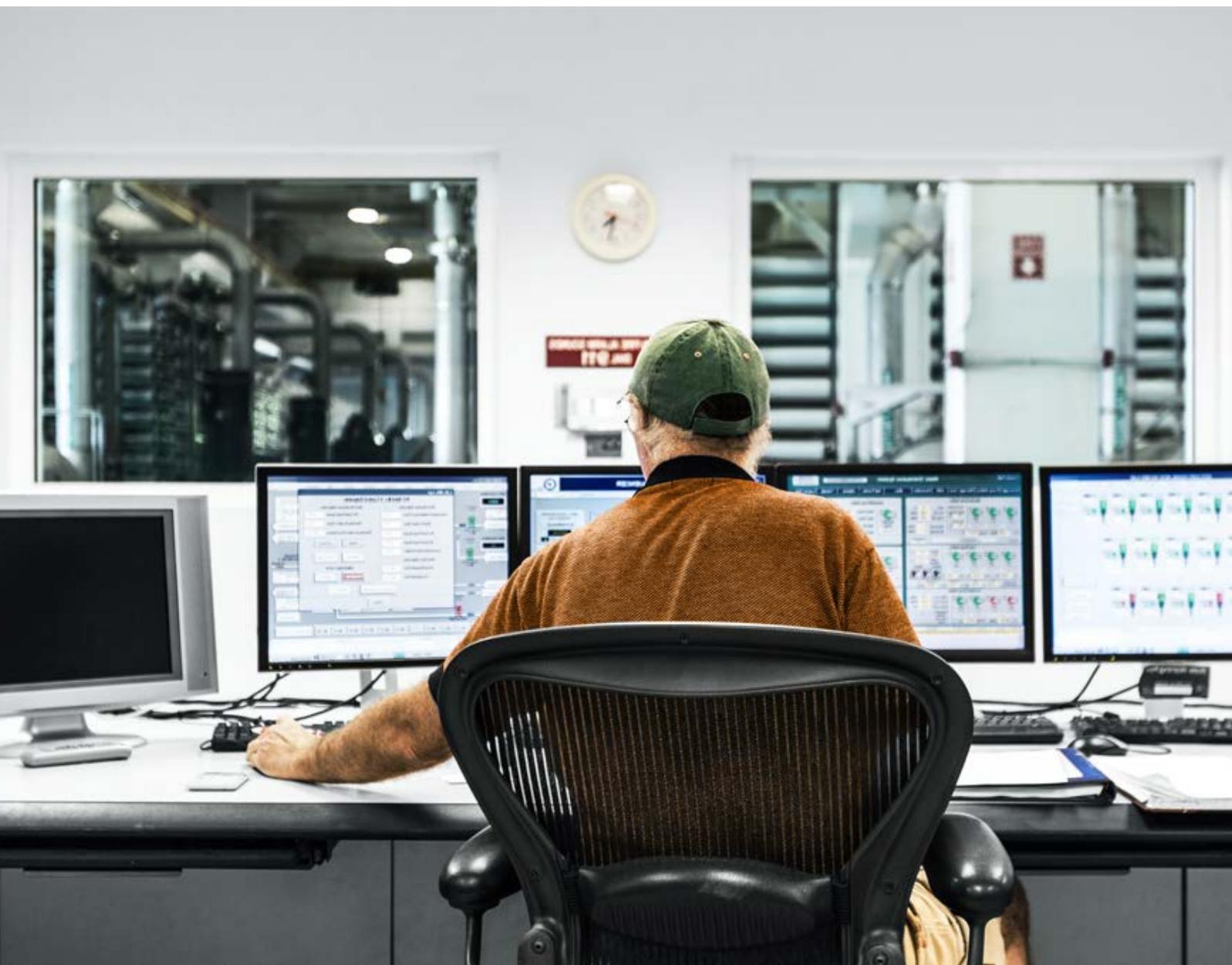
Viele Organisationen stehen außerdem vor der Herausforderung, eine erheblich engere Zusammenarbeit zwischen Netzwerk- und Sicherheitsteams zu organisieren, als diese gewohnt sind. Bislang haben beide Teams beim Kauf jeder neuen Netzwerktechnologie und jedes neuen Sicherheitssystems den jeweils besten Anbieter gewählt, anstatt nach Anbietern zu suchen, die Expertise in beiden Bereichen besitzen. Oft sind sich alle einig, dass SASE prinzipiell die richtige Lösung ist, aber dennoch fällt es den Netzwerk- und Sicherheitsteams nicht leicht, sich auf einen oder einige wenige Anbieter zu einigen. Um hier die Erfolgchancen zu erhöhen, sollten Organisationen zusätzliche Zeit für Analysen und Diskussionen in ihren Teams einplanen.

“

Es geht nicht nur darum, alte Architektur durch eine funkelnagelneue SD-WAN- oder SASE-Umgebung zu ersetzen. Die Integration ist immer eine Herausforderung.

**Jeff Paterson**

Lösungsarchitekt, Verizon Business



### 3 Erste Schritte bei der Integration mehrerer Technologien

Es ist mitunter schwierig, Technologien von verschiedenen Anbietern so miteinander zu verknüpfen, dass sie nahtlos zusammenarbeiten, da sie – im Gegensatz zu SASE-Lösungen aus einer Hand – in vielen Fällen nicht dafür konzipiert wurden. Deshalb können zum Beispiel die Bereitstellung von Cloud-Sicherheitsdiensten und ihre Integration in die SD-WAN-Lösung, die Konfiguration von SaaS-Richtlinien oder die Zusammenführung von Einblicken und Daten von verschiedenen Technologieanbietern in einer zentralen Konsole zur echten Herausforderung werden.

Hinzu kommt, dass Unternehmen die (oft sehr unterschiedlichen) Anforderungen ihrer Netzwerk- und Sicherheitsteams unter einen Hut bringen müssen. Zum Beispiel benötigen Sicherheitsteams häufig vollständigen Zugang zu Tools für die Konfiguration von Sicherheitsrichtlinien, um nahezu in Echtzeit auf Vorfälle und Bedrohungen reagieren zu können. Netzwerkteams hingegen bevorzugen vielleicht einen begrenzten Zugriff auf die SD-WAN-Richtlinienkonfiguration, weil sie autonome Self-Service-Funktionen nutzen möchten, ohne befürchten zu müssen, dass Änderungen versehentlich netzwerkweit angewendet werden und möglicherweise katastrophale Folgen haben.

Wie also können Unternehmen diese Herausforderungen und den Umstieg auf SASE meistern und gewährleisten, dass diese neue Technologie ihren Geschäftsanforderungen entspricht?





## Erarbeiten Sie ein Erfolgskonzept

Sie sollten Ihre Integration sorgfältig planen, sich mit jeder Phase vertraut machen und genau festlegen, wer wofür verantwortlich ist. Erstellen Sie eine Roadmap mit klar definierten Etappen, die zu Ihrem anvisierten Wunschzustand führen, und sorgen Sie dafür, dass alle Beteiligten dieser Roadmap folgen. Jeff Paterson sagt dazu: „Definieren Sie Ihre Ziele klar und deutlich, gegebenenfalls in Zusammenarbeit mit Ihrem Technologiepartner. Halten Sie unbedingt alles schriftlich fest und lassen Sie es von sämtlichen Stakeholdern unterschreiben.“

“

Definieren Sie Ihre Ziele klar und deutlich, gegebenenfalls in Zusammenarbeit mit Ihrem Technologiepartner. Halten Sie unbedingt alles schriftlich fest und lassen Sie es von sämtlichen Stakeholdern unterschreiben.

**Jeff Paterson**

Lösungsarchitekt, Verizon Business

## Beziehen Sie zur richtigen Zeit die richtigen Leute ein

Der Umstieg auf SASE ist ein komplexer Prozess mit vielen Teilschritten und zahlreichen Beteiligten. Sorgen Sie unbedingt dafür, dass allen Beteiligten von Anfang an alle wichtigen Informationen zur Verfügung stehen und dass sie Ihre Ziele vollkommen unterstützen. Ansonsten, sagt Fyllon Papadopoulos, Associate Fellow und technischer Leiter für SASE im Tier-2-Design-Authority-Team bei Verizon Business, „verfolgen die Netzwerk- und Sicherheitsteams bei der Anbieterauswahl möglicherweise verschiedene Ansätze und das kann dazu führen, dass die SD-WAN- und SSE-Komponenten der Architektur zu Silos werden.“

Wenn diese Komponenten nicht von Anfang an miteinander verknüpft werden, kann die resultierende SASE-Lösung den in sie gesetzten Erwartungen möglicherweise nicht gerecht werden. „Je nachdem, welche Anbieter gewählt werden, könnte es sein, dass die Vorgänge für die Bereitstellung von SSE-Tunneln auf SD-WAN-Endpunkten nicht automatisiert werden können, was die Konfigurationskosten steigert“, sagt Papadopoulos. „Oder vielleicht funktioniert das automatische Failover zwischen den Tunneln nicht, weil der Zustand der Tunnel nicht automatisch überwacht werden kann oder weil es keine APIs für die Kommunikation zwischen SD-WAN- und SSE-Komponenten gibt, sodass jedes Failover manuell eingeleitet werden muss.“

Mitunter steckt der Teufel im Detail. Wenn wir zum Beispiel eine bestimmte Art von Anwendung einer Sicherheitsprüfung unterziehen wollen, kann es sein, dass das Konfigurieren der entsprechenden SD-WAN-Richtlinie sehr kompliziert ist.“

Um solche Probleme und Herausforderungen zu vermeiden, sollten Netzwerk- und Sicherheitsteams von der ersten Phase des Projekts an eng zusammenarbeiten. Dadurch können sie:



**Anbieter auswählen**, deren Lösungen miteinander kompatibel sind



**Sicherstellen**, dass Architektur und Design die vereinbarten Anforderungen erfüllen



**Einsparpotenziale nutzen**, die durch die Integration und Konsolidierung entstehen



**Sicherstellen**, dass die gewählte Technologie die vorgesehenen Anwendungsfälle unterstützt



## Legen Sie den Projektumfang gemeinsam fest

Machen Sie sich zunächst ein Bild Ihrer Geschäftsanforderungen, Ihres Budgets und Ihrer aktuellen Infrastruktur.

Behalten Sie all das klar im Auge, um sicherzugehen, dass Sie Ihr Budget nicht überschreiten und dass das ausgewählte Produkt Ihre Anforderungen erfüllt. Jeff Paterson meint dazu: „Wollen Sie sich auf die geschäftskritischen Anwendungen konzentrieren oder alle Anwendungen im Unternehmen abdecken – vielleicht Hunderte oder sogar Tausende von Anwendungen – und den damit einhergehenden zusätzlichen Zeit- und Kostenaufwand in Kauf nehmen?“ Wenn Sie zu Anfang den richtigen Plan erstellen, wird die Implementierung einfacher und erfolgreicher verlaufen.

“

Wollen Sie sich auf die geschäftskritischen Anwendungen konzentrieren oder alle Anwendungen im Unternehmen abdecken?

**Jeff Paterson**

Lösungsarchitekt, Verizon Business





## Erwägen Sie einen schrittweisen Ansatz

Es gibt keine Universalmethode für die Implementierung einer SASE-Lösung; stattdessen sollten Sie Ihre Roadmap auf Ihre geschäftlichen Anforderungen abstimmen. Doch die gesamte Netzwerk- und Sicherheitsinfrastruktur auf einmal zu migrieren ist für viele große Unternehmen zu aufwendig und mit einem zu großen Risiko für die Geschäftskontinuität verbunden. „Für Kunden mit vielen Standorten und älteren Anwendungen empfehlen wir einen schrittweisen Ansatz“, sagt Mike Hannan, Sicherheitslösungsarchitekt bei Verizon. „Wir konzentrieren uns dabei auf geschäftskritische Anwendungen, beginnen mit Machbarkeitsstudien und kleineren Pilotprojekten, gehen dann zu größeren Pilotprojekten und erst danach zur Ausweitung auf die gesamte Produktionsumgebung über.“

“

Für Kunden mit vielen Standorten und älteren Anwendungen empfehlen wir einen schrittweisen Ansatz.

**Mike Hannan**

Sicherheitslösungsarchitekt, Verizon Business

## Legen Sie realistische Zeitrahmen fest

Ebenso individuell wie die Vorgehensweise bei der Implementierung ist der Zeitrahmen. Hannan merkt an: „Wenn Sie Netzwerk und Sicherheit zusammen migrieren wollen, ist das eine sehr große Veränderung, für die Sie wahrscheinlich nicht nur die Unterstützung eines erfahrenen professionellen Partners, sondern auch viele interne Ressourcen benötigen.“ Daher ist es wichtig, bei der Festlegung des Projektumfangs, der Ziele und der Termine realistisch zu sein. Hannan fährt fort: „Ein schrittweiser Ansatz kann die Erfolgchancen verbessern. Zum Beispiel können Sie zunächst den Fernzugriff in Angriff nehmen, dann die On-Premises-Kommunikation, um sich einen besseren Überblick zu verschaffen und Zero Trust einfacher durchsetzen zu können.“

“

Wenn Sie Netzwerk und Sicherheit zusammen migrieren wollen, ist das eine sehr große Veränderung.

**Mike Hannan**

Sicherheitslösungsarchitekt, Verizon Business





## Finden Sie den richtigen Partner

Die Integration von SASE ist oft ein sehr komplexer Prozess. Daher lohnt es sich vielleicht, mit einem erfahrenen Partner zusammenzuarbeiten. „Suchen Sie nach einem Anbieter, der Erfahrung bei der Entwicklung, Implementierung und beim Betrieb komplexer, sicherer Netzwerke in Ihren Regionen hat – und Erfolge vorweisen kann“, betont Jeff Paterson.

Bei einer solch umfassenden IT-Transformation sollten Sie auch darauf achten, dass etwaige Partner erfolgreich abgeschlossene Transformationen der Netzwerk- und Sicherheitsinfrastrukturen anderer großer Unternehmen vorweisen und Sie in allen Phasen sachkundig beraten können, von der Ermittlung Ihrer Anforderungen an eine SASE-Umgebung über die Migration bis hin zum Support nach dem Umstieg. Paterson sagt: „Sie sollten unbedingt einen Partner wählen, der bei der Bereitstellung sicherer Netzwerke bereits Erfolge vorzuweisen hat, damit Sie sich darauf verlassen können, dass die Implementierung und Integration mit vorhandenen Systemen nahtlos verlaufen, und dass Sie auch in Zukunft bei der Verwaltung der Umgebung von fachkundigen Teams unterstützt werden.“

“

Sie sollten unbedingt einen Partner wählen, der bei der Bereitstellung sicherer Netzwerke bereits Erfolge vorzuweisen hat.

**Jeff Paterson**

Sicherheitslösungsarchitekt, Verizon Business

# Wenden Sie sich **an uns.**

Wir können Sie in jeder Phase des Umstiegs auf SASE unterstützen, denn wir haben über 20 Jahre Erfahrung im Netzwerkdesign, bei der verwalteten Integration vorhandener in neue IT-Infrastrukturen und bei der Transformation, Verwaltung und Sicherung von Unternehmensnetzwerken. Unsere Expertenteams können zahlreiche anbieter- und branchenspezifische Zertifizierungen vorweisen und Sie bei der Wahl der besten und vor allem richtigen Technologie für Ihre Geschäftsanforderungen fachkundig beraten. Außerdem investieren wir fortlaufend in unsere NOC- und SOC-Funktionen, um unseren Kunden digitale, automatisierte Co-Managed- oder vollständig verwaltete sichere Netzwerklösungen zu bieten.

Hier erfahren Sie, wie Verizon Sie bei der Planung und Verwaltung einer erfolgreichen SASE-Integration unterstützen kann: [verizon.com/business/de-de](https://www.verizon.com/business/de-de). Melden Sie sich [hier](#) an, um E-Mails zu unseren Sicherheits- und SASE-Lösungen zu erhalten.

## Ressourcen

### SASE-Management

Straffen Sie die Sicherheit unternehmensweit. SASE-Management vereint Netzwerk- und Cloud-Sicherheit und unterstützt Sie so beim Vernetzen von Menschen, Daten und Geräten am Edge, im Büro und in der Cloud.

[Mehr dazu >](#)

### Partner

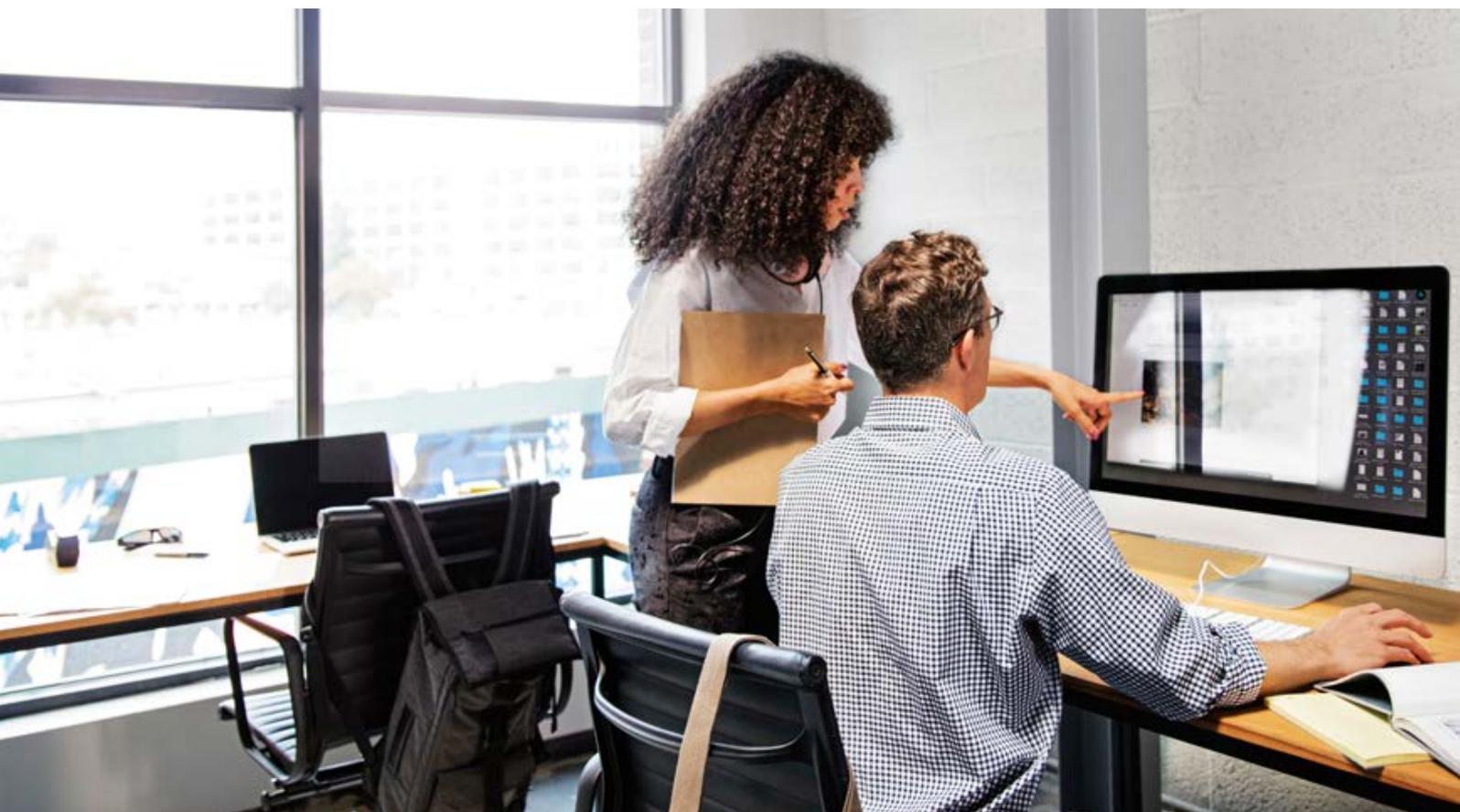
Aufgrund unserer Zusammenarbeit mit branchenführenden Anbietern in diversen Produktkategorien sind wir perfekt positioniert, unseren Kunden nahtlose, hervorragende Lösungen bereitzustellen, die die Leistung steigern und sich rasch amortisieren.

[Mehr dazu >](#)

### Digital Enablement Platform

Integrieren Sie Ihre APIs in die Digital Enablement Platform von Verizon, um die Verwaltung Ihres API-Katalogs sowie das Vorfalls- und Änderungsmanagement zu straffen.

[Video ansehen >](#)



**verizon**  
**business**