The bridge to possible

Global Networking Trends Report 2022

Sonderausgabe: „SASE als Zukunftstreiber“ und „Steigende Nutzung von Network-as-a-Service (NaaS)“

Sonderausgabe: SASE als Zukunftstreiber

Inhalt

SASE – Einführung 04

Herausforderung für die IT 05

Die Beziehung zwischen SD-WAN und SASE 07

Gewünschte Funktionen von SASE 09

Warum Integration so wichtig ist 12

Trends bei der SASE-Annahme 15

SASE-Nutzungsmodelle 17

SASE – Fazit 18

Einführung einer Strategie für Secure Access Service Edge (SASE)

Hybride Arbeit erfordert eine kohärente SASE-Strategie für ein konsistentes, außergewöhnliches Benutzererlebnis unabhängig vom Standort.

Als Reaktion auf das wachsende Interesse und die zunehmenden Unklarheiten am Markt beim Thema Secure Access Service Edge (SASE) haben wir diesen speziellen Nachtrag zum Global Networking Trends Report 2022 zur steigenden Nutzung von Network-as-a-Service (NaaS) erstellt.

SASE (Aussprache wie Englisch „sassy“) wird von der starken Zunahme von Remote-Arbeit und Hybrid-Cloud-Annahmen vorangetrieben und bietet sichere, nahtlose Anbindung an alle Anwendungen unabhängig vom Netzwerk, Standort und Gerät.

SASE integriert Netzwerk- und Sicherheitsfunktionen in eine vereinheitlichte, Cloud-native Lösung oder einen entsprechenden Service.

Im Vergleich zu herkömmlichen Sicherheitslösungen rücken bei SASE Sicherheitsrichtlinien und deren Durchsetzung näher an die zunehmend verteilten BenutzerInnen und Anwendungen. SASE erweitert Zero Trust und macht den konstanten Backhaul von Daten zu einem Rechenzentrum überflüssig. So reduziert es die Netzwerklast und typische Engpässe effektiv und bietet so ein besseres Benutzererlebnis.

Als Alternative zu einem traditionellen Sicherheits-Stack bietet SASE sicheren Zugriff von Edge zu Edge – für Rechenzentren, Außenstellen, Roaming-BenutzerInnen und darüber hinaus.

In diesem Nachtrag werden aktuelle Trends und Einblicke rund um SASE vorgestellt. Die Daten stammen aus verschiedenen Umfragen am Markt sowie von bekannten BranchenanalystInnen und -expertInnen. Wir hoffen, dass Sie sich auf der Grundlage dieser Informationen ein besseres Bild von den Vorteilen und Implikationen von SASE machen können, wenn Sie Ihre Strategien für Netzwerk, Sicherheit und Cloud zusammenstellen.

– Omri Guelfand, VP, Network Services bei Cisco

> „Am Markt herrscht immer noch Unklarheit darüber, was SASE ausmacht. Es zeichnet sich jedoch ab, dass SASE in Übereinstimmung mit unserer Meinung keine völlig neue Technologie ist, sondern eine Integration bestehender Netzwerklösungen (z. B. Software-Defined WAN (SD-WAN)) mit Sicherheitstechnologien (z. B. Secure Web Gateway (SWG)), aus der sich eine Cloud-basierte Lösung für sichere Netzwerkverbindungen ergibt.“
>
> – Dell'Oro Group[1]

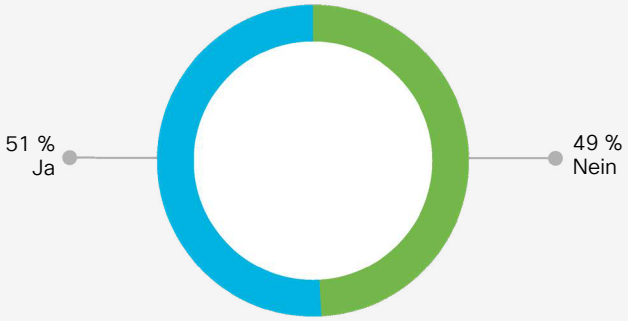
Herausforderung für die IT: Bereitstellung einer sicheren Cloud-First-Umgebung für hybride Arbeit

Die zwei wichtigsten aktuellen IT-Trends sind zum einen der Übergang zu einer Multicloud-Anwendungsstrategie und zum anderen die Annahme von hybriden Arbeitsmodellen. Da die BenutzerInnen und Anwendungen heute stärker verteilt sind als je zuvor, sind die Themen Konnektivität und Sicherheit erheblich komplexer geworden.

Zur Verteilung der Anwendungen über mehrere Private und Public Clouds kommen die aufgrund hybrider Arbeit geografisch weit verteilten MitarbeiterInnen und Arbeitsumgebungen. Angesichts dieser Situation ist es eine Herausforderung, einerseits ein hohes, inklusives Benutzererlebnis zu bieten und andererseits nicht die Kontrolle zu verlieren, die bei lokalen Unternehmensumgebungen üblich war.

In aktuellen Umfragen geben 76 % der IT-Teams an, Remote-MitarbeiterInnen seien schwerer zu schützen[2], und 51 % der Unternehmen berichten von Schwierigkeiten mit der Anbindung der MitarbeiterInnen an Unternehmensressourcen in den letzten 18 Monaten.[3]

Hatten Sie/Ihr Unternehmen in den letzten 18 Monaten Schwierigkeiten mit der Anbindung Ihrer MitarbeiterInnen an das Unternehmensnetzwerk?



Vor dem Hintergrund des Übergangs von einem rechenzentrumsorientierten Anwendungsmodell zu einem internetbasierten, Cloud-zentrierten Modell müssen IT-Teams ihre Netzwerkstrategie umfassend überdenken. Auch die Sicherheitsteams haben Schwierigkeiten, ein sicheres, nahtloses Benutzererlebnis zu bieten, wenn sich BenutzerInnen und Anwendungen nicht am Unternehmensstandort befinden und somit das Risiko versehentlicher Offenlegungen oder gezielter Angriffe höher ist.

Dies erklärt das große Interesse an einem Cloud-basierten SASE-Modell, das Netzwerklösungen wie SD-WAN mit Cloud-Security-Lösungen wie Security Service Edge (SSE) und Zero Trust Network Access (ZTNA) vereint.

SASE soll BenutzerInnen und Anwendungen unabhängig vom Standort und Hosting anbinden und schützen, sodass letztlich ein besseres, konsistenteres und sichereres Benutzererlebnis gegeben ist. Darüber hinaus verspricht SASE geringere IT-Kosten und weniger Komplexität sowie mehr Flexibilität und Leistung für das Netzwerk und damit auch für das Anwendungserlebnis.

> „Auf dem Höhepunkt der Pandemie im Jahr 2020 arbeiteten in den USA 450 % mehr MitarbeiterInnen ausschließlich oder teilweise im Homeoffice als vor der Pandemie. Die Zahlen sind zwar inzwischen wieder zurückgegangen, doch wir gehen davon aus, dass Remote-Arbeit langfristig um 200 % häufiger stattfinden wird als vor der Pandemie."
>
> – Dell'Oro Group[4]

Fazit:

An der räumlichen Verteilung und Diversität der MitarbeiterInnen wird sich in absehbarer Zeit nichts ändern. Bei richtiger Implementierung verbindet und schützt SASE BenutzerInnen und Anwendungen, stimmt Netzwerk- und Sicherheitsrichtlinien aufeinander ab und verringert den Aufwand und das Risiko beim Netzwerk- und Sicherheitsmanagement.

Die Beziehung zwischen SD-WAN und SASE

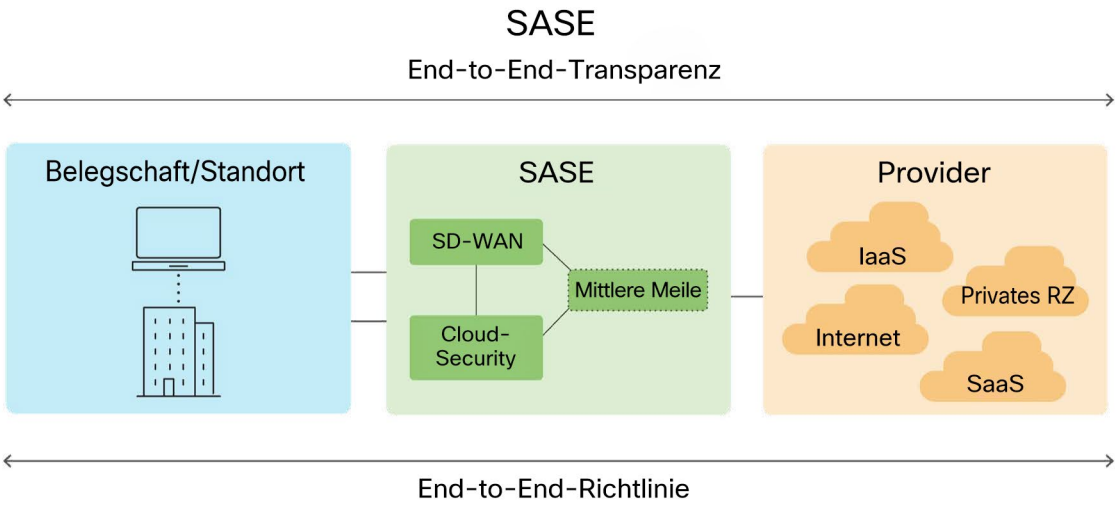
Angesichts der am Markt herrschenden Unklarheit über SASE stellen sich verschiedene Fragen in Bezug auf die vorhandenen SD-WAN-Lösungen: Ist SASE ein Ersatz für SD-WAN? Ergänzen sie sich gegenseitig? Oder handelt es sich um ganz verschiedene Lösungen für unterschiedliche Anforderungen?

Die Antwort ist einfach: SD-WAN ist eine Grundvoraussetzung für SASE

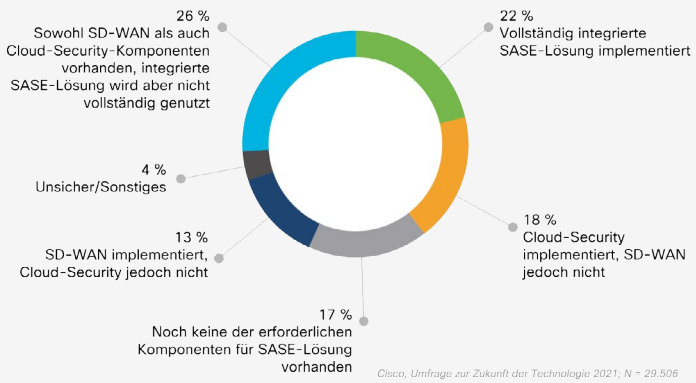
SASE vereint die nativen Sicherheitsfunktionen von SD-WAN mit Cloud-zentrierter Sicherheit, um BenutzerInnen und Anwendungen unabhängig vom Standort und Hosting anzubinden und zu schützen. Als Overlay-Architektur kann SASE selbst keine umfassende Sicherheit bieten. Dafür sind die Sicherheitsmaßnahmen von SD-WAN erforderlich, zu denen folgende zählen:

- Unterstützung von Network Address Translation (NAT)
- Segmentierung des Netzwerks in mehrere Subnetzwerke
- Monitoring und Blockierung von Malware und schädlichem Datenverkehr
- Einschränkung des Zugriffs nicht autorisierter BenutzerInnen
- Abwehr unerwünschter Inhalte und Anwendungen
- Firewall für unerwünschten eingehenden und VLAN-zu-VLAN-Datenverkehr
- Sicheres Site-to-Site-/Tunnel-VPN
- Geofencing für standortbasierte Zugriffskontrolle

> „Durch SASE wird SD-WAN keineswegs überflüssig. SD-WAN ist vielmehr eine Grundvoraussetzung für SASE. SASE-Angebote führen verschiedene Netzwerk- und Security-as-a-Service-Funktionen zusammen, beispielsweise SD-WAN, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Next-Generation Firewall (NGFW) und Zero Trust Network Access (ZTNA).“
> – Gartner®, „Quick Answer: Does SASE Replace SD-WAN?“, 2021[5]



In welcher Phase der SASE-Annahme befinden Sie sich?



Sollten IT-Abteilungen erst SD-WAN oder erst Cloud-Security implementieren? Viele IT-Teams entscheiden sich dazu, SASE in mehreren Phasen einzuführen. Die meisten befinden sich noch auf dem Weg zu SASE und verwenden derzeit SD-WAN- und Cloud-Security-Komponenten, die noch nicht vollständig integriert sind oder nicht komplett genutzt werden.

18 % der Unternehmen haben Cloud-Security bereits eingeführt, SD-WAN jedoch noch nicht. Bei 13 % der Unternehmen ist SD-WAN vorhanden, Cloud-Security aber noch nicht.[6]

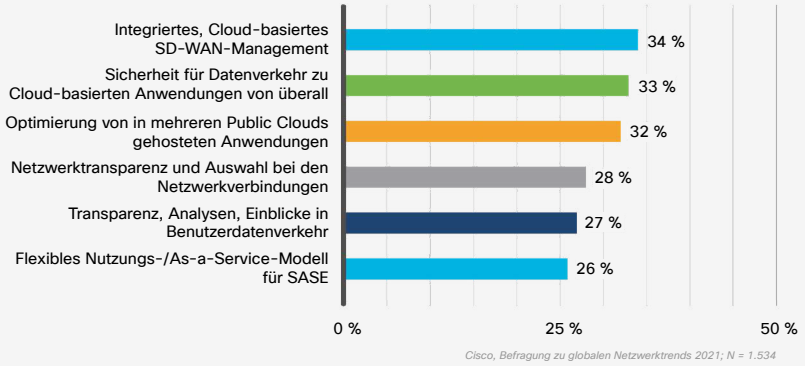
Fazit:

SD-WAN ist eine Grundvoraussetzung für SASE, die in Kombination mit Cloud-zentrierten Sicherheitslösungen oder -services BenutzerInnen und Daten am Unternehmensstandort, in der Cloud und am Edge schützt.

Gewünschte Funktionen von SASE

Da SASE für die Integration von Netzwerk- und Sicherheitsfunktionen steht, legen 34 % der Unternehmen Wert auf Lösungen und Services für integriertes, Cloud-basiertes SD-WAN-Management. Ebenfalls als wichtige Prioritäten angegeben wurden Sicherheit für Datenverkehr zu Cloud-basierten Anwendungen (33 %), die Optimierung von in mehreren Public Clouds gehosteten Anwendungen (32 %) und die Verbesserung der Netzwerktransparenz und -flexibilität (28 %).

Welche Funktionen von SASE sind Ihrer Meinung nach für Ihr Unternehmen am wichtigsten?



Für die Anbindung von Remote-MitarbeiterInnen:

43 % der Unternehmen planen, VPN-as-a-Service zu nutzen.

36 % möchten Zero Trust Network Access (ZTNA) und Multi-Faktor-Authentifizierung annehmen.

35 % sind an Host-basierten, vereinheitlichten Clients interessiert.

35 % haben vor, SD-WAN auf mobile BenutzerInnen und BenutzerInnen im Homeoffice auszudehnen.

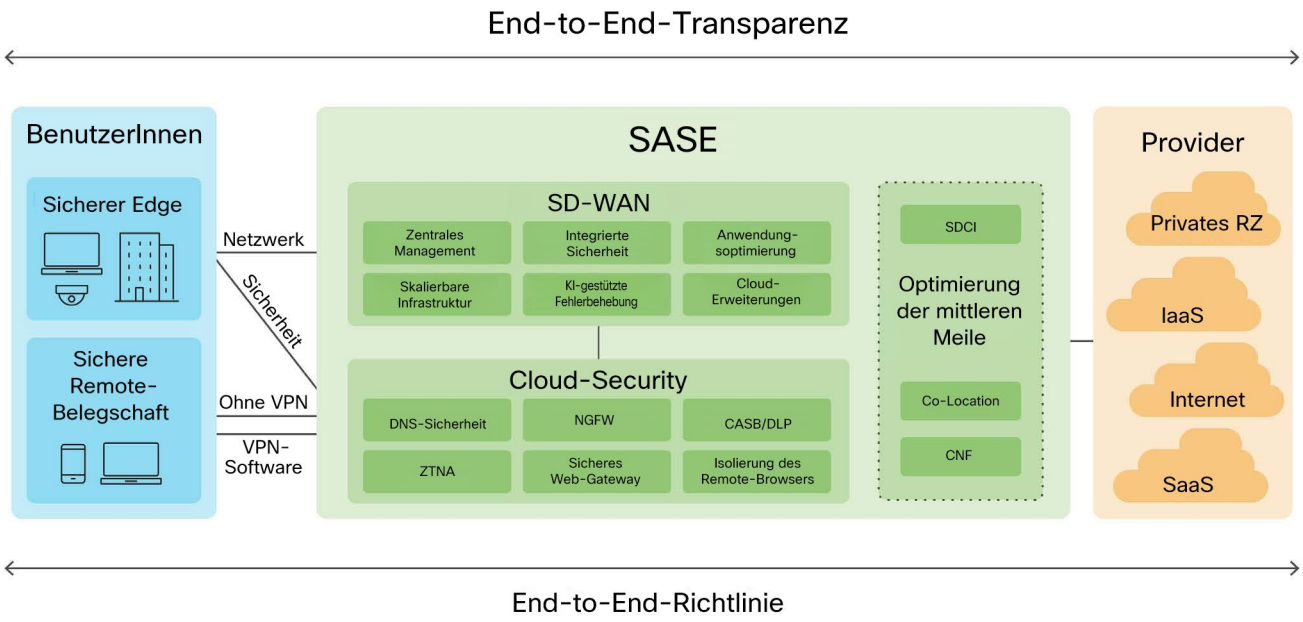
SASE-Architekturen, -Lösungen und -Services werden ständig weiterentwickelt. Grundsätzlich sind sie jedoch alle darauf ausgelegt, einige oder alle Kernfunktionen von SD-WAN und Cloud-Security zu vereinen:

SD-WAN	Cloud-Security
Zentrales Management Ein zentrales, hochgradig visuelles Dashboard vereinfacht die Gerätekonfiguration sowie Management, Monitoring und Automatisierung im Netzwerk. Dies umfasst auch Zero-Touch-Bereitstellung am Netzwerk-Edge.	**Zero Trust Network Access (ZTNA)** Ein Sicherheits-Framework, das nicht autorisierte Zugriffe verhindert, Sicherheitsverletzungen eindämmt und das Risiko der lateralen Bewegung von Angreifern im Netzwerk mindert. ZTNA sollte mit starkem Identitäts- und Zugriffsmanagement kombiniert werden, sodass die Benutzeridentität und die Vertrauenswürdigkeit von Geräten überprüft werden, bevor autorisierten Anwendungen Zugriff gewährt wird.
Erweiterung des Cloud-Netzwerks und Optimierung der mittleren Meile Durch umfassende Cloud-Integrationen sind nahtlose, automatisierte Verbindungen bei jeder beliebigen Site-to-Cloud- und Site-to-Site-Konfiguration möglich. Dabei wird die Anbindung auf der mittleren Meile durch Software-Defined Cloud Interconnect (SDCI) und Co-Location-Integration optimiert.	**Secure Web Gateway (SWG)** Ein Gateway, das den Web-Datenverkehr protokolliert und überprüft und so vollständige Transparenz, URL-Filterung, Anwendungskontrolle und Schutz vor Malware bietet.
Anwendungserlebnis Möglichkeit des Monitorings und der Validierung der Funktionsfähigkeit und Leistung von Web-Anwendungen. Die detaillierten Metriken und Modelle zeigen das sequenzielle Abrufen und Laden von Web-Komponenten, um Fehler und Engpässe sowie deren Auswirkungen auf die Anwendungsleistung zu ermitteln.	**Cloud-basierte Firewall mit Intrusion Prevention System (IPS)** Softwarebasierte, über die Cloud bereitgestellte Services, die das Management und die Überprüfung des Netzwerkverkehrs erleichtern.
Flexible und skalierbare Infrastruktur Eine Auswahl an physischen und virtuellen Plattformen, die Hochverfügbarkeit und einen hohen Durchsatz, Multigigabit-Port-Optionen, 5G-Mobilfunklinks und leistungsstarke Verschlüsselungsfunktionen bieten. Zur Optimierung des WAN-Datenverkehrs werden dynamisch jeweils die effizientesten WAN-Links ausgewählt, die den Servicelevel-Anforderungen genügen.	**Cloud Access Security Broker (CASB**) Software, welche die in einem Netzwerk genutzten Cloud-Anwendungen erkennt und dazu Meldungen erstellt, Schatten-IT aufdeckt und die Möglichkeit bietet, riskante SaaS-Anwendungen und bestimmte Aktionen wie Posts und Uploads zu blockieren.
KI-gestützte Fehlerbehebung Robuste KI/ML zur Optimierung der Netzwerkperformance, Automatisierung von Routineaufgaben und Beschleunigung der Fehlerbehebung. Damit einher gehen intelligente Warnungen, Self-Healing-Funktionen und vorausschauendes Internet-Rerouting.	**Schutz vor Datenverlusten (Data Loss Prevention, DLP)** Software, die durch Inline-Datenanalysen Transparenz und Kontrolle für vertrauliche Daten bietet, die außerhalb der unternehmenseigenen Netzwerk- oder Cloud-Umgebung übertragen werden.
Integrierte Sicherheit Robuste Sicherheitsfunktionen, die mit Cloud-Security ineinandergreifen, um Zweigstellen, BenutzerInnen im Homeoffice und Cloud-basierte Anwendungen vor Angriffen zu schützen.	**Isolierung des Remote-Browsers (Remote Browser Isolation, RBI)** Software, die Web-Datenverkehr von den Benutzergeräten isoliert, um das Risiko von über den Browser verbreiteten Bedrohungen zu mindern.
Identitätsbasiertes Richtlinienmanagement Mikrosegmentierung und identitätsbasiertes Richtlinienmanagement für mehrere Standorte und Domänen.	**Sicherheit auf DNS-Ebene** Software, die als erste Verteidigungslinie gegen Bedrohungen im Internet fungiert und schädliche DNS-Anfragen blockiert, bevor eine Verbindung zu einer IP-Adresse überhaupt zustande kommt. Starke DNS-Sicherheit kann die Anzahl der Bedrohungen, die Sicherheitsteams täglich vorselektieren müssen, erheblich reduzieren.
Erweiterte Einblicke Optimierte Transparenz für Anwendungs-, Internet-, Cloud- und SaaS-Umgebungen mit umfassender Hop-by-Hop-Analyse. Ermöglicht die Isolierung von Fehlerquellen und liefert aussagekräftige Einblicke, um die Fehlerbehebung zu beschleunigen und Auswirkungen auf BenutzerInnen zu minimieren oder ganz zu verhindern.	**Threat-Intelligence** ExpertInnen für Bedrohungsforschung, Entwicklung und Daten, die mithilfe von Telemetrie und komplexen Systemen genaue, schnelle und aussagekräftige Threat-Intelligence erstellen. Mit Regelsätzen, die auf die Tools in Ihrem Sicherheits-Stack abgestimmt sind, können neue Bedrohungen und Schwachstellen ermittelt und vorhandene Bedrohungen schon vor einem tatsächlichen Angriff abgewehrt werden.

SASE-Modelle integrieren nicht nur SD-WAN- und Cloud-Security-Funktionen, sondern tragen auch zum Abbau von betrieblichen Silos bei und fördern die Abstimmung zwischen Netzwerk- und Sicherheitsteams. Mit standardisierten Richtlinien, gemeinsam genutzter Telemetrie und koordinierten Warnungen über alle Sicherheits- und Netzwerkkomponenten hinweg versetzt SASE NetOps- und SecOps-Teams in die Lage, die Effizienz, Transparenz und Sicherheit der IT zu stärken.

Vor diesem Hintergrund benötigen Unternehmen eine umfassende SASE-Strategie, die sowohl NetOps- als auch SecOps-Ziele berücksichtigt, die betriebliche Abstimmung erhöht und die Anforderungen des Unternehmens auch in der absehbaren Zukunft erfüllen kann.

SASE: Detail



„Bis 2024 werden 30 % der Unternehmen in den Bereichen Cloud-basiertes Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA) und Firewall-as-a-Service-Funktionen (FWaaS) für Zweigstellen auf Lösungen aus einer Hand setzen. 2020 lag der Anteil noch bei weniger als 5 %."

– Gartner[7]

Fazit:

Unternehmen, die SASE-Strategien und -Angebote evaluieren, suchen nach Lösungen und Services, die mit den grundlegenden Funktionen von SD-WAN *und* Cloud-Security ihre aktuellen und künftigen Anforderungen erfüllen können.

Warum Integration so wichtig ist

Moderne Unternehmen nutzen eine ganze Reihe von Netzwerkumgebungen (Rechenzentrumsnetzwerke, LANs, WANs) und Sicherheitslösungen (Firewalls, Gateways und Zugriffskontrolle für lokale und Cloud-basierte Systeme). Durch Technologie- und Serviceintegrationen kann SASE Transparenz, Richtlinienorchestrierung und Sicherheit für alle diese Umgebungen bieten.

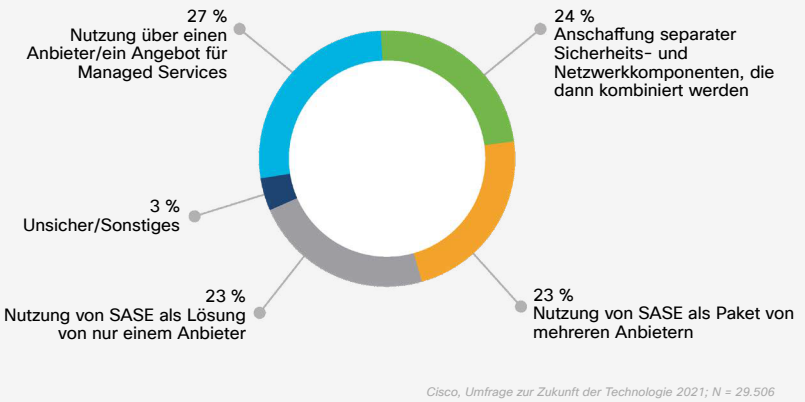
Das letztliche Ziel besteht darin, BenutzerInnen und Anwendungen unabhängig vom Standort oder Hosting sicher anzubinden. Zu diesem Zweck leisten die Integrationen auch Folgendes:

- Verringerung der Anzahl an Sicherheitsvorfällen
- Beschleunigung der Fehlerbehebung und Problemlösung
- Vereinfachung von System-Monitoring und -management
- Verbesserung der Richtlinienstandardisierung und -durchsetzung
- Unterstützung von regionalen Compliance- und Datenanforderungen
- Reduzierung der Investitions- und Betriebskosten

„Es gibt zwei wesentliche SASE-Implementierungsvarianten am Markt: vereinheitlicht und disaggregiert. Bei der vereinheitlichten Implementierung handelt es sich um eng integrierte SASE-Plattformen von nur einem Anbieter. Die disaggregierte Implementierung besteht aus Lösungen von mehreren Anbietern oder aus mehreren Produkten mit einem geringeren Maß an Integration als bei der vereinheitlichten Variante.“

– Dell’Oro Group[9]

Wie werden Sie Ihre SASE-Lösung bereitstellen und nutzen?



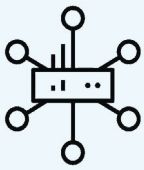
Cisco, Umfrage zur Zukunft der Technologie 2021; N = 29.506

Da Unternehmen Lösungen und Services sowohl von einem einzelnen als auch von mehreren Anbietern zusammen nutzen oder aber eigene Architekturen aus Einzellösungen aufbauen können, stehen ihnen viele Möglichkeiten zum Bereitstellen und Nutzen von SASE zur Verfügung.

Beim Erstellen und Integrieren einer individuellen Lösung und auch bei der Nutzung eines SASE-Pakets von mehreren Anbietern können Komplexität, betriebliche Herausforderungen und Sicherheitsschwachstellen unerwünschterweise zunehmen. Aus diesem Grund sucht rund die Hälfte aller Unternehmen nach einer vereinheitlichten und/oder gemanagten Lösung von nur einem Anbieter.

- 70 % stimmen zu oder stimmen vollkommen zu, dass das effektive Management eines Netzwerk- und Sicherheits-Stacks von mehreren Anbietern sehr komplex geworden ist.
- 26 % haben zwar bereits Cloud-Security- und SD-WAN-Funktionen, diese werden jedoch nicht komplett genutzt und sind noch nicht in ein vollständiges SASE-Modell integriert.[10]

Unabhängig davon, ob es sich um eine individuell zusammengestellte Architektur, ein Paket von mehreren Anbietern, einen vollständig gemanagten Service von nur einem Anbieter oder eine andere Variante handelt, sollte jede SASE-Lösung eine bessere Abstimmung und Integration zwischen folgenden Aspekten bieten:



SD-WAN und Cloud-Security

- Automatisierung des Routings von Datenverkehr zwischen dem SD-WAN-Gerät und den Cloud-Security-PoPs (Points of Presence).
- Aus Gründen der Widerstandsfähigkeit wird Datenverkehr automatisch zu einem alternativen PoP umgeleitet, wenn Leistungsprobleme auftreten.
- KI-gestützte vorausschauende Analysen ermöglichen das automatische Rerouting von Datenverkehr zu alternativen PoPs, bevor das Benutzererlebnis beeinträchtigt wird.

NetOps- und SecOps-Teams

- Sicherheitsrichtlinien (z. B. Zugriffsautorisierung und Segmentierung) können dauerhaft für SD-WAN- und Cloud-Security-Implementierungen gleichermaßen genutzt werden.
- Aus dem Datenaustausch zwischen den SD-WAN- und Cloud-Security-Managementplattformen ergibt sich konsistente Transparenz für Richtlinien und Ereignisse.
- Unternehmensnetzwerkkonstrukte (wie VPNs und Security Group Tags) und Richtlinien werden auf Cloud-Security-Plattformen erweitert und übertragen.
- Für die SD-WAN- und Cloud-Security-Managementplattformen kann einmalige Anmeldung (Single Sign-On) zur administrativen Authentifizierung genutzt werden.

BenutzerInnen und Anwendungen

- Ermöglicht direkte Verbindungen zwischen SD-WAN, der mittleren Meile (z. B. SDCI), Multicloud und SaaS-Services.
- Mit vollständiger Transparenz und umfassenden Analysen erhalten Unternehmen eine Möglichkeit für das Monitoring und die Optimierung des Benutzererlebnisses für SD-WAN, Cloud-Security, PoPs und IaaS/SaaS-Verbindungen.

„Für ein effektives Netzwerkmanagement ist integrierte Sicherheit unverzichtbar. Sicherheit sollte ganzheitlich betrachtet werden – vom Endpunkt über das Netzwerk bis hin zur Anwendung. Im Fall von Network-as-a-Service muss die Zuständigkeit für das Netzwerk und die Sicherheit beim Anbieter liegen. Wenn er sich nur um das Netzwerk kümmert, benötige ich Transparenz und Kontrolle, um vollständigen Schutz und schnelle Bedrohungsbekämpfung zu gewährleisten. Im Idealfall übernimmt der Anbieter sowohl das Netzwerk als auch die Sicherheit.“

– Führungskraft im Bereich IT-Infrastruktur bei einem weltweit tätigen Anbieter für Verbraucherprodukte

Fazit:

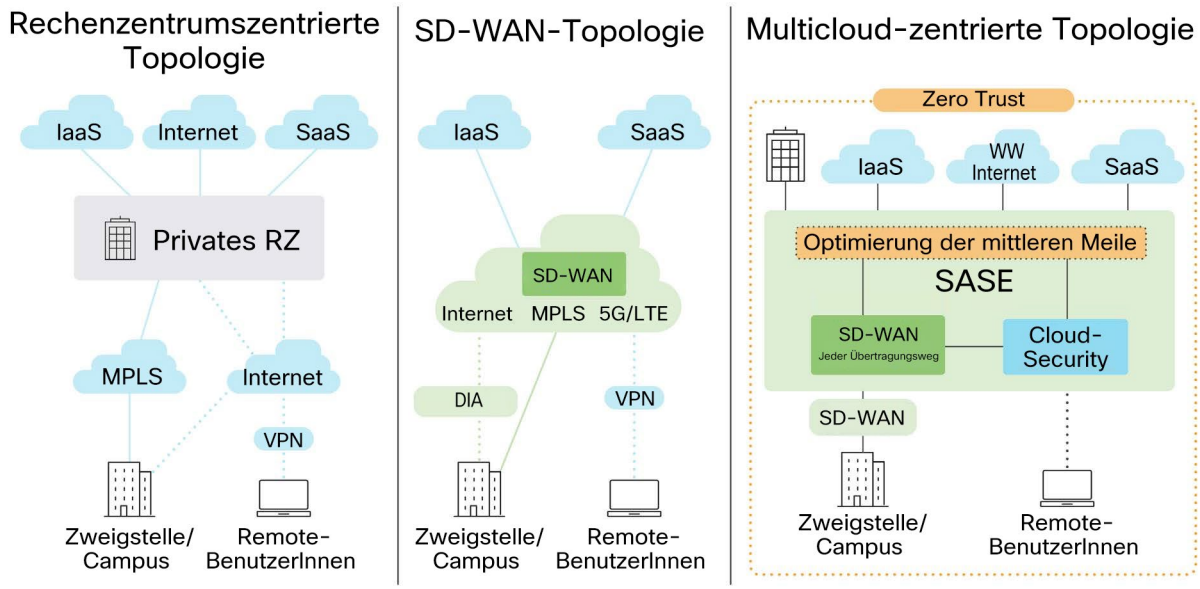
Unabhängig davon, ob eine individuelle SASE-Variante oder Lösungen/Services von einem oder mehreren Anbietern genutzt werden, sollten diese eine enge Integration zwischen SD-WAN- und Cloud-Security-Systemen bieten, um das sichere Benutzererlebnis zu optimieren sowie die Zusammenarbeit zwischen NetOps und SecOps zu rationalisieren.

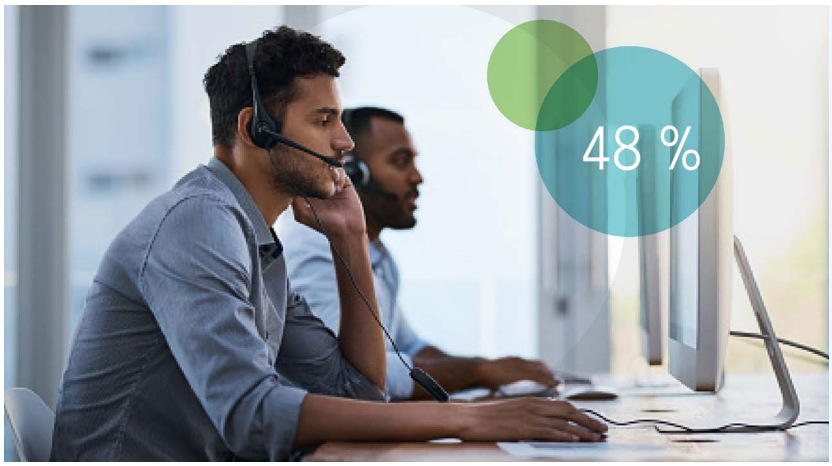
Trends bei der SASE-Annahme

Wie bei jeder Technologieentscheidung kommt es bei der Auswahl des SASE-Modells und des Bereitstellungsansatzes auf die individuelle Situation des Unternehmens an. Die bereits vorhandenen Netzwerk- und Sicherheitslösungen sowie die übergeordneten betrieblichen Strategien und geschäftlichen Prioritäten sollten bei jeder SASE-Entscheidung sorgfältig berücksichtigt werden. Ebenfalls einzubeziehen sind wichtige Initiativen, behördliche Auflagen, Fusionen und Übernahmen, die Lieferkette und Anforderungen an die geschäftliche Flexibilität.

Unternehmen, die von einem rechenzentrumsorientierten Anwendungsmodell zu einem Cloud- oder Multicloud-zentrierten Modell migrieren, können den Weg zu SASE mit SD-WAN beginnen und dann die mittlere Meile optimieren und Cloud-Security integrieren.

Von einer rechenzentrumszentrierten zu einer Multicloud-zentrierten Topologie

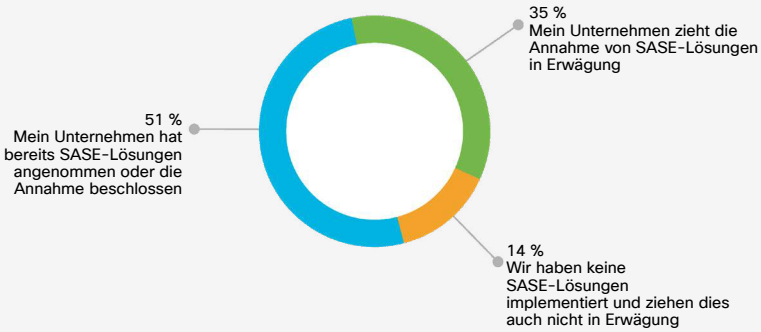




48 % der an SASE interessierten Unternehmen planen, zuerst bei der Sicherheit anzusetzen, 31 % beim Netzwerk und 21 % bei beidem gleichzeitig.[8]

Unabhängig vom konkreten Modell oder Bereitstellungsansatz geben viele Unternehmen an, bei der SASE-Annahme auf einem guten Weg zu sein: 86 % der Unternehmen ziehen die Annahme von SASE in Erwägung oder haben SASE schon angenommen.[11]

Hat Ihr Unternehmen SASE-Lösungen angenommen, deren Annahme beschlossen oder sie zumindest in Erwägung gezogen?



Cisco, Umfrage zur Zukunft der Technologie 2021; N = 34.351

„Bis 2025 werden mindestens 60 % der Unternehmen explizite Strategien und Zeitpläne für die Annahme von SASE haben, die den Benutzer-, Zweigstellen- und Edge-Zugriff umfassen – 2020 waren es erst 10 %.“

– Gartner[12]

Fazit:

Der Ansatz zur SASE-Bereitstellung wird von den Lebenszyklen der vorhandenen Infrastruktur, den betrieblichen Prioritäten und den geschäftlichen Initiativen beeinflusst. IT-Teams sollten einen strategischen Planungsansatz annehmen, der auf den inkrementellen Aufbau einer vollständigen SASE-Architektur abzielt.

SASE-Nutzungsmodelle

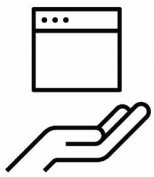
Es gibt drei wesentliche Nutzungsmodelle für SASE-Lösungen und -Services. Diese Nutzungsmodelle wirken sich unterschiedlich auf die internen Teams und Betriebsabläufe aus. Sie tragen jedoch alle zum Abbau der herkömmlichen Netzwerk- und Sicherheitssilos bei. So kann SASE die betriebliche Abstimmung und Effizienz verbessern.

As-a-Service-Modell

Wenn eine schnelle Bereitstellung mit minimalen Auswirkungen auf Betriebsabläufe und MitarbeiterInnen gewünscht ist und das mit SLAs verbundene Risiko gemindert werden soll, bietet SASE-as-a-Service zahlreiche vollständig integrierte, über die Cloud bereitgestellte Funktionen mit zentralem Dashboard und Support über den gesamten Lebenszyklus. 26 % der Unternehmen geben SASE-as-a-Service als bevorzugtes Nutzungsmodell an.

Hybrides Modell oder Modell mit gemeinsamem Management

Für Unternehmen, die noch nicht für ein vollständiges As-a-Service-Modell bereit sind oder mehr Anpassungsmöglichkeiten benötigen als bei diesen Services gegeben, eignet sich ein hybrider Ansatz. Das heißt, Cloud-basierte Sicherheitsfunktionen werden in eine vorhandene SD-WAN-Lösung integriert, oder die Zuständigkeit für Netzwerk und Sicherheit wird zwischen dem Unternehmen und einem Managed-Services-Anbieter aufgeteilt. Diese hybriden Ansätze bieten mehr Sicherheit und Support und ermöglichen den IT-Teams ein gewisses Maß an Transparenz und Kontrolle, während gleichzeitig der Aufwand für das Lebenszyklusmanagement sinkt.



Stark angepasstes oder selbst erstelltes Modell

Unternehmen, die umfassende Anpassbarkeit wünschen und die volle Kontrolle über ihre Netzwerk- und Sicherheitsumgebung behalten möchten, können SASE-Funktionen selbst erstellen, integrieren und managen. Dieses Maß an Anpassbarkeit und Kontrolle geht in der Regel zulasten von Geschwindigkeit und Flexibilität, erfordert zusätzliches Management von Hardware, Software und Lizenzen über den gesamten Lebenszyklus hinweg und ist nur mit spezialisierten Sicherheits- und Compliance-Kräften zu bewältigen. Diese Option eignet sich gut für Unternehmen mit sehr speziellen Anforderungen, die mit ihrem bestehenden Netzwerk und den vorhandenen MitarbeiterInnen die architekturbezogenen und betrieblichen Voraussetzungen für SASE erfüllen können.

Weitere Erkenntnisse finden Sie in dieser Kundenreferenz zur Bereitstellung von Cisco Secure Access Service Edge (SASE).

Fazit:

Es gibt verschiedene SASE-Nutzungsmodelle mit unterschiedlichen betrieblichen Auswirkungen. Welches Modell für welches Unternehmen am besten geeignet ist, hängt von einer Reihe von Faktoren ab, u. a. von der Größe, den Kompetenzen und der Bandbreite des internen IT-Teams und von der Priorisierung der Anforderungen an Spezialisierung, Geschwindigkeit, Flexibilität, Transparenz und Kontrolle.

SASE – Fazit

SASE-Architekturen, -Lösungen und -Services bieten sichere Verbindungen zwischen beliebigen BenutzerInnen und Anwendungen unabhängig vom Standort und Hosting. Der Weg zu SASE gestaltet sich jedoch bei jedem Unternehmen anders. Das am besten geeignete Modell und der entsprechende Ansatz richten sich nach den vorhandenen Technologien sowie den IT- und geschäftlichen Prioritäten.

Cisco und sein Partner-Ecosystem können Ihnen mit der umfassendsten, flexibelsten und widerstandsfähigsten SASE-Lösung am Markt helfen, Ihre speziellen Netzwerk- und Sicherheitsanforderungen zu erfüllen.

Sie können aus unserem umfangreichen SASE-Portfolio wählen, das erstklassige Funktionen für Netzwerk, Client-Verbindungen und Sicherheit sowie einzigartige Beobachtbarkeit für das Internet bietet. So erzielen Sie die gewünschten Ergebnisse. Ebenfalls zur Auswahl stehen verschiedene unkomplizierte, flexible SASE-Bereitstellungs- und -Nutzungsmodelle für unterschiedliche Situationen und Anforderungen.

Unsere hochverfügbare globale Cloud-Security-Infrastruktur bietet sicheren Zugriff überall dort, wo sich BenutzerInnen und Anwendungen befinden. Mit unseren marktführenden SD-WAN-Lösungen erhalten Sie die Flexibilität und die Funktionen, die Sie für ein durchgehend hochwertiges Benutzererlebnis benötigen. Zusammen bilden unsere Cloud-Security- und SD-WAN-Lösungen das branchenweit umfassendste und am stärksten integrierte SASE-Angebot.

Für die Zukunft plant Cisco weitere schnelle Innovationen rund um SASE durch kontinuierliche Integrationen und Funktionsverbesserungen. Wir entwickeln unsere Angebote ständig weiter, um Ihnen die flexibelsten und am einfachsten nutzbaren SASE-Services ganz nach Ihren Vorstellungen zu bieten.

Weitere Informationen finden Sie im Cisco SASE-Ressourcen-Center.

Cisco wurde im Gartner Magic Quadrant™ für WAN-Edge-Infrastruktur hinsichtlich Abdeckungsgrad und Handlungsfähigkeit als Leader eingestuft.[13]

Zusätzliche Ressourcen und Hilfe

Link zur SASE-Roadmap >

Cisco Partner suchen >

Cisco Vertrieb kontaktieren >

SASE – Quellen

1. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, September 2021.
2. The State of Security 2021, Splunk, Februar 2021.
3. Future of Technology, Cisco, November 2021.
4. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, September 2021.
5. Gartner Quick Answer: Does SASE Replace SD-WAN?, Andrew Lerner, Neil MacDonald, Dezember 2021.
6. Cisco Global Networking Trends Report 2022: Bericht zur stärkeren Nutzung von Network-as-a-Service (NaaS), Cisco, Oktober 2021.
7. 2021 Strategic Roadmap for SASE Convergence, Gartner, März 2021.
8. SASE Trends: Plans Coalesce but Convergence Will Be Phased, ESG Research Report, Dezember 2021.
9. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, September 2021.
10. Cisco Global Networking Trends Report 2022: Bericht zur stärkeren Nutzung von Network-as-a-Service (NaaS), Cisco, Oktober 2021.
11. Future of Technology, Cisco, November 2021.
12. 2021 Strategic Roadmap for SASE Convergence, Gartner, März 2021.
13. Gartner Magic Quadrant für WAN-Edge-Infrastruktur, September 2021.

Bericht zur stärkeren Nutzung von Network-as-a-Service (NaaS)

Inhalt

Willkommen 22

Wichtigste Ergebnisse 23

Ein anderes Netzwerkmodell 25

Herausforderungen meistern, Vorteile realisieren 27

So verändert NaaS den Netzwerkbetrieb 29

Rollen, Zuständigkeiten und Kompetenzen 31

Bedenken und Vorbehalte 33

Trends bei der Einführung 35

Auswählen eines NaaS-Anbieters 36

SASE und die verschiedenen NaaS-Varianten 38

Fazit 40

Zusätzliche Ressourcen und Hilfe 40

Über diesen Bericht 41

Nutzungsgenehmigung für diesen Bericht 42

Willkommen

Willkommen beim *Global Networking Trends Report 2022* zur steigenden Nutzung von Network-as-a-Service (NaaS).

Wir leben als Privatmenschen und auch als Netzwerkfachleute in einer bemerkenswerten Zeit. Im Verlauf des letzten Jahres mussten IT-Führungskräfte und Netzwerkfachleute dafür sorgen, dass Mitarbeiter remote arbeiten können, Daten in einer stärker verteilten Computing-Umgebung geschützt bleiben und Benutzern, Kunden und Partnern neue Services zur Verfügung stehen. Viele Unternehmen haben ihre digitale Transformation schneller vorangetrieben, um den neuen Anforderungen gerecht zu werden. Sie setzen auf die Cloud und auf Software-as-a-Service (SaaS), um die Flexibilität und Geschwindigkeit zu erhöhen.

Im Global Networking Trends Report 2021 haben wir dargelegt, wie Netzwerktechnologien eingesetzt werden, um ungeachtet der Umstände die geschäftliche Flexibilität zu verbessern.

Im diesjährigen Global Networking Trends Report konzentrieren wir uns auf einen neuen Trend, der große Auswirkungen auf die Zukunft hat: Network-as-a-Service.

NaaS ist vor dem Hintergrund der zunehmend beliebten As-a-Service-Modelle wie SaaS und Infrastructure-as-a-Service (IaaS) entstanden und wird die Beschaffung, Bereitstellung und Verwaltung von Netzwerkfunktionen durch Unternehmen grundlegend verändern. Um mehr zu erfahren, haben wir mit 20 IT-Führungskräften gesprochen und 1.534 IT-Fachleute in 13 Ländern dazu befragt, wie sie NaaS sehen, wo ihrer Meinung nach seine Stärken und Grenzen liegen und ob sie eine Einführung des neuen Netzwerknutzungsmodells planen.

Wir hoffen, dass die Daten, Einblicke und Tipps aus diesem Bericht Ihnen helfen, die Vorteile und Implikationen von NaaS besser zu beurteilen, während Sie Ihre Netzwerkstrategien weiterentwickeln.

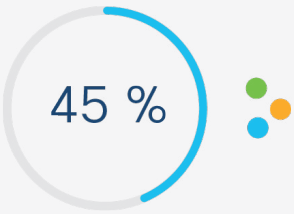
– James Mobley, SVP Network Services, Cisco

Wichtigste Ergebnisse

Es ist keine einfache Aufgabe, die Nutzung und den Betrieb Ihres Netzwerks komplett zu transformieren. Sie müssen gute geschäftliche und technologische Gründe haben, um diesen Wechsel zu einem As-a-Service-Modell zu vollziehen. Außerdem benötigen Sie vertrauenswürdige Partner, die Ihr Unternehmen zuverlässig am Laufen halten. Viele Unternehmen sind dennoch äußerst motiviert, diesen Schritt zu wagen. Dies sind die wichtigsten Ergebnisse unserer NaaS-Studie 2022:

Wichtiges Ergebnis Nr. 1: Herausforderungen

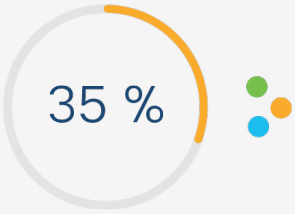
Wenn es um Widerstandsfähigkeit und Flexibilität geht, setzen viele Unternehmen auf NaaS.



- Als größte Herausforderungen 2021 im Bereich Netzwerk werden die Reaktion auf Störungen (45 %) und das Eingehen auf neue geschäftliche Anforderungen (40 %) genannt.
- Gleichzeitig sehen IT-Teams bei NaaS den großen Vorteil, dass es ihnen Zeit für Innovationen und wertschöpfende Aufgaben verschafft (46 %). Weitere 40 % geben an, dass NaaS die Reaktion auf Störungen verbessert, und 34 % erkennen eine Verbesserung der Netzwerkflexibilität.

Wichtiges Ergebnis Nr. 2: Vorteile

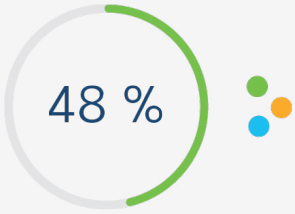
Große Erwartungen: Schneller Zugriff auf die neuesten Technologien ist das Hauptziel.



- Technologie entwickelt sich weiterhin schneller, als Unternehmen darauf reagieren können. Dementsprechend geben 35 % der Teilnehmer als wichtigsten Grund für die Einführung von NaaS an, dass sie kontinuierlich die neuesten Netzwerktechnologien wie Wi-Fi 6, Software-Defined WAN (SD-WAN), Secure Access Service Edge (SASE), 5G und KI bereitstellen müssen.

Wichtiges Ergebnis Nr. 3: Betriebsabläufe

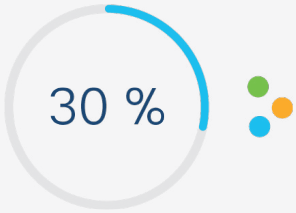
NaaS ist nützlich – allerdings nur, wenn das Netzwerkteam damit Service Level Agreements (SLAs) besser einhalten kann.



- Die am häufigsten bei NaaS-Anbietern angeforderten Services sind Netzwerklebenszyklusverwaltung (48 %), Ausfallsicherheit für Netzwerke (42 %) sowie Überwachung und Fehlerbehebung für die Einhaltung von SLAs (38 %).

Wichtiges Ergebnis Nr. 4: Bedenken

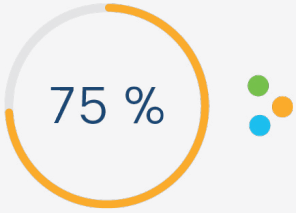
Unternehmen sehen nicht nur die Vorteile. Es gibt durchaus Bedenken hinsichtlich eines Kontrollverlusts und möglicher Kosten.



- Die Studienteilnehmer fragen sich unter anderem, ob NaaS ganz neuen Anforderungen gerecht werden kann (30 %) und ob sie die Kontrolle über die Sicherheit verlieren (26 %).
- Weitoben auf der Liste der Bedenken rangieren auch die mit der Umstellung verbundenen Kosten und Störungen (28 %).

Wichtiges Ergebnis Nr. 5: Rollen

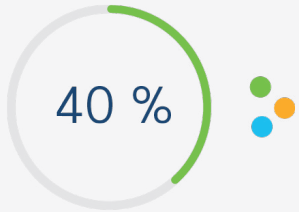
NaaS eröffnet IT-Fachleuten neue Möglichkeiten, doch sie müssen auch ihr Know-how erweitern.



- Mehr als 75 % der Unternehmen sind davon überzeugt bzw. fest davon überzeugt, dass NaaS den IT-Teams Möglichkeiten zur Erweiterung ihrer Kompetenzen bietet.
- Derzeit traut jedoch nur ein Viertel der Unternehmen seinen eigenen IT-Mitarbeitern eher als einem Systemintegrator, Managed Services-Anbieter oder NaaS-Anbieter zu, die geschäftlichen Anforderungen in technische Richtlinien umsetzen zu können.

Wichtiges Ergebnis Nr. 6: Akzeptanz

Es gibt verschiedene Möglichkeiten für den Einstieg in NaaS. Eine davon ist SASE.



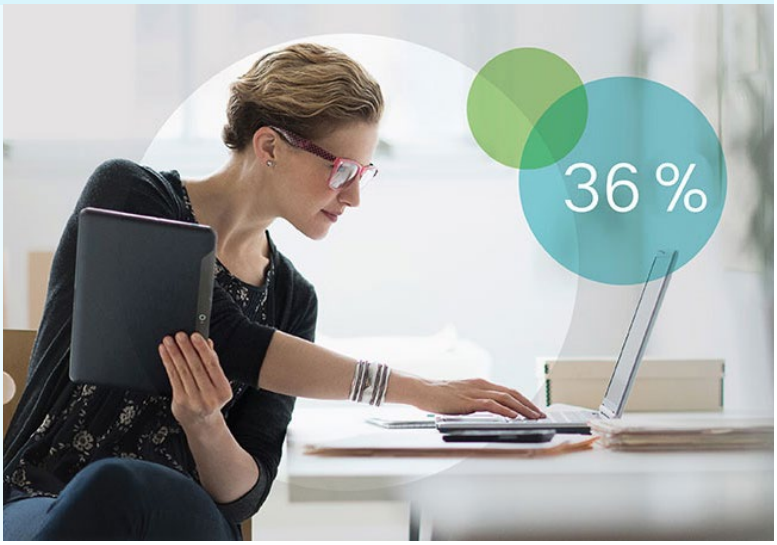
- SASE ist ein möglicher Einstiegspunkt für NaaS, da viele Unternehmen angeben, dass Multicloud-Zugriff (40 %) und Sicherheit (34 %) sich gut für NaaS eignen.
- Immerhin 49 % der Unternehmen planen die Einführung von NaaS im Rahmen eines Aktualisierungs- oder Upgrade-Zyklus, und 34 % haben vor, zunächst einen vorhandenen Standort anzupassen.

Ein anderes Netzwerkmodell

Nach mehr als 18 Monaten mit ständigen Störungen und Anpassungen ist die Rolle der Netzwerktechnologie für das Überleben und den Erfolg von Unternehmen klarer – und wichtiger – denn je. Netzwerke sind eine wichtige Voraussetzung für Remote-Arbeit. Jetzt sollen sie zudem sichere Arbeitsumgebungen, hybride Arbeitsmodelle und den sich weiterentwickelnden Geschäftsbetrieb unterstützen. Zu diesem Zweck müssen sie über lokale, Multicloud- und Edge-Umgebungen hinweg nahtlos funktionieren. Sie müssen allen Benutzern unabhängig von Standort, Gerät und Verbindungsmethode eine sichere, konsistente Erfahrung bieten. Außerdem müssen sie sowohl herkömmliche als auch moderne Microservices-basierte Anwendungen unterstützen.

Da die Ressourcen und die Bandbreite oft begrenzt sind, informieren sich viele Führungskräfte im IT- und Netzwerkbereich derzeit über NaaS als mögliche Alternative für diese Herausforderungen. Doch was genau ist NaaS?

Als wir IT-Führungskräfte nach ihrer Definition von NaaS fragten, wurde schnell klar, dass der Begriff sehr unterschiedlich interpretiert wird. In der Umfrage gaben zu unserer Überraschung 36 % der Teilnehmer an, sie würden NaaS bereits nutzen. Auf den ersten Blick wirkte dieser Anteil für eine so junge Technologie sehr groß, doch in den Interviews erkannten wir, dass viele Unternehmen schon von NaaS sprechen, sobald ein Teil ihres Netzwerks von einem Drittanbieter verwaltet wird. Wir empfinden diese Definition als zu weit gefasst und halten es für wichtig, sie einzugrenzen.



NaaS ist ein über die Cloud bereitgestelltes, nutzungsbasiertes Modell, bei dem Benutzer Netzwerkfunktionen beschaffen und orchestrieren können, ohne eine eigene Infrastruktur besitzen, erstellen oder unterhalten zu müssen.

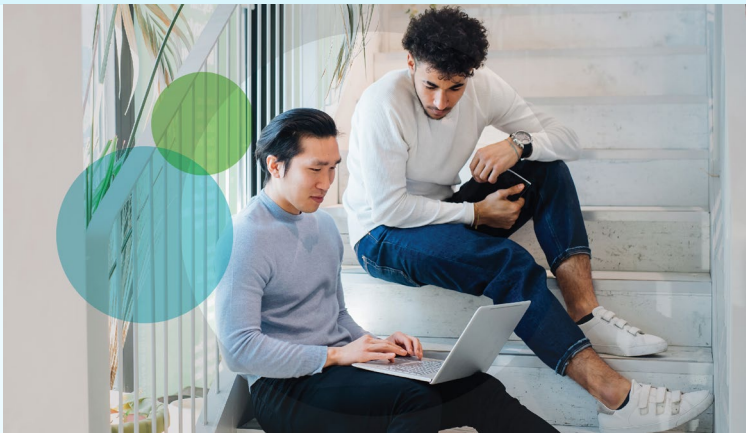
„Unternehmen versuchen, die optimale Kombination aus internen und externen, von Partnern bereitgestellten Ressourcen zu finden. Viele investieren in Mitarbeiter, Analysen, Beobachtbarkeit und Automatisierung im Unternehmen und fragen sich, wie sie das Management und die Pflege der Infrastruktur an strategische Anbieter auslagern können."

– Mary Turner, Research Vice President, IDC

NaaS kann als alternatives Nutzungsmodell für viele Netzwerkelemente fungieren, beispielsweise für LAN, WLAN, WAN und VPN sowie Zweigstellen-, Rechenzentrums-, Edge-, Multicloud- und Hybrid Cloud-Umgebungen. Es kann auch für die Bereitstellung neuer Netzwerkmodelle wie SASE genutzt werden. Es kann Veränderungen in Organisationsmodellen bewirken, zum Beispiel den Übergang zu hybrider Arbeit. Als On-Demand-Service kann NaaS es den IT-Teams ermöglichen, einfacher nach oben oder unten zu skalieren, neue Services schnell bereitzustellen und das Verhältnis zwischen CapEx und OpEx zu harmonisieren.

Manche der von uns interviewten IT-Führungskräfte sehen in NaaS eine dringend benötigte neuere, bessere Form des Netzwerks.

Sie erkennen, dass sie ins Hintertreffen geraten und das Vertrauen ihrer Benutzer verlieren. Und sie denken, dass NaaS ihnen helfen kann, die neuesten Technologien zu erhalten, den wachsenden Anforderungen gerecht zu werden und mit der immer schnelllebigeren Geschäftswelt Schritt zu halten.



> „Da Netzwerke heute so komplex sind, Unternehmen sehr schnell auf Marktveränderungen reagieren müssen und die Reichweite moderner Netzwerke enorm ist, wird vielen IT-Mitarbeitern gerade klar, dass sie überfordert sind und Hilfe benötigen."
>
> – Mark Leary, Research Director, Network Analytics, IDC

Fazit:

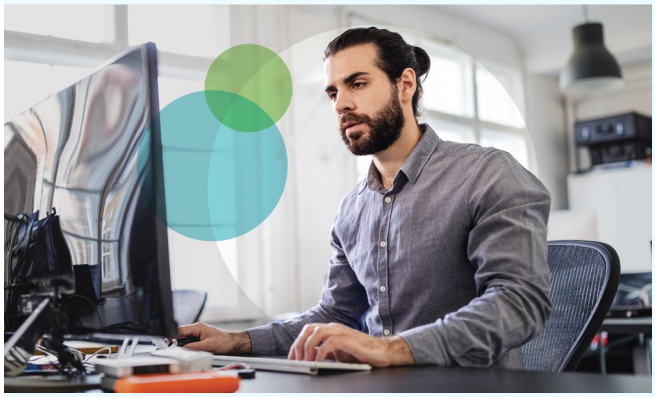
Für die NaaS-Einführung wird eine durchschnittliche jährliche Wachstumsrate von 40,7 % zwischen 2021 und 2027 erwartet[1].

Herausforderungen meistern, Vorteile realisieren

Bei der Frage, ob ein NaaS-Modell eingeführt werden soll, kommt es letztlich darauf an, welche geschäftlichen und technologischen Herausforderungen damit gemeistert werden können und welche Vorteile es bietet.

Den von uns befragten Unternehmen ist Flexibilität immer noch am wichtigsten. Auf die Frage, welche großen geschäftlichen Herausforderungen Einfluss auf die Gestaltung des Netzwerks haben, nannten knapp 50 % der Teilnehmer die Reaktion auf Störungen und 40 % die Einführung neuer Geschäftsanwendungen und -projekte. Mehr als ein Drittel der Befragten gab den Bedarf an Netzwerkflexibilität als wichtigen Faktor für die Einführung von NaaS an, und jeder zweite Teilnehmer erwartet, mit NaaS mehr Innovation und geschäftlichen Wert schaffen zu können.

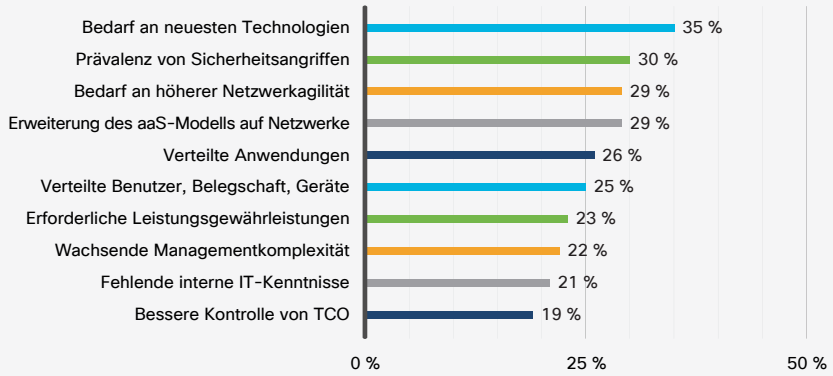
Um flexibler zu werden, verlagern viele IT-Abteilungen ihre Anwendungen und Services in die Cloud. Daraus können sich neue Herausforderungen bei Sicherheit, Governance und Compliance ergeben.



Laut den von uns befragten IT-Fachleuten betreffen die aktuell größten technologischen Herausforderungen beim Netzwerkmanagement Verbindungen mit mehreren Clouds (36 %), die Sicherheit der Netzwerke, Benutzer und Anwendungen (34 %) sowie die Ursachenermittlung und schnelle Behebung von Sicherheits- oder Leistungsproblemen (31 %).

Ein Drittel der Teilnehmer nannte die Anforderung, kontinuierlich die neuesten Netzwerktechnologien (wie Wi-Fi 6, SD-WAN, SASE, 5G und KI) bereitzustellen, als einen wichtigen Motivationsfaktor für den Umstieg auf NaaS. Ebenfalls ein Drittel nannte die Möglichkeit zur Verteidigung gegen Sicherheitsbedrohungen, die immer häufiger und raffinierter werden.

Was würde Ihr Unternehmen am ehesten dazu bewegen, zu einem NaaS-Modell zu wechseln?



„Unsere Führungskräfte sehen keinen Wert darin, dass meine Mitarbeiter Geräte konfigurieren oder die Infrastruktur betreiben. Sie möchten, dass sich die IT an den geschäftlichen Zielen orientiert. Wenn wir externe Services für grundlegende Betriebsabläufe nutzen, kommen meine Mitarbeiter den geschäftlichen Zielen näher."

– Leiter IT-Infrastruktur bei einem weltweit tätigen Anbieter für Verbraucherprodukte

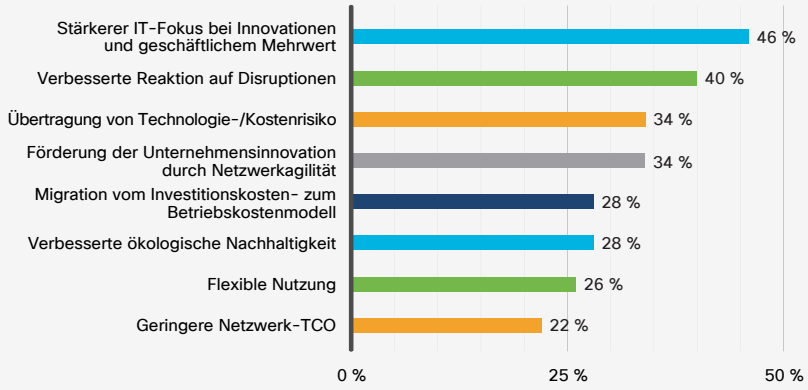
Auf die Frage, welche Hauptvorteile sich IT-Fachleute von NaaS erhoffen, nannten die primären Entscheidungsträger die Möglichkeit für Mitarbeiter, sich auf die Wertschöpfung statt auf das routinemäßige Infrastrukturmanagement zu konzentrieren.

Ein weiterer oft genannter Vorteil war die Verbesserung der Reaktion auf Störungen im Netzwerk und bei der Sicherheit (45 % der Netzwerktechniker und 40 % der primären Entscheidungsträger). Während die Priorisierung von Verbesserungen bei der Sicherheit nicht weiter überrascht, war es interessant zu sehen, dass mehr als 25 % der Netzwerktechniker und 33 % der primären Entscheidungsträger die Verbesserung der ökologischen Nachhaltigkeit als einen großen Vorteil von NaaS angaben.

Noch überraschender war die geringe Bedeutung, die die Befragten den finanziellen Vorteilen von NaaS beimessen.

Dank des flexiblen Nutzungsmodells und der abonnementbasierten Preise können IT-Teams mit NaaS von CapEx zu OpEx wechseln und wiederholte große Investitionen in die Netzwerkinfrastruktur umgehen. Die Ausgaben werden konstanter und planbarer, und das Unternehmen muss nur für die tatsächlich genutzten Ressourcen zahlen. Dennoch messen die IT-Führungskräfte und Netzwerkfachleute diesen finanziellen Vorteilen eine deutlich geringere Bedeutung zu als den NaaS-Vorteilen hinsichtlich Flexibilität, Innovation und Auslagerung des Managements.

Was sind Ihrer Meinung nach die drei wichtigsten geschäftlichen Vorteile, die sich aus der Nutzung eines NaaS-Modells ergeben könnten?



Fazit:

Die Gesamtbetriebskosten stehen im Zusammenhang mit NaaS relativ weit unten auf der Prioritätenliste, weil es Unternehmen wesentlich wichtiger ist, einen geschäftlichen Wert zu schaffen und schnell auf Störungen zu reagieren. Von den befragten IT-Führungskräften sind 68 % überzeugt bzw. fest überzeugt, dass NaaS ihre Teams von der routinemäßigen Netzwerkverwaltung entlastet und ihnen so mehr Zeit für Innovationen und wertschöpfende Aufgaben verschafft.

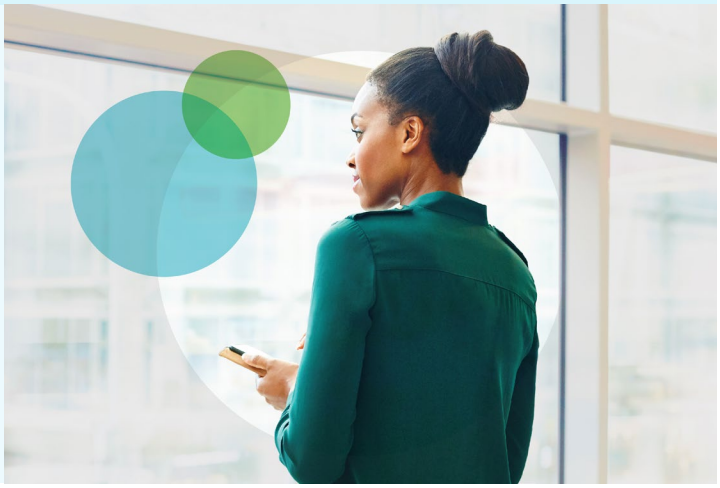
So verändert NaaS den Netzwerkbetrieb

Wenn es um Bedenken in Bezug auf NaaS geht, wurde häufig genannt, dass die internen IT-Teams den Netzwerkbetrieb völlig aus der Hand geben und dem NaaS-Anbieter überlassen müssten. So würden keine Aufgaben für das NetOps-Team des Unternehmens übrig bleiben. In Wahrheit liegt bei NaaS gar nicht die gesamte Zuständigkeit für den Betrieb in nur einer Hand.

Bei einem NaaS-Modell übernimmt der Anbieter die Verantwortung für alle Aspekte der Netzwerklebenszyklusverwaltung. Dies umfasst die Bereitstellung, Integration, Kontrolle, Aktualisierung, Überwachung und Korrektur aller Elemente der Netzwerkinfrastruktur (ggf. einschließlich lokaler Systeme der Kunden), die zum Erreichen der vertraglich vereinbarten Ergebnisse erforderlich sind. Diese Ergebnisse können sich auf die Anzahl der verbundenen Benutzer, Standorte, Cloud-Provider und Anwendungen sowie auf die vereinbarten Service Level, Bandbreiten, Sicherheitsmaßnahmen, Compliance-Vorgaben und andere Anforderungen beziehen.

Was muss dann überhaupt noch verwaltet werden? Die NetOps-Teams der NaaS-Kunden können mehr Zeit in wichtige oder wertschöpfende Aktivitäten investieren.

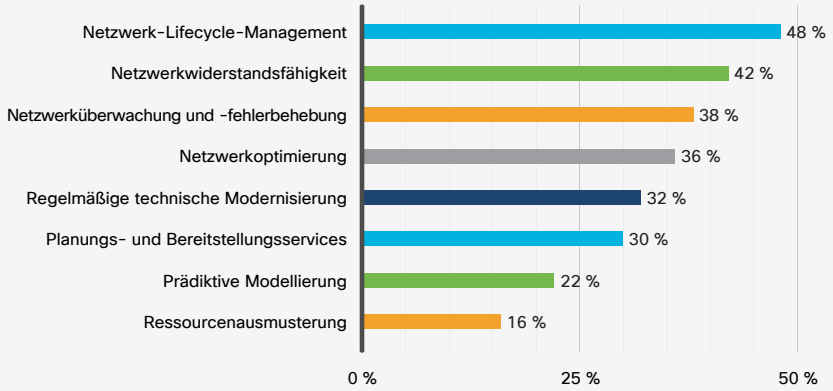
Dazu könnte beispielsweise zählen, die gewünschten Netzwerkergebnisse zu definieren und zu überwachen – etwa in Bezug auf Zugriffsrichtlinien für Benutzer und Anwendungen oder auf die Anwendungsleistung. Wenn das NetOps-Team des Kunden die Netzwerkleistung und die zugehörigen Informationen überwacht, kann es die Netzwerkrichtlinien und das Verhalten in den verschiedenen Domänen kontinuierlich anpassen und optimieren.



Mit APIs kann das NetOps-Team des Kunden auch die Integrationen zwischen NaaS und den vorhandenen Systemen des Unternehmens verwalten, um IT-Workflows und -Prozesse zu straffen. Eine enge Zusammenarbeit mit dem NaaS-Anbieter ist empfehlenswert, um sicherzustellen, dass SLAs und SLOs (Service Level Objectives) eingehalten werden. Ungeachtet der betrieblichen Zuständigkeiten und Übergaben liegt auf der Hand, dass IT-Fachleute den Aufwand beim Infrastrukturmanagement gerne reduzieren möchten.

Die Netzwerklebenszyklusverwaltung wurde von 48 % der befragten IT-Fachleute als wichtigster Service genannt, der in einem NaaS-Modell enthalten sein muss. Auf dem zweiten Platz steht die Ausfallsicherheit des Netzwerks (42 %), auf dem dritten stehen Netzwerküberwachung und Fehlerbehebung (38 %). Dies verstärkt den Eindruck, dass die Verwaltung einer immer stärker verteilten und immer komplexeren Kombination aus Standorten, Benutzern, Geräten, Anwendungen und Cloud-Ressourcen den Mitarbeitern zu wenig Zeit für wertschöpfende Aktivitäten und Innovationen lässt.

Welche der folgenden Services sollten unbedingt in einem NaaS-Modell enthalten sein?



„Der Anbieter übernimmt die alltäglichen Aufgaben. Das interne Team kann sich dann darauf konzentrieren, den Wert des Netzwerks zu erhöhen, indem es auf neue Anforderungen reagiert. Unsere Entwickler und Techniker müssen nicht ihre Arbeit unterbrechen, um Probleme zu beheben. Sie können sich ganz auf neue Projekte konzentrieren.“

– Erfahrener Netzwerktechniker bei einem globalen Consulting-Unternehmen

Fazit:

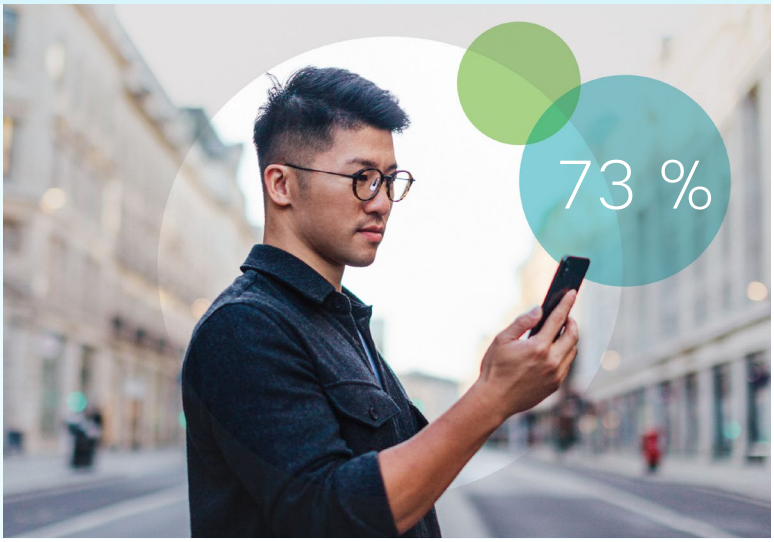
Bei einem NaaS-Modell werden die Zuständigkeiten für den Betrieb aufgeteilt. Der Anbieter übernimmt die aufwendige Netzwerklebenszyklusverwaltung, sodass sich das IT-Team des Kunden stärker auf betriebliche Aktivitäten konzentrieren kann, die den geschäftlichen Wert steigern.

Rollen, Zuständigkeiten und Kompetenzen

Da die Verantwortung für die Infrastrukturwartung und Lebenszyklusverwaltung auf den NaaS-Anbieter verlagert wird, bleibt den internen IT-Teams deutlich mehr Zeit. Das NetOps-Team des Kunden kann sich auf die gewünschten Netzwerkergebnisse statt auf die technischen und betrieblichen Aspekte der Infrastrukturwartung konzentrieren.

Mit anderen Worten: Die Netzwerktechniker müssen sich nicht mehr um alles selbst kümmern, sondern agieren auf einer höheren Ebene. Doch welche Aufgaben erwarten sie?

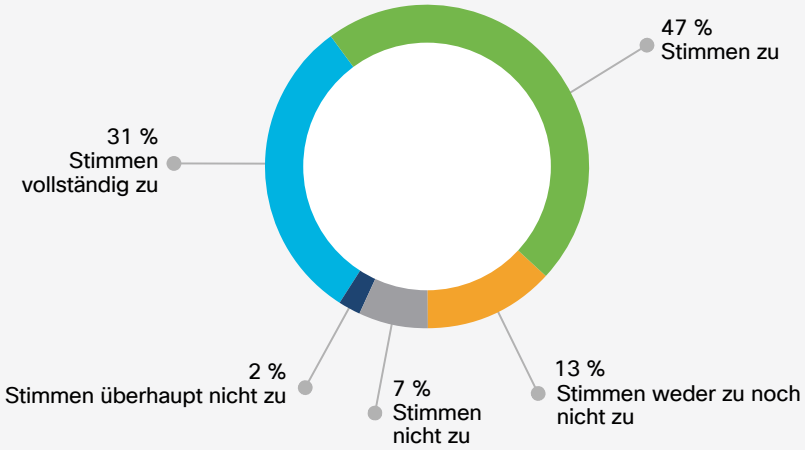
Von unseren Teilnehmern sind 27 % der Meinung, ihre IT-Mitarbeiter würden ihre technische Kompetenz und ein NaaS-Dashboard nutzen, um geschäftliche Anforderungen in Netzwerkrichtlinien umzusetzen. Überraschenderweise geben 73 % der Befragten an, ihnen wäre es lieber, wenn Drittanbieter diese geschäftskritische Rolle übernehmen würden. Dies ist möglicherweise ein Hinweis auf eine empfundene Knappheit oder einen Mangel an Vertrauen in die intern vorhandenen Kompetenzen.

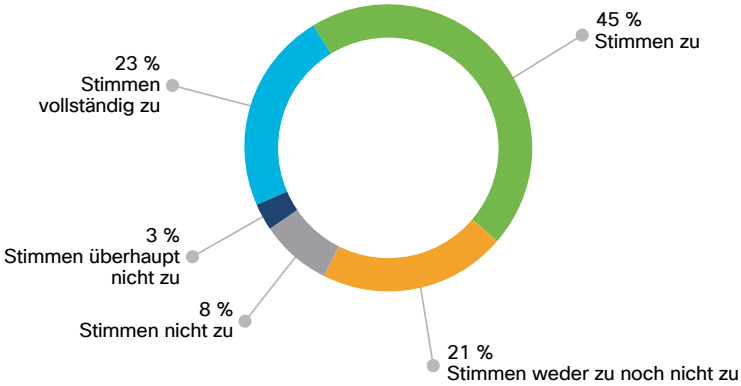


„Wenn der Löwenanteil der Routineaufgaben auf den NaaS-Anbieter übergeht, verlegt sich das NetOps-Team des Kunden vermutlich auf allgemeine Netzwerk- und Sicherheitskompetenzen sowie Design-Know-how, mit dem sich geschäftliche Ziele in übergeordnete Netzwerkkonzepte umsetzen lassen. Eine enge Zusammenarbeit mit dem NaaS-Anbieter ist unverzichtbar, um das Design, die Richtlinien, die Leistung und die SLAs für das Netzwerk zu optimieren. Zudem sind solide Kenntnisse im Bereich Data Science erforderlich, um diese Änderungen zu identifizieren und zu orchestrieren.“

– Joe Clarke, Distinguished Engineer, Cisco

Die Einführung eines NaaS-Modells würde den Mitgliedern unseres Netzwerkteams Gelegenheit bieten, Kompetenzen zu erweitern und einen Mehrwert für das Unternehmen zu schaffen.





Mit NaaS bleibt meinem Netzwerkteam mehr Zeit für IT-Innovationen und wertschöpfende Aufgaben, weil es sich nicht mehr um die alltägliche Netzwerkverwaltung kümmern muss.

Fazit:

Mehr als 75 % der Unternehmen sind davon überzeugt bzw. fest davon überzeugt, dass NaaS-Modelle ihren Teams Möglichkeiten zur Erweiterung ihrer Kompetenzen und zur Wertschöpfung bieten.

Bedenken und Vorbehalte

NaaS wirkt sich auf viele Bereiche einer IT-Abteilung aus. Es erfordert neue Betriebsmodelle, neue Integrationen mit bestehenden Prozessen und Technologien, Änderungen bei Rollen und Kompetenzen sowie eine finanzielle Umstellung von CapEx auf OpEx. Angesichts dieser weitreichenden Implikationen waren die Reaktionen der von uns befragten IT-Fachleute auf NaaS gemischt. Die meisten standen an einem der beiden Enden des Spektrums – sie waren entweder begeistert von einer NaaS-Einführung oder lehnten sie völlig ab.

Die Einstellung der IT-Führungskräfte gegenüber NaaS schien sich nach ihrer jeweiligen übergeordneten Netzwerkphilosophie zu richten. Die Philosophien wiederum teilten sich überwiegend in zwei Lager: „kontrollierte IT“ und „Lean IT“. Die Unternehmen mit der ersten Philosophie verfügen über sehr kompetente Mitarbeiter und sind zudem der Meinung, dass ihre Teams unbedingt die Verantwortung und Kontrolle über den gesamten Netzwerk-Stack haben sollten. Die zweite Gruppe dagegen strebt danach, die IT zu konsolidieren, wertschöpfende Aufgaben gegenüber Routineabläufen zu priorisieren und die Infrastrukturwartung auszulagern. Es überrascht wenig, dass die Unternehmen mit dem „Lean IT“-Ansatz, die bereits einige ihrer IT-Ressourcen in die Cloud verlagert haben, NaaS-Lösungen sehr aufgeschlossen gegenüberstehen.

> „Wir stemmen uns gegen NaaS, weil wir glauben, dass das Netzwerk dabei nicht mit der nötigen Sorgfalt und Priorität gehandhabt würde und eine solche Lösung nicht zu unserer Umgebung passen würde.“
>
> – IT-Manager im Bereich Netzwerke bei einer US-Militärbehörde

Einige der von uns interviewten IT-Führungskräfte gaben an, ihre Netzwerke und Prozesse seien sehr speziell. Sie glauben nicht, dass NaaS diesem Maß an Komplexität und ihren besonderen Herausforderungen gerecht werden könnte.

Andere hatten klare Bedenken, dass NaaS in ihrer IT-Abteilung auf Widerstand stoßen würde.

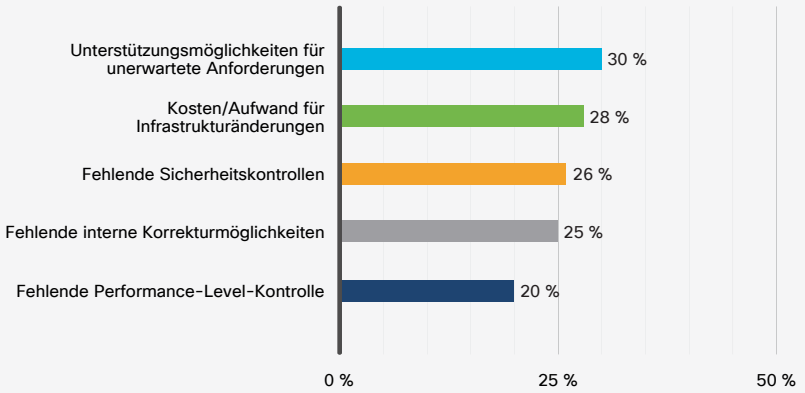
Viele Bedenken wurden von fast allen Führungskräften gleichermaßen geäußert. Am häufigsten wurde der empfundene Kontrollverlust genannt. Immerhin 30 % der Teilnehmer stellten infrage, ob sie nach der Einführung von NaaS auch künftige Anforderungen erfüllen können. Andere hatten Bedenken hinsichtlich des Kontrollverlusts bei Sicherheit (26 %) und Leistung (20 %). In Wahrheit ist NaaS auf eine hohe On-Demand-Skalierbarkeit und eine schnellere Unterstützung neuer Technologien ausgelegt. Entscheidungen in Bezug auf Sicherheit, Leistung und andere für die Kontrolle wichtige Aspekte werden weiterhin vom IT-Team selbst getroffen und nicht vom NaaS-Anbieter.

„Der Anbieter muss auf unsere Sicherheitsrichtlinien eingehen und unseren Anweisungen folgen. Das ist ein wichtiges Differenzierungsmerkmal bei NaaS.“

– Leiter Architektur bei einem globalen Technologieunternehmen

Von den Teilnehmern gaben 28 % die mit einer Änderung der vorhandenen Infrastruktur und Betriebsabläufe verbundenen Kosten und Störungen als Hemmnisse an. Viele Unternehmen haben zahlreiche Technologien und Investitionen, für die oft unterschiedliche Abschreibungszeiträume gelten. Andere Unternehmen arbeiten mit Legacy-Technologien und -Anwendungen, die sich nicht gut für NaaS eignen. Und wieder andere möchten das alltägliche Management ihrer Infrastruktur schlicht nicht aus der Hand geben.

Was sind Ihre größten Bedenken hinsichtlich der Bereitstellung eines NaaS-Modells?



Um diese Bedenken und Vorbehalte auszuräumen, können Unternehmen das NaaS-Modell zunächst in einer einzelnen Domäne testen. So können sie sich einen besseren Eindruck der Funktionen und Kontrollpunkte von NaaS verschaffen, ohne die Netzwerkinfrastruktur oder die Betriebsabläufe zu sehr zu verändern. Sie können die geteilte Verantwortung zwischen Anbieter und internem Team ausprobieren und optimieren und zudem lernen, wie sie bei der Zusammenarbeit die besten Ergebnisse erzielen. Sobald die Rollen, Zuständigkeiten und Kontrollpunkte geklärt und alle damit einverstanden sind, kann die Lösung unter Berücksichtigung der bereits vorliegenden Erkenntnisse und Best Practices nach und nach auf weitere Domänen skaliert und erweitert werden.

Fazit:

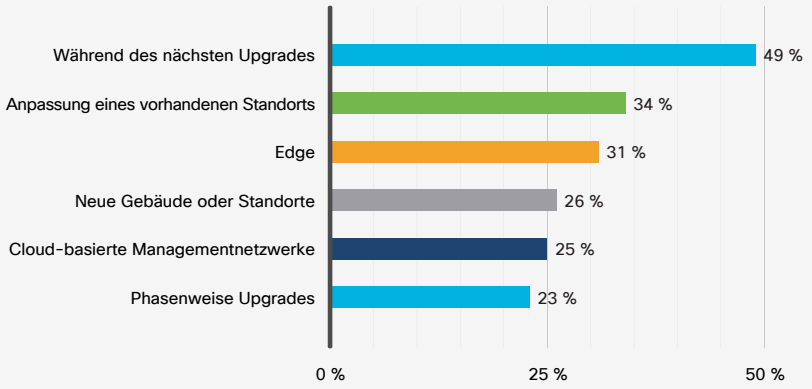
Bei jedem Transformationsmodell ist anfangs mit Bedenken zu rechnen. IT-Führungskräfte können im Kleinen beginnen, um zunächst die Risiken und Vorteile von NaaS zu evaluieren und herauszufinden, ob die Lösung zu ihrem Unternehmen passt.

Trends bei der Einführung

Aufgrund der Auswirkungen auf den Netzwerkbetrieb und der vielen verschiedenen Einsatzmöglichkeiten gestaltet sich die NaaS-Einführung bei jedem Unternehmen anders. Mit einer Bewertung der NaaS-Bereitschaft und einer Bereitstellungs-Roadmap können Unternehmen mögliche Komplikationen minimieren und für den größtmöglichen Erfolg sorgen.

In unserer Studie waren 49 % der IT-Führungskräfte und 57 % der Netzwerktechniker der Meinung, der beste Zeitpunkt und die optimalen Umstände für eine NaaS-Einführung seien bei Netzwerkinfrastruktur-Upgrades und Technologieaktualisierungen gegeben, wenn Zugriff auf neue Technologie (z. B. Automatisierung, 100-Gigabit-Ethernet, Wi-Fi 6, 5G, SD-WAN, SASE) gewünscht sei. Immerhin 34 % der Teilnehmer nannten die Anpassung eines bestehenden Standorts mit schon bereitgestellter Netzwerktechnologie als ideales Szenario für die NaaS-Einführung. Interessanterweise hielten nur 26 % einen bestehenden Standort für den optimalen Ansatzpunkt zur NaaS-Einführung. Gerade einmal 23 % sagten, ein Ansatz mit mehreren Phasen, bei dem NaaS nach und nach in den Domänen eingeführt wird, sei für ihr Unternehmen ideal.

Für welche der folgenden Szenarien wäre NaaS Ihrer Meinung nach in Ihrem Unternehmen am besten geeignet?



Fazit:

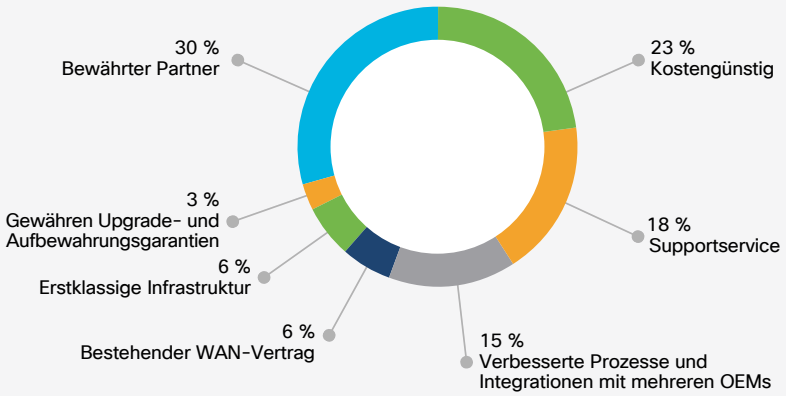
Wie, wann und warum NaaS bereitgestellt wird, variiert je nach Unternehmen.

Auswählen eines NaaS-Anbieters

Da das Netzwerk für die Mitarbeiterproduktivität, die Kundeneinbindung und die Geschäftsabläufe von entscheidender Bedeutung ist, sollten Unternehmen die Auswahl des NaaS-Anbieters nicht auf die leichte Schulter nehmen. Einige der von uns interviewten IT-Führungskräfte haben große Bedenken, die Kontrolle zu verlieren. Dennoch sind sie bereit, ein gewisses Maß an Kontrolle anzugeben, sofern sie auf einen vertrauenswürdigen Anbieter übergeht. Dabei kann es sich um einen Systemintegrator, einen Anbieter von Managed Services oder einen Value-Added-Reseller handeln. Am wohlsten fühlen sich die Befragten mit etablierten Partnern, die ihre Netzwerkumgebung, die Geschäftsziele und den Supportbedarf bereits gut kennen.

In Bezug auf NaaS-Bereitstellungen hält knapp ein Drittel der IT-Fachleute aus unserer Umfrage Systemintegratoren für vertrauenswürdiger und kostengünstiger als Netzwerkanbieter. Sie gaben außerdem an, bewährtes Fachwissen sei wesentlich wichtiger als eine erstklassige Infrastruktur.

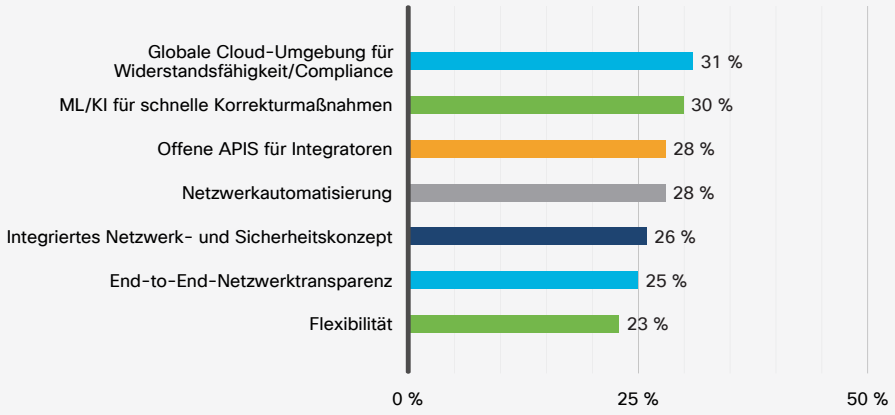
Aus welchem Hauptgrund würden Sie bei der NaaS-Bereitstellung lieber mit einem Partner zusammenarbeiten statt direkt mit einem Netzwerkanbieter?



Wenn es um das Umsetzen von geschäftlichen Anforderungen in technische Richtlinien geht, haben IT-Fachleute zwei- bis dreimal mehr Vertrauen in einen Systemintegrator oder ihre internen IT-Mitarbeiter als in einen NaaS-Anbieter. Dies unterstreicht, dass Unternehmen bei NaaS nicht einfach nur nach einer Lösung suchen, sondern auch Beratung und Unterstützung von einem vertrauenswürdigen Partner wünschen, der sie gut kennt.

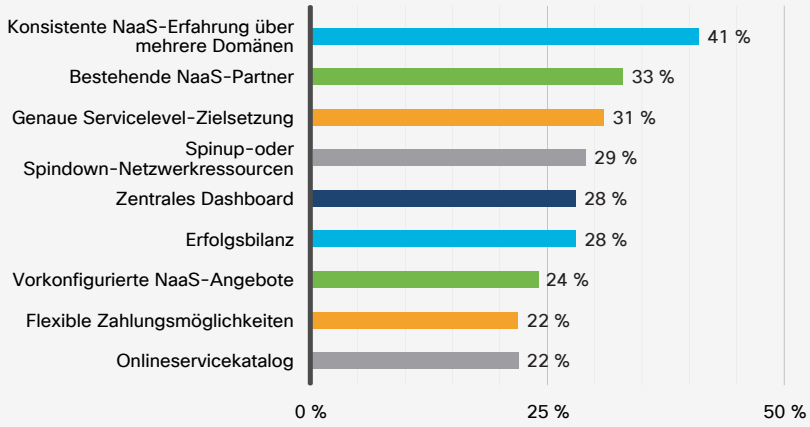
Was die technischen Merkmale von NaaS-Anbietern und -Lösungen anbelangt, sind den Teilnehmern folgende Punkte am wichtigsten: globale Cloud-Umgebung für Zuverlässigkeit, Leistung und regionale Compliance (31 %) sowie Funktionen im Bereich Machine Learning (ML) und künstliche Intelligenz, die eine kontinuierliche Optimierung des NaaS-Service ermöglichen (30 %). Auch APIs, Automatisierung, integrierte Sicherheit, Netzwerksichtbarkeit und Netzwerkflexibilität stehen weit oben auf der Liste.

Was sind Ihrer Meinung nach die zwei wichtigsten technischen Merkmale eines NaaS-Angebots?



Für 41 % der Befragten ist es wichtig, dass ein NaaS-Anbieter eine über verschiedene Domänen (Zugriff, WAN, Rechenzentrum, Cloud etc.) hinweg konsistente NaaS-Plattform bietet. Viele IT-Teams haben Schwierigkeiten mit dem Management mehrerer Umgebungen, Toolsets und Betriebsmodelle. NaaS-Anbieter bieten ihnen die Möglichkeit, Netzwerkressourcen, -richtlinien und -abläufe zu konsolidieren.

Welcher der folgenden Aspekte wäre Ihnen beim Auswählen eines Angebots von einem NaaS-Anbieter am wichtigsten?



„Eigentlich suche ich nach jemandem, der die routinemäßigen Managementaktivitäten für unser Netzwerk und unsere Systeme übernimmt, beispielsweise Firmware-Updates, Konfigurationen und Änderungen. Mein Team kann sich dann verstärkt auf Verbesserungen, Neuentwicklungen und Strategieimplementierungen konzentrieren. Vielleicht ist die Aufgabenverteilung auch flexibel. Eventuell übernehme ich diesen Monat bestimmte Aufgaben selbst, hole mir aber für die nächsten Monate Hilfe, um die Nutzung auszudehnen und meine Arbeit zu unterstützen.“

– VP Technologie und Sicherheit bei einer gemeinnützigen US-Organisation, Umsatz 100 Mio. USD

Fazit:

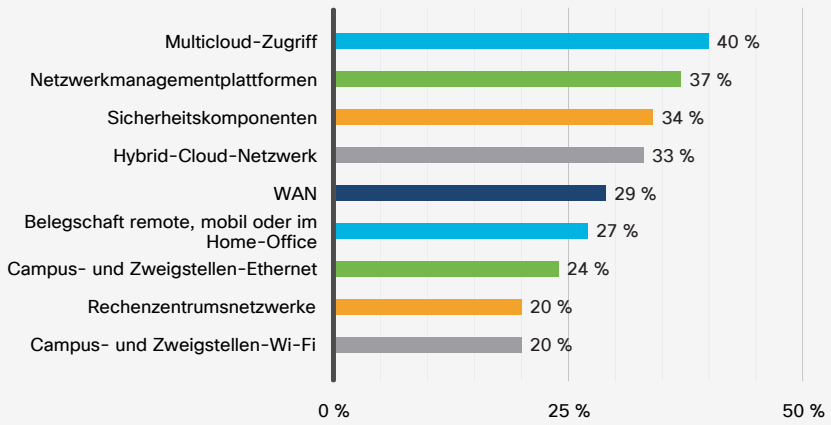
Systemintegratoren werden im Vergleich zu NaaS-Anbietern als vertrauenswürdiger, kostengünstiger und serviceorientierter betrachtet. Unabhängig vom Anbieter suchen Kunden nach einer Service- und Betriebserfahrung, die sich über alle Netzwerkdomänen erstreckt.

SASE und die verschiedenen NaaS-Varianten

Die Auswahl an NaaS-Angeboten wird stetig größer. Es gibt beispielsweise Lösungen für LAN, WLAN, WAN, Netzwerksicherheit, Remote- oder Homeoffice-Zugriff, Rechenzentrumsnetzwerke und Cloud-Netzwerke. Laut unserer Studie sind NaaS-Modelle mit Multicloud-Zugriff und Sicherheit am gefragtesten. Demzufolge sollte SASE – eine Lösung, die sicheren Multicloud-Zugriff überall bietet – für viele IT-Abteilungen ein erstrebenswertes As-a-Service-Angebot sein.

Angesichts der mit dem Vernetzen mehrerer separater Clouds verbundenen Herausforderungen überrascht es nicht, dass Multicloud-Zugriff bei NaaS als am wichtigsten genannt wurde (40 %). NaaS-Anbieter können mit SD-WAN-Services eine konsistente, optimierte Möglichkeit zum Vernetzen vieler verschiedener Cloud-basierter Anwendungen (IaaS und SaaS) bieten.

Zu welchen Aspekten Ihrer Netzwerkgeräte und Ihrer Netzwerkverwaltung würde NaaS gut passen?

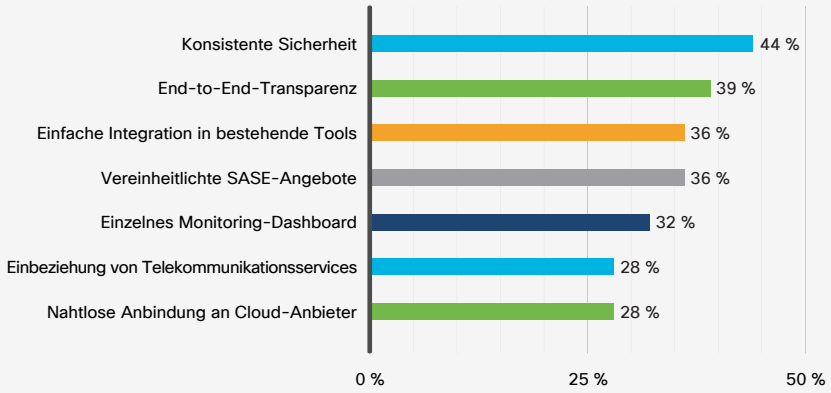


Für 34 % der Befragten haben sicherheitsorientierte NaaS-Lösungen Priorität, darunter VPN, Security Information and Event Management (SIEM), Secure Web Gateway (SWG), Firewalls sowie Intrusion Prevention and Detection Services (IPS/IDS.) Diese können Benutzer, Geräte und Anwendungen in verschiedenen Clouds und Computing-Umgebungen konsistent schützen.

NaaS-Anbieter, die eine Kombination aus Multicloud-Zugriff und Sicherheit am Edge bieten, sind für die wachsende Nachfrage nach SASE-Lösungen gut aufgestellt.

Knapp die Hälfte (44 %) der Befragten nannten konsistente Sicherheit mit Bedrohungserkennung und -beseitigung für alle Benutzer und Geräte unabhängig vom Ort des Zugriffs als wichtigen Aspekt von SASE. Angesichts der zunehmenden Abhängigkeit vom Internet für den Zugriff auf Cloud-basierte Anwendungen sind 39 % der Teilnehmer an Transparenz und Einblick in den Netzwerkverkehr über Internet- und Cloud-Infrastrukturen hinweg interessiert. Ganze 36 % wünschen SASE-Lösungen, die sich leicht mit ihren vorhandenen Tools integrieren lassen.

Welche der folgenden Funktionen wären am wichtigsten, wenn Ihr Unternehmen SASE-as-a-Service bereitstellen wollte?



Fazit:

Multicloud-Zugriff und Sicherheit sind bei NaaS die wichtigsten Aspekte. Anbieter, die eine SASE-Option in ihr NaaS-Portfolio aufnehmen, können den wachsenden Bedarf an Abstimmung und Schutz für lokale und Cloud-Ressourcen erfüllen.

Schlussfolgerung

Viele IT-Abteilungen haben Schwierigkeiten, die Netzwerkkomplexität zu verwalten, auf Störungen zu reagieren, Benutzer und Daten zu schützen und mit der schnelllebigen Geschäftswelt Schritt zu halten. Um diese Herausforderungen zu meistern, befassen sich viele Unternehmen derzeit mit neuen Netzwerkmodellen wie NaaS.

NaaS ermöglicht den kontinuierlichen Zugriff auf die neuesten Netzwerktechnologien über ein On-Demand- bzw. abonnementbasiertes Modell Mühsame routinemäßige Netzwerkverwaltungsaufgaben werden an einen Drittanbieter delegiert. Dadurch ermöglicht es NaaS den IT-Teams, sich auf wertschöpfende Aktivitäten zu konzentrieren, welche die Flexibilität und Ausfallsicherheit erhöhen und Innovationen vorantreiben.

Wie bei jedem anderen Transformationsmodell gibt es Bedenken und Vorbehalte gegenüber NaaS. Der Grundsatz lautet jedoch nicht „alles oder nichts“. IT-Teams können mit zuverlässigen Partnern zusammenarbeiten, um NaaS im kleinen Rahmen zu testen, die Chancen und Risiken zu bewerten und zu ermitteln, ob die Lösung den übergeordneten Geschäfts- und Technologiestrategien entspricht.

Zusätzliche Ressourcen und Hilfe

Was ist Network-as-a-Service (NaaS)? >

Cisco+ Lösungen >

Cisco Partner suchen >

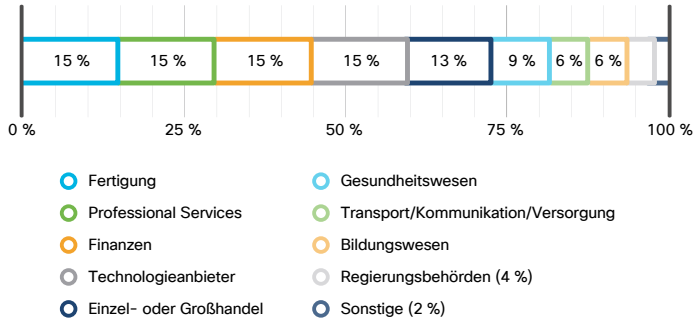
Cisco Vertrieb kontaktieren >

Über diesen Bericht

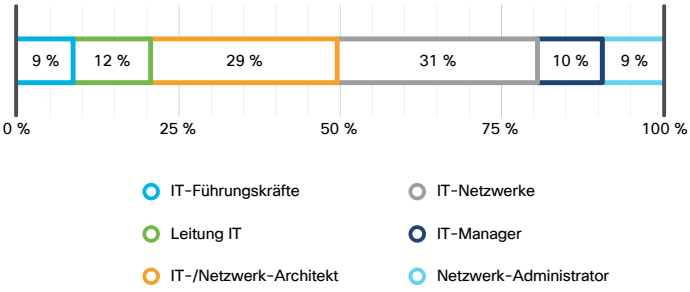
Der Global Networking Trends Report wurde erstmals 2019 veröffentlicht und gibt einen Überblick über die neuesten Strategien und Technologien in der Unternehmensnetzwerk- und Cloud-Branche. Der auf Branchenanalysen basierende Bericht bietet Perspektiven, Einblicke und Unterstützung für IT-Abteilungen und hilft ihnen, aktuelle Technologietrends zu verstehen, ihre Netzwerkmodelle weiterzuentwickeln und dynamische Geschäftsanforderungen zu unterstützen.

Für den Global Networking Trends Report 2022 haben wir Interviews mit 20 IT-Führungskräften geführt und 1.534 IT-Fachleute in 13 Ländern dazu befragt, was sie von NaaS halten und ob die Lösung ihren Netzwertstrategien für die nächsten zwei Jahre entspricht bzw. diese sogar fördert. Die Befragten durften bis zu drei Antworten pro Frage auswählen.

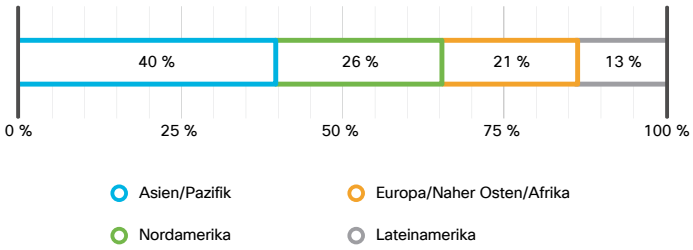
Branche des Teilnehmers



Rolle des Teilnehmers



Standort des Teilnehmers



Nutzungsgenehmigung für diesen Bericht

Cisco gestattet ausdrücklich die Verwendung der in diesem Bericht enthaltenen Informationen durch Pressevertreter, Analysten, Service-Provider und andere Interessenten. Alle Daten aus dem Cisco Global Networking Trends Report 2022, die gedruckt oder in elektronischer Form veröffentlicht oder privat oder öffentlich geteilt werden, sind mit einer entsprechenden Quellenangabe zu versehen (d. h. „Quelle: Cisco Global Networking Trends Report 2022“). Ein zusätzliches schriftliches Einverständnis oder Unterschriften sind zur Bezugnahme auf unsere öffentlich zugänglichen Whitepaper und Berichte nicht erforderlich.

Wir sind stets daran interessiert, in welchen Zusammenhängen unsere Daten verwendet werden. Falls Sie unsere Inhalte verwenden, würden wir uns freuen, wenn Sie uns Kopien der von Ihnen erstellten Dokumente, die Daten des Cisco Global Networking Trends Report 2022 enthalten, zukommen lassen würden. Bitte leiten Sie Dokumente, die auf den Cisco Global Networking Trends Report 2022 Bezug nehmen, an networkingtrends-inquiries@cisco.com. weiter.

Quellen für den Global Networking Trends Report 2022

1. Global Network-as-a-Service (NaaS) Market Industry Dynamics, Market Size, and Opportunity Forecast to 2027, März 2021.