The bridge to possible

Global Networking Trends Report 2023

Vereinfachung sicherer Multicloud-Konnektivität für verteilte Belegschaften

The bridge to possible

Global Networking Trends Report 2023

Vereinfachung sicherer Multicloud-Konnektivität für verteilte Belegschaften

Inhalt

The bridge to possible

Willkommen

Der jährliche Cisco Global Networking Trends Report beleuchtet wichtige Strategien und Technologien im Bereich der Unternehmensnetzwerke und der Cloud-Branche. Der Bericht kombiniert Erkenntnisse aus der Primär- und Branchenforschung mit Perspektiven und Einblicken von Führungskräften, um die neuesten Technologietrends zu identifizieren, und dient IT-Teams als Leitfaden bei der Weiterentwicklung ihrer Netzwerkmodelle zur Unterstützung dynamischer Geschäftsanforderungen.

Im Bericht 2023 untersuchen wir, wie Unternehmen ihre Netzwerke bereitstellen und weiterentwickeln, um sichere Verbindungen für verteilte Anwendungen, Belegschaften, Orte und Geräte zu unterstützen. Wir haben mehr als 2.500 IT-Verantwortliche in 13 Ländern in Nord-, Mittel- und Südamerika, im Asien-Pazifik-Raum und in Westeuropa befragt.

The bridge to possible

Zentrale Erkenntnisse: Aktuelle Netzwerkstandards für die Verbindung mehrerer Clouds

Aufgrund der mittlerweile allgegenwärtigen Hybrid-Work-Modelle ist die Bereitstellung sicherer Verbindungen weiterhin eine Herausforderung.

Das Zeitalter der hybriden Arbeit erfordert neue Ansätze, um Remote-MitarbeiterInnen sicher mit Unternehmensdaten und -ressourcen zu verbinden, die über Multicloud-Umgebungen verteilt sind.

- Die Mitarbeitenden werden zwar ermutigt, ins Büro zurückzukehren, doch mehr als 40 % arbeiten weiterhin entweder vollständig oder an einigen Tagen pro Woche remote.
- Anwendungen werden heute über mehrere Clouds und eine stark verteilte Belegschaft hinweg bereitgestellt. Herkömmliche Sicherheitsmodelle können da nicht mithalten – und IT-Fachleute müssen neue Lösungen finden. Mehr als die Hälfte (51 %) geben als größte Herausforderung Sicherheitsrisiken in der Cloud an und 39 % nennen die steigende Anzahl von Remote-MitarbeiterInnen.

Der Übergang zu Cloud und Multicloud beschleunigt sich.

Wenn geschäftliche Flexibilität die Frage ist, ist die Antwort für viele nach wie vor die Cloud.

- Unternehmen setzen weiterhin auf Cloud-Plattformen. 78 % der Befragten geben an, dass ihre Unternehmen bis 2025 planen, mehr als 40 % ihrer Workloads in der Cloud zu hosten. Bislang tun dies 63 %.
- Auch die Einführung von Multiclouds ist auf dem Vormarsch: 42 % der Cloud- und Netzwerkfachleute berichten, dass eine flexiblere und skalierbarere Anwendungsentwicklung eine zentrale Motivation für die Verwendung mehrerer Clouds ist.

Die Sicherung des Benutzerzugriffs auf Cloud-Anwendungen steht an der Spitze der Netzwerkanforderungen 2023.

Die Aufrechterhaltung der End-to-End-Transparenz in der gesamten digitalen Servicebereitstellungskette (z. B. zwischen Benutzern und der Cloud) zur Sicherstellung eines konsistenten Anwendungserlebnisses ist ein weiteres wichtiges Feld für IT-Fachkräfte in Unternehmen.

- Die Bereitstellung von sicherem Zugriff auf Anwendungen, die über mehrere Clouds verteilt sind, ist die größte Herausforderung, die von 41 % der Netzwerkfachleute genannt wird.
- Die zweitgrößte Herausforderung, angegeben von 37 % der Befragten, ist die End-to-End-Transparenz der Netzwerkleistung und -sicherheit, wenn mehr Datenverkehr von jenseits der Grenzen des Unternehmensnetzwerks ausgeht oder dort endet.

The bridge to possible

Orientierungshilfe: Erfolgreiche Netzwerkstrategien für den sicheren Zugriff auf Cloud-basierte Anwendungen

Konvergenz von Netzwerk und Sicherheit

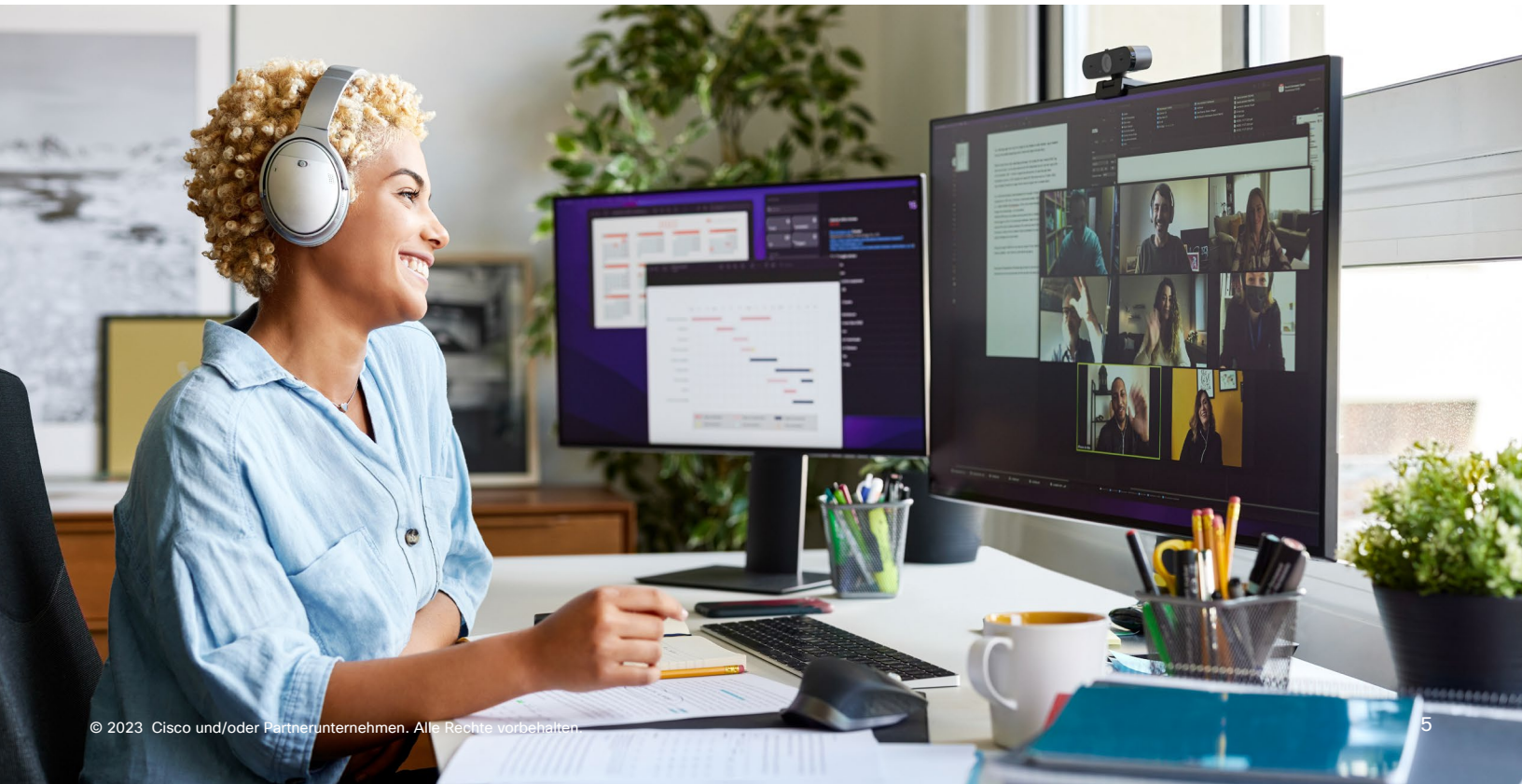
Verbessern Sie die Zusammenarbeit zwischen IT-Teams, um den Betrieb vom Zugriffsnetzwerk bis zur Cloud zu vereinfachen.

Isolierte Unternehmen und herkömmliche Modelle für die Bereitstellung von Konnektivität können die dynamischen Sicherheitsanforderungen von verteilten Anwendungen, Personen, Orten und Ressourcen nicht mehr erfüllen.

- Standardisierte Richtlinien, gemeinsam genutzte Telemetrie und optimierte Workflows in den Bereichen Sicherheit, Netzwerk und Cloud-Betrieb bieten bessere und schnellere IT- und Geschäftsergebnisse als Umgebungen, die als Technologiesilos arbeiten.
- 40 % der Befragten geben an, dass isolierte Betriebsabläufe eine wichtige Herausforderung darstellen, wenn es um den sicheren Zugriff auf mehrere Cloud-basierte Anwendungen von verteilten Standorten aus geht.
- Cloud-ExpertInnen sind der Meinung, dass der Netzwerkbetrieb eine bessere Abstimmung auf den Cloud-Betrieb erfordert: 38 % wünschen sich eine engere Integration mit Netzwerkteams, und 34 % nennen die betriebliche Konsistenz als Hauptziel.

Erzielen Sie mit einer SASE-Architektur den reibungslosen Übergang zu einem konvergenten Netzwerk- und Sicherheitsmodell.

Secure Access Service Edge (SASE) bietet die betriebliche Vereinfachung sowie die konsistente Sicherheit und Performance, die für den Multicloud-Zugriff hybrider Belegschaften nötig sind.



- Unternehmen vereinen Software-Defined WAN (SD-WAN) und Cloud-Security, um eine SASE-Architektur bereitzustellen.
- 47 % der Befragten erwarten, ihre Zweigstellen und Remote-Clients innerhalb von zwei Jahren zu verbinden, indem sie ihre SD-WAN-Umgebungen auf eine vollständige SASE-Architektur erweitern.

Annahme von Cloud-First-Networking und -Sicherheit

Erweitern Sie die SD-WAN-Konnektivität konsistent auf mehrere Clouds, um ein einfaches IT-Management und ein besseres Anwendungserlebnis zu erzielen.

Wenden Sie Richtlinien konsistent auf alle Clouds an, um Cloud-unabhängige Verbindungen zu automatisieren und das Anwendungserlebnis zu optimieren und zu sichern.

- Durch die Erweiterung von Transparenz, Kontrolle und Zero-Trust-Zugriff auf Cloud-, SaaS- und Provider der mittleren Meile kann die IT ein besseres und sichereres Benutzererlebnis bieten.
- Mehr als die Hälfte (53 %) der Befragten geben an, dass sie die Integration mit Cloud-Service-Providern priorisieren, um in den nächsten zwei Jahren die Anbindung an Cloud-basierte Anwendungen von allen Standorten aus zu verbessern.

Steigen Sie um auf Cloud-zentrierte Sicherheit und schaffen Sie konsistente Betriebsabläufe und Richtlinien.

Durch die Kombination verschiedener Sicherheitsbereiche in einer Cloud-Plattform werden Transparenz, Richtlinienverwaltung und -kontrolle einfacher, umfassender und effektiver gestaltet.

- 59 % der Befragten geben an, dass ihre Priorität für Cloud-Zugriffsnetzwerke in den nächsten zwei Jahren die Zentralisierung der Sicherheit in der Cloud ist. Dabei wird anerkannt, dass eine konsistente Richtlinie für BenutzerInnen und Geräte an jedem Standort eine wichtige Anforderung ist.

Übergang zu einem proaktiven Betrieb

Erzielen Sie durch End-to-End-Netzwerktransparenz ein konsistentes Benutzererlebnis in der immer komplexeren digitalen Servicebereitstellungskette.

Ohne die Transparenz über das eigene Netzwerk hinaus auf das Internet und Cloud-Umgebungen auszudehnen, können IT-Teams kein konsistentes, hochwertiges Benutzererlebnis für Cloud-basierte Anwendungen und Services sicherstellen.

- 51 % der Befragten priorisieren die Verwendung von End-to-End-Netzwerktelemetrie und -transparenz für die proaktive Erkennung und Behebung von Problemen.
- Die Transparenz des Internet- und Cloud-Datenverkehrs ist besonders wichtig, wenn die Mehrheit der Benutzer- und Gerätetransaktionen über den Unternehmensperimeter hinausgeht.

Wechseln Sie von reaktiven zu prädiktiven Betriebsabläufen, um Verfügbarkeit und Performance zu verbessern.

Prädiktive Analysen werden als wichtiger Bestandteil eines AIOps-Toolkits (Artificial Intelligence for IT Operations, künstliche Intelligenz für den IT-Betrieb) für einfachere, schnellere und effektivere IT-Gesamtoperationen zunehmend anerkannt.

- 47 % der Befragten beabsichtigen, Netzwerkverschlechterungen zu verhindern, anstatt Ausfälle reaktiv zu beheben, und priorisieren die Einführung prädiktiver Netzwerkanalysen in den nächsten zwei Jahren.

The bridge to possible

Einleitung: Trends beim Multicloud-Zugriff

„Computing kann eines Tages als Teil der öffentlichen Versorgung genutzt werden, genauso wie es heute bei Telefonen der Fall ist. Dabei zahlen BenutzerInnen dann nur für die Kapazität, die sie tatsächlich verwenden.“[1] Dies waren die prophetischen Worte, die Professor John McCarthy 1961 an ein MIT-Publikum richtete.

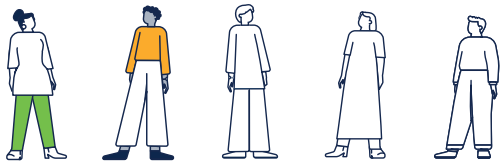
Mehr als sechs Jahrzehnte später hat sich McCarthys Vision einer gemeinsamen On-Demand-Computing-Versorgung nicht nur verwirklicht, sondern ist jetzt einer der wichtigsten Faktoren, die die globale digitale Revolution vorantreiben.

Der Umstieg auf die Multicloud geht weiter

Heute nutzen die meisten Unternehmen mehrere Clouds. Die Cisco Global Networking Trends-Studie 2023 hat ergeben, dass zwei Drittel der Unternehmen bereits mehr als 40 % ihrer Workloads in mehreren Clouds hosten. Darüber hinaus nutzen die meisten Unternehmen mehr als zwei Cloud-Anbieter, die große Mehrheit nutzt mehr als fünf SaaS-Provider (siehe Abbildung 1).

Hybride Arbeit bleibt ein dauerhafter Trend

Nicht nur die Anwendungen sind stark verteilt. Die weit verbreitete Einführung von hybrider Arbeit bedeutet auch, dass Menschen und Geräte heute stärker verteilt sind als je zuvor.



40 % aller Beschäftigten arbeiten mindestens einen Teil der Woche remote.

Laut einer aktuellen Studie arbeiten zwar 59 % der Beschäftigten wieder Vollzeit im Büro, doch die verbleibenden 41 % arbeiten hybrid (28 %) oder sogar vollständig remote (13 %).[2] Diese Zahlen variieren je nach Branche und Rolle erheblich.

Gleichzeitig erhöht die rasante Einführung von IoT-Technologie und Edge-Computing die ständig wachsende Anzahl von Verbindungen und Datenströmen, die täglich verwaltet und geschützt werden müssen.

Die verteilte Belegschaft und die Verbreitung von IoT und Edge-Computing erfordern skalierbare, sichere Verbindungen und Zugriff auf Multicloud-Anwendungen und global gehostete Services in jedem Netzwerk (Abbildung 2). Dies wurde von NetzwerkexpertInnen als ihre größte Herausforderung für 2023 identifiziert.

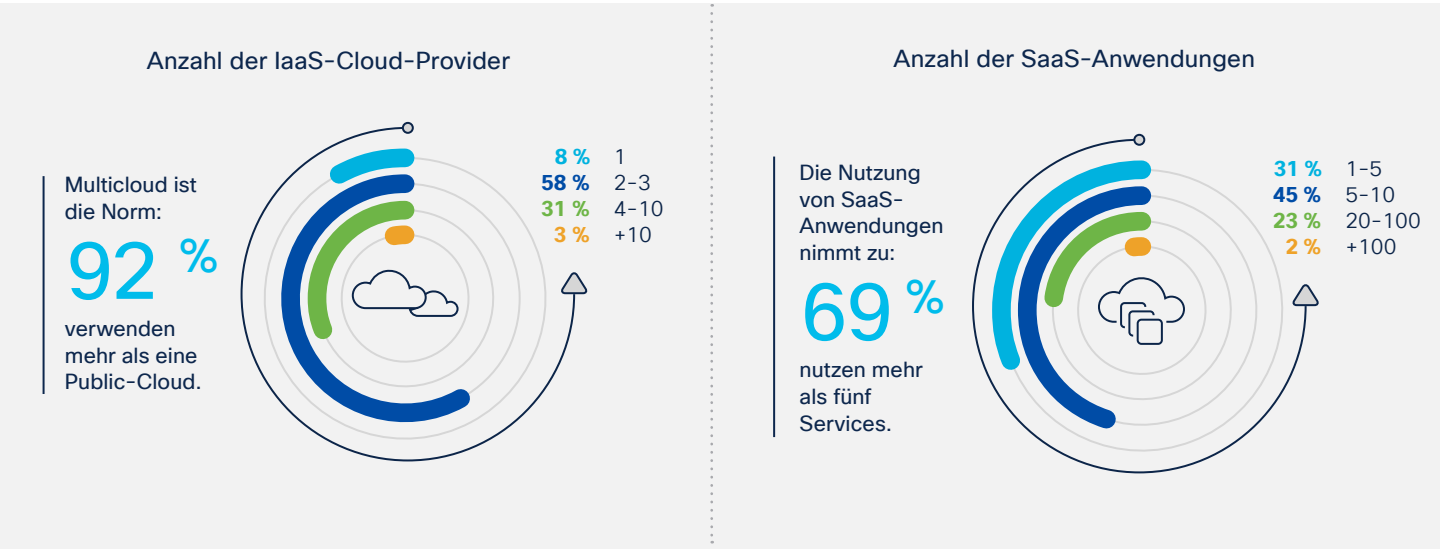


Abbildung 1: Die Verwendung mehrerer Cloud- und SaaS-Provider ist zur Norm geworden.

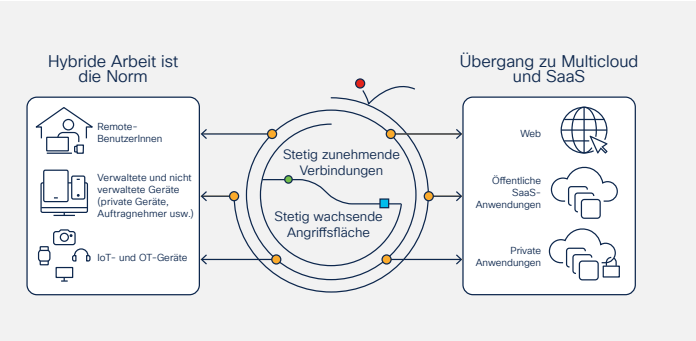


Abbildung 2: Hybride Arbeit und der Übergang zu Cloud und SaaS bedeuten, dass die Herausforderungen der Netzwerksicherheit die menschlichen Kapazitäten überschritten haben.

Die Konnektivität über das Internet erschwert diese Herausforderung, da die Infrastruktur sich von internen Netzwerk- und Sicherheitsfachleuten nicht überblicken oder kontrollieren lässt. Dennoch sind sie weiterhin für das digitale Erlebnis und den Schutz ihrer Mitarbeitenden, Kunden und Partner verantwortlich.

Die zunehmende Bedeutung von Geschwindigkeit und Flexibilität

Flexibilität ist für die meisten Unternehmen heutzutage ein Muss. Die Umfrageergebnisse zeigen, dass der Hauptgrund für den Übergang in die Multicloud nicht die Kosten sind, wie McCarthy ursprünglich prognostiziert hatte, sondern der Bedarf an geschäftlicher Flexibilität und Innovation sowie die Notwendigkeit, schnell neue hochwertige Anwendungen und Services bereitzustellen. Infolge einer globalen Pandemie, geopolitischer und wirtschaftlicher Disruptionen sowie von Herausforderungen in der Lieferkette ist die Fähigkeit, sich schnell an aufkommende Markttrends anzupassen, zu einer wichtigen Priorität geworden.

Unternehmen erkennen, dass isolierte Technologien und Betriebsmodelle in der heutigen Umgebung zu einschränkend sind, nicht mehr gut funktionieren und neue Tools und Prozesse erfordern. Aufgrund von Konnektivitäts- und Sicherheitsherausforderungen wird ein ganzheitlicher Ansatz benötigt, der eine einfachere, sicherere und flexiblere Netzwerkinfrastruktur und entsprechende Betriebsmodelle bereitstellen kann.

Der nächste Teil dieses Berichts befasst sich mit diesen Herausforderungen und bietet Best-Practice-Leitfäden für Ihren Weg zu flexibler und sicherer Konnektivität.

„Die Mitarbeitenden möchten nicht wochen- oder monatelang auf die Umsetzung ihrer geschäftlichen Prioritäten warten. Sie erwarten bei jeder Initiative, die vom Unternehmen ausgeht, eine sofortige Erfüllung ihrer Bedürfnisse anstatt der Engpässe der Vergangenheit.“

– IT Director, Einzelhandel

Außerdem wird erläutert, wie und warum Netzwerk- und Sicherheitsteams zusammenarbeiten müssen, um MitarbeiterInnen, Partnern und Kunden überall zuverlässige, sichere, robuste und Cloud-basierte Erlebnisse zu bieten.

1 https://www.technologyreview.com/2011/10/03/190237/the-cloud-imperative

2 https://wfhresearch.com/wp-content/uploads/2023/02/WFHResearch_updates_February2023.pdf

The bridge to possible

Orientierungshilfe: Sechs Best Practices für sicheren Zugriff auf die Multicloud

Orientierungshilfe Nr. 1: Verbessern Sie die Zusammenarbeit zwischen IT-Teams, um den Betrieb vom Zugriff bis zur Cloud zu vereinfachen.

Silos im Unternehmen und herkömmliche Modelle für die Bereitstellung von Konnektivität verhindern die Erfüllung der dynamischen Sicherheitsanforderungen von verteilten Anwendungen, Personen, Orten und Geräten.

Angesichts der zunehmenden Komplexität und der wachsenden Bedrohungslandschaft müssen IT-Verantwortliche die Zusammenarbeit zwischen Teams verbessern, damit sie schneller, effizienter und sicherer auf sich schnell ändernde Geschäftsanforderungen reagieren können.

Vier der fünf größten Herausforderungen bei der Bereitstellung des standortunabhängigen Benutzerzugriffs auf mehrere Cloud-basierte Anwendungen (z. B. Infrastructure-as-a-Service [IaaS] und Software-as-a-Service [SaaS]) betreffen die Sicherheit. 40 % der Befragten sehen isolierte Cloud-, Netzwerk- und Sicherheitsverfahren als größte Herausforderung bei der Bereitstellung eines sicheren Zugriffs von mehreren verteilten Standorten auf mehrere Cloud-basierte Anwendungen.

In vielen IT-Abteilungen planen und arbeiten die Netzwerk- und Sicherheitsteams separat. IT-Verantwortliche können

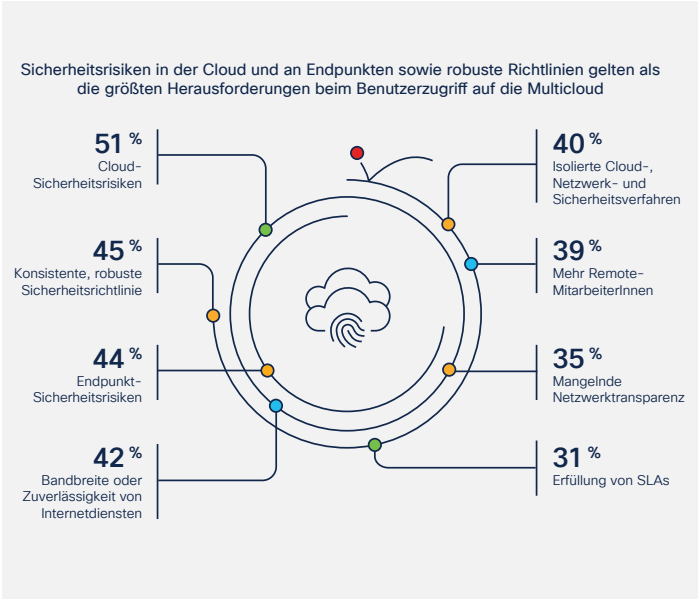


Abbildung 3: Herausforderungen bei der Bereitstellung des sicheren Zugriffs von Remote-Standorten auf mehrere Cloud-basierte Anwendungen.

die heutigen Sicherheitsherausforderungen jedoch nur bewältigen, indem sie Technologie- und Betriebssilos beseitigen und die Anzahl der nur punktuell integrierten Systeme reduzieren.

Die Ausrichtung von Teams, Tools und Prozessen zur Optimierung der Betriebsabläufe erfordert eine größere Konsistenz der Betriebsmodelle. Untersuchungen von Cisco haben ergeben, dass 86 % der CIOs und IT-Verantwortlichen die Notwendigkeit erkennen, ein konsistenteres

The bridge to possible

38 % der Cloud-Fachleute sehen in einer besseren Netzwerkintegration eine große betriebliche Herausforderung.

Betriebsmodell zu entwickeln, das lokale, Private-Cloud-, Public-Cloud- und SaaS-Systeme umfasst.[3] Es ist allgemein anerkannt, dass sich die Prinzipien des Cloud-Betriebsmodells für DevOps- und CloudOps-Teams bei der Vereinfachung des Betriebs und der Bereitstellung von mehr Flexibilität bewährt haben. IT-Teams können ähnliche Vorteile erzielen, wenn sie die Prinzipien eines Cloud-Betriebsmodells übernehmen. Umfragedaten bestätigen dies: 38 % der Cloud-Fachleute geben an, dass ihre größte betriebliche Herausforderung die bessere Integration in das Netzwerk ist, und weitere 34 % sagen, dass ihre größte Herausforderung die Aufrechterhaltung der betrieblichen Konsistenz zwischen der Cloud und dem Netzwerk ist.

Durch die Einführung von Cloud-Betriebsmodellprinzipien in das Netzwerk und den gesamten Cloud-/Netzwerk-IT-Stack können IT-Teams Innovationen beschleunigen, die Sicherheit verbessern und Risiken aus dem Cloud-Betrieb beseitigen. Sie können die Komplexität und Fragmentierung reduzieren, die die Zusammenarbeit zwischen Netzwerk-, Sicherheits- und Cloud-Betriebsabläufen einschränken, und letztendlich die dynamischen Anforderungen ihrer Organisation unterstützen.

Fazit

Die Konvergenz von Netzwerk- und Sicherheitsrichtlinien, Technologien, Tools und betrieblichen Workflows auf Basis eines Cloud-orientierten Modells ermöglicht es Unternehmen, mit einem gemeinsamen Satz von Tools zu arbeiten, um so eine gleichbleibend sichere Konnektivität zu fördern und gleichzeitig für mehr Effizienz und weniger Risiken zu sorgen.

3 https://ebooks.cisco.com/story/accelerating-digital-agility-2021/page/7/1

Fachmeinung

Eine starke Abstimmung im Team schafft mehr Sicherheit, Einfachheit und Leistung.

„Früher kannte das Betriebsteam jede Ebene in jedem System – von der Verkabelung bis zu den finalen Anwendungen – und verwaltete alles als ein großes Ganzes. Wir müssen zu diesem Modell zurückkehren.

Auch wenn Netzwerke in der Cloud nicht dasselbe sind wie Netzwerke vor Ort und das Unternehmen nicht mehr alle Geräte und die gesamte Software im Ecosystem kontrolliert, ist der Bedarf an Sicherheit gleich. Wichtig ist, dass die Sicherung des Zugriffs von Personen auf Cloud-Anwendungen einheitliche Richtlinien erfordert, unabhängig davon, wo sich BenutzerInnen befinden oder welche Anwendungen sie gerade nutzen. Dies kann als Leitstern für die Kombination von Design, Betrieb und Architektur dienen.

In Zukunft werden wir sehen, dass mehr Netzwerk- und Sicherheitsteams an einer End-to-End-Infrastruktur zusammenarbeiten, die auf den Prinzipien von Sicherheit und Einfachheit statt auf der betrieblichen Performance allein basiert. Denn all dies führt zum selben Ziel.“

Wendy Nather
Head of Advisory, CISOs
Cisco

The bridge to possible

Orientierungshilfe Nr. 2: Erzielen Sie mit einer SASE-Architektur den reibungslosen Übergang zu einem konvergenten Netzwerk- und Sicherheitsmodell.

SASE bietet die betriebliche Vereinfachung sowie die konsistente Sicherheit und Performance, die für den Multicloud-Zugriff hybrider Belegschaften nötig sind.

Dies geschieht durch die Zusammenführung von Netzwerk- und Sicherheitsdomänen zu einem dringend benötigten Framework für die sichere und nahtlose Verbindung von BenutzerInnen mit Anwendungen in komplexen und stark verteilten Umgebungen.

SASE entwickelt sich immer mehr zur bevorzugten Konvergenzarchitektur für sicheren Multicloud-Zugriff. 47 % der Befragten erwarten, ihre Zweigstellen und Remote-Clients innerhalb der nächsten zwei Jahre hauptsächlich über ein SASE-Modell zu verbinden.

Allerdings haben viele Unternehmen Schwierigkeiten, das volle Potenzial von SASE auszuschöpfen, weil ihren Lösungen bestimmte Funktionen fehlen oder sie keine vollständig konvergente Netzwerk- und Sicherheitslösung bereitstellen können.

SASE-Konvergenz erfordert eine solide SD-WAN-Grundlage in Kombination mit einer umfassenden Cloud-Security- oder Security-Service-Edge(SSE)-Lösung (Abbildung 4). Nur wenn diese Architekturen vollständig konvergent sind, können IT-Unternehmen alle Vorteile von SASE nutzen. Diese Vorteile umfassen ein optimiertes Betriebsmodell, um die Transparenz, das Management und die Kontrolle der sicheren Vernetzung von BenutzerInnen an jedem Ort so einfach und konsistent wie möglich zu gestalten.

Mit standardisierten Richtlinien, gemeinsam genutzter Telemetrie und koordinierten Warnungen über alle Sicherheits- und Netzwerkkomponenten hinweg versetzt eine vereinheitlichte SASE-Lösung NetOps- und SecOps-Teams in die Lage, die Effizienz, Performance und Sicherheit der IT zu stärken. Effizientere und konsistentere Betriebsmodelle und Workflows für alle NetOps- und SecOps-Teams führen zwangsläufig zu höherer Benutzerfreundlichkeit.

Voll funktionsfähige SASE-Implementierungen können eine höhere betriebliche Effizienz, ein optimiertes Benutzererlebnis und verbesserten Schutz bieten. Hier einige Beispiele für diese Vorteile:

„Secure Access Service Edge (SASE) bietet konvergente Netzwerk- und Security-as-a-Service-Funktionen, einschließlich SD-WAN, SWG, CASB, Next-Generation Firewall (NGFW) und Zero-Trust-Netzwerkzugriff (Zero Trust Network Access, ZTNA). SASE unterstützt Anwendungsfälle für Zweigstellen, Remote-MitarbeiterInnen und lokale Anwendungen mit sicherem Zugriff. SASE wird in erster Linie als Service bereitgestellt und ermöglicht Zero-Trust-Zugriff basierend auf der Identität des Geräts oder der Entität, kombiniert mit Echtzeitkontext sowie Sicherheits- und Compliance-Richtlinien.“

– Gartner IT Glossary, Secure Access Service Edge (SASE), abgerufen am 2. Mai 2023.

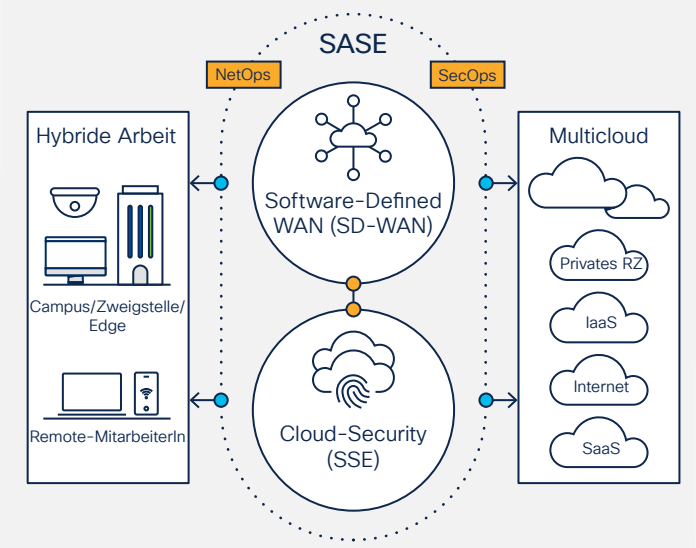


Abbildung 4: Netzwerk- und Sicherheitstechnologien sowie die Betriebskonvergenz schaffen ein neues Modell für sichere Verbindungen: Secure Access Service Edge.

The bridge to possible

Gartner® prognostiziert, dass bis 2025 50 % der SD-WAN-Einkäufe Teil des SASE-Angebots eines einzelnen Anbieters sein werden – 2021 waren es noch weniger als 10 %.[4]

- Das interne IT-Team von Cisco meldet eine Senkung der Betriebskosten um 40 % mit SASE.
- Eine gründliche Leistungsbewertung durch ein unabhängiges Testunternehmen hat gezeigt, dass Cisco Umbrella (eine Kernkomponente von Cisco SASE) mit implementierten Sicherheitsrichtlinien genauso gut funktioniert wie der Zugriff auf SaaS-Anwendungen über das Internet ohne Sicherheitslösung – oft sogar besser.
- TechValidate Customer Research ergibt, dass 85 % der Cisco Kunden Malware-Infektionen mit einer SASE-Architektur um 50 % reduzieren.

Es gibt zwei grundlegende Ansätze, um diese gewünschten Ergebnisse zu erzielen.

Die erste besteht aus separaten Netzwerk- und Sicherheits-/SSE-Produkten, die in der Regel von einem einzigen oder von zwei Anbietern bereitgestellt werden und in eine vollständige SASE-Lösung integriert werden können. Dieser Ansatz kann von Organisationen verwendet werden, die bereits SSE oder SD-WAN bereitstellen und möglicherweise eine größere Anpassungsfähigkeit und Flexibilität benötigen.

Der zweite ist ein einheitlicher Ansatz, der alle Netzwerk- und Sicherheitskomponenten in einem einzigen, schlüsselfertigen Cloud-Service mit einheitlichem Management bereitstellt. Eine gut konzipierte, einheitliche SASE-Lösung bietet Geschwindigkeit, Einfachheit und eine schnellere Time-to-Value.

4 Gartner, 2022 Strategic Roadmap for SASE Convergence, Neil MacDonald, Andrew Lerner, John Watts, Juni 2022. GARTNER ist eine in den USA und international eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. und/oder seinen Partnerunternehmen und wird in diesem Dokument mit Genehmigung verwendet. Alle Rechte vorbehalten.

Fachmeinung

Was macht eine SASE-Lösung aus?

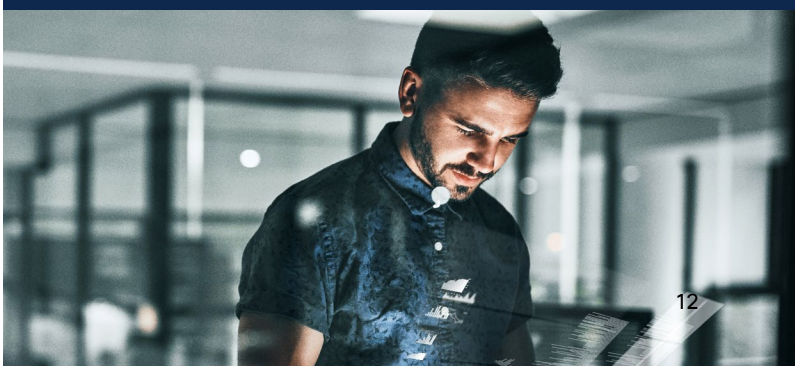
„Jedes Unternehmen verfügt über eine installierte Technologiebasis. Möglicherweise besteht hier die Versuchung, die fehlenden SASE-Funktionen einfach zur bestehenden Infrastruktur hinzuzufügen. Allerdings ist es wichtig zu beachten, dass SASE eine langfristige strategische Entscheidung ist und die einfache Bereitstellung aller Komponenten eines SASE-Modells ohne ein hohes Maß an Integration keine voll funktionsfähige SASE-Lösung darstellt und nicht die gewünschten Ergebnisse liefern kann.

Abhängig von ihren Prioritäten sollten sich Netzwerk- und Sicherheitsverantwortliche entweder für eine gut integrierte SASE-Lösung oder für einen schlüsselfertigen einheitlichen Service entscheiden.

Durch die Entscheidung für einen einheitlichen, schlüsselfertigen Cloud-Service können NetOps- und SecOps-Teams von zentralisiertem Management mit intelligenter verteilter Richtliniendurchsetzung, Kontrollen und Transparenz von Endpunkten bis hin zum Unternehmens- und Cloud-Edge profitieren, um eine sicherere End-to-End-Lösung bereitzustellen, die das Endbenutzererlebnis weiter optimiert.

„Egal, welche Technologie- und Architektur-entscheidungen Sie treffen, um Ihre Anforderungen besser zu erfüllen – entscheidend ist, sicherzustellen, dass die Anbieter sich kontinuierlich verpflichten, alle Komponenten zu einem gut integrierten oder einheitlichen System zu kombinieren.“

Omri Guelfand
VP of Product Management, NaaS/SASE
Cisco Meraki



The bridge to possible

Fazit

Im Gegensatz zu herkömmlichen Sicherheitslösungen rückt die einheitliche, Cloud-orientierte Architektur von SASE zentral verwaltete Sicherheitsrichtlinien und deren Durchsetzung näher an EndbenutzerInnen und Anwendungen heran und bietet flexible, nahtlose und sichere Konnektivität.

Mehr über SASE

Orientierungshilfe Nr. 3: Erweitern Sie die SD-WAN-Konnektivität konsistent auf mehrere Clouds, um ein vereinfachtes IT- und Anwendungserlebnis zu erzielen.

Wenden Sie Richtlinien konsistent auf alle Clouds an, um Cloud-unabhängige Verbindungen zu automatisieren und das Anwendungserlebnis zu optimieren und zu sichern.

Die Cloud ist zu einer Erweiterung des Unternehmensnetzwerks geworden. Für viele ist SD-WAN der Grundstein für eine vollständige SASE-Implementierung. Durch die automatisierte Erweiterung der SD-WAN-Fabric bei großen IaaS-, SaaS- und Providern der mittleren Meile erhält die IT mehr betriebliche Kontrolle, um ein besseres Benutzererlebnis zu bieten.

Und eine optimierte Kontrolle des Benutzererlebnisses ist bei Netzwerkteams oberstes Gebot: 53 % der Befragten gaben an, dass sie die Integration mit Cloud-Service-Providern priorisieren, um die Verbindung zu Cloud-basierten Anwendungen von verteilten Standorten aus zu verbessern. Zudem ergreifen Netzwerkteams aktiv Maßnahmen. 49 % der Befragten gaben an, dass sie SD-WAN- und Multicloud-Integrationen in den nächsten 24 Monaten als wichtigste Initiative priorisieren.

SD-WAN-Multicloud-Integrationen ermöglichen es Netzwerk- und Cloud-Teams, Erweiterungen von Unternehmensstandorten zu den verschiedenen Cloud-Providern und anderen Unternehmensstandorten per Internet, Interconnect oder Colocation und Cloud-Provider-Netzwerken zu beschleunigen und zu automatisieren (Abbildung 5). Mit diesen Integrationen können AdministratorInnen das Anwendungserlebnis optimieren und ein konsistentes Betriebserlebnis an allen Cloud- und lokalen Standorten erreichen. Darüber hinaus kann die IT durch die Integration mit globalen Netzwerk-Interconnect-Providern wie Equinix und Megaport einen sicheren, skalierbaren Zugriff auf Cloud-Anwendungen und Points-of-Presence bieten. Mit diesen Integrationen kann die IT innerhalb von Minuten ein globales Netzwerk auf vereinfachte, vollständig automatisierte Weise aufbauen.

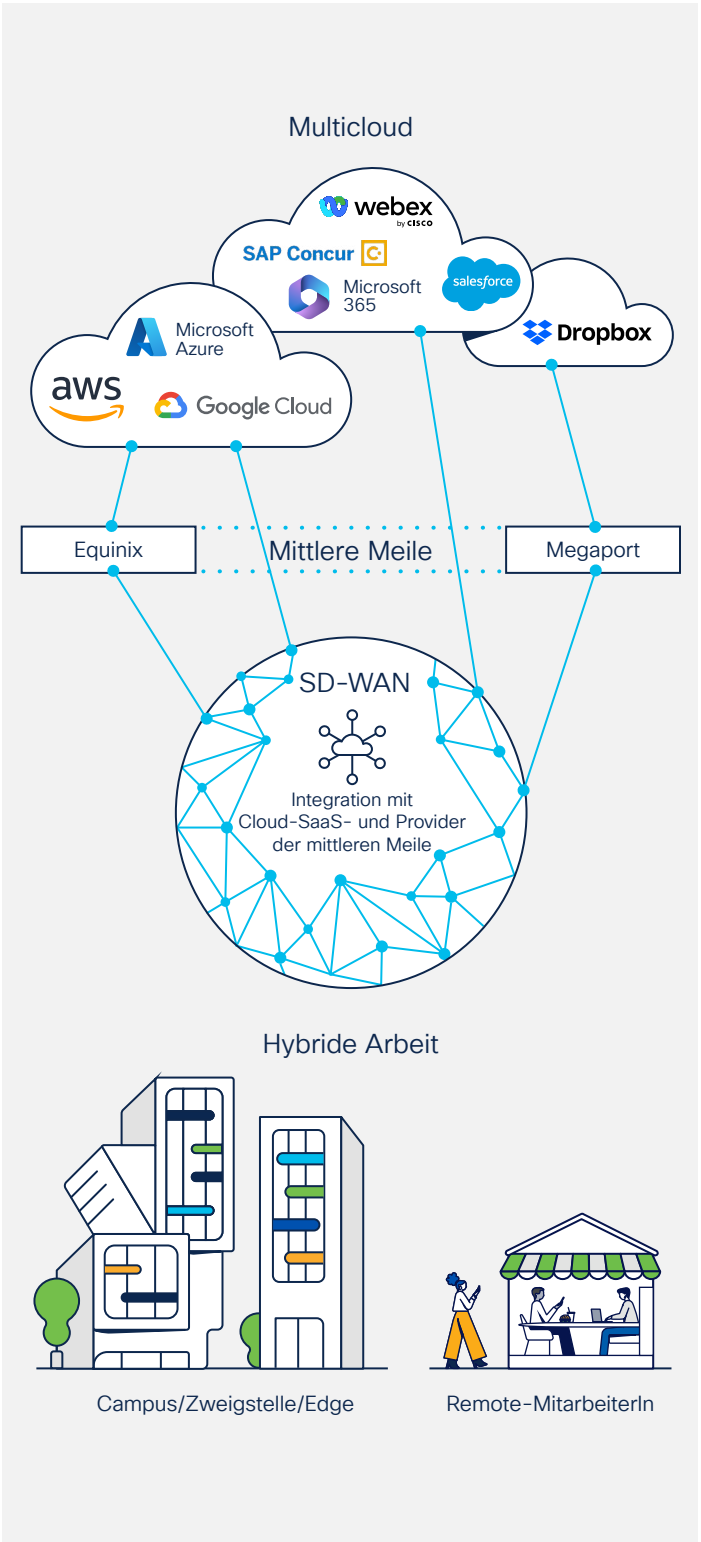


Abbildung 5: SD-WAN-Integrationen mit IaaS-, SaaS- und Providern der mittleren Meile sind für ein besseres IT- und Benutzererlebnis unerlässlich.

The bridge to possible

Fazit

SD-WAN-Multicloud-Integrationen sind entscheidend für jedes IT-Team, das Erweiterungen vom Unternehmen zu einer oder mehreren Clouds beschleunigen und vereinfachen, das Anwendungserlebnis für Benutzer optimieren und Cloud-Anwendungen mit Zero-Trust-Zugriff besser schützen möchte.

Mehr über SD-WAN erfahren

Fachmeinung

Wir können die Komplexität und die Risiken der Multicloud-Konnektivität nicht ignorieren.

„In der heutigen Cloud-orientierten Welt ist es unvorstellbar, eine SD-WAN-Lösung bereitzustellen, die über keine engen Integrationen mit führenden Cloud-, SaaS- und Providern der mittleren Meile verfügt. Kunden können ihre Cloud-Journey beschleunigen, indem sie die Erweiterung der SD-WAN-Fabric zwischen ihren globalen Standorten und Cloud-Workloads automatisieren und so von einem vereinfachten Netzwerkbetrieb, der Gewährleistung von End-to-End-Verschlüsselung und Flexibilität für schnelle Geschäftsinnovationen profitieren.

Darüber hinaus müssen Netzwerke angesichts der zunehmenden und sich ständig weiterentwickelnden Bedrohungslandschaft im Zusammenhang mit der Nutzung verteilter Cloud- und SaaS-Anwendungen einen Zero-Trust-Ansatz und dessen Kernprinzipien verfolgen: ‚niemals von Vertrauenswürdigkeit ausgehen, immer verifizieren und den Zugriff mit geringstmöglichen Berechtigungen durchsetzen‘. Durch die Integration von SD-WAN in einen Zero-Trust-Ansatz können Unternehmen einen Sicherheitsstatus schaffen, der kontrolliert, wer auf welche Cloud-Services zugreifen kann, automatisierte Sicherheitskontrollen für den zugelassenen Datenverkehr bereitstellt, eine kontinuierliche Durchsetzung ermöglicht und eine sofortige Anpassung an Änderungen des Sicherheitsstatus bietet.“

JL Valente
VP, Product Management, Enterprise Routing, SD-WAN and Cloud Networking
Cisco

Orientierungshilfe Nr. 4 Steigen Sie um auf Cloud-zentrierte Sicherheit und schaffen Sie konsistente Betriebsabläufe und Richtlinien.

Durch die Kombination verschiedener Sicherheitsbereiche in einer Cloud-Plattform werden Transparenz, Richtlinienverwaltung und -kontrolle einfacher, umfassender und effektiver gestaltet.

Da die hybride Arbeit so weit verbreitet ist, nutzen MitarbeiterInnen zunehmend sowohl unternehmenseigene als auch private Geräte sowie Anwendungen aus verwalteten und nicht verwalteten Netzwerken innerhalb und außerhalb des Unternehmensnetzwerks. Herkömmliche Perimetersicherheit ist dafür nicht mehr ausreichend. Die Sicherheit aller Endpunkte, Anwendungen und Daten muss für die IT also oberste Priorität haben.

Traditionell unterscheiden sich die Sicherheitsrichtlinien für Remote-Mitarbeitende von Beschäftigten vor Ort. Remote-Sicherheitsrichtlinien haben unterschiedliche Vertrauensstufen und werden von separaten Sicherheitstools verwaltet. Die Unterstützung eigener Richtlinien erhöht den IT-Aufwand und kann EndbenutzerInnen frustrieren. Auf die Frage nach Sicherheitsrichtlinien in der Studie gaben 45 % der Befragten an, dass eine konsistente, robuste Sicherheitsrichtlinie die größte Herausforderung bei der Bereitstellung eines sicheren Multicloud-Zugriffs von verteilten Standorten aus darstellt.

Sicherheitsteams müssen nicht nur eine unermüdliche Flut von Cyberbedrohungen bewältigen, sondern auch Sicherheitsrichtlinien regelmäßig aktualisieren. Die Notwendigkeit konsistenter Aktualisierungen von Anwendungssicherheitsrichtlinien für verteilte Belegschaften ist ein wichtiger Faktor für die Zentralisierung der Sicherheit. Dies bestätigen 59 % der Befragten, die außerdem angeben, dass sie die Zentralisierung von Cloud-Sicherheit als eine der wichtigsten Cloud-Access-Netzwerkinitiativen in den nächsten 24 Monaten priorisieren (Abbildung 6).

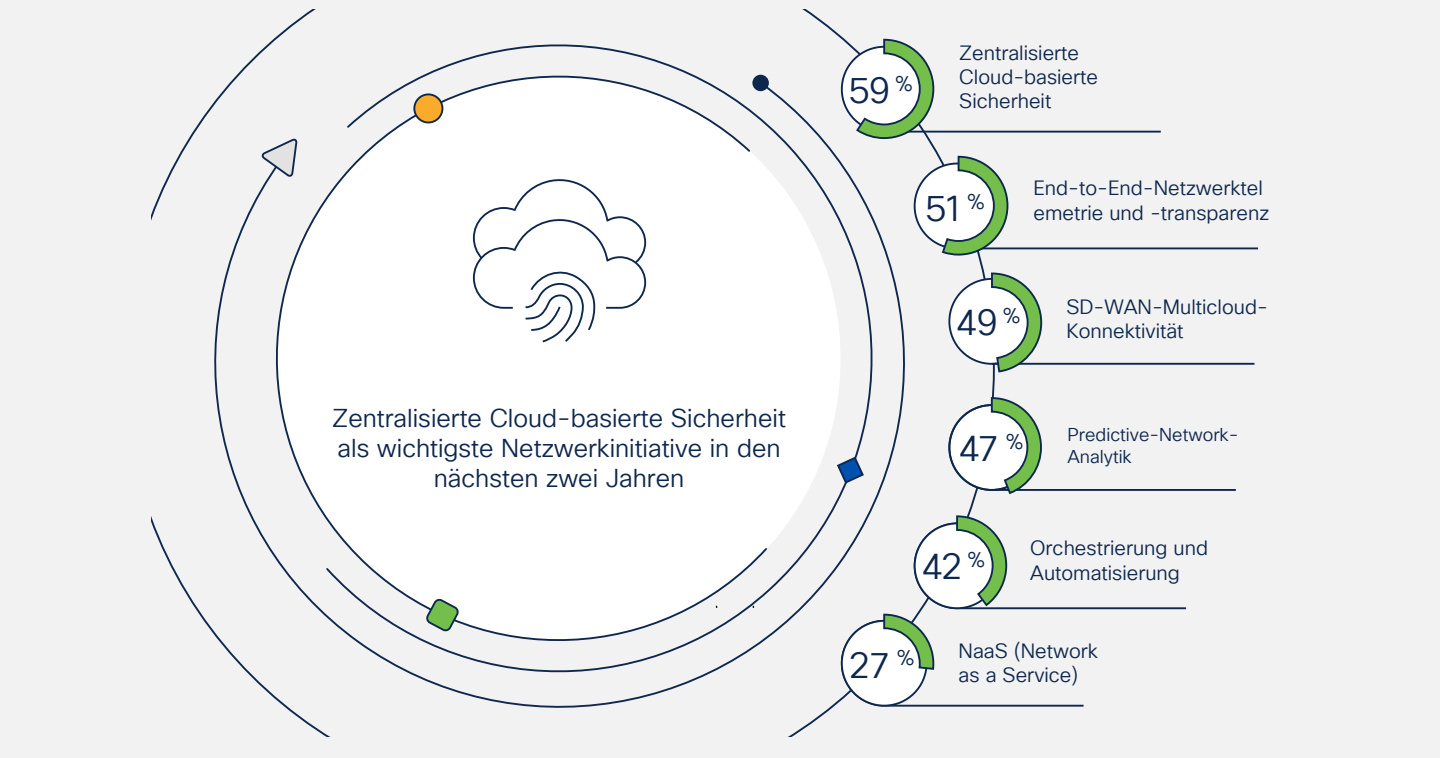


Abbildung 6: Die wichtigsten Netzwerkinitiativen für den Cloud-Zugriff in den nächsten 24 Monaten.

The bridge to possible

Herkömmliche Abwehrmechanismen am Perimeter sind allein nicht mehr effektiv. Als Teil einer zentralisierten Cloud-Sicherheitslösung ist eine intelligentere Möglichkeit erforderlich, um den skalierten Zugriff auf Anwendungen und Workloads zu sichern. Hier kommt SSE ins Spiel – eine zentrale Säule von SASE.

Fazit

Durch standortunabhängige Arbeitsmodelle, BYOD und die Verbreitung von Cloud-Services sind einst klar definierte Sicherheitsperimeter heute veraltet. Da sich viele der täglich genutzten Anwendungen in der Cloud befinden, ist es für Unternehmen sinnvoll, eine umfassende SSE-Strategie zu entwickeln, die mehrere Sicherheitsfunktionen konsolidiert und effektiv aus der Cloud heraus bereitstellt.

Fachmeinung

Cloud-Security-Konvergenz ist der Schlüssel zu einem zentralisierten und integrierten Modell.

„Jahrelang haben Unternehmen punktuelle Sicherheitsprodukte hinzugefügt, um auf immer größere Bedrohungen zu reagieren. So wurde die Sicherheit zwar verbessert, doch in letzter Zeit überwiegt dadurch die extrem ansteigende betriebliche Komplexität. Durch den Wechsel zu einer SSE-Lösung entsteht ein konvergenter Satz skalierbarer, Cloud-nativer Sicherheitsbereiche – Secure Web Gateway, Cloud Access Security Broker, Zero Trust Network Access und Firewall-as-a-Service –, der EndbenutzerInnen ein besseres Erlebnis und bessere Sicherheitsergebnisse bietet und IT-Teams entlastet.

Durch die Wahl dieses integrierten und zentralisierten Ansatzes können Sie die Vereinfachung von Verwaltungsaufgaben erzielen, die Leistung einfach skalieren, umfassende Transparenz erhalten und robuste Sicherheit im gesamten Unternehmen erreichen. Eine konvergente SSE-Lösung ist für eine vollständige SASE-Architektur unerlässlich. “

Jeff Scheaffer
VP, Product Management, Security/SSE
Cisco

The bridge to possible

Orientierungshilfe Nr. 5: Erzielen Sie durch End-to-End-Netzwerktransparenz ein konsistentes Benutzererlebnis in der immer komplexeren digitalen Servicebereitstellungskette.

Ohne die Transparenz über das eigene Netzwerk hinaus auf das Internet und Cloud-Umgebungen auszudehnen, können IT-Teams kein konsistentes, hochwertiges Benutzererlebnis für Cloud-basierte Anwendungen und Services sicherstellen.

Die Verbesserung der Benutzerfreundlichkeit ist ein wichtiges Ziel für die IT. Für ein optimales Benutzererlebnis blicken Netzwerkteams über herkömmliche Tools hinaus und übernehmen Lösungen, die in Echtzeit die Transparenz von Ereignissen innerhalb und außerhalb ihrer eigenen Netzwerke erhöhen. Durch die Korrelation dieser erweiterten Kennzahlen mit der Anwendungsleistung kann die IT die daraus resultierenden Erkenntnisse nutzen, um das digitale Erlebnis für alle Mitarbeitenden und Kunden zu optimieren.

Unternehmen beschleunigen ihre Einführung von SaaS- und Cloud-Lösungen immer weiter und erhöhen dabei die Nutzung öffentlicher Netzwerke wie dem Internet für den Zugriff auf diese Anwendungen. Da diese Multi-Hop-Netzwerke selbst immer komplexer werden, ist es unverzichtbar, in fortschrittliche Transparenzlösungen zu investieren. Mehr als die Hälfte der Befragten (51 %) erkennen dies als oberste Priorität an und konzentrieren sich auf End-to-End-Netzwerktelemetrie und Transparenz als wichtige Netzwerkinitiativen.

Jede Anwendungstransaktion kann mehrere Netzwerke, Netzwerksegmente und Services durchlaufen (Abbildung 7). Dies macht es schwierig, die Performance und Verfügbarkeit einer bestimmten Anwendung nachzuverfolgen. Fast die Hälfte (48 %) der Befragten erkennt die Notwendigkeit an, die Transparenz und Einblicke im Internet zu priorisieren, um die Konnektivität zu verbessern. Dies unterstreicht die Notwendigkeit von Tools, die der IT dabei helfen, den gesamten Transaktionspfad einzusehen und zu visualisieren, einschließlich externer Netzwerke und Umgebungen, die sie nicht selbst besitzen oder kontrollieren.

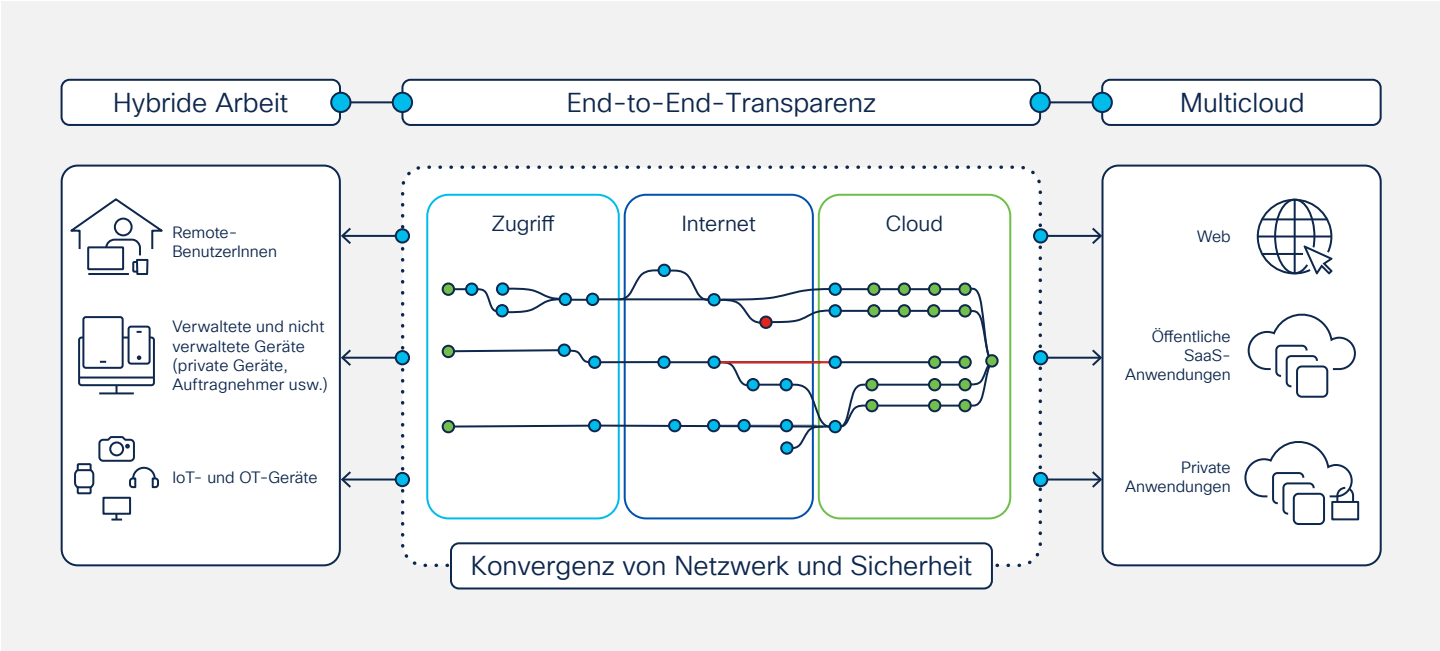


Abbildung 7: Die zunehmende Komplexität der Vernetzung verteilter Umgebungen über das Internet erfordert eine bessere End-to-End-Transparenz.

The bridge to possible

Fazit

Die Cloud ist das neue Rechenzentrum. Das Internet ist das neue Netzwerk. Und Cloud-Angebote dominieren Anwendungen. Indem sie einen Überblick über die globale Internetintegrität und die Leistung der wichtigsten SaaS-Anwendungen erhalten, können IT-Teams wichtige unerwartete Netzwerk- oder Anwendungsprobleme, die sich auf sie auswirken, proaktiv erkennen und beheben, sobald sie auftreten.

Fachmeinung

Betrachten Sie das Internet als neues Kernstück Ihrer Infrastruktur.

„Die Lieferketten für das digitale Erlebnis haben sich von einer einzigen Domäne zu kollaborativen Systemen und Netzwerken mehrerer Anbieter entwickelt. BenutzerInnen können von überall aus zugreifen. Anwendungen sind auf Flexibilität ausgelegt und basieren auf APIs und verteilten Mikroservices. Unternehmen müssen ein nahtloses Erlebnis über viele Anwendungen, Services, Clouds und Netzwerke hinweg ermöglichen – und das mit weniger Kontrolle als je zuvor.

Daher erfordern moderne digitale Erlebnisse einen anderen Ansatz für Transparenz und Sicherheit – einen Ansatz, mit dem Teams Störungen schnell erkennen und diagnostizieren können und ihre Erkenntnisse mit Infrastruktur- und Netzwerkproblemen verknüpfen können – und zwar unabhängig von der Domäne: zu Hause, im Büro, in der Cloud oder im Internet. Dies erfordert den Zugriff auf die richtigen Daten zum richtigen Zeitpunkt und die Möglichkeit, diese Daten intern über den Anwendungs-, Netzwerk- und Infrastrukturbetrieb hinweg und gemeinsam mit Drittanbietern innerhalb des vernetzten Ecosystems einfach zu erfassen und zu korrelieren.“

Joe Vaccaro
VP, Product Management
ThousandEyes, Cisco

The bridge to possible

Orientierungshilfe Nr. 6: Wechseln Sie von reaktiven zu prädiktiven Betriebsabläufen, um Verfügbarkeit und Performance zu verbessern.

Prädiktive Analysen werden zunehmend als wichtiger Bestandteil eines AIOps-Toolkits (Artificial Intelligence for IT Operations) für einfachere, schnellere und effektivere IT-Betriebsabläufe anerkannt.

Da das erweiterte Netzwerk entscheidend für die Geschäftsabläufe in Unternehmen ist, sind Beeinträchtigungen der Services oder Ausfallzeiten untragbar. IT-Verantwortliche möchten Probleme bereits proaktiv identifizieren und beheben, bevor sie auftreten und das Benutzererlebnis beeinträchtigen.

Mit der Einführung von Cloud-basierten Managementplattformen haben Unternehmen besseren Zugriff auf Echtzeit- und historische Telemetriedaten aus mehr Quellen als je zuvor. Jüngste Fortschritte bei prädiktiven analytischen Modellen mit künstlicher Intelligenz und Machine Learning (KI/ML) können auf Basis all dieser historischen und Echtzeitdaten aussagekräftige Intelligence ableiten. Auf diese Weise können Unternehmen Muster rund um die Daten verstehen und Probleme präzise prognostizieren und beheben, bevor sie sich auf das Netzwerk auswirken. Diese Modelle werden im Laufe der Zeit intelligenter, da sie aus den Daten lernen, die sie über eine kontinuierliche Feedback-Schleife erhalten,.

47 % der Befragten berichten, dass sie die Einführung prädiktiver Netzwerkanalysen priorisieren, um die Cloud-Konnektivität in den nächsten zwei Jahren zu verbessern.

Proaktive IT-Abläufe werden besonders wichtig für die Bereitstellung konsistenter, leistungsstarker Services für verteilte BenutzerInnen, die auf verteilte Cloud-Anwendungen zugreifen. Die Befragten sehen dies als wichtige zukünftige Richtung: 47 % geben an, dass sie die Einführung prädiktiver Netzwerkanalysen priorisieren, um die Cloud-Konnektivität in den nächsten zwei Jahren zu verbessern.

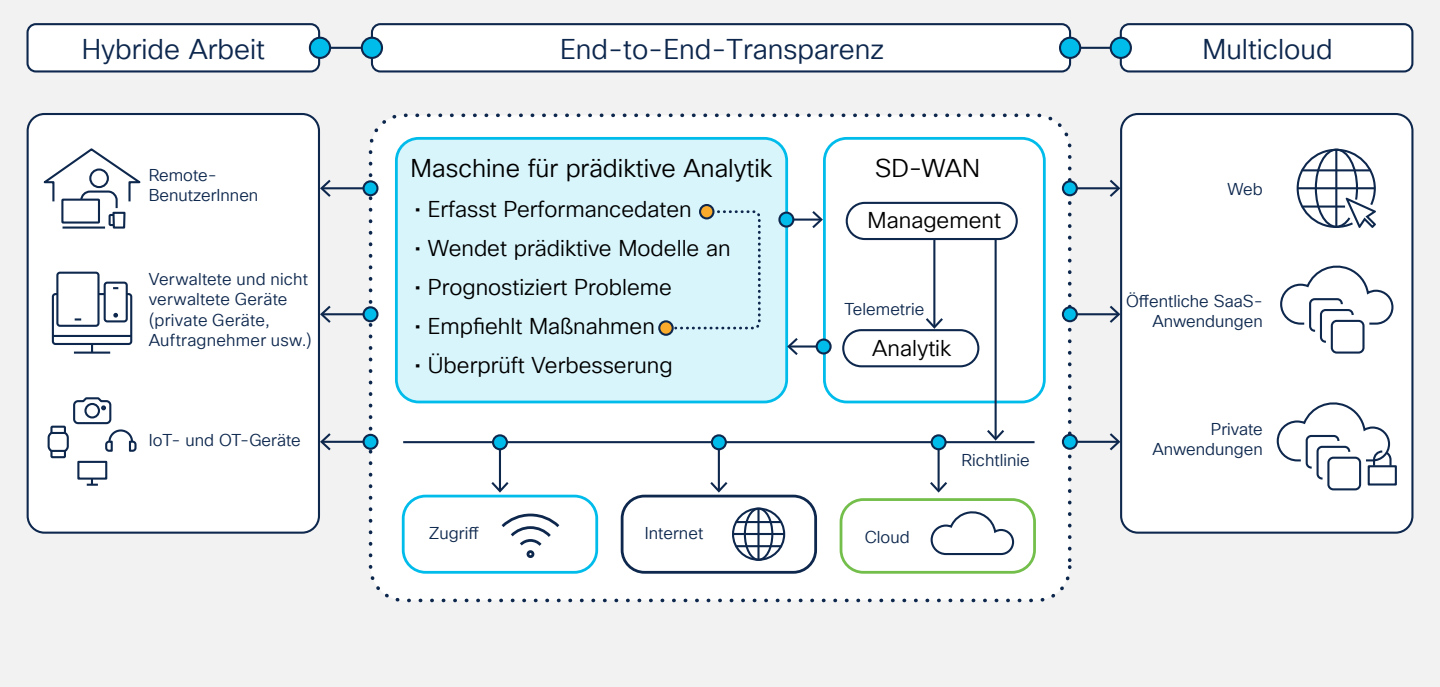


Abbildung 8: Integrieren Sie prädiktive Analysen in das SD-WAN-Management, um Netzwerkverschlechterungen zu identifizieren und verhindern, bevor sie sich auf das Benutzererlebnis auswirken.

The bridge to possible

Fazit

Während sich das Internet verändert und weiterentwickelt, müssen Geschwindigkeit, Qualität und Kosten digitaler Erlebnisse in der Waage gehalten werden. Unternehmen müssen prädiktive Modi und proaktive Betriebsabläufe einführen, die sich im Laufe der Zeit durch kontinuierliche Daten-Feedback-Schleifen optimieren und eine höhere Elastizität und Ausfallsicherheit der Infrastruktur gewährleisten.

Fachmeinung

Prädiktive Analysen wurden entwickelt, weil IT-Teams sie benötigen, und die Technologie ist jetzt in der Lage, sie umfassend bereitzustellen.

„Herkömmliche reaktive Betriebsmodi leiten den Datenverkehr auf alternative Pfade um – allerdings erst nach der Erkennung eines Problems, welches häufig durch Verbindungsprobleme oder beeinträchtigte Services verursacht wird. Das große Potenzial der prädiktiven Analysen ist, dass sie Telemetrie, statistische Daten und KI-/ML-basierte Computing-Modelle verwenden, um potenzielle Probleme bereits vorherzusagen, bevor sie auftreten. Cloud-orientierte Umgebungen sind von Natur aus unberechenbar. Die Möglichkeit, Maßnahmen automatisch zu empfehlen oder Datenverkehr proaktiv umzuleiten, ist der Schlüssel zur Optimierung der Leistung und zur Minimierung des Risikos von Systemausfällen. Davon profitieren Unternehmen, indem sie die Benutzerfreundlichkeit verbessern und die IT in die Lage versetzen, sich auf strategische Initiativen statt auf reaktive Vorselektierung zu konzentrieren.“

Murtaza Doctor
VP, Engineering
ThousandEyes, Cisco

The bridge to possible

Abschließendes Fazit

Sowohl Remote- als auch Hybrid-Arbeit werden fester Bestandteil unserer Zukunft sein. Auch Multicloud-Konzepte finden immer mehr Zuspruch. Doch die Bereitstellung sicherer, konsistenter Konnektivität für hochgradig verteilte MitarbeiterInnen, Geräte und Anwendungen bleibt aufgrund der wachsenden Bedrohungslandschaft und der Komplexität von Tools und Techniken in Netzwerk-, Cloud- und Sicherheitsteams eine Herausforderung.

Allein können IT-Teams weder diese Netzwerk- und Sicherheitsherausforderungen bewältigen noch die digitale Erfahrung und Flexibilität liefern, die Unternehmen benötigen, um im Wettbewerb zu bestehen. Die meisten IT-Verantwortlichen verstehen das. Sie bringen Netzwerk-, Cloud- und Sicherheitstechnologie proaktiv zusammen und testen innovative Betriebsmodelle, um diesen sich dynamisch verändernden Anforderungen gerecht zu werden.

Ein vielversprechender Ansatz ist der Wechsel zu SASE: Fast die Hälfte unserer Befragten plant, innerhalb der nächsten zwei Jahre eine gut integrierte SASE-Architektur für die Verbindung ihrer Zweigstellen und Remote-Clients bereitzustellen. Der Leistungsumfang von SASE verspricht ein einfacheres und sichereres IT-Erlebnis, das auf der vereinfachten und flexibleren Möglichkeit aufbaut, verteilte MitarbeiterInnen und Kunden sicher und bei maximaler Skalierbarkeit mit Cloud-Anwendungen zu verbinden. Die Kombination aus Netzwerk- und Sicherheitsplattformen, die Cloud-basierte Automatisierung und Netzwerkeinblicke unterstützen, ermöglicht stärker integrierte Workflows und eine bessere Zusammenarbeit zwischen NetOps- und SecOps-Teams.

Ein Cloud-orientiertes SASE-Modell nutzt das Potenzial von Daten, um Funktionen wie End-to-End-Transparenz und prädiktive Analysen bereitzustellen, die für ein konsistentes Benutzererlebnis entscheidend sind.

Abhängig von Ihren geschäftlichen und technologischen Prioritäten gibt es mehrere Möglichkeiten, um Ihre SASE-Journey zu beginnen.

Erfahren Sie mehr über SASE und wie Cisco Sie auf Ihrem Weg unterstützen kann.

The bridge to possible

Über diesen Bericht

Der Global Networking Trends Report wurde im Februar 2023 erstellt und basiert auf Umfragen in 13 Ländern in Nord-, Mittel- und Südamerika, im Asien-Pazifik-Raum und in Westeuropa.

Der diesjährige Bericht umfasst Umfragedaten von Netzwerkbetriebsfachleuten aus Unternehmen, die Cloud-Services nutzen. Bei der Berichterstellung wurden Umfragedaten verwendet, um Einblicke darin zu bieten, wie Multicloud-Umgebungen die Netzwerktechnologie und die Prioritäten, Präferenzen und Auswahlmöglichkeiten für den Unternehmensbetrieb beeinflussen.

Die in diesem Bericht zitierten Umfrageinhalte wurden von Cisco in Auftrag gegeben, durch 451 Research, einem Teil von S&P Global Market Intelligence, gesammelt und von Cisco analysiert. Sie sind Teil einer unabhängigen Web-Umfrage unter mehr als 2.500 globalen IT-EntscheidungsträgerInnen und Fachleuten aus den Bereichen Cloud-Computing, DevOps und Unternehmensnetzwerke.

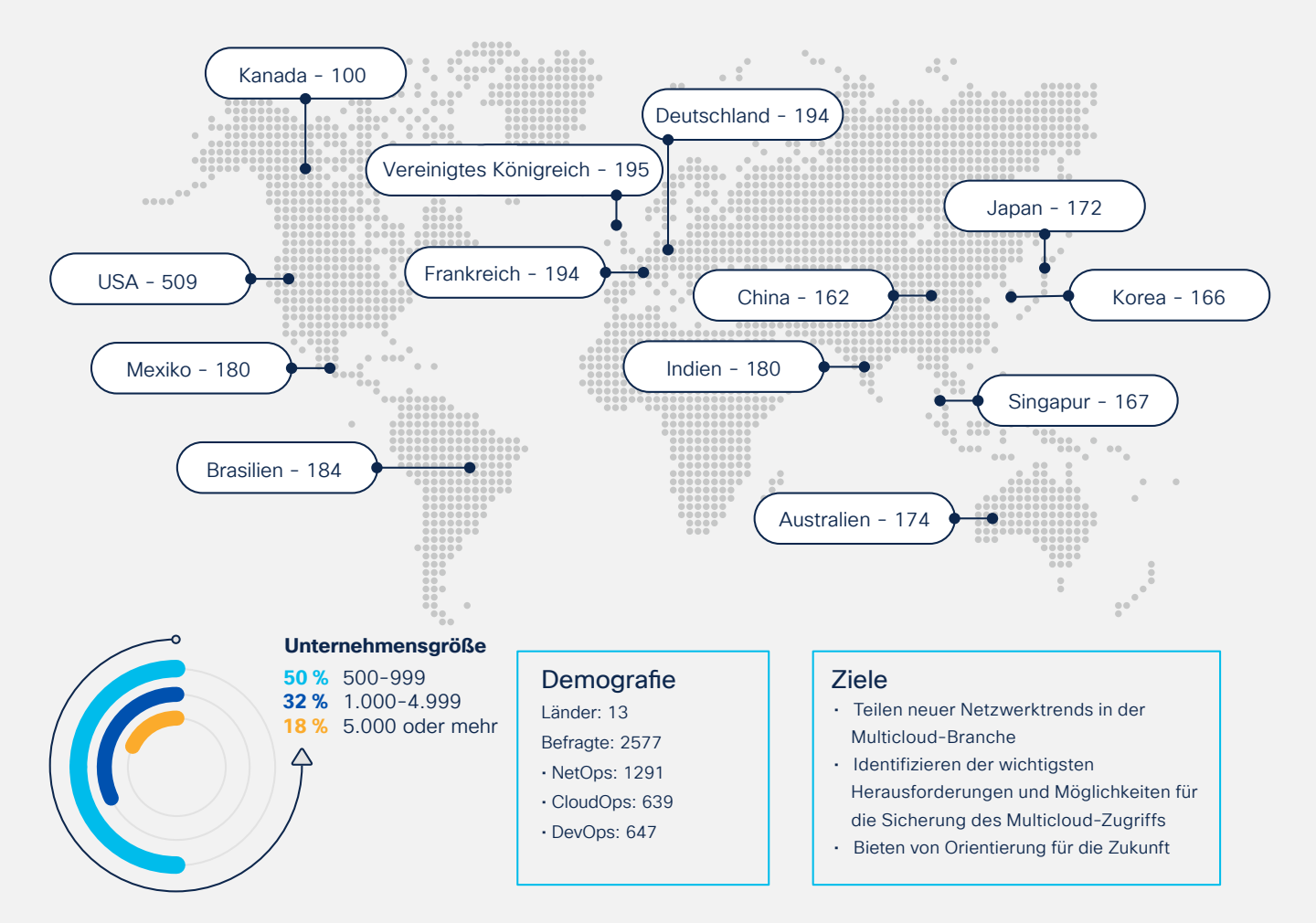


Abbildung 9: Cisco Global Networking Trends Report 2023 – Umfragemethoden und Ziele