Aktueller Stand bei SD-WAN, SASE und Zero-Trust-Sicherheitsarchitekturen

Gesponsert von Aruba

Unabhängig durchgeführt von Ponemon Institute LLC

Veröffentlichung: April 2021

Aktueller Stand bei SD-WAN, SASE und Zero-Trust-Sicherheitsarchitekturen

Präsentiert von Ponemon Institute, April 2021

Teil 1. Einführung

Mit dieser Studie sollen wichtige Informationen zur Nutzung von Software-defined Networking in Wide Area Networks (SD-WANs), Secure Access Service Edge (SASE) und Zero-Trust-Architekturen gewonnen werden. Das Ponemon Institute wurde von Aruba gesponsert und befragte 1.826 Sicherheits- und Netzwerkspezialisten in Nord- sowie Lateinamerika, der EMEA- sowie LATAM-Region und im asiatisch-pazifischen Raum. In Rahmen dieser Studie werden diese Technologien folgendermaßen definiert.

- **SD-WAN** vereinfacht die Verwaltung und den Betrieb eines Wide Area Networks (WANs), indem die Netzwerkhardware vom Steuerungsmechanismus entkoppelt und die Transportdienste virtualisiert werden.

- **SASE und Zero-Trust** sind Sicherheitsarchitekturen, die zur Implementierung von Sicherheitskontrollen verwendet werden.

Nachfolgend sind die Ergebnisse aufgeführt, die den aktuellen Stand der Akzeptanz und Implementierung dieser Technologien aufzeigen.

- **Die Auswahl einer marktführenden SASE-Architektur wird bevorzugt.** 71 Prozent der Befragten würden sich bei der Bereitstellung von SD-WAN und cloudbasierter Sicherheit für eine SASE-Architektur für den besten Anbieter entscheiden.

- **Organisationen, die der Meinung sind, dass ihre Sicherheitsarchitektur und -implementierung effektiv ist, sind führend bei der Einführung von Zero-Trust, SASE und SD-WAN.** In fast der Hälfte der leistungsstarken Organisationen (48 Prozent der Befragten) wurde die Bereitstellung von Zero-Trust bereits durchgeführt oder ist zumindest geplant – im Vergleich zu nur 35 Prozent aller Befragten. 43 Prozent der Befragten aus leistungsstarken Organisationen haben SASE bereits bereitgestellt oder haben es vor – im Gegensatz zu nur 24 Prozent aller Befragten.

- **Nordamerika führt bei der Bereitstellung von Zero-Trust, SD-WAN und SASE.** 43 Prozent der nordamerikanischen Befragten stellen bereits Zero-Trust bereits bereit – gegenüber 33 Prozent in der EMEA-Region, 31 Prozent im asiatisch-pazifischen Raum und 26 Prozent in Lateinamerika. Laut diesem Bericht treffen ähnliche Zahlen auf die Bereitstellung von SD-WAN und SASE zu.

- **Die Zero-Trust-Sicherheitsarchitektur ist bekannter als SD-WAN und SASE.** 62 Prozent der Befragten sind mit Zero-Trust vertraut oder sehr vertraut. Es folgt die Vertrautheit mit der SASE-Sicherheitsarchitektur (45 Prozent der Befragten).

- **Eine steigende Annahme von Zero-Trust- und SASE-Architekturen ist zu erwarten.** 57 Prozent der Befragten geben an, dass in ihren Organisationen entweder Zero-Trust bereitstellt wird oder werden soll, 49 Prozent der Befragten sagen, dass in ihren Organisationen SASE-Architekturen bereitstellt werden oder werden sollen.

- **Das Netzwerkteam hat den größten Einfluss auf die Bereitstellung von SD-WAN.** 46 Prozent der Befragten geben an, dass das Netzwerkteam den größten Einfluss auf die Bereitstellung von SD-WAN-Lösungen hat, wobei das Sicherheitsteam beratend zur Seite steht. 37 Prozent der Befragten geben an, dass das Sicherheitsteam die Bereitstellung mit Beratung durch das Netzwerkteam leitet.

- **Wie würden Organisationen einen Anbieter beauftragen, wenn sie in der Cloud bereitgestellte Sicherheitsdienste wie eine cloudbasierte Firewall-as-a-Service oder**

einen CASB implementieren würden? 44 Prozent der Befragten geben an, dass in ihren Organisationen führende Anbieter genutzt werden würden, deren Fokus auf cloudbasierten Sicherheitsdiensten liegt.

Teil 2. Wesentliche Ergebnisse

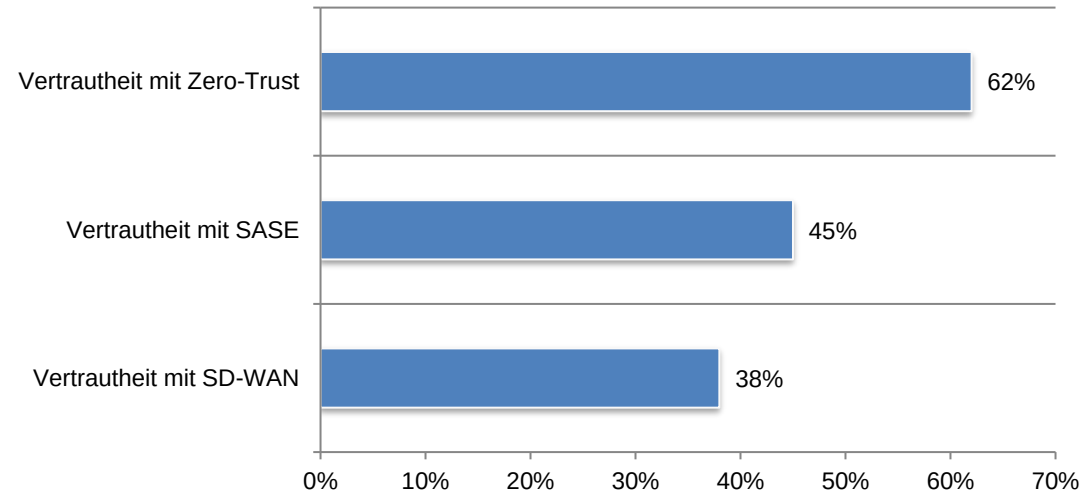
In diesem Abschnitt finden Sie eine Analyse der Forschungsergebnisse. Die vollständig geprüften Ergebnisse sind im Anhang dieses Berichts dargestellt. Folgende Themen werden in diesem Bericht behandelt.

- Vertrautheit mit und Bereitstellung von SD-WAN, cloudbasierter Sicherheit, SASE-Architektur und Zero-Trust-Sicherheitsarchitektur
- Regionale Unterschiede
- Die Vorgehensweisen von Organisationen mit hocheffektiver Sicherheitsarchitektur und -implementierung

Vertrautheit mit und Bereitstellung von SD-WAN, cloudbasierter Sicherheit, SASE-Architektur und Zero-Trust-Sicherheitsarchitektur

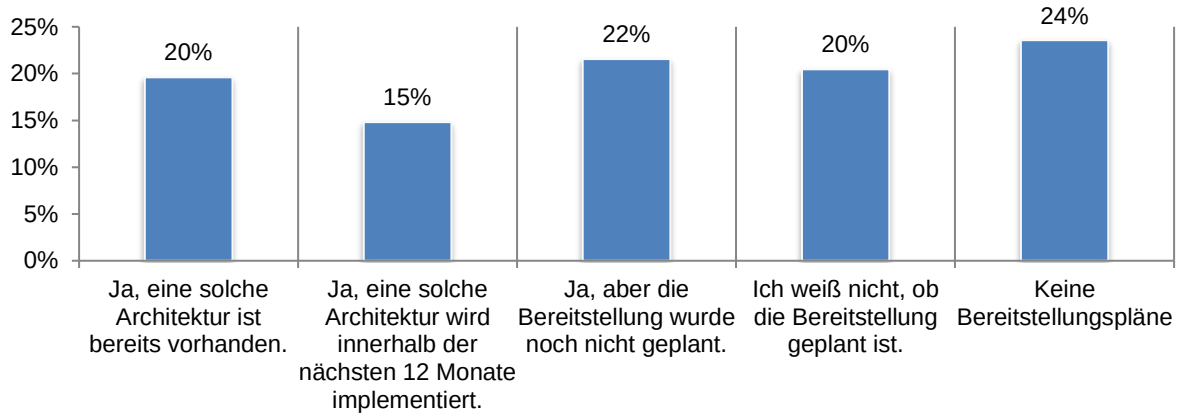
Die Zero-Trust-Sicherheitsarchitektur ist bekannter als SD-WAN und SASE. Wie in Abbildung 1 zu sehen ist, sind 62 Prozent der Befragten mit Zero-Trust vertraut oder sehr vertraut. Es folgt die Vertrautheit mit der SASE-Sicherheitsarchitektur (45 Prozent der Befragten). Nur 38 Prozent der Befragten geben an, dass sie mit SD-WAN-Lösungen vertraut oder sehr vertraut sind.

Abbildung 1. Vertrautheit mit Zero-Trust, SD-WAN und SASE
Angaben von „vertraut“ und „sehr vertraut“ wurden zusammengefasst.



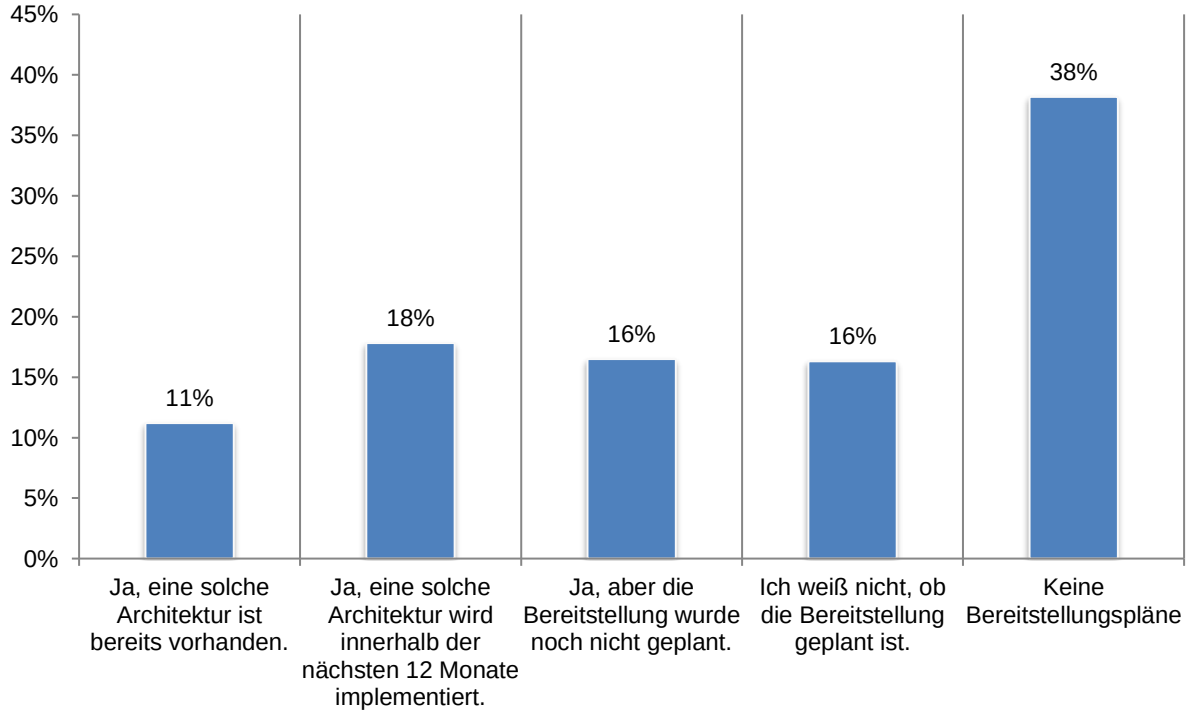
In der Mehrheit der Organisationen ist die Bereitstellung einer Zero-Trust-Sicherheitsarchitektur bereits vorhanden oder geplant. Laut Abbildung 2 geben dazu insgesamt 57 Prozent der Befragten Folgendes an: Zero-Trust wird bereits bereitgestellt (20 Prozent), Zero-Trust wird in den nächsten 12 Monaten implementiert (15 Prozent) oder die Bereitstellung von Zero-Trust ist für die Zukunft geplant (22 Prozent).

Abbildung 2. Ist die Bereitstellung einer Zero-Trust-Sicherheitsarchitektur in Ihrer Organisation bereits vorhanden oder geplant?



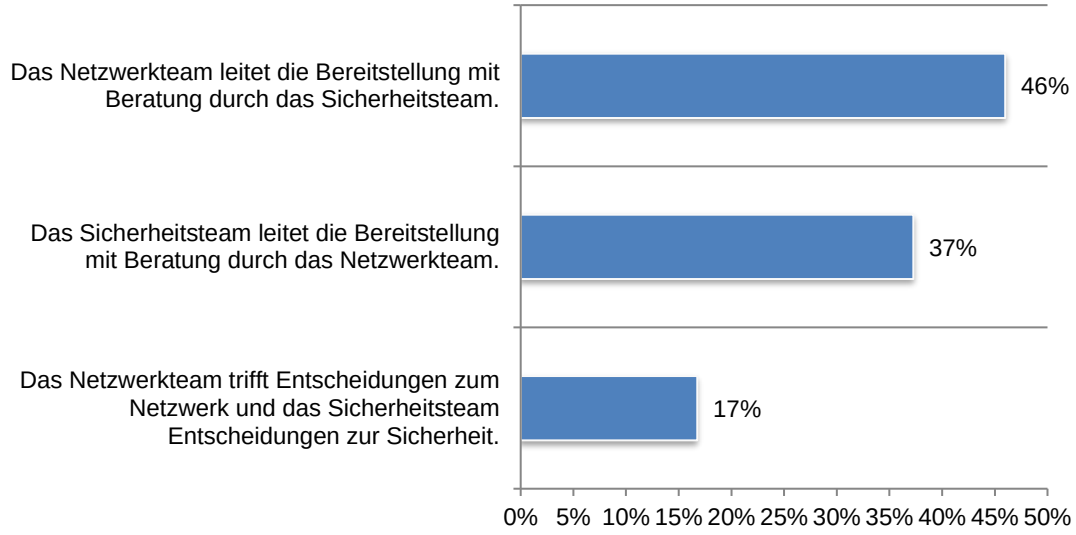
45 Prozent der Befragten geben an, dass in ihrer Organisation die Bereitstellung von SD-WAN-Lösungen bereits vorhanden oder geplant ist. Laut Abbildung 3 geben 11 Prozent der Befragten an, dass SD-WAN bereits bereitgestellt wird, 18 Prozent, dass es in den nächsten 12 Monaten bereitgestellt wird und 16 Prozent, dass die Bereitstellung für die Zukunft geplant ist.

Abbildung 3. Ist die Bereitstellung von SD-WAN-Lösungen in Ihrer Organisation bereits vorhanden oder geplant?



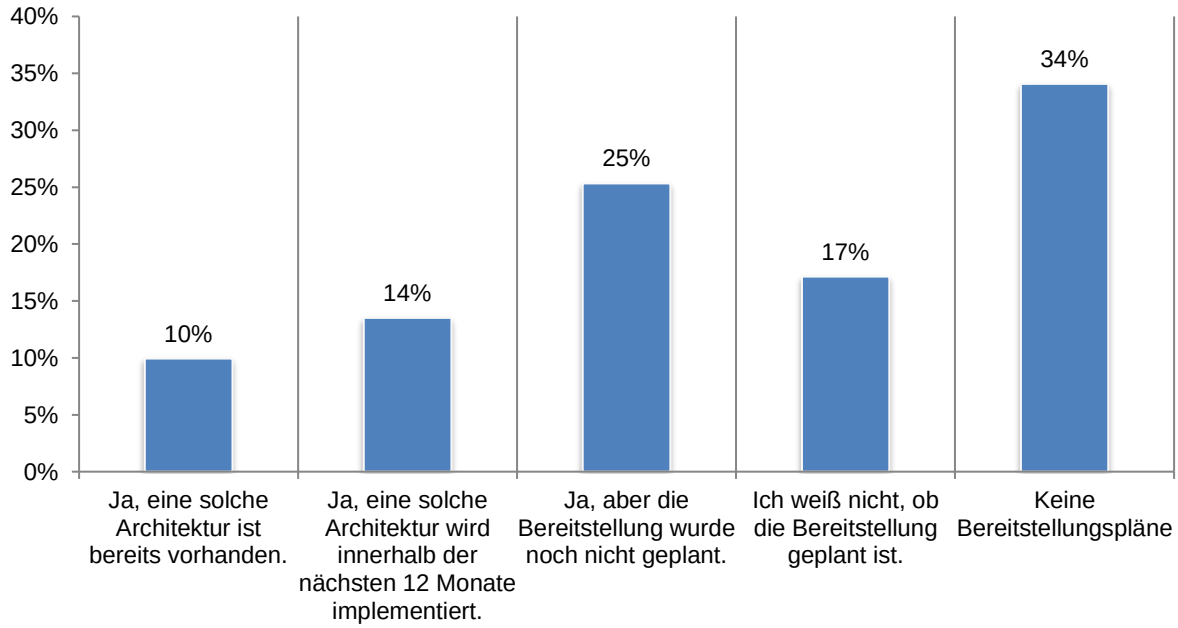
Das Netzwerkteam hat den größten Einfluss auf die Bereitstellung von SD-WAN-Lösungen. Wie in Abbildung 4 zu sehen ist, geben 46 Prozent der Befragten an, dass das Netzwerkteam den größten Einfluss hat, wobei das Sicherheitsteam beratend zur Seite steht. Nur 17 Prozent der Befragten sagen, dass das Netzwerkteam Entscheidungen zum Netzwerk und das Sicherheitsteam Entscheidungen zur Sicherheit trifft.

Abbildung 4. Wer hat bei der Bereitstellung von SD-WAN den größten Einfluss?



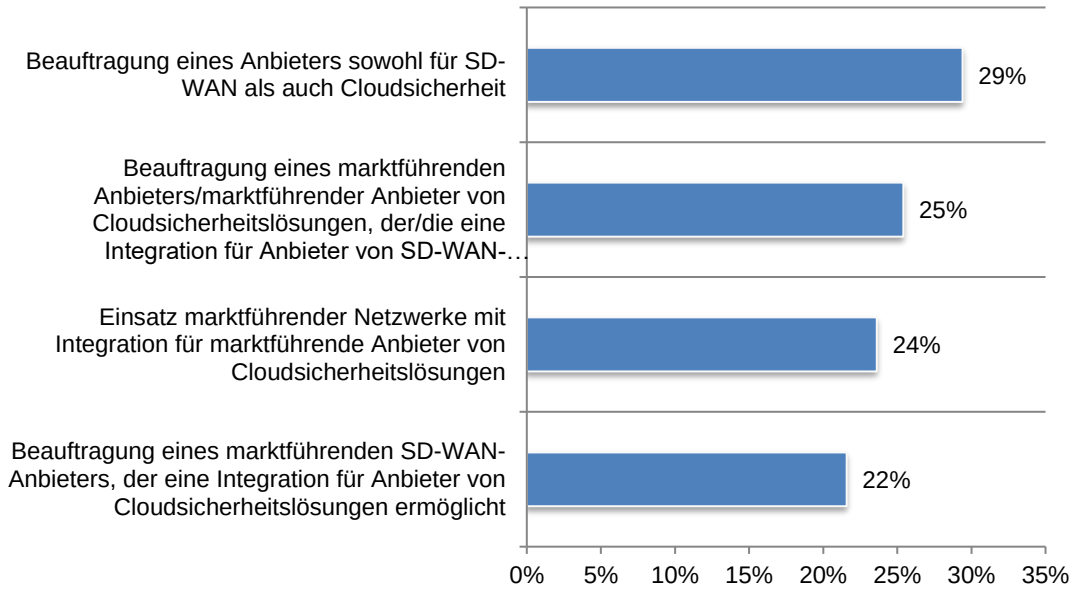
Fast die Hälfte der Befragten gibt an, dass in ihrer Organisation eine SASE-Sicherheitsarchitektur bereitgestellt wird oder werden soll. Laut Abbildung 5 geben dazu insgesamt 49 Prozent der Befragten Folgendes an: Eine SASE-Sicherheitsarchitektur wird bereits bereitgestellt (10 Prozent), eine SASE-Sicherheitsarchitektur wird in den nächsten 12 Monaten implementiert (14 Prozent) oder die Bereitstellung einer SASE-Sicherheitsarchitektur ist für die Zukunft geplant (25 Prozent).

Abbildung 5. Ist die Bereitstellung einer SASE-Sicherheitsarchitektur in Ihrer Organisation bereits vorhanden oder geplant?



Bei der Bereitstellung von SD-WAN und cloudbasierter Sicherheit für eine SASE-Architektur ist der beste Anbieter bevorzugt.. Wie zu sehen ist, geben insgesamt 71 Prozent der Befragten Folgenden dazu an: Ihre Organisation würde einen marktführenden Anbieter für Cloudsicherheit beauftragen, der eine Integration für SD-WAN-Anbieter ermöglicht (25 Prozent), einen marktführenden Netzwerkanbieter, der eine Integration für marktführende Anbieter von Cloudsicherheitslösungen ermöglicht (24 Prozent) und einen marktführenden SD-WAN-Anbieter, der eine Integration für Anbieter von Cloudsicherheitslösungen ermöglicht (22 Prozent).

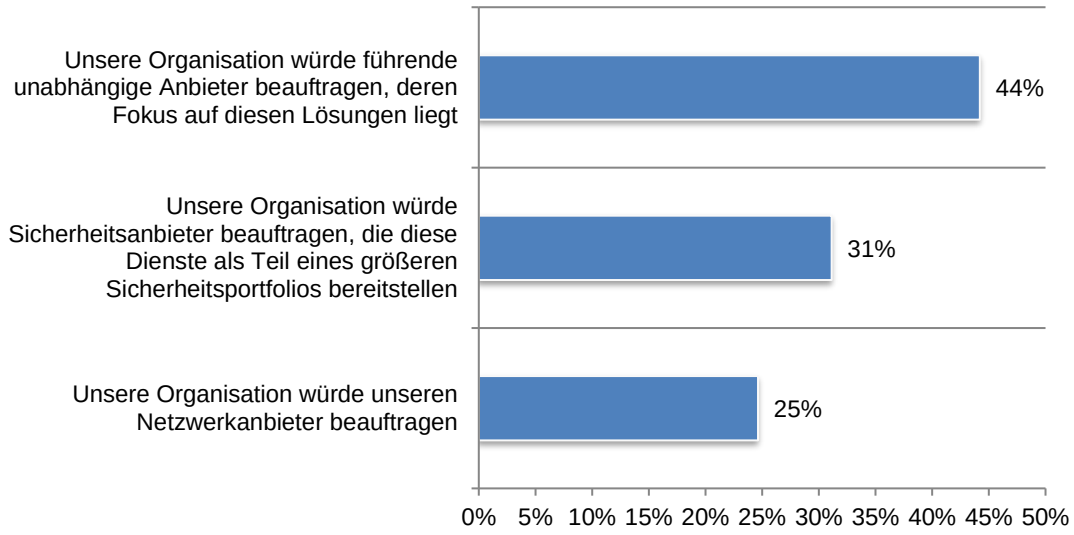
Abbildung 6. Wenn Ihre Organisation sowohl SD-WAN als auch cloudbasierte Sicherheit für eine SASE-Architektur einsetzt, wie würden die Anbieter ausgewählt?
Nur eine Auswahl zulässig



Das Netzwerkteam trifft am ehesten Entscheidungen für die Produkte einer Sicherheitsarchitektur. 42 Prozent der Befragten geben an, dass in ihrer Organisation das Netzwerkteam diese Entscheidungen trifft, gefolgt von 31 Prozent der Befragten, bei denen das Sicherheitsteam diese Aufgabe übernimmt, und schließlich 27 Prozent, die angeben, dass sowohl das Netzwerk- als auch das Sicherheitsteam die Entscheidungen über die Architektur/Produkte der Sicherheitslösung trifft.

In Abbildung 7 ist zu sehen, dass die Beauftragung eines Anbieters für die Implementierung von cloudbasierten Sicherheitsdiensten (z. B. cloudbasierte Firewall-as-a-Service, CASB) auf dem Wunsch basiert, führende unabhängige Anbieter beauftragen zu können, deren Fokus auf diesen Lösungen liegt (44 Prozent der Befragten), Sicherheitsanbieter, die diese Dienste als Teil eines größeren Sicherheitsportfolios bereitstellen (31 Prozent der Befragten) oder ihren Netzwerkanbieter damit beauftragen zu können (25 Prozent der Befragten).

Abbildung 7. Wie werden Entscheidungen zu den Anbietern bei der Implementierung von cloudbasierten Sicherheitsdiensten getroffen?

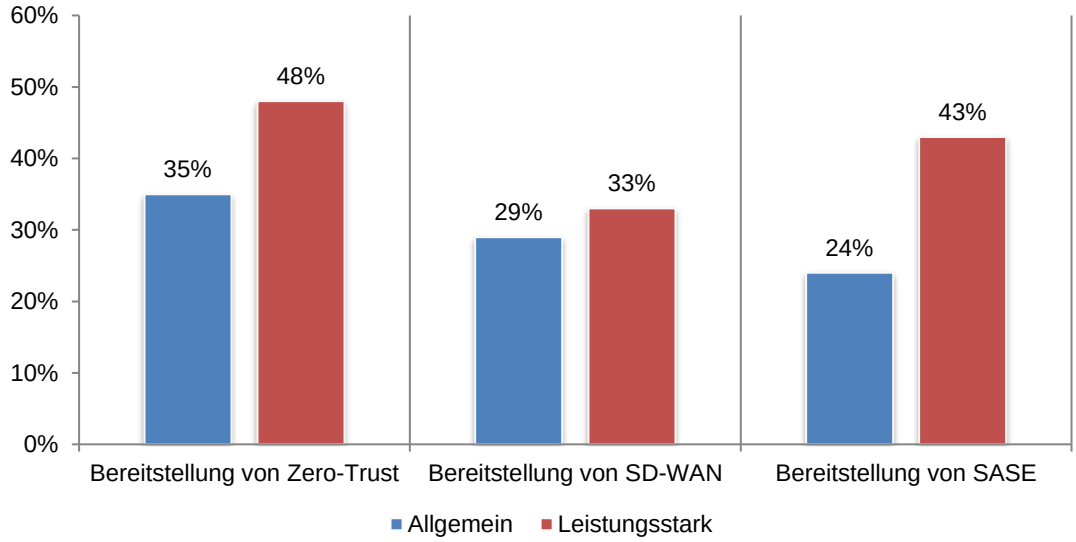


Die Vorgehensweisen von Organisationen mit hocheffektiver Sicherheitsarchitektur und -implementierung

In diesem Abschnitt finden Sie eine Analyse der Ergebnisse von Befragten, die nach eigenen Angaben sehr zuversichtlich sind, dass in ihrer Organisation eine effektive Sicherheitsarchitektur und Implementierung vorhanden ist (22 Prozent der Befragten). Diese Befragten werden von uns als „leistungsstarke Organisationen“ bezeichnet.

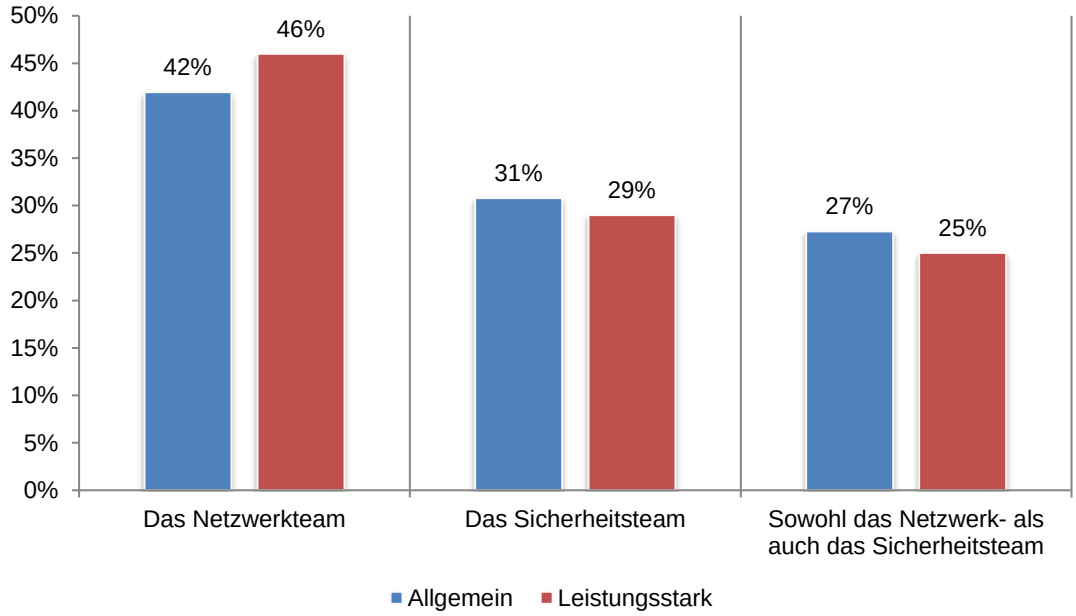
In leistungsstarken Organisationen ist es wahrscheinlicher, dass Zero-Trust, SD-WAN und SASE bereitgestellt werden. Laut Abbildung 8 wurde in fast der Hälfte der leistungsstarken Organisationen (48 Prozent der Befragten) die Bereitstellung von Zero-Trust bereits durchgeführt – im Vergleich zu nur 35 Prozent der Befragten aus der allgemeinen Auswahl. 43 Prozent der Befragten aus leistungsstarken Organisationen haben SASE bereits bereitgestellt – im Gegensatz zu nur 24 Prozent der Befragten aus der allgemeinen Auswahl.

Abbildung 8. Bereitstellung von Zero-Trust, SD-WAN und SASE
Angaben von „wird bereitgestellt“ und „wird innerhalb der nächsten 12 Monate bereitgestellt“ wurden zusammengefasst.



In leistungsstarken Organisationen wird etwas häufiger angegeben, dass das Netzwerkteam die Produktentscheidungen für die Architektur von Sicherheitslösungen trifft, wie in Abbildung 9 zu sehen ist.

Abbildung 9. Wer trifft die Produktentscheidungen für die Architektur von Sicherheitslösungen?

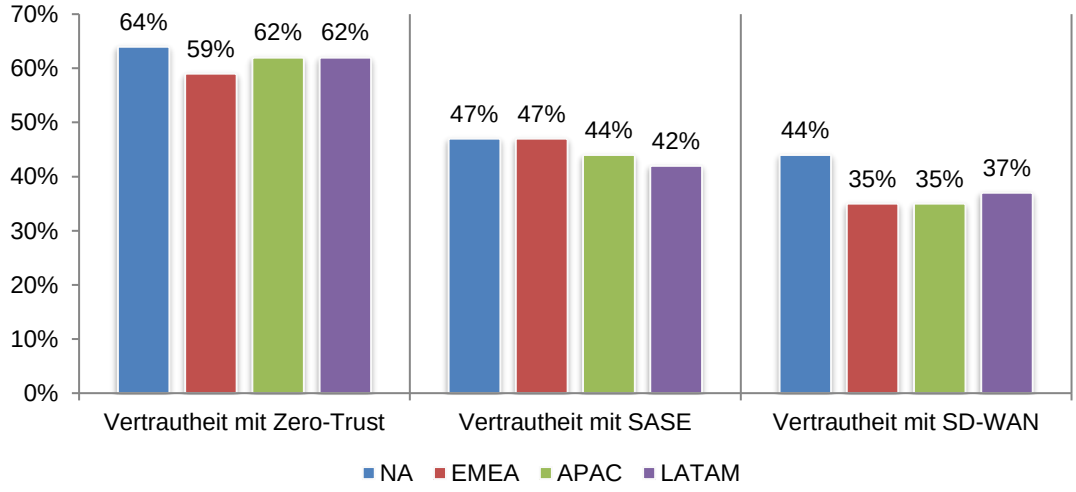


Regionale Unterschiede

In diesem Abschnitt präsentieren wir einen Vergleich zwischen den vier Regionen, die in dieser Studie vertreten sind: Nordamerika (598 Befragte), EMEA-Region (454 Befragte), asiatisch-pazifischer Raum (402 Befragte) und Lateinamerika (372 Befragte).

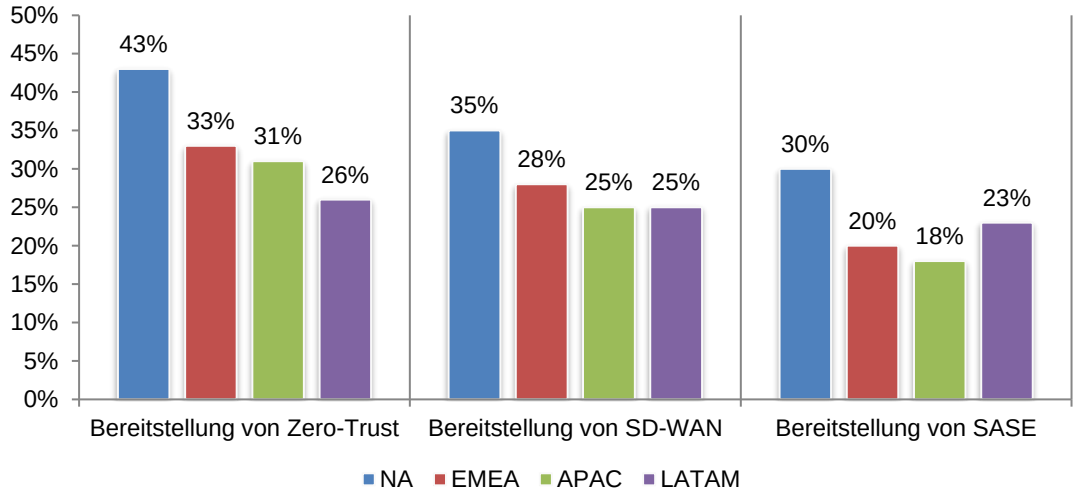
Die Zero-Trust-Sicherheitsarchitektur ist in allen Regionen bekannter als SD-WAN und SASE. Wie in Abbildung 10 zu sehen ist, sind die meisten Befragten aller Regionen mit Zero-Trust vertraut oder sehr vertraut. Befragte aus Nordamerika und der EMEA-Region sind mit SASE etwas vertrauter als die aus dem asiatisch-pazifischen Raum und Lateinamerika. Nordamerikanische Befragte sind am meisten mit SD-WAN vertraut (44 Prozent der Befragten).

Abbildung 10. Vertrautheit mit Zero-Trust, SD-WAN und SASE
Angaben von „vertraut“ und „sehr vertraut“ wurden zusammengefasst.



Die Bereitstellung von Zero-Trust, SD-WAN und SASE ist in Nordamerika am stärksten vertreten, wie aus Abbildung 11 hervorgeht.

Abbildung 11. Bereitstellung von Zero-Trust, SD-WAN und SASE
Angaben von „wird bereitgestellt“ und „wird innerhalb der nächsten 12 Monate bereitgestellt“ wurden zusammengefasst.



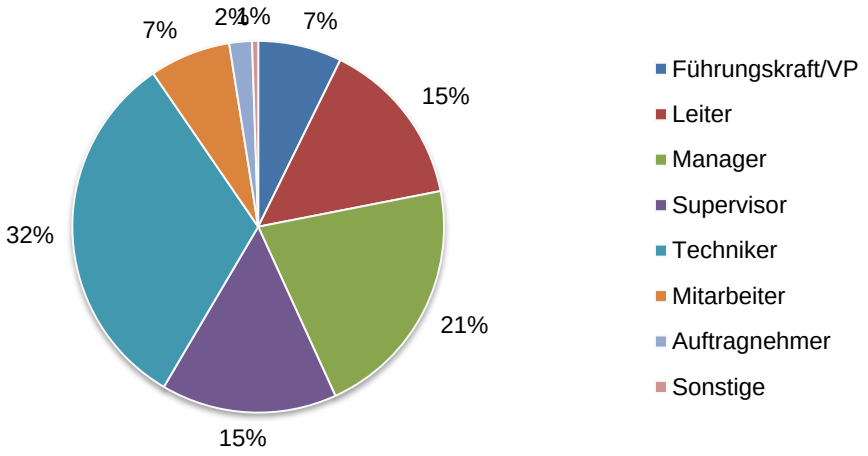
Teil 3. Methodik

Die Stichprobe setzt sich aus 51.248 IT- und IT-Sicherheitsspezialisten aus folgenden Regionen zusammen: Asiatisch-pazifischer Raum, EMEA-Region, Nordamerika und Lateinamerika. Wie in Tabelle 1 zu sehen ist, haben 2.040 Befragte an der Umfrage teilgenommen. Beim Screening wurden 214 Umfragen entfernt. Die endgültige Auswahl umfasste 1.826 Umfragen (entspricht einer Teilnahmerate von 3,6 Prozent).

Tabelle 1. Antwortrate aus der Stichprobe	**Anzahl**	**%**
Stichprobe gesamt	51.248	100.0 %
Reaktionen gesamt	2.040	3.9 %
Abgelehnte oder ungültige Antworten	214	0.4 %
Endgültige Stichprobe	1.826	3.6 %

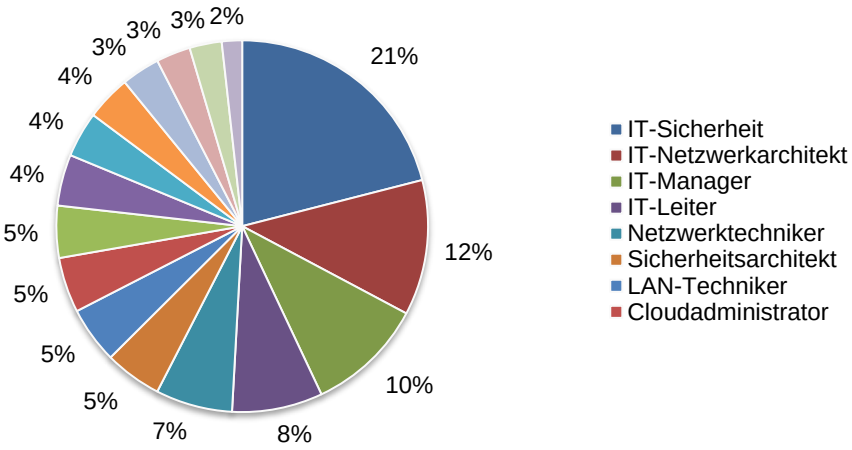
Das Kreisdiagramm 1 zeigt die aktuelle Position bzw. die Organisationsebene der Befragten. 58 Prozent der Befragten gaben an, aktuell Position in einer leitenden Position oder höher zu sein und 32 Prozent der Befragten gaben für ihre Position Techniker an.

Kreisdiagramm 1. Verteilung der Befragten nach Position



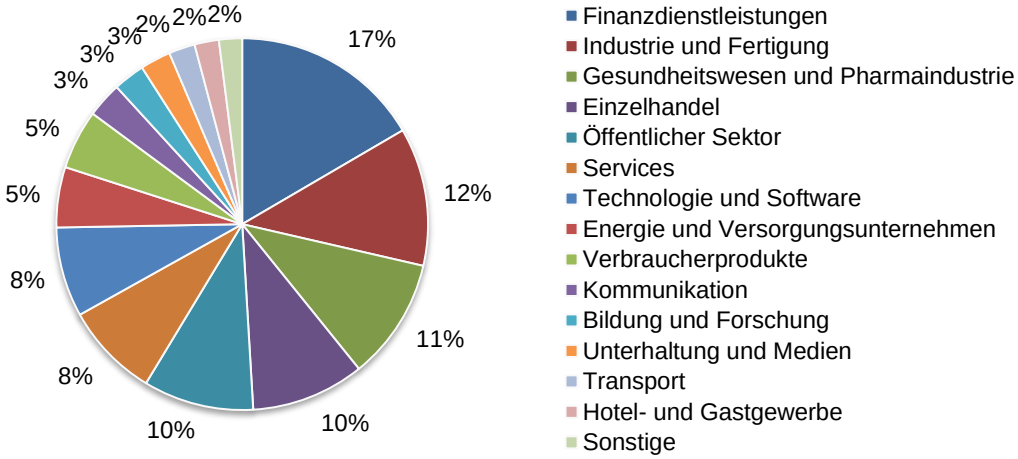
Kreisdiagramm 2 zeigt die primäre Rolle der Befragten. 21 Prozent der Befragten gaben ihre Rolle im Bereich IT-Sicherheit an, 12 Prozent als IT-Netzwerkarchitekt, 10 Prozent als IT-Manager und 8 Prozent als IT-Leiter.

Kreisdiagramm 2. Verteilung der Befragten nach primärer Rolle in der Organisation



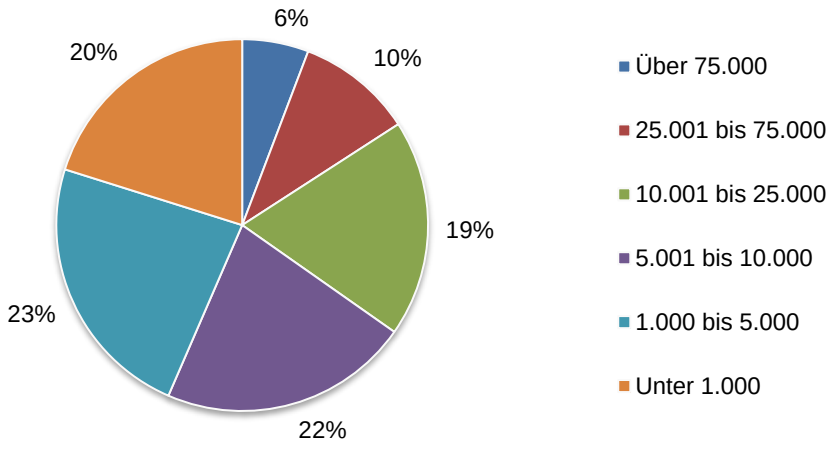
Kreisdiagramm 3 zeigt die primäre Branchenklassifizierung der Organisationen der Befragten. In diesem Diagramm werden Finanzdienstleistungen (17 Prozent der Befragten) als größtes Segment identifiziert. Hierzu zählen Banken, Versicherungen, Maklertätigkeiten, Vermögensverwaltung und Zahlungsabwicklung. Darauf folgen die Bereiche Industrie/Fertigung (12 Prozent der Befragten), Gesundheitswesen und Pharmaindustrie (11 Prozent der Befragten) sowie Einzelhandel und öffentlicher Sektor (jeweils 10 Prozent der Befragten).

Kreisdiagramm 3. Verteilung der Befragten nach primärer Branchenklassifizierung



Laut Kreisdiagramm 4 stammt mehr als die Hälfte der Befragten (57 Prozent) aus Organisationen mit mit weltweit mehr als 5.000 Mitarbeitern.

Kreisdiagramm 4. Verteilung der Befragten nach Anzahl der Mitarbeiter in der Organisation



Teil 4. Einschränkungen

Bestimmte Einschränkungen, die bei der Umfrageforschung vorhanden sind, müssen sorgfältig berücksichtigt werden, bevor Rückschlüsse auf Grundlage der Ergebnisse gezogen werden. Folgende Punkte sind spezifische Einschränkungen, die für die meisten webbasierten Umfragen relevant sind.

Schweigeverzerrung: Die aktuellen Ergebnisse beruhen auf einer Auswahl von Umfragereaktionen. Die Umfragen wurde an eine repräsentative Stichprobe von Personen gesendet, was zu einer großen Anzahl verwertbarer Reaktionen führt. Trotz Tests zur Schweigeverzerrung ist es immer möglich, dass sich Personen, die nicht teilgenommen haben, in ihren zugrunde liegenden Überzeugungen wesentlich von denen unterscheiden, die an der Umfrage teilgenommen haben.

Stichprobenverzerrung: Die Genauigkeit basiert auf den Kontaktinformationen und dem Grad der Repräsentativität der Liste für Personen, die in verschiedenen Organisationen im asiatisch-pazifischen Raum, in der EMEA-Region sowie in Nord- und Lateinamerika im Bereich IT-Sicherheit oder Netzwerke tätig sind. Wir berücksichtigen auch, dass die Ergebnisse durch externe Ereignisse wie die derzeitige Medienberichterstattung verzerrt sein können. Außerdem beachten wir eine Verzerrung, die dadurch entstehen kann, dass Teilnehmer dafür entschädigt werden, diese Untersuchung innerhalb einer bestimmten Zeitspanne abzuschließen.

Selbst gemeldete Ergebnisse: Die Qualität der Studie basiert auf der Integrität der vertraulichen Antworten der Teilnehmer. Auch wenn bestimmte Kontrollmechanismen in den Befragungsprozess integriert werden können, besteht immer die Möglichkeit, dass Teilnehmer keine genauen Antworten geben.

Anhang: Detaillierte Umfrageergebnisse

In folgenden Tabellen wird die Häufigkeit bzw. die prozentuale Häufigkeit der Antworten auf alle bei dieser Studie gestellten Fragen gezeigt. Die Umfrageergebnisse wurden im Februar 2021 erfasst.

Umfrageergebnisse	NA	EMEA	APAC	LATAM	Gesamt
Stichprobe gesamt	16.248	12.445	11.891	10.664	51.248
Reaktionen gesamt	663	501	456	420	2.040
Abgelehnte Umfragen	65	47	54	48	214
Endgültige Stichprobe	598	454	402	372	1.826
Teilnahmerate	3.7 %	3.6 %	3.4 %	3.5 %	3.6 %
Auswahlgewichtung	32.7 %	24.9 %	22.0 %	20.4 %	100.0 %

Teil 1. Screening

S1. Wie wird Ihre Rolle innerhalb Ihrer Organisation am besten beschrieben?	NA	EMEA	APAC	LATAM	Gesamt
Ich bin hauptsächlich Sicherheitsspezialist.	41 %	35 %	36 %	30 %	36 %
Ich bin hauptsächlich Netzwerkspezialist.	27 %	37 %	39 %	42 %	35 %
Ich bin sowohl Sicherheits- als auch Netzwerkspezialist.	32 %	28 %	25 %	28 %	29 %
Keine der genannten Optionen (Ende)	0 %	0 %	0 %	0 %	0 %
Gesamt	100 %	100 %	100 %	100 %	100 %

Teil 2. Verwendung von SD-WAN, cloudbasierter Sicherheit, SASE-Architektur und Zero-Trust-Sicherheitsarchitektur

F1. Wie vertraut sind Sie mit der Zero-Trust-Sicherheitsarchitektur?	NA	EMEA	APAC	LATAM	Gesamt
Sehr vertraut	34 %	30 %	28 %	27 %	30 %
Vertraut	30 %	29 %	34 %	35 %	32 %
Etwas vertraut	27 %	30 %	28 %	17 %	26 %
Nicht vertraut	9 %	11 %	10 %	21 %	12 %
Gesamt	100 %	100 %	100 %	100 %	100 %

F2. Ist die Bereitstellung einer Zero-Trust-Sicherheitsarchitektur in Ihrer Organisation bereits vorhanden oder geplant?	NA	EMEA	APAC	LATAM	Gesamt
Ja, eine solche Architektur ist bereits vorhanden.	24 %	19 %	18 %	15 %	20 %
Ja, eine solche Architektur wird innerhalb der nächsten 12 Monate implementiert.	19 %	14 %	13 %	11 %	15 %
Ja, aber die Bereitstellung wurde noch nicht geplant.	23 %	19 %	20 %	24 %	22 %
Ich weiß nicht, ob die Bereitstellung geplant ist.	16 %	25 %	27 %	15 %	20 %
Keine Bereitstellungspläne	18 %	23 %	22 %	35 %	24 %
Gesamt	100 %	100 %	100 %	100 %	100 %

F3. Wie vertraut sind Sie mit SD-WAN-Lösungen?	NA	EMEA	APAC	LATAM	Gesamt
Sehr vertraut	21 %	16 %	13 %	17 %	17 %
Vertraut	23 %	19 %	22 %	20 %	21 %
Etwas vertraut	32 %	23 %	30 %	33 %	30 %
Nicht vertraut	24 %	42 %	35 %	30 %	32 %
Gesamt	100 %	100 %	100 %	100 %	100 %

F4. Ist die Bereitstellung von SD-WAN-Lösungen in Ihrer Organisation bereits vorhanden oder geplant?	NA	EMEA	APAC	LATAM	Gesamt
Ja, eine solche Architektur ist bereits vorhanden.	15 %	9 %	11 %	8 %	11 %
Ja, eine solche Architektur wird innerhalb der nächsten 12 Monate implementiert.	20 %	19 %	14 %	17 %	18 %
Ja, aber die Bereitstellung wurde noch nicht geplant.	11 %	20 %	23 %	14 %	16 %
Ich weiß nicht, ob die Bereitstellung geplant ist.	18 %	12 %	19 %	16 %	16 %
Keine Bereitstellungspläne	36 %	40 %	33 %	45 %	38 %
Gesamt	100 %	100 %	100 %	100 %	100 %

F5. Wer hat bei der Bereitstellung von SD-WAN-Lösungen den größten Einfluss bzw. wird diesen haben?	NA	EMEA	APAC	LATAM	Gesamt
Das Sicherheitsteam leitet die Bereitstellung mit Beratung durch das Netzwerkteam.	40 %	34 %	38 %	36 %	37 %
Das Netzwerkteam leitet die Bereitstellung mit Beratung durch das Sicherheitsteam.	45 %	47 %	50 %	42 %	46 %
Das Netzwerkteam trifft Entscheidungen zum Netzwerk und das Sicherheitsteam Entscheidungen zur Sicherheit.	15 %	19 %	12 %	22 %	17 %
Gesamt	100 %	100 %	100 %	100 %	100 %

F6. Wie vertraut sind Sie mit der SASE-Sicherheitsarchitektur?	NA	EMEA	APAC	LATAM	Gesamt
Sehr vertraut	24 %	18 %	17 %	19 %	20 %
Vertraut	23 %	29 %	27 %	23 %	25 %
Etwas vertraut	30 %	28 %	25 %	28 %	28 %
Nicht vertraut	23 %	25 %	31 %	30 %	27 %
Gesamt	100 %	100 %	100 %	100 %	100 %

F7. Ist die Bereitstellung einer SASE-Sicherheitsarchitektur in Ihrer Organisation bereits vorhanden oder geplant?	NA	EMEA	APAC	LATAM	Gesamt
Ja, eine solche Architektur ist bereits vorhanden.	12 %	8 %	9 %	10 %	10 %
Ja, eine solche Architektur wird innerhalb der nächsten 12 Monate implementiert.	18 %	12 %	9 %	13 %	14 %
Ja, aber die Bereitstellung wurde noch nicht geplant.	23 %	28 %	27 %	24 %	25 %
Ich weiß nicht, ob die Bereitstellung geplant ist.	15 %	21 %	18 %	15 %	17 %
Keine Bereitstellungspläne	32 %	31 %	37 %	38 %	34 %
Gesamt	100 %	100 %	100 %	100 %	100 %

F8. Wenn Ihre Organisation sowohl SD-WAN als auch cloudbasierte Sicherheit für eine SASE-Architektur einsetzt, wie würden die Anbieter ausgewählt? Bitte wählen Sie nur eine Option.	NA	EMEA	APAC	LATAM	Gesamt
Beauftragung eines Anbieters sowohl für SD-WAN als auch Cloudsicherheit	29 %	28 %	31 %	30 %	29 %
Einsatz marktführender Netzwerke mit Integration für marktführende Anbieter von Cloudsicherheitslösungen	23 %	27 %	25 %	19 %	24 %
Beauftragung eines marktführenden SD-WAN-Anbieters, der eine Integration für Anbieter von Cloudsicherheitslösungen ermöglicht	25 %	24 %	18 %	17 %	22 %
Beauftragung eines marktführenden Anbieters/marktführender Anbieter von Cloudsicherheitslösungen, der/die eine Integration für Anbieter von SD-WAN-Lösungen ermöglicht/ermöglichen	23 %	21 %	26 %	34 %	25 %
Gesamt	100 %	100 %	100 %	100 %	100 %

F9. Wer trifft die Entscheidungen zur Architektur/zu Produkten für Sicherheitslösungen?	NA	EMEA	APAC	LATAM	Gesamt
Das Netzwerkteam	40 %	48 %	38 %	42 %	42 %
Das Sicherheitsteam	33 %	29 %	33 %	27 %	31 %
Sowohl das Netzwerk- als auch das Sicherheitsteam	27 %	23 %	29 %	31 %	27 %
Gesamt	100 %	100 %	100 %	100 %	100 %

F10. Wie werden Entscheidungen zu den Anbietern bei der Implementierung von cloudbasierten Sicherheitsdiensten getroffen (z. B. cloudbasierte Firewall-as-a-Service, Cloud Access Security Broker)? Bitte wählen Sie nur **die** zutreffendste Option.	NA	EMEA	APAC	LATAM	Gesamt
Unsere Organisation würde führende unabhängige Anbieter beauftragen, deren Fokus auf diesen Lösungen liegt	47 %	41 %	43 %	45 %	44 %
Unsere Organisation würde unseren Netzwerkanbieter beauftragen	23 %	26 %	28 %	22 %	25 %
Unsere Organisation würde Sicherheitsanbieter beauftragen, die diese Dienste als Teil eines größeren Sicherheitsportfolios bereitstellen	30 %	33 %	29 %	33 %	31 %
Gesamt	100 %	100 %	100 %	100 %	100 %

F11. Wie hoch ist die Zuversicht in Ihrer Organisation hinsichtlich der Effektivität der vorhandenen Sicherheitsarchitektur und Implementierung auf einer Skala von 1 (nicht zuversichtlich) bis 10 (sehr zuversichtlich)?	NA	EMEA	APAC	LATAM	Gesamt
1 oder 2	5 %	8 %	11 %	9 %	8 %
3 oder 4	15 %	6 %	8 %	13 %	11 %
5 oder 6	25 %	15 %	8 %	25 %	19 %
7 oder 8	33 %	36 %	35 %	34 %	34 %
9 oder 10	22 %	35 %	38 %	19 %	28 %
Gesamt	100 %	100 %	100 %	100 %	100 %
Hochgerechneter Wert	6.54	7.18	7.12	6.32	6.78

F12. Ist es Ihrer Meinung nach möglich, dass alle Ihre **Sicherheitsanforderungen** von einem einzigen Anbieter erfüllt werden?	NA	EMEA	APAC	LATAM	Gesamt
Ja	68 %	64 %	59 %	57 %	63 %
Nein	27 %	30 %	37 %	36 %	32 %
Nicht sicher	5 %	6 %	4 %	7 %	5 %
Gesamt	100 %	100 %	100 %	100 %	100 %

F13. Ist es Ihrer Meinung nach möglich, dass alle Ihre **Netzwerkanforderungen** von einem einzigen Anbieter erfüllt werden?	NA	EMEA	APAC	LATAM	Gesamt
Ja	48 %	45 %	41 %	39 %	44 %
Nein	45 %	47 %	53 %	55 %	49 %
Nicht sicher	7 %	8 %	6 %	6 %	7 %
Gesamt	100 %	100 %	100 %	100 %	100 %

F14. Ist es Ihrer Meinung nach möglich, dass alle Ihre **Sicherheits- und Netzwerkanforderungen** von einem einzigen Anbieter erfüllt werden?	NA	EMEA	APAC	LATAM	Gesamt
Ja	57 %	52 %	50 %	47 %	52 %
Nein	35 %	42 %	43 %	45 %	41 %
Nicht sicher	8 %	6 %	7 %	8 %	7 %
Gesamt	100 %	100 %	100 %	100 %	100 %

Teil 3. Ihre Rolle und organisatorischen Merkmale

D1. Welche Organisationsebene beschreibt Ihre derzeitige Position am besten?	NA	EMEA	APAC	LATAM	Gesamt
Führungskraft/VP	8 %	6 %	7 %	8 %	7 %
Leiter	16 %	14 %	13 %	15 %	15 %
Manager	21 %	23 %	19 %	22 %	21 %
Supervisor	15 %	17 %	15 %	14 %	15 %
Techniker	30 %	31 %	35 %	33 %	32 %
Mitarbeiter	7 %	8 %	8 %	5 %	7 %
Auftragnehmer	2 %	1 %	3 %	2 %	2 %
Sonstige	1 %	0 %	0 %	1 %	1 %
Gesamt	100 %	100 %	100 %	100 %	100 %

D2. Was beschreibt Ihre primäre Rolle in der Organisation am besten?	NA	EMEA	APAC	LATAM	Gesamt
Cloudadministrator	5 %	6 %	3 %	5 %	5 %
Datenschutzbeauftragter	0 %	0 %	0 %	0 %	0 %
IT-Leiter	7 %	8 %	9 %	8 %	8 %
IT-Manager	11 %	8 %	9 %	13 %	10 %
IT-Netzwerkarchitekt	12 %	10 %	13 %	12 %	12 %
IT-Sicherheit	20 %	19 %	23 %	23 %	21 %
LAN-Techniker	5 %	3 %	6 %	6 %	5 %
Netzwerkadministrator	3 %	3 %	2 %	4 %	3 %
Netzwerktechniker	6 %	7 %	8 %	6 %	7 %
Netzwerkbetriebsleiter	4 %	3 %	4 %	2 %	3 %
Netzwerkspezialist	3 %	6 %	4 %	3 %	4 %
Sicherheitsadministrator	5 %	3 %	5 %	2 %	4 %
Sicherheitsanalyst	6 %	5 %	2 %	4 %	4 %
Sicherheitsarchitekt	4 %	8 %	3 %	5 %	5 %
Sicherheitsspezialist	3 %	3 %	3 %	2 %	3 %
WAN-Techniker	4 %	7 %	3 %	4 %	5 %
Sonstige (bitte angeben)	2 %	1 %	3 %	1 %	2 %
Gesamt	100 %	100 %	100 %	100 %	100 %

D3. Welche Branche beschreibt den Branchenschwerpunkt Ihrer Organisation am besten?	NA	EMEA	APAC	LATAM	Gesamt
Landwirtschaft und Lebensmitteldienstleistungen	1 %	1 %	1 %	1 %	1 %
Kommunikation	3 %	2 %	4 %	3 %	3 %
Verbraucherprodukte	5 %	5 %	5 %	6 %	5 %
Verteidigung/Luft- und Raumfahrt	1 %	1 %	2 %	1 %	1 %
Bildung und Forschung	2 %	2 %	4 %	3 %	3 %
Energie und Versorgungsunternehmen	5 %	5 %	6 %	5 %	5 %
Unterhaltung und Medien	2 %	2 %	3 %	4 %	3 %
Finanzdienstleistungen	18 %	15 %	17 %	15 %	17 %
Gesundheitswesen und Pharmaindustrie	11 %	12 %	9 %	10 %	11 %
Hotel- und Gastgewerbe	2 %	2 %	2 %	3 %	2 %
Industrie und Fertigung	12 %	15 %	11 %	10 %	12 %
Öffentlicher Sektor	9 %	10 %	9 %	11 %	10 %
Einzelhandel	10 %	10 %	9 %	10 %	10 %
Services	9 %	9 %	8 %	7 %	8 %
Technologie und Software	8 %	8 %	8 %	7 %	8 %
Transport	2 %	2 %	2 %	3 %	2 %
Sonstige	0 %	0 %	0 %	0 %	0 %
Gesamt	100 %	100 %	100 %	100 %	100 %

D4. Welcher Bereich beschreibt die Anzahl der Vollzeitbeschäftigten in Ihrer globalen Organisation am besten?	NA	EMEA	APAC	LATAM	Gesamt
Unter 1.000	18 %	24 %	21 %	18 %	20 %
1.000 bis 5.000	20 %	25 %	24 %	26 %	23 %
5.001 bis 10.000	19 %	20 %	23 %	27 %	22 %
10.001 bis 25.000	22 %	17 %	19 %	16 %	19 %
25.001 bis 75.000	13 %	9 %	8 %	9 %	10 %
Über 75.000	8 %	5 %	5 %	4 %	6 %
Gesamt	100 %	100 %	100 %	100 %	100 %

Wenden Sie sich bei Fragen per E-Mail an research@ponemon.org oder telefonisch unter 800-887-3118 an uns.

Ponemon Institute

Verantwortungsvolles Informationsmanagement fördern

Das Ponemon Institute widmet sich der unabhängigen Forschung und Bildung, durch die verantwortungsvolle Praktiken bei der Informations- und Datenschutzverwaltung in Unternehmen und Behörden gefördert werden. So führen wir qualitativ hochwertige, empirische Studien zu kritischen Themen durch, die Verwaltung und Sicherheit sensibler Informationen über Personen und Organisationen betreffen.

Wir sind Mitglied der **Insights Association** und halten uns schon deswegen an strenge Normen für Datenvertraulichkeit, Datenschutz und ethische Forschung. Wir erfassen keine personenbezogene Informationen von Einzelpersonen (bzw. unternehmensbezogene Informationen bei unseren Unternehmensnachforschungen). Außerdem halten wir strenge Qualitätsnormen ein, um sicherzustellen, dass Teilnehmern keine missverständlichen, irrelevanten oder unangemessenen Fragen gestellt werden.