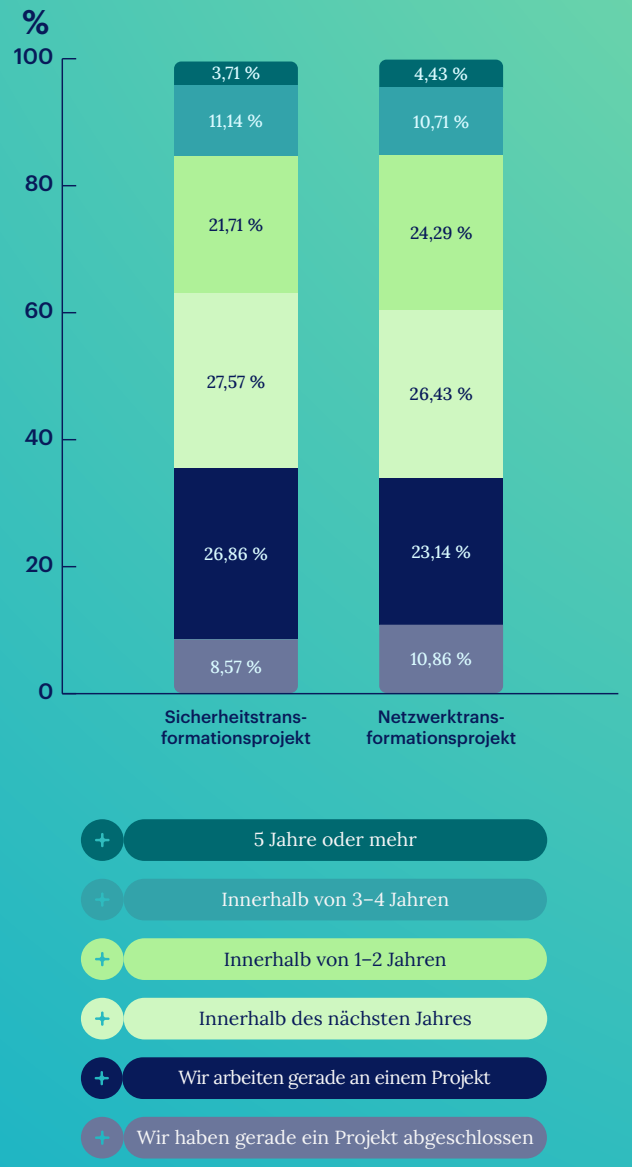

e-book
Sicherheits-und Netzwerktransformation im Zeitalter von SASE
netskope

Im Zuge ihrer anhaltenden digitalen Transformation verlagern Unternehmen immer mehr operative Ressourcen in die Cloud. Diese operativen Ressourcen erstrecken sich über ihre gesamte IT-Struktur und der Erfolg dieser Projekte erfordert ein Überdenken von sowohl Netzwerk- als auch Sicherheitsarchitekturen.

Der globale Markt für Netzwerktransformation soll Prognosen zufolge bis 2026 ein Marktvolumen von 122,73 Milliarden US-Dollar erreichen – mit einer durchschnittlichen jährlichen Wachstumsrate (Compound Annual Growth Rate, CAGR) von 39,7% .[1] Ebenso wird erwartet, dass der globale Markt für Cloud-Sicherheit bis zum gleichen Jahr mit einer CARG von 13,7% wachsen und 77,5 Milliarden US-Dollar erreichen wird.[2]

Der Wandel ist in vollem Gange, doch bei Unternehmen besteht nach wie vor wenig Konsens darüber, wie sie ihre Netzwerk-und Sicherheitsprojekte in Bezug auf Budgets, Änderungsmanagement oder technologische Rationalisierung angehen sollen.

Dieses eBook zeigt einige der wichtigsten Herausforderungen auf, die die von Netskope bei Censuswide in Auftrag gegebene Studie über europäische Unternehmen aufgedeckt hat. Ergänzt werden diese Erkenntnisse durch Studien Dritter, um ein umfassendes Bild zu vermitteln. Unser Ziel ist es, besser zu verstehen, wie führende IT-Experten die Transformation im Zeitalter der SASE-Architekturen (Secure Access Service Edge) angehen, und Einblicke dazu zu geben, wie Unternehmen Teams, Prozesse und Technologien rationalisieren und so ihre SASE-Projekte zum Erfolg führen können.



[1] "Global Network Transformation Market Research Report," Market Research Future, 2021.

[2] "Cloud Security Market Report," MarketsandMarkets, Januar 2022.

Die Kosteneinsparungen durch die Verlagerung der Sicherheit in die Cloud

Eine Studie von Deloitte zeigt, dass Sicherheit und Datenschutz heute weltweit einer der Hauptgründe für die Einführung von Cloud Computing sind. 58 % der IT-Führungskräfte nennen dies als wichtigsten oder zweitwichtigsten Grund.[3] Laut einer Umfrage unter US-Führungskräften sehen außerdem 60 % der Befragten Sicherheit als den größten Vorteil von Cloud Computing.[4]

Auch unsere eigene Forschung spiegelt dies wider. Die überwiegende Mehrheit der CIOs und CISOs (98 %), mit denen wir gesprochen haben, haben zumindest einige Ressourcen in die Cloud verlagert, obwohl weniger als jeder Fünfte (18,5 %) mehr als drei Viertel seiner Sicherheitsinfrastruktur verlegt haben.

Die meisten derjenigen, die Cloud-Sicherheit nutzen, haben ihre Ausgaben in einigen der erwarteten Bereiche bereits reduziert: 25 % erzielen Einsparungen bei der Hardware und 23 % bei der Bandbreite. Zudem haben 21 % ihre Kosten durch die Konsolidierung von Anbietern gesenkt und 21 % haben durch den Umstieg auf Cloud-Alternativen ihre Ausgaben für Firewall-Appliances reduziert. Das steht im Einklang mit weltweiten Forschungsstudien. So legen Untersuchungen von Secure Data beispielsweise nahe, dass ein Unternehmen mit 500 Mitarbeitern seine Firewall-Kosten um 37 % senkt und durchschnittlich 139.000 US-Dollar spart.[5]

Da sich die meisten Unternehmen jedoch noch in der digitalen Transformation befinden, müssen diese tatsächlichen Kosteneinsparungen korrekterweise noch als vorläufig betrachtet werden – oder zumindest als Werte, die regelmäßig neu analysiert werden sollten. Unserer Studie zufolge erwarten beispielsweise 30 % der Befragten, dass sie durch die Einführung von FWaaS-Technologien (Firewall-as-a-Service) Kosten einsparen werden, aber nur 22 % geben an, diese Einsparungen bisher erzielt zu haben.

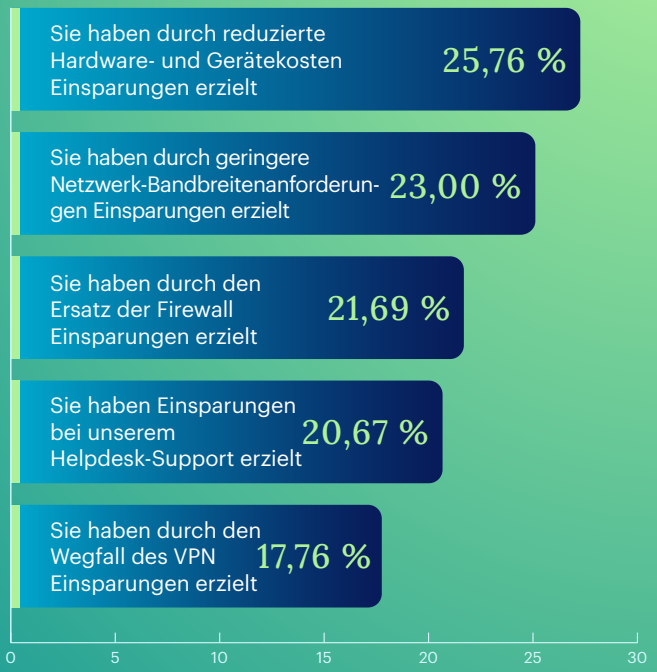
Die Sicherheit wird von 60 % der C-Level-Führungskräfte weltweit als der größte Vorteil von Cloud Computing angesehen[6]

Sicherheit wird im Jahr 2023 6 % der Cloud-Ausgaben ausmachen[7]

98 % der europäischen CIOs/CISOs haben zumindest einige Ressourcen in die Cloud verlagert

Nur 18,5 % haben mehr als drei Viertel ihrer Sicherheitsinfrastruktur verlagert

Welche dieser Aussagen trifft als Folge der Verlagerung der Sicherheit in die Cloud ggf. auf Sie und Ihr Unternehmen zu?



Die wichtigste Erkenntnis

Die Umstellung auf die Cloud ist ein laufender Prozess. Das bedeutet, dass die Einsparungen durch die Cloud und SASE mit der Zeit noch zunehmen werden. Für die nächsten ein bis zwei Jahre konzentrieren sich Unternehmen auf kurzfristige Projekte wie die Ablösung von VPNs und die Konsolidierung von Anbietern als beste Quelle für Kosteneinsparungen.

[3] Karthik Ramachandran und David Linthicum, „Why organizations are moving to the cloud: Security, data modernization, and cost among top drivers for cloud migration“, Deloitte, 5. März 2020.

[4] „55 Cloud Computing Statistics That Will Blow Your Mind“, CloudZero, 21. Oktober 2022.

[5] Abdul Moiz, „12 Reasons to Choose Firewall as a Service for your Business“, ExterNetworks, 8. Dezember 2022.

[6] „55 Cloud Computing Statistics That Will Blow Your Mind“, CloudZero, 21. Oktober 2022.

[7] Matt Ashare, „Security to take an outsized role in IT spending in 2023“, CIO Dive, 4. Oktober 2022.

Die Zusammenführung der Bereiche Netzwerk und Sicherheit

Die Zusammenführung von Sicherheits- und Netzwerkfunktionen ist eine Best Practice für Unternehmen auf ihrem Weg in die Cloud. Die Befragten in der Netskope Umfrage gaben hierfür auch einen sinnvollen Grund an: Etwa ein Drittel der CIOs und CISOs ist der Meinung, dass eine Trennung der Teams beim Management von Cloud-Ressourcen nicht hilfreich ist.

Wir haben jedoch festgestellt, dass die große Mehrheit der Unternehmen, die Sicherheits- und Netzwerkziele miteinander verbinden, ihre Budgets getrennt halten. Nur 8% der Befragten gaben an, vorzuhaben, ihre Sicherheits-und Netzwerkbudgets zusammenzulegen. Selbst wenn beide Teams dem CIO unterstellt sind – etwa zwei Drittel dieser IT-Teams sind entweder disziplinarisch oder fachlich sowohl dem CIO als auch dem CISO unterstellt –, könnten sie um Ressourcen und Verantwortung für Cloud-Technologien konkurrieren. 28% der Befragten erwarten genau das.

Diese Ungewissheit bezüglich der richtigen Cloud-Strategie spiegelt sich in der allgemeinen Ungewissheit darüber wider, wie man am besten mit der Sicherheit ganz oben in der Unternehmenshierarchie umgeht. Laut einer weltweiten Studie der Economist Intelligence Unit sind fast 40% der Führungskräfte der Meinung, dass der Unternehmensvorstand die Cybersicherheit überwachen sollte, während 24% der Meinung sind, dass dies die Aufgabe eines speziellen Cyber-Ausschusses sein sollte.[8]

Zuteilung von Budgets für die Cybersicherheit in Unternehmen[9]

Annahmen der Netzinvestitionsplanung für 2025[10]

50% der SD-WAN-Käufe werden im Rahmen eines SASE-Angebots eines einzigen Anbieters erfolgen

10% der Unternehmen werden 5G als primäre oder zusätzliche drahtlose Verbindung in ihrem WAN nutzen

25% der Unternehmen werden mehr als die Hälfte ihrer Netzwerkaktivitäten automatisieren

15% aller Unternehmen werden Network-as-a-Service (NaaS) als On-Premises-Lösung nutzen

30%
der Sicherheits- und Netzwerkteams haben bereits oder werden ihre entsprechenden Funktionen zusammenführen

aber nur
8%
planen die Zusammenlegung von Sicherheits- und Netzwerkbudgets

Die wichtigste Erkenntnis

Während sich die Best Practices für die Cloud-Sicherheit weiterentwickeln, verfolgen nur wenige Unternehmen einen optimal effizienten Ansatz: die Zusammenführung der Sicherheits-und Netzwerkbereiche sowohl aus personeller als auch aus Budgetperspektive.

[8] Nick Ismail, „Who is responsible for cyber security in the enterprise?“, Information Age, 25. Oktober 2022.

[9] Toby Shackleton, „Cyber Security Budget Trends in 2022“, Six Degrees, 17. August 2021.

[10] „The top 5 trends in enterprise networking and why they matter: A Gartner® trend insight report“, DE-CIX Management GmbH, 22. September 2022.

Eine Frage der Verantwortung

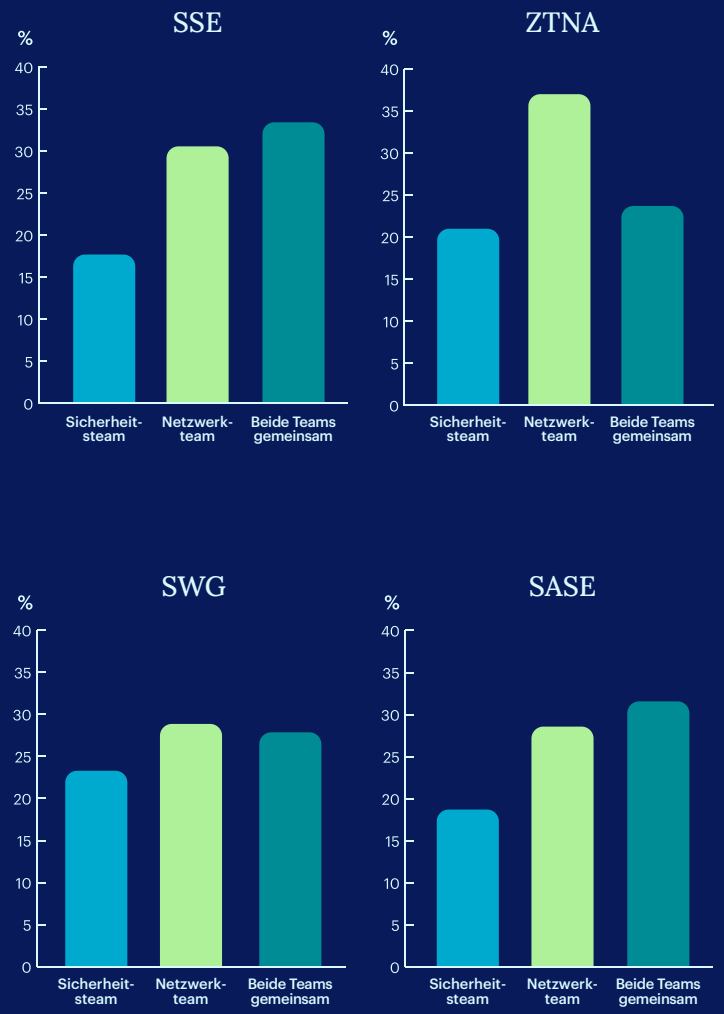
Transformative Sicherheitstechnologien und Frameworks – einschließlich SASE, SSE, ZTNA und SWG – stehen im Fokus von CIOs und CISOs in aller Welt. So wird zum Beispiel erwartet, dass die weltweiten Ausgaben für SASE mit einer CAGR von 26,4% bis 2026 auf 4,1 Milliarden US-Dollar steigen werden.[11] Ebenso wird prognostiziert, dass die weltweiten Gesamtausgaben für Zero-Trust-Sicherheitssoftware und -Lösungen mit einer CAGR von 17,3% von 27,4 Milliarden US-Dollar im Jahr 2022 auf 60,7 Milliarden US-Dollar im Jahr 2027 steigen werden.[12]

Ein gemeinsames Interesse an diesen Technologien bedeutet jedoch nicht, dass auch Einigkeit darüber besteht, welcher Unternehmensbereich für welche Produkte oder Transformationsprojekte zuständig sein sollte. Unsere Umfrage ergab, dass 28% der Unternehmen ihre Netzwerkteams mit ihren SASE-Projekten beauftragen und 18% ihre Sicherheitsorganisation. In 31% der europäischen Unternehmen dagegen teilen sich die beiden Teams die Verantwortung für SASE-Projekte.

Obwohl SSE ein relativ neuer Begriff ist und als die Sicherheitsdienste betrachtet wird, die zu SASE gehören, haben wir eine sehr ähnliche Aufteilung der Verantwortungsverhältnisse zwischen den beiden festgestellt. In 30% der Unternehmen sind die Netzwerkteams für SSE-Lösungen verantwortlich, in 18% die Sicherheitsteams und in 33% beide gemeinsam.

Bei ZTNA ist die Verantwortung eher in Richtung Netzwerkteams verlagert (37% Netzwerk, 21% Sicherheit und 23% beide gemeinsam). Bei SWG ist die Wahrscheinlichkeit, dass die Technologie in den Zuständigkeitsbereich des Sicherheitsteams fällt, etwas größer als bei den anderen Technologien (23% Sicherheit, 28% Netzwerk und 27% beide gemeinsam).

Für wann plant Ihr Unternehmen ein Sicherheits- und/oder Netzwerktransformationsprojekt?



Die wichtigste Erkenntnis

Das Ergebnis dieses Tauziehens zwischen den internen Netzwerk- und Sicherheitsteams um die Verantwortung wird die Richtung bestimmen, die das Unternehmen mit ihrem SASE-Projekt einschlägt.

Da es keinen breiten externen Konsens darüber gibt, welche Teams für welche Initiativen zuständig sind, müssen der CIO und der CISO gemeinsam eine Entscheidung treffen und dann klar und konsequent festlegen, welches Team die Verantwortung für die einzelnen Bereiche der Transformation trägt.

[11] „Secure Access Service Edge Market Report", MarketsandMarkets, August 2021.

[12] „Zero Trust Security Market Report", MarketsandMarkets, August 2021.

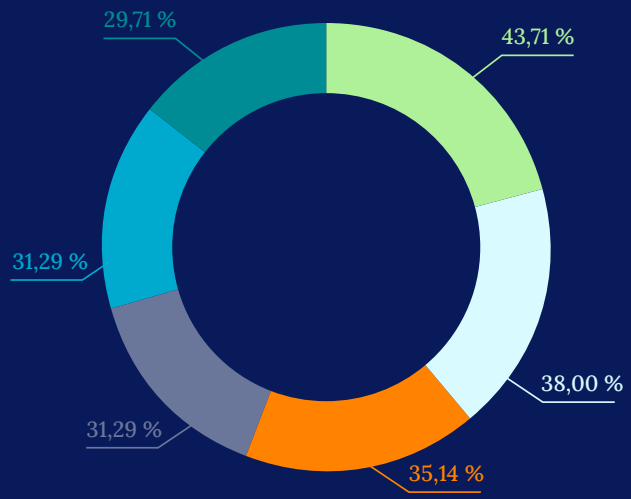
Die Qualifikationslücke im Sicherheitsbereich

Laut dem „Cost of a Data Breach Report 2022“ von IBM und dem Ponemon Institute sind 62% der Unternehmen der Meinung, dass ihr Sicherheitsteam nicht ausreichend ausgestattet ist.[13] Unsere Untersuchung zeigt, dass die Verlagerung in die Cloud das Problem der Qualifikationslücke weiter verschärfen wird: Fast ein Drittel der Befragten stockt derzeit das Sicherheitsteam auf und wird das voraussichtlich tun, um seinem breiteren Aufgabenbereich gerecht zu werden, wenn das Unternehmen seinen Betrieb in der Cloud ausweitet.

Ein bedeutender Anteil der befragten CIOs/CISOs (29%) gab an, keine Probleme damit zu haben, qualifizierte Kandidaten für diese Sicherheitspositionen zu finden. Eine noch größere Gruppe (46%) hat jedoch entweder derzeit Schwierigkeiten, geeignete Kandidaten zu finden, oder rechnet damit, in Zukunft Schwierigkeiten damit zu haben. Vielleicht planen aufgrund dieser Bedenken 38% aller Befragten, neue Mitglieder für ihr Sicherheitsteam außerhalb der Cybersicherheit oder sogar des IT-Bereichs zu suchen.

Die Qualifikationslücke zu schließen, ist von entscheidender Bedeutung, denn solange sie nicht behoben ist, besteht für Unternehmen ein größeres Risiko, Opfer eines Angriffs zu werden. Nach Angaben des Weltwirtschaftsforums wäre es für 59% der Unternehmen weltweit derzeit aufgrund fehlender Fähigkeiten in ihrem Team eine Herausforderung, auf einen Cybersicherheitsvorfall zu reagieren.[14] Dies ist nicht verwunderlich, wenn man bedenkt, dass nur 8% der IT-Fachkräfte weltweit über signifikante Fähigkeiten und Erfahrungen im Cloud-Bereich verfügen.[15] Unternehmen, die über ein ausreichend besetztes Sicherheitsteam verfügen, berichten dagegen, dass die durchschnittlichen Kosten einer Datenschutzverletzung bei ihnen unter dem Durchschnitt liegen.[16]

Wenn Sie neue Mitarbeiter für Ihr Sicherheitsteam einstellen müssten, wo würden Sie versuchen, diese zu finden?



- Wir würden nach Kandidaten mit vorhandenen Cloud-/SaaS-/IaaS-Kenntnissen und -Erfahrungen suchen
- Wir würden nach Kandidaten außerhalb des Cyber- oder IT-Marktes und in der Ausbildung/Umschulung suchen
- Bei unseren Konkurrenten, anderen Unternehmen der Branche oder anderen ähnlichen Unternehmen
- Wir würden unter Hochschulabsolventen suchen
- Wir würden das Team outsourcen
- Wir würden Mitarbeiter in unseren Netzwerk-, Helpdesk- und anderen Teams intern umschulen

40%

der Unternehmen weltweit sind sich einig, dass die Sicherheit die größte Qualifikationslücke darstellt.[17]

28%

haben bereits Änderungen an der Struktur oder dem Personal des Netzwerkteams vorgenommen.

26%

haben Änderungen am Sicherheitsteam vorgenommen.

Die wichtigste Erkenntnis

Die Bereitschaft der Unternehmen, nach Kandidaten zu suchen, die noch nicht über Kenntnisse und Erfahrungen im Bereich Cloud-Sicherheit verfügen, zeugt von einem beruhigenden Maß an Kreativität. Aber das ist nicht nur kreativ, sondern angesichts der Schwierigkeiten bei der Personalsuche auch notwendig. Für CIOs und CISOs, die bereit sind, neue Sicherheitsteammitglieder auszubilden, passende Qualifikationen zu finden oder einsatzbereite Kandidaten an unkonventionellen Orten zu fördern, ist das Risiko eines Fachkräftemangels viel geringer.

[13] „Cost of a Data Breach Report 2022“, Ponemon Institute und IBM Security, Juli 2022.

[14] „What you need to know about cybersecurity in 2022“, Weltwirtschaftsforum, 18. Januar 2022.

[15] „State of Cloud: The cloud skills vs. expectation gap“, Pluralsight, 2022.

[16] „Cost of a Data Breach Report 2022“, Ponemon Institute und IBM Security, Juli 2022.

[17] „State of Cloud: The cloud skills vs. expectation gap“, Pluralsight, 2022.

Budgets, Personalausstattung und Aufgabenteilung in einem SASE-Zeitalter

Die Verlagerung von Unternehmensabläufen in die Cloud stellt für IT-Organisationen und ihre CIOs und CISOs einen echten, einmaligen Generationenwechsel dar. Wie jede bedeutende Veränderung wird auch die digitale Transformation wahrscheinlich unangenehm sein, aber für Unternehmen ist sie eine Priorität. Durch die Verlagerung wichtiger Systeme in die Cloud verändern sich auch die Netzwerke und die Sicherheit.

Viele Unternehmen sind immer noch dabei, sich durch Versuch und Irrtum an die besten Verfahren heranzutasten. Einige gehen in die Cloud und verwenden die gleichen Managementstrukturen, die bei On-Premises-Lösungen gut funktioniert haben, und hoffen auf das Beste. Dieser Ansatz ist riskant. Es macht keinen Sinn zu erwarten, dass veraltete Fähigkeiten und Budgetstrategien in der Cloud genauso gut funktionieren wie im eigenen Rechenzentrum des Unternehmens.

Diejenigen, die wahrscheinlich am besten auf die digitale Transformation vorbereitet sind, leiten ihre Projekte in die Wege, indem sie ihre Budgets neu ausrichten und sowohl ihre Teamressourcen als auch ihre Einstellungspraktiken neu überdenken. Diese Unternehmen werden gut aufgestellt sein, um die Chancen zu nutzen, die sich in der neuen Ära der SASE-first-Unternehmen auftun werden.

Über Netskope

Netskope ist ein führender Anbieter von Secure Access Service Edge, der Cloud-, Daten- und Netzwerksicherheit neu definiert und Unternehmen bei der Anwendung von Zero-Trust-Prinzipien unterstützt.
Die Netskope Intelligent Security Service Edge (SSE)-Plattform ist schnell und leicht zu bedienen; sie schützt Menschen und sichert Geräte sowie Daten überall – ganz gleich, wo sie sich befinden. Netskope hilft Unternehmen, Risiken zu reduzieren, die Effektivität zu steigern und einen ganzheitlichen Einblick in alle Cloud-, Web- und privaten Anwendungsaktivitäten zu erhalten.

Tausende Kunden, darunter mehr als 25 der Fortune 100-Unternehmen, vertrauen Netskope mit dem leistungsstarken NewEdge-Netzwerk, um Bedrohungen zu minimieren und auf technologische, organisatorische, netzwerkbezogene und regulatorische Veränderungen reagieren zu können.

Methodik

Die Studie wurde im Oktober 2021 von Censuswide im Auftrag von Netskope durchgeführt. Dabei wurden 700 IT-Fachkräfte in Deutschland und Großbritannien befragt. Die Teilnehmer sind alle CIOs, CISOs oder IT-Leiter von Unternehmen mit mehr als 5.000 IT-Benutzern.

netskope