

Nutzen Sie Cloud Services schon so effizient wie möglich?

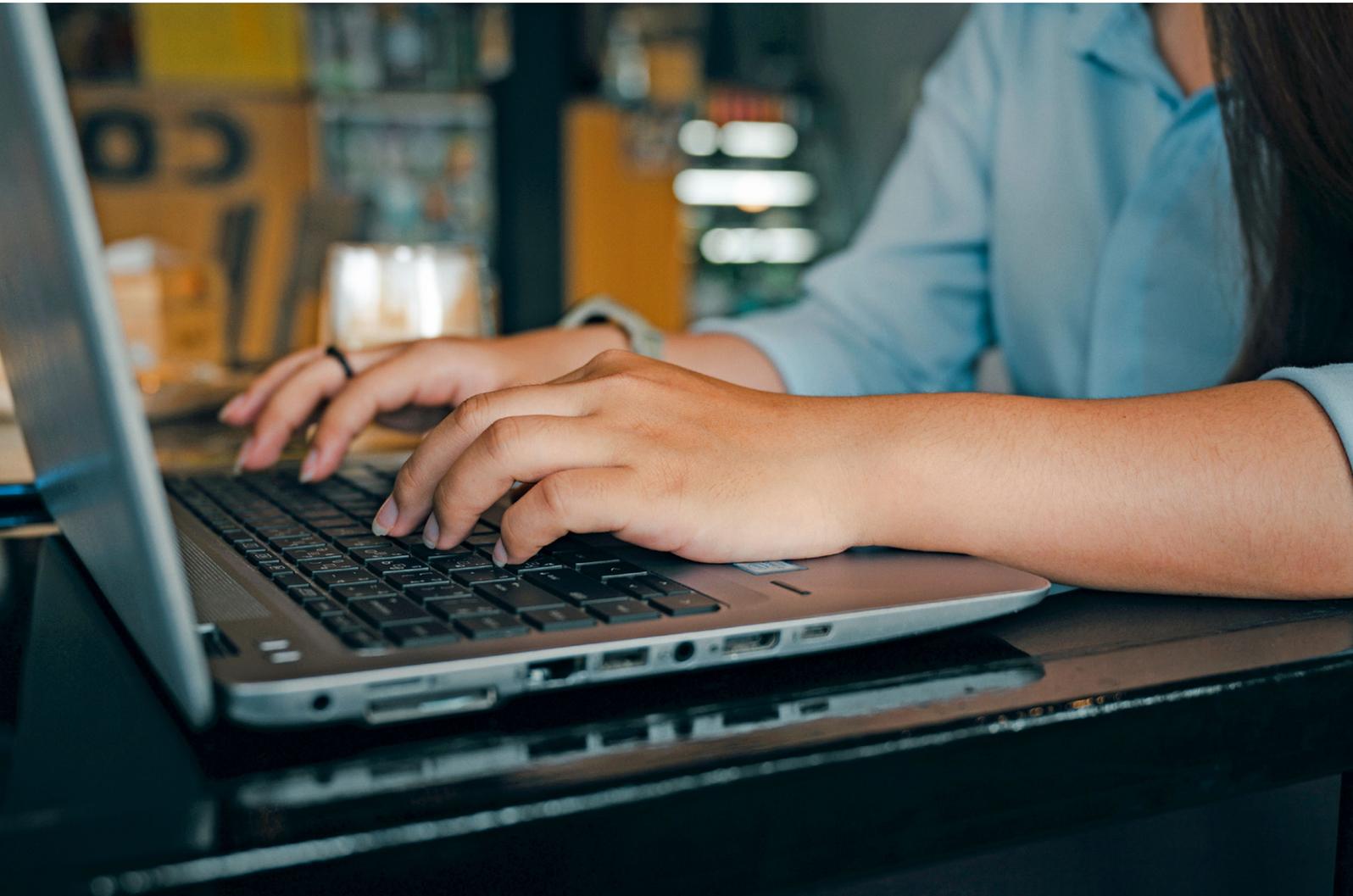
Self Check: Wie Ihre Nutzer mit SASE einen schnellen und sicheren Zugang zu Cloud Services erhalten



Erleben,
was verbindet.

Inhalt

1. Ist Ihr Netzwerk der Flaschenhals für die Cloudnutzung?
2. Mehr Tempo mit moderner Netz- und Sicherheitsarchitektur:
Wie Sie durch SASE in der Cloud produktiver arbeiten
3. Self Check SASE:
Unterstützt Ihre Infrastruktur den digitalen Wandel?
4. Auswertung:
Hier liegt für Sie das größte Potenzial für SASE
5. Sie wollen Ihre Netz- und Sicherheitsarchitektur zukunftsfähig machen?
Wir unterstützen Sie dabei.



1. Ist Ihr Netzwerk der Flaschenhals für die Cloudnutzung?

Immer mehr Unternehmen nutzen Cloud Services, um Geschäftsprozesse zu digitalisieren, agiler auf neue Anforderungen zu reagieren oder Innovationen auf den Weg zu bringen. Laut einer Studie von IDC haben bereits 95 Prozent der deutschen Firmen eine Cloud-Strategie entwickelt.¹ Cloud Services und Digitalisierung sind also in den Unternehmen angekommen. Doch wächst ihre Infrastruktur entsprechend mit? Kann das bestehende Unternehmensnetz die Anforderungen von digitalen Prozessen und Cloud Services insbesondere an Performance und Sicherheit adäquat abbilden?

Die Cloud-Transformation stellt das Netzwerk vor neue Herausforderungen. Griffen Mitarbeiter früher zentral auf Geschäftsanwendungen im Rechenzentrum zu, dominieren heute komplexe, dezentrale Strukturen: Anwendungen wie Microsoft 365 oder Cloud-Dienste wie AWS liegen verteilt in der Cloud. Um die Produktivität im Unternehmen nicht auszubremsen, müssen sich Mitarbeiter und vernetzte Geräte jederzeit und von überall aus schnell und sicher an Cloud Services anbinden lassen.

Dabei kommt es gerade an der Peripherie des Netzwerks auf leistungsfähige Cloud-Verbindungen an. Warum gerade dort? Weil Unternehmen hier nicht nur Filialen, Niederlassungen und Produktionsstandorte anbinden müssen, sondern auch immer mehr Mitarbeiter im Homeoffice, mobile User oder im Internet of Things vernetzte Produktionsmaschinen.

Ein zentraler Netzzugang stößt hier schnell an Grenzen, langsame Verbindungen und mangelhafte User Experience sind die Folgen. Um das zu vermeiden, verbinden Local Breakouts die Mitarbeiter über cloudbasierte Zweigstellen direkt mit AWS oder der Microsoft-Cloud – ohne lange Umwege über das Firmennetzwerk. Das sorgt für geringe Latenz, hohe Konnektivität und positive Nutzererlebnisse. Es wirft allerdings auch die Frage auf, wie sich solche Endpunkte effizient verwalten und ausreichend schützen lassen. Hier kommt Secure Access Service Edge (SASE) ins Spiel.

AKTUELLE HERAUSFORDERUNGEN IN DER DIGITALEN INFRASTRUKTUR

144 Mio.

neue Schadprogramme gab es 2020, im Durchschnitt 394.000 täglich.²

43%

der Nutzer glauben, dass schlechte Konnektivität die größte Herausforderung für Remote-Arbeitsplätze sei.³

~ 3/4

der Security-Entscheider weltweit bemerkten im Zuge des Homeoffice-Trends einen erheblichen Anstieg der Sicherheitsereignisse.⁴

2. Mehr Tempo mit moderner Netz- und Sicherheitsarchitektur: Wie Sie durch SASE in der Cloud produktiver arbeiten

Mit Secure Access Service Edge (SASE) schützen Unternehmen ihre Infrastruktur bis zum Rand ihres Netzwerks, ohne Performance einzubüßen. Dabei steht SASE für ein Architekturkonzept – und einen Paradigmenwechsel: Security verlagert sich aus dem zentralen Rechenzentrum heraus an den Netzwerkrand. SD-WAN oder MPLS-Netze sorgen mit Features wie Zero Trust Network Access (ZTNA) oder Cloud Access Security Broker (CASB) für umfassenden Schutz an jedem Endpunkt. Der Vorteil: SASE bündelt alle Sicherheitslösungen auf einer Cloud-Plattform, die sich einfach und zentral administrieren lässt. Außerdem stärkt SASE die Compliance, da Unternehmen Sicherheitsrichtlinien einmal installieren und an jedem Punkt im Netzwerk einhalten können.

Das Cloud-Versprechen einlösen

Da sich Cybersicherheit mit SASE in die Cloud verlagert, profitieren Unternehmen vom Cloud-Versprechen: Wächst das Unternehmen außerordentlich schnell, lassen sich die Sicherheitsfunktionen flexibel skalieren. Der Aufwand für Patches und Releases entfällt, da diese automatisiert eingespielt werden. Das entlastet die IT-Teams, die sich auf wertschöpfende Projekte konzentrieren können. Außerdem macht das As-a-Service-Modell die Kosten plan- und überschaubar. Betriebe müssen weder in teure Sicherheitshardware investieren noch diese aufwendig installieren und betreiben.

WAS IST SECURE ACCESS SERVICE EDGE?

Ende 2019 definierten die Marktanalysten von Gartner den Begriff SASE. Anlass dafür waren steigende Herausforderungen bei der Netzwerksicherheit. Die zunehmende Cloud-Nutzung, höhere Datenvolumina und immer mehr Nutzer oder Geräte, die verteilt aufs Netzwerk zugreifen, erfordern dynamische und sichere Zugänge. Heißt: Am Rande des Netzwerks müssen Konnektivität und Sicherheit stimmen. Dafür kombiniert SASE wichtige Netzwerksicherheits-Features – darunter Secure Web Gateway, Cloud Access Security Broker oder Zero Trust Network Access – mit Wide-Area-Network-Funktionen wie Software-defined WAN (SD-WAN). Das Ziel: Mit SASE jederzeit und von überall einen sicheren Zugriff auf Daten und Anwendungen garantieren, und zwar schnell und compliancekonform.

Bei SASE handelt es sich um ein neues Architekturmodell, das sämtliche Security-Funktionen cloudbasiert bereitstellt. Alle Zugriffe und Sitzungen, die Nutzer oder Endgeräte im Netzwerk starten, überwachen die Sicherheitslösungen kontinuierlich auf Risiken und Vertrauensstufen. Durch Zero Trust lassen sich sensible Daten besser schützen und Sicherheitslücken, Malware oder andere Cyberattacken leichter identifizieren.⁵

WICHTIGE KOMPONENTEN FÜR EIN SICHERHEITSMODELL AUF BASIS VON SASE:

- Secure Web Gateway
- Firewall-as-a-Service
- Remote Access VPN und Zero Trust Network Access (ZTNA)
- Cloud Access Security Broker (CASB)
- Advanced Threat Protection
- Data Loss Prevention
- Sandboxing
- Threat Prevention



3. Self Check SASE: Unterstützt Ihre Infrastruktur den digitalen Wandel?

Sie möchten herausfinden, wie Ihr Unternehmen in puncto Netzwerksicherheit und Performance aufgestellt ist? Wie Ihre Mitarbeiter Cloud Services wie AWS oder Microsoft 365 produktiver nutzen können? Und ob die aktuellen Sicherheitsmaßnahmen dafür ausreichen?

Wir zeigen Ihnen, an welcher Stelle Ihr Unternehmen gerade steht und wie Sie Ihre Cyber- und Netzwerksicherheit mit SASE auf ein neues Level bringen können. Machen Sie unseren Self Check:

Kreuzen Sie die für Ihr Unternehmen zutreffenden Antworten an.
Dabei steht 1 für „trifft überhaupt nicht zu“ sowie 5 für „trifft voll und ganz zu“.

1

Mehr als die Hälfte der Unternehmen weltweit hat im Zuge der COVID-19-Pandemie ihr Arbeitsplatzmodell neugestaltet. Die Belegschaft arbeitet flexibel von zu Hause oder im Büro und greift von überall auf Daten und Anwendungen zu.⁶ Wie viel New Work steckt in Ihrem Unternehmen?

Auch bei uns arbeitet inzwischen ein Großteil der Mitarbeiter flexibel vom Homeoffice aus. Dies wird sich auch nach der Pandemie kaum ändern, da wir zukünftig verstärkt auf hybride Arbeitsplatzkonzepte setzen.

1 2 3 4 5

2

Nicht nur die Anzahl der Remote-Arbeitsplätze ist zuletzt gestiegen. Mobiles Arbeiten bleibt im Trend. Knapp 40 Prozent der Mitarbeiter⁷ arbeiteten im Jahr 2020 mobil und haben regelmäßig von unterwegs auf die Unternehmens-IT zugegriffen. Wie wichtig ist ein mobiler Zugriff bei Ihnen?

Kundenservice, Vertrieb oder Top-Management: In unserem Unternehmen greifen immer mehr Nutzer über mobile Geräte auf Anwendungen, Daten und Cloud Services zu.

1 2 3 4 5

3

Die Cloud ist aus Unternehmen nicht mehr wegzudenken, wie die steigende Nachfrage unterstreicht: Um rund 20 Prozent auf 342 Milliarden US-Dollar nahm der weltweite Umsatz mit Public Cloud Services im letzten Jahr zu.⁸ Wie wichtig sind Cloud Services für Ihre IT?

In unserem Unternehmen schreitet die Cloud-Transformation kontinuierlich voran. Ständig kommen neue Cloud Services hinzu – darunter viele Public-Cloud-Dienste der großen Hyperscaler.

1 2 3 4 5

4

Nach Einschätzung von Branchenkennern soll die weltweite Datenmenge bis 2024 auf 143 Zettabyte anwachsen. Zum Vergleich: 2018 betrug das digitale Datenvolumen erst 33 Zettabyte. Wie schätzen Sie die Situation in Ihrem Unternehmen ein?

In den letzten Jahren ist die Datenmenge im Unternehmen stark gestiegen. Die Gründe: Wir nutzen datenintensivere Anwendungen etwa für Analytics und setzen auf neue, datengetriebene digitale Geschäftsmodelle.

1 2 3 4 5

5

Im Zuge des pandemiebedingten Homeoffice-Trends müssen Unternehmen ihre Infrastruktur bis an den Rand des Netzwerks voll absichern können. Laut einer ISG-Studie kommen sie dabei um softwarebasierte Lösungen wie SD-WAN nicht mehr herum.⁹ Nutzen Sie softwaredefinierte Netzwerkkomponenten?

Als solide Basis für unsere digitale Transformation möchten wir unser Netzwerk mit softwaredefinierten Lösungen modernisieren und setzen daher zunehmend auf SD-WAN.

1 2 3 4 5

6

Videokonferenzen, Echtzeit-Analytics oder Streaming – der Bedarf an leistungsfähigen Netzen stieg zuletzt weltweit an. Im November 2020 verzeichnete DE-CIX in Frankfurt am Main, einer der weltweit größten Internetknoten, einen Rekordwert im Datendurchsatz von mehr als 10 TBit/s.¹⁰ Welches Tempo kann Ihr Firmennetzwerk leisten?

Wir haben unser Netzwerk den digitalen Anforderungen angepasst. Die Nutzer greifen direkt und zügig – ohne Umweg über ein zentrales Rechenzentrum – beispielsweise auf cloudbasierte Anwendungen zu.

1 2 3 4 5

7

Cloud Access Security Broker (CASB) oder Zero Trust Network Access (ZTNA), Advanced Threat Protection oder Data Loss Prevention: Mit solchen aktuellen Sicherheitstechnologien lassen sich Netzwerk und Edge umfangreich schützen. Kennen Sie die aktuellen Security-Lösungen?

Wir versuchen stets, neue Sicherheitsfunktionen und State-of-the-Art-Technologien nutzen, um beispielsweise den Zugriff auf Cloud-Dienste bestmöglich abzusichern.

1 2 3 4 5



4. Auswertung: Hier liegt für Sie das größte Potenzial für SASE

Überwiegend Antwort 1 und 2

In Ihrem Unternehmen steckt noch viel Potenzial für digitale Prozesse. Stellen Sie schon jetzt die Weichen für die Digitalisierung, um auch künftig wettbewerbsfähig zu bleiben. Spezielle Anforderungen, gewachsene Strukturen oder abschreibungspflichtige Security-Hardware machen es Ihnen nicht leicht, eine moderne Netz- und Sicherheitsarchitektur aufzusetzen. Hier helfen wir weiter: Unsere Security-Experten führen eine Bestandsaufnahme von Netzwerk und Sicherheitsstruktur durch. Dabei berücksichtigen sie alle individuellen Anforderungen – wie zum Beispiel vorhandene On-Prem-Systeme oder Compliance-Vorgaben – und ermitteln anhand dieser Ergebnisse die beste Lösung. Wir begleiten Sie bei Ihrem digitalen Wandel und schaffen mit SASE eine Netz- und Sicherheitsarchitektur, mit der Sie künftigen Herausforderungen gelassen entgegensehen können.

Überwiegend Antwort 3

Die Digitalisierung ist in Ihrem Unternehmen angekommen. Hinsichtlich neuer digitaler Geschäftsmodelle oder softwaredefinierter Netzwerkkomponenten gibt es allerdings noch etwas Luft nach oben. Unsere Expertenteams zeigen Ihnen, an welchen Stellen Sie mit aktuellen Technologien auf Basis von SASE Ihr Netzwerk leistungsfähiger machen und Ihre Anwendungen, Daten und Nutzer besser schützen können. Braucht Ihr Unternehmen eine neue Web Application Firewall, ein neues Secure Web Gateway oder einen Zero Trust Network Access? Egal, wo Sie stehen – wir holen Sie genau dort ab und passen die Security entsprechend Ihrer Bedürfnisse an. Verlassen können Sie sich dabei auf unsere mehr als 20-jährige Praxiserfahrung aus internationalen Projekten sowie auf die Zero-Outage-Strategie für den weltweiten stabilen Betrieb von Netz- und Sicherheitsstrukturen.

Überwiegend Antwort 4 und 5

New Work, Data Analytics, SD-WAN: Glückwunsch, die digitale Transformation ist in Ihrem Unternehmen voll im Gange. Doch wächst Ihre Sicherheitsarchitektur mit den digitalen Anforderungen mit? Ist Ihr Netzwerk leistungsfähig genug, um jederzeit für die bestmögliche User Experience zu sorgen? Setzen Sie aktuelle Netzwerk- und Security-Lösungen ein, um Daten, User und Cloud Services in der digitalen Welt bestmöglich abzusichern? Oder gibt es noch Schwachstellen in Ihrer Infrastruktur, die Hacker ausnutzen könnten? Gemeinsam mit Ihnen ermitteln unsere Experten den Ist-Zustand Ihrer Netzwerk- und Security-Landschaft und spüren vorhandenes Verbesserungspotenzial auf. Wir zeigen Ihnen, wie Sie mit einer neuen Architektur auf Basis von SASE schneller mit Cloud-Services arbeiten und sich noch besser schützen als bisher. Zusammen entwickeln wir das entsprechende Netzwerk- und Sicherheitskonzept, setzen es um und übernehmen für Sie den hochverfügbaren Betrieb.

5. Sie wollen Ihre Netz- und Sicherheitsarchitektur zukunftsfähig machen? Wir unterstützen Sie dabei.

Mit über 20 Jahren Praxiserfahrung in Sachen Cyber- und Netzwerksicherheit sowie mehr als 1.600 Security-Experten bieten wir branchenübergreifende und moderne Lösungen – individuell zugeschnitten oder automatisiert und hoch standardisiert.

Um von allen Vorteilen von SASE zu profitieren, ermittelt unser großes Security-Expertenteam mit Ihnen den Ist-Zustand Ihrer Infrastruktur und plant die passende Sicherheitsarchitektur.

Gemeinsam führen wir eine Machbarkeitsstudie für SASE durch und realisieren Konfiguration, Integration, Testing sowie die Inbetriebnahme des neuen Security Frameworks.

Wir übernehmen den Betrieb Ihrer Netzwerk- und Sicherheitsarchitektur, sodass Sie SASE und damit ein umfassendes Sicherheitsportfolio aus einer Hand erhalten. Vertrauen Sie unserer hohen Betriebs- sowie Technologiekompetenz und konzentrieren Sie sich auf Ihr Kerngeschäft – wir machen Ihre digitale Welt ein Stück sicherer!



Quellenverzeichnis:

- ¹ IDC, Oktober 2021,
https://www.idc.com/getdoc.jsp?containerId=prEUR148293821&utm_medium=rss_feed&utm_source=alert&utm_campaign=rss_syndication
- ² BSI,
https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html
- ³ Citrix, September 2021,
https://www.citrix.com/content/dam/citrix/en_us/documents/off-site/the-state-of-security-in-a-hybrid-world.pdf
- ⁴ Citrix, September 2021,
https://www.citrix.com/content/dam/citrix/en_us/documents/off-site/the-state-of-security-in-a-hybrid-world.pdf
- ⁵ Gartner, Dezember 2019,
<https://blogs.gartner.com/andrew-lerner/2019/12/23/say-hello-sase-secure-access-service-edge>
- ⁶ Citrix, September 2021,
https://www.citrix.com/content/dam/citrix/en_us/documents/off-site/the-state-of-security-in-a-hybrid-world.pdf
- ⁷ DGB, Oktober 2020,
<https://index-gute-arbeit.dgb.de/++co++6bbbd7ec-0c7f-11eb-8fc7-001a4a160123>
- ⁸ Statista, Technology Market Outlook, Oktober 2021,
https://de.statista.com/outlook/technology-outlook, study_id84972_infrastructure-as-a-service-report.pdf
- ⁹ ISG, August 2021,
<https://www.pressebox.de/inaktiv/information-services-group/Mobiles-Arbeiten-und-Homeoffice-lassen-Markt-fuer-Software-Defined-Networking-SDN-rasant-wachsen/boxid/1074109>
- ¹⁰ DE-CIX,
https://www.de-cix.net/_Resources/Persistent/4/5/6/c/456cf64d570b8a83fc42503d7f99677a547da4ec/DE-CIX%20Gesch%C3%A4ftsbericht%20im%20Corona-Jahr%202020.pdf

Sie möchten mehr über einen schnellen und sicheren Zugang zur Cloud erfahren?

Unsere Expertenteams beraten Sie gerne, wie Sie Cloud Services so effizient wie möglich nutzen können.

KONTAKT

security@telekom.de
0228 181 0

HERAUSGEBER

Deutsche Telekom Security GmbH
Bonner Talweg 100
53113 Bonn
Deutschland



Erleben,
was verbindet.