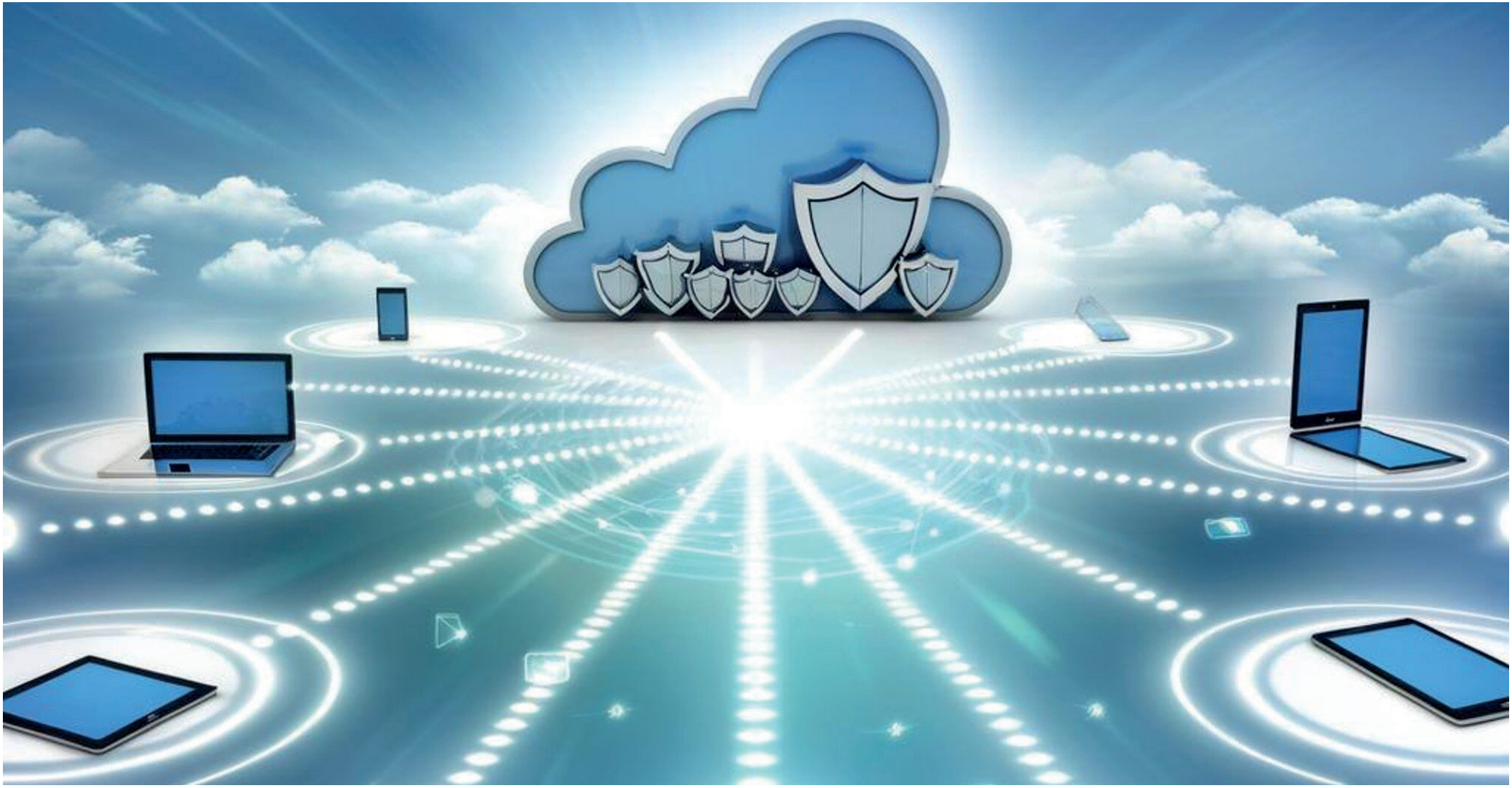
xantaro
connecting the world.

ALLES, WAS SIE SCHON IMMER ÜBER SASE WISSEN WOLLTEN

e-book



Inhalt

In der Vergangenheit wurden zahlreiche Netzwerk- und Cybersecurity-Konzepte entwickelt – meist getrennt voneinander, von unterschiedlichen Abteilungen mit unterschiedlichen Interessen. Die Folge: Einige Vorteile auf der einen Seite führten zu Nachteilen auf der anderen Seite.

Mit SASE hat sich ein neuer Ansatz etabliert, der beide Themen wieder zusammenbringt – bis hin zu einer integrierten Management-Konsole für sämtliche Funktionen. Wir haben in diesem e-book zusammengefasst, was hinter dem SASE-Konzept steckt und wie es sich in der Praxis umsetzen lässt.

Enterprise-Netzwerke müssen sich ständig neuen Herausforderungen anpassen, um den Anforderungen der Unternehmensstrategie und den Bedürfnissen der Anwender zu genügen. Zwar sind die grundsätzlichen Ziele, unter denen sich die Netzwerke großer Unternehmen weiterentwickeln müssen, immer noch die gleichen:

- **Skalierbarkeit**
- **Sicherheit**
- **Verfügbarkeit und Zuverlässigkeit**
- **Managebarkeit und Überwachung**
- **Integration neuer Technologien**

Doch nicht nur die technischen Voraussetzungen und Konzepte der IT-Welt ändern sich rasend schnell. Technische Innovationen stehen oft in Wechselbeziehung zum Wandel der Umgebungsbedingungen – sprich: Sie sind einerseits Antwort auf Trends, andererseits aber auch Verstärker dieses Wandels.

Zu den wichtigsten Faktoren, die Einfluss auf die Gestaltung von Enterprise-Networks nahmen, gehören vor allem:

- **Remote-Arbeit und hybride Arbeitsmodelle:**

  Die COVID-19-Pandemie hat den Trend zu Home Office und Mobile Working erheblich beschleunigt. Für Unternehmensnetzwerke stellt die sichere und zuverlässige Konnektivität für Mitarbeiter außerhalb des Büros eine enorme Herausforderung dar. Lösungen sind unter anderem VPNs, Zero-Trust-Sicherheitsmodelle und cloudbasierte Lösungen.

- **Zunehmende Cyberbedrohungen:**

  Die starke Zunahme von Cyberangriffen, allen voran mit Ransomware, die teils milliardenschwere Schäden nach sich ziehen, erfordert deutlich umfangreichere Sicherheitsmaßnahmen. Investiert wird vor allem in Sicherheitsprotokolle, Echtzeit-Überwachung und Bedrohungsabwehrmechanismen.

- **Cloud-Migration:**

  Die immer weiter fortschreitende Migration von Unternehmensanwendungen und -diensten in die Cloud bedingt Anpassungen an der Netzwerkarchitektur. Flexibilität, Skalierbarkeit und Zuverlässigkeit sowie steigende Bandbreiten stehen an erster Stelle, um die Infrastruktur für Hybride und Multi-Cloud-Umgebungen zu ertüchtigen. Für eine Cloud-First-Strategie müssen neue Technologien her, da z.B. MPLS lediglich das WAN-Umfeld unterstützt, aber nicht den Cloud-Zugang. Nachdem zunächst SD-WAN als Mittel der Wahl galt, das weniger starr ist als MPLS und kostengünstigere Vernetzungsvarianten kombinieren kann, rückt inzwischen das umfangreichere SASE-Konzept ins Interesse von Unternehmen.

- **5G-Mobilfunk:**

  Der neue Mobilfunkstandard 5G, der z.B. in Deutschland seit 2019 aufgebaut wird, ist speziell auf die Kommunikationsanforderungen der Industrie ausgerichtet. Hohe Bandbreite, geringe Latenz, umfangreiche Clientzahlen, Energie-Effizienz und zahlreiche Funktionen zur Unterstützung von IoT (Internet of Things)

und andere Anwendungen haben neue Möglichkeiten für Unternehmensnetzwerke geschaffen. Diese gilt es nun in die bestehenden Netzwerk-Infrastrukturen und Management-Anwendungen zu integrieren.

- **Automatisierung und KI:**

  Die vorstehend genannten Trends haben dazu beigetragen, die Komplexität moderner Netzwerke zu erhöhen. Als Reaktion darauf setzen Unternehmen verstärkt auf Automatisierung. In einem weiteren Schritt hält inzwischen auch KI Einzug ins Netzwerkmanagement. Ziele sind die Optimierung des Netzwerkbetriebs, der vorausschauenden Wartung und ein schnelles Erkennen von Anomalien oder Sicherheitsvorfällen.

- **Gesetzliche Anforderungen:**

  Nicht zuletzt müssen sich Unternehmen auch den Anforderungen des Gesetzgebers stellen, die darauf abzielen, eine zunehmend digitalisierte, vernetzte Wirtschaft und Gesellschaft funktionsfähig zu erhalten sowie z.B. Bürger-, Konsumenten- und Arbeitnehmerrechte durchzusetzen. Neben DSGVO / GDPR und DigiNetzG 2 ist hier insbesondere die zweite Richtlinie über Netz- und Informationssicherheit (NIS2) der EU zu nennen, die sich der Cybersicherheit von kritischen Infrastrukturen und digitalen Dienstleistern widmet. Die 2021 verabschiedete Richtlinie stellt ab Oktober 2024 neue Anforderungen insbesondere an große Unternehmen.

Komplexität am Limit

Das Management und die Absicherung eines Unternehmensnetzwerks sind inzwischen mit so vielen unterschiedlichen Aspekten behaftet, dass die IT-Administration ans Limit kommt. Das wir schnell deutlich, wenn man sich vor Augen führt, welche verschiedenen Technologien und Anwendungen in einem modernen, flexiblen Netzwerk zum Einsatz kommen. So gilt es, zentrale Unternehmensressourcen, entfernte Unternehmensstandorte, externe DataCenter, mobile Anwender, Kunden und Dienstleister sowie Ressourcen in der Cloud (XaaS) miteinander zu verbinden. MPLS, SD-WAN, VPN oder andere Technologien leisten zwar gute Dienste, wenn Netzknoten direkt bzw. in einem mehr oder minder geschlossenen Unternehmensnetzwerk miteinander verbunden werden. Jedoch sind inzwischen diese Netzwerke mit

Cloud-Anwendungen, Home- und Mobile-Mitarbeitenden etc. nicht mehr geschlossen. Daraus ergeben sich ganz neue Anforderungen in Bezug auf Cybersecurity an den einzelnen Netzknoten, wie z.B. Filialen oder Home Offices. Um die Sicherheit zu gewährleisten, können Unternehmen aus einer ganzen Reihe unterschiedlicher Konzepte und Maßnahmen wählen, wobei stets eine Kombination mehrerer, unterschiedlicher Prozesse und Anwendungen nötig sind.

Hier ein Überblick über die wichtigsten Themen:

- **Firewalls in unterschiedlicher Ausführung (On Premise, NGFW, FWaaS, WAF)**
- **Endpoint-Absicherung (EDR, EPP)**
- **Erkennung von und Reaktion auf Cyberangriffe (XDR, NGAM, NTA, IPS, DNS Protection)**
- **Konzepte zur Zugriffssicherung (ZTNA, RBAC, RBI)**

Gewachsene Strukturen bedrohen die Sicherheit

Ein großes Problem für viele Unternehmen: Sie integrieren immer wieder neue Tools und Technologien in die Netzwerk-Infrastrukturen, um das immer komplexer werdende Unternehmensnetzwerk zu managen und abzusichern. Doch jede Lösung hat ihre eigene Konsole und ihren eigenen Lösungslebenszyklus. So muss sich die IT-Administration zigfach um Ressourcenbedarf und Lizenzverwaltung, Kauf, Bereitstellung und Konfiguration der verschiedenen Tools und Anwendungen kümmern, und diese bei Bedarf skalieren, aktualisieren, patchen oder außer Betrieb nehmen. Und natürlich müssen die damit verbundenen Dashboards und Alarmsysteme überwacht werden, um im Fall einer Anomalie schnell reagieren zu können. Immer wieder werden im Kampf gegen die wachsende Komplexität neue Systeme irgendwo „angeflanscht“, sprich: mittels rudimentärer APIs und gar selbstprogrammierter Schnittstellen mit anderen Systemen verbunden, wobei auf diesem Weg oft nur ein Teil der Funktionalität zugänglich ist.

Erste Ansätze, diesem Problem zu begegnen, waren bereits in der Vergangenheit zu sehen. Im Bereich der Cybersecurity ist hier beispielsweise Unified Threat Management (UTM) zu nennen. Also eine umfassende Sicherheitslösung, die verschiedene Aspekte der Gefahrenerkennung und -abwehr in einem System zusammenfasst. Die Vorteile liegen auf der Hand: Aufeinander abgestimmte Anwendungen kommen sich nicht gegenseitig ins Gehege, und eine einheitliche Management-Oberfläche reduziert die Komplexität, vereinfacht die Bedienung und trägt so dazu bei, dass Konfigurationsfehler vermieden werden.

UTM versammelt unter anderem Firewall-Schutz, Antivirus, Intrusion Detection und Prevention, Spamfilterung, VPN-Unterstützung und Web-Filterung unter einem Dach. Diese Zentralisierung ist zugleich der größte Nachteil des Konzepts: Wird die UTM-Appliance überwunden, sind mit einem Schlag zahlreiche Sicherheitsmaßnahmen außer Kraft gesetzt.

Ähnliche Überlegungen stehen im Bereich des Netzwerkmanagements hinter dem Konzept SD-WAN. Das software-definierte WAN erlaubt es Unternehmen, verschiedene Verbindungstypen unter einer Oberfläche verwalten, von klassischen Breitbandverbindungen über LTE bis zu MPLS. Dabei können Anwendungen eigene Verbindungen zugwiesen werden, die jeweils auf ihre Anforderungen an Bandbreite und Latenz optimiert sind. Einfachere Geräteverwaltung, Automatisierungsfunktionen und eine Optimierung der Leitungskosten tragen zur Reduzierung von Personalaufwand und Kosten bei. Doch es zeigte sich, dass das Konzept in dieser Form auch Schattenseiten hat. Diese betreffen insbesondere das Zusammenspiel mit Cybersecurity-Anwendungen, aber auch SD-WAN-spezifische Eigenschaften wie „Full Mesh“, also eine alles umfassende Vernetzung, sprich: keine oder nur geringe Barrieren im Inneren des Netzwerks. Dies bedingt zwangsläufig höhere Anstrengungen bei der Absicherung des Netzwerks nach außen.

So können beide Ansätze zwar in ihrem jeweiligen Themengebiet – einmal Security, einmal Netzwerkkonfiguration und -management – jeweils spezifische Verbesserungen erreichen. In Summe jedoch erweisen sich jedoch weder UTM noch SD-WAN bislang als optimale Lösung, da sie den jeweils anderen Themenbereich ausblenden und dadurch an anderer Stelle den Aufwand erhöhen.

SASE-Vorteile bei der WAN-Transformation

	MPLS ersetzen/ Bandbreite erhöhen	Globale Konnektivität	Sichere DIA	Optimieren Sie den Cloud Zugriff	Optimieren Sie den mobilen Zugriff	Wirklich einfache Verwaltung
SASE	✔	✔	✔	✔	✔	✔
Edge-SD-WAN	✔	✘	✘	◐	✘	✘
Privates globales Backbone	✘	✔	✘	✔	✘	✘
NGFW/UTM	✔	✘	✔	✘	◐	✘
SWGs	✘	✘	✔	✘	✔	✘

Security Service Edge für komplexe Netzwerk-Infrastrukturen

Wenn Ressourcen verstreut bereitgestellt sind und die klassische Perimeter-Absicherung dadurch nicht mehr durchgängig greift, werden die Absicherung des Dienstes und der Identität an sich sowie sinnvolle Autorisierungen an allen relevanten Stellen wichtig. Aus diesen Überlegungen heraus hat das Konzept „Zero Trust Network Access (ZTNA)“ an Bedeutung gewonnen. Dabei wird zunächst unterstellt, dass ein Account aus seiner Existenz heraus nicht vertrauenswürdig ist und immer wieder überprüft wird, auf welche freigeschalteten Ressourcen diesem Zugriff gegeben werden soll.

Ein weiteres Security-Element für solche komplexen Netzwerk-Strukturen liefert der Cloud Access Security Broker (CASB). Er fungiert als Vermittler zwischen Nutzern und Cloud-Service-Anbietern. Die Fähigkeit, damit Sicherheitsrichtlinien durchzusetzen und Sicherheitslücken zu schließen, erstreckt sich auf Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) und Infrastructure-as-a-Service (IaaS) Umgebungen.

Zusätzlichen Schutz vor Bedrohungen aus dem Internet bietet das SWG (Secure Web Gateway), indem es zwischen Benutzer und Webseite Filterungen und Prüfungen durchführt. Weiterer Datenverkehr aus verschiedenen Quellen sichert die FWaaS (Firewall as a service) ab. Dabei handelt es sich um einen Next-Generation-Firewall-Service, der die Datenströme analysiert und konsolidiert sowie IDS/IPS Dienste liefert und durchsetzt.

Es sind mindestens CASB, ZTNA, SWG und FWaaS, die unter dem Begriff SSE (Security Service Edge) zusammengefasst werden. Es gibt aber auch noch weitere Features wie DLP (Data Loss Prevention) oder RBI (Remote Browser Isolation), die ebenfalls Bestandteil eines SSE-Konzepts sein können.

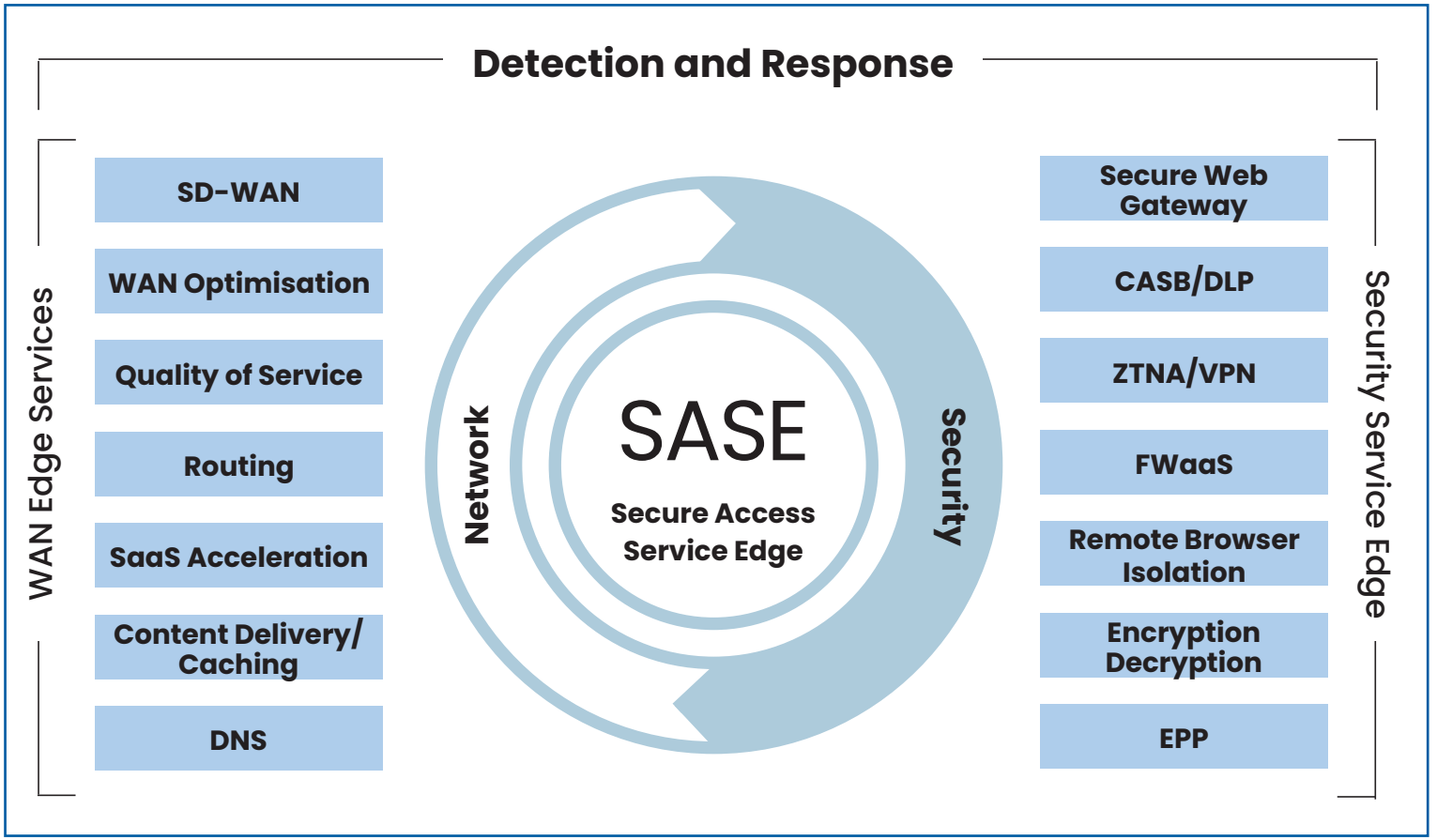
SASE: Netzwerk und Sicherheit gemeinsam denken

Das Spannende: SASE ist wiederum ein Baustein einer Architektur, die sowohl die Konfiguration und das Management von Unternehmensnetzwerken als auch deren Sicherheitsaspekte zusammenbringt. Die Analysten von Gartner prägten dafür den Begriff SASE, als Akronym für „Secure Access Service Edge“. SASE steht für die Bereitstellung von möglichst konvergenten, also überein- und aufeinander abgestimmten Netzwerk- und Security-Funktionen aus einer Hand, egal von wo ein Zugriff erfolgt, auf der Grundlage einer gesicherten Identität sowie der Security-und Compliance-Richtlinien des Unternehmens.

Oder anders gesagt: SASE ist die Kombination aus SSE (Sicherheitsrichtlinien) und Netzwerkkonnektivität In einer einheitlichen, konvergenten, cloud-nativen Architektur. Auf diese Weise wird ein gleichmäßig hohes, transparentes Sicherheitslevel bei flexibler, dezentraler Netzwerk-Skalierung gewährleistet. Zugleich dient SASE dem Ziel, die Komplexität hybrider und verteilter Netzwerke und Konfigurationen einzufangen und diese über eine einheitliche Bedienung administrierbar halten – im Idealfall sogar unter einer einheitlichen Management-Oberfläche.

So lassen sich Aufwand und Kosten, die in einer komplexen und fragmentierten Infrastruktur aus Einzellösungen zu explodieren drohen, wieder auf ein vernünftiges Maß absenken. Zugleich werden aufgrund der besseren Bedienbarkeit die Risiken von Sicherheitsverletzungen und Datenverlusten durch eine optimale Sicherheitslage reduziert. Weitere Vorteile sind ein sicheres Arbeiten von überall aus und der verbesserte Zugriff auf globale Anwendungen vor Ort und in der Cloud.

SASE vereint Punktlösungen für SD-WAN und Netzwerksicherheit

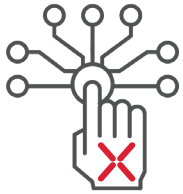


xantaro
connecting the world.

Die wichtigsten Aspekte von SASE

SASE bietet einen integrierten cloudbasierten Service, der alle Standorte, Benutzer, Geräte und Anwendungen vor Ort und in der Cloud verbindet und absichert.

Eine SASE-Lösung umfasst vier Hauptmerkmale:



• Identitätsgesteuert

Die Benutzeridentität bildet die Grundlage für risikobasierte Zugriffsrichtlinien, die auch den Gerätestatus des Benutzers, die Sensibilität der Daten oder Anwendungen, auf die zugegriffen wird, und die gewünschte Funktion berücksichtigen. Benutzer unterliegen den festgelegten Unternehmensrichtlinien nahtlos im Büro, unterwegs und zu Hause – so wird eine konsistente Durchsetzung in allen Situationen gewährleistet.

• Unterstützung für alle Randbereiche

SASE bietet konsistente Sicherheit und Optimierung für jeden Knoten am Rand des Unternehmensnetzwerkes (Edge), einschließlich On-Premises- und Cloud-Rechenzentren, Zweigstellen, bis hinunter zum einzelnen Benutzer oder Gerät.

• Cloud-nativ

Cloud-natives SASE ist flexibel, selbstreparierend und selbstverwaltend. SASE wird als globaler Cloud-Service bereitgestellt. Es passt sich schnell an neue Geschäftsanforderungen an und macht alle Netzwerk- und Sicherheitsfunktionen überall verfügbar.

• Global verfügbar

SASE basiert auf einem erweiterbaren globalen Cloud-Netzwerk, um Netzwerk- und Sicherheitsfunktionen mit geringer Latenz für alle Benutzer und Unternehmensstandorte überall auf der Welt bereitzustellen.

xantaro
connecting the world.

Eine detailliertere Betrachtung listet neben diesen vier Kernfunktionalitäten einer SASE-Lösung noch weitere Eigenschaften auf:

- **Integrierte Architektur**
  Netzwerk und Sicherheit immer zusammen denken.

- **Globales, Cloud-basiertes Backbone-Netzwerk**
  mit „Points-of-Presence" (PoPs) als Einsprungs-Punkt für Standorte und Remote User; dabei werden SD-WAN-Funktionen genutzt, um einen optimalen und ausfallsicheren Einstieg in den SASE-Cloud-Service zu ermöglichen.

- **Einheitliches Management**
  mittels Management-Anwendung (CMA) und Plattform-API.

- **„Built-in Self Healing",**
  also automatische Fehlererkennung und -mitigation.

- **Dynamisches, intelligentes und automatisches Traffic-Management**

- **Lokale Datenverarbeitung**
  Wann immer möglich, sollen Daten möglichst nahe ihrer Quelle verarbeitet werden; das Cloud Network optimiert das globale Routing beispielsweise für latenzempfindlichen Datenverkehr wie Sprache und Video sowie den Zugriff auf Cloud- und On-Premises-Anwendungen für alle Quellen und Ziele.

- **Identitäts-Fokus**
  User- und Ressourcen-Identitäten sind bestimmend für Zugriffe und Zugriffslevel; sie werden im Rahmen des Zero-Trust-Netzwerkzugriffs (ZTNA) von Fall zu Fall neu evaluiert.

- **Next-Generation-Security**

  für alle Benutzer, Dienste und Geräte, egal von welcher Lokation aus sie sich einwählen; insbesondere Firewall-as-a-Service (FWaaS), Cloud Access Security Broker (CASB) und Sicheres Web-Gateway (SWG) sind hier zu nennen.

- **Data Protection für Daten in Transit**,

  zum Beispiel mittels IPSec und TLS, zusätzlich Network Access Control (NAC) und Data Loss Prevention (DLP).

- **Threat Prevention in Echtzeit**

  mit Sandboxing sowie IDS/IPS und Secure Web Access sowie erweiterte Erkennung und Reaktion (XDR) und Endpunktschutz (EPP/EDR).

- **Multi-Cloud-Konnektivität**

  Zusätzlich werden in letzter Zeit auch Features wie AIOps (AI Operations, Künstliche Intelligenz für den IT-Betrieb), Internet of Things-Integration (IoT-Integration), Multi-Tenant-Fähigkeit und Managed SASE genannt, also die Verwaltung der SASE-Ressourcen durch einen externen Dienstleister.

Praktische Umsetzung

Das Herzstück einer SASE-Lösung ist das Cloud-basierte Netzwerk, das als globaler privater Backbone fungiert. Der Zugang erfolgt über die sogenannten PoPs (Points of Presence). PoPs sind Einstiegsknoten in den Service des SASE-Anbieters. Der Betrieb und die sinnvolle weltweite geographische Verteilung möglichst vieler PoPs ist genauso wichtig wie die „Vollwertigkeit" eines PoPs. Jeder PoP stellt bestenfalls alle Leistungen in punkto Netzwerk und Sicherheit bereit. PoPs, die lediglich als Netzwerkzugang dienen, würden ein Weiterrouten zu einem leistungsfähigeren PoP erfordern, was wiederum die Latenz erhöht.

Um einen optimalen und ausfallsicheren Einstieg in den SASE-Cloud-Service zu ermöglichen, setzt die SASE-Lösung am PoP auf ein optimales WAN-Management mittels SD-WAN. Dementsprechend können Unternehmen mit der Einführung von SASE direkt den Schritt weg von MPLS hin zu einer End-to-End-Netzwerkoptimierung inklusive SD-WAN-Funktionalität gehen. Die Kombination aus PoPs und einem globalen privaten Backbone mit definierten Eigenschaften bietet sowohl Kostenvorteile als auch Qualitätsverbesserungen gegenüber starren, teueren MPLS-Strukturen, Premium-Cloud-Konnektivitätslösungen wie AWS DirectConnect und Microsoft ExpressRoute oder dem Internet mit seinen unvorhersehbaren Zuständen.

Ein PoP kann zwar als Einstieg ins Internet dienen – er ist aber zunächst Teil des SASE-Netzwerks. Darüber angebundene Zweigstellen werden über die integrierte Security-as-a-Service abgesichert. Damit entfällt die Notwendigkeit für den Einsatz von Security Point Solutions. Ebenso kann ein SASE-Netzwerk Funktionen zur sicheren und netzwerkoptimierten Anbindung von Home Offices und Geräten im mobilen Einsatz bieten, oder für Remote-Zugriffe, beispielsweise im Rahmen einer Internet-of-Things-Anwendung (IoT).

Kein „alter Wein in neuen Schläuchen“

Auf den ersten Blick mag es so scheinen, als sei SASE eine Art „Suite“, die sich einfach aus bereits bekannten Netzwerk- und Security-Bausteinen zusammenbauen lässt. Verschiedene Hersteller versuchen dementsprechend, ihre Angebote anzupassen und je nach bisherigem Fokus auf Netzwerk oder Security zu ergänzen und bestenfalls alle Optionen in einer einzigen Konfigurationsoberfläche zu bündeln – sei es durch eigene Entwicklungen oder integrierte Tools.

Doch das funktioniert nur bedingt – schließlich liegt das Versprechen des SASE-Konzepts in einer nahtlosen Integration aller enthaltenen Eigenschaften, was sowohl funktionale Abstimmung der verschiedenen Komponenten umfasst, als auch eine einheitliche Bedienbarkeit – bis hin zu einer vollintegrierten Managementkonsole. Man muss also wie immer genau hinsehen, was die präferierte Herstellerimplementierung qualitativ leistet.

Integrierte SASE-Lösung von Cato

Die weltweit erste Single-Vendor-Implementierung einer SASE-Plattform, die SD-WAN und Netzwerksicherheit zu einem globalen Cloud-nativen Service „aus einer Hand“ zusammenführt, stammt von Cato. Die Cato SASE Cloud vereint alle Netzwerkressourcen des Unternehmens, indem der gesamte WAN- und Internetverkehr in der Cloud konsolidiert und über eine Reihe von Sicherheitsservices abgesichert wird.

Das globale private Backbone von Cato besteht aus rund 90 PoPs weltweit, die über mehrere SLA-gesicherte Tier-1-Provider miteinander verbunden sind. Auf jedem PoP läuft der Cloud-native Software-Stack von Cato, der vollständig mandantenfähig und skalierbar ist. Er liefert alle nötigen Netzwerkfunktionen, wie globale Routenoptimierung, dynamische Pfadauswahl, Verkehrsoptimierung und

Ende-zu-Ende-Verschlüsselung. Desweiteren übernimmt der Stack auch die Durchsetzung der Funktionen, die von den Cato-Security-Services benötigt werden, beispielsweise zur Analyse des Datenverkehrs oder zur Durchsetzung von Unternehmensrichtlinien.

So sind alle Funktionen in einem einzigen System vereint und können Hand in Hand funktionieren. Zu den integralen Bestandteilen des Cato SASE Stack zählen beispielsweise:

- **WAN-Optimierung zur Maximierung des Datendurchsatzes**
- **globale Routenoptimierung unter Berücksichtigung von Latenzzeiten, Paketverluste und Jitter**
- **Ende-zu-Ende-Verschlüsselung unter Verwendung der stärksten Industriestandard-Chiffriersuiten oder auch**
- **eine selbstheilende Architektur, die eine Dienstverfügbarkeit von 99,999 Prozent garantiert**

Zugang und Sicherheit

Der Zugang zum Cato Edge SD-WAN erfolgt über Cato Socket, ein Zero-Touch-Gerät, das in wenigen Minuten einsatzbereit ist, sobald es mit Strom und Internet verbunden ist. Die Appliance wird von Catos Network Operations Center (NOC) kontinuierlich überwacht und aktualisiert. Cato Socket kümmert sich unter anderem um Link Aggregation, dynamische Pfadauswahl, Anwendungsidentifizierung mittels Deep Packet Inspection (DPI) auf Basis einer eigenen Cato Engine, Regeln für das Bandbreitenmanagement, Techniken zur Verringerung von Paketverlusten, Integration von Routing-Protokollen und das Sicherstellen von Hochverfügbarkeit der Netzwerkverbindung – ohne großen Konfigurationsaufwand und ohne zusätzliche Kosten.

Abgesichert wird der Datenverkehr im Cato SASE Network durch den Cloud-nativen Security Service Edge (SSE), Cato SSE 360, auf Basis der Cato Single Pass Cloud Engine (SPACE) Architektur. Darin sind

alle wesentlichen Security-Funktionen enthalten: Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Datenverlust Prävention (DLP), Zero Trust Netzwerkzugang (ZTNA) und Firewall as a Service (FWaaS) mit Advanced Threat Prevention (IPS, Next Generation Anti-Malware). Cato IPS setzt auf Echtzeit-Deep-Learning-Algorithmen zur Bedrohungsprävention. Nach Angaben des Herstellers können darüber sechsmal mehr bösartige Domänen identifiziert werden als nur mit Reputationsfeeds allein. Verwaltet und aktualisiert werden die Dienste vom Cato SOC (Security Operations Center).

Mobile sowie Remote-Zugriffe laufen zunächst über einen Cato-Client oder einen clientlosen Browser-Zugang, über die sich Benutzer mit dem nächstgelegenen Cato-PoP verbinden. So haben auch diese vollen Zugriff auf sämtliche Netzwerk- und Sicherheitsfunktionen im Cato SASE Network, so dass der Schutz der Daten und der Benutzeraktivitäten auf Unternehmensniveau erfolgt.

Darüber hinaus ermöglicht Cato die Regulierung des Zugangs von Remote- und mobilen Anwendern mittels Zero Trust Network Access (ZTNA) und Software-Defined Perimeter (SDP) auf granularer Ebene, bis hin zu spezifischen Anwendungen. Herkömmliche VPN-Lösungen ermöglichen demgegenüber lediglich die Zugriffskontrolle auf der Ebene ganzer Subnetze.

Anbindung von Cloud-Ressourcen

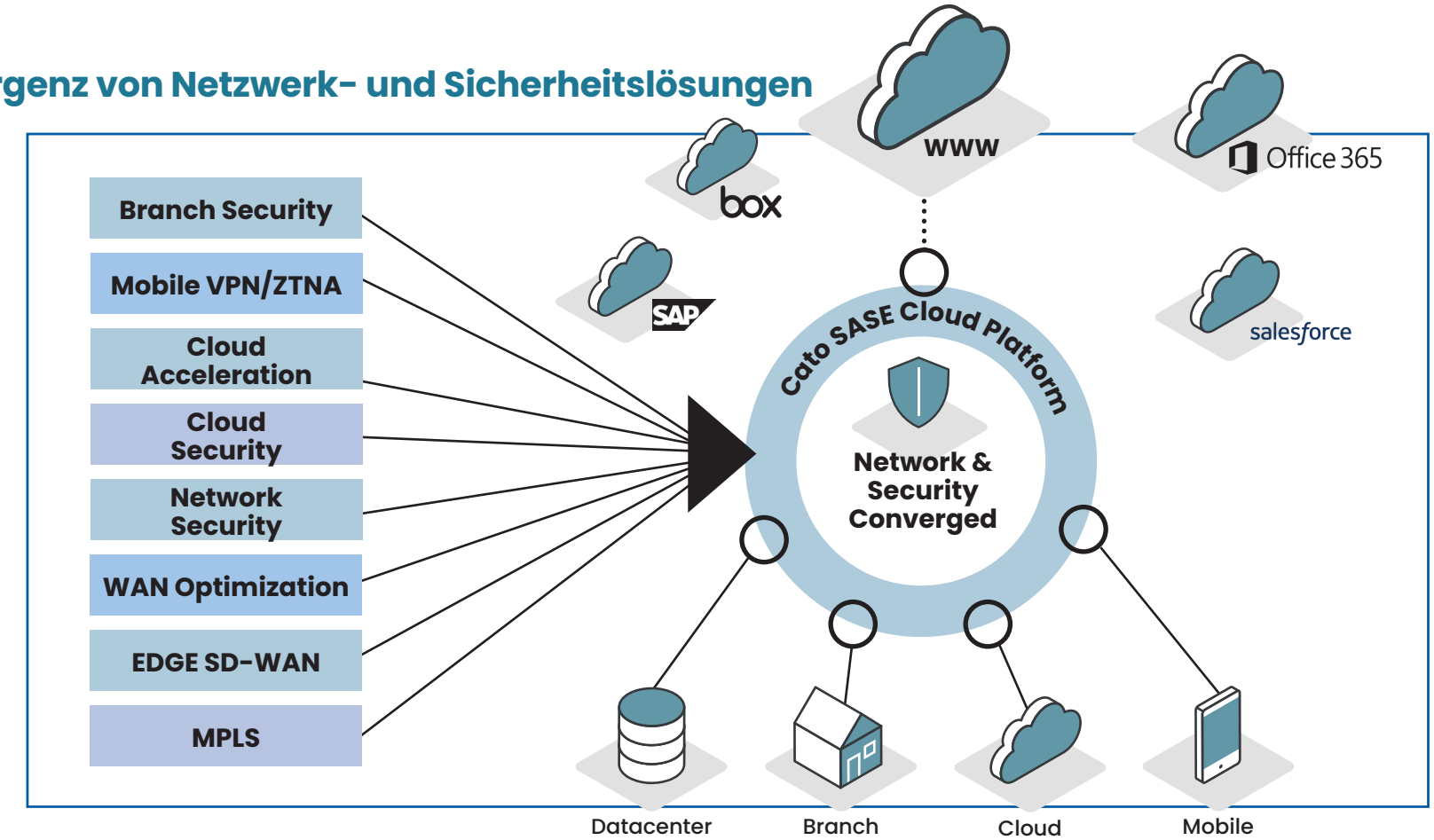
Cloud-Anbieter, wie Amazon AWS, Microsoft Azure, Google Cloud und andere, verbinden sich mit dem globalen privaten Backbone von Cato genauso wie andere Standorte auch, indem die Clouds mittels einer virtuellen Variante des Cato Sockets (vSocket) oder über IPsec in das Unternehmensnetzwerk eingebunden werden. Da die Cato PoPs in der Regel lediglich 1-2ms Latenz zu den großen Hyperscale-Clouds aufweisen, wird der Datenverkehr optimal geroutet und benötigt keine zusätzlichen, teuren Express-Services.

Auf ähnliche Weise funktioniert auch die Beschleunigung von Public-Cloud-Anwendungen, wie Office

365, Cloud ERP, UCaaS und Cloud Storage. Die Latenz wird durch optimales Routing des Cloud-Anwendungsdatenverkehrs über Catos globales, privates Backbone zum Cato-PoP, der dem Rechenzentrum des Cloud-Anwendungsanbieters am nächsten liegt, reduziert. Die integrierte WAN-Optimierung von Cato maximiert den End-to-End-Durchsatz, insbesondere bei bandbreitenintensiven Vorgängen.

Die SaaS-Integration ist agentenlos und erfordert keine virtuellen Appliances. Die agentenlose Konfiguration nutzt die IPsec-Gateway-Konnektivität, die von allen Cloud-Anbietern zur Verfügung gestellt wird. Für Anwender, die eine virtuelle Appliance bevorzugen, greifen die Smart Egress Regeln, nach denen SaaS Traffic, z.B. O365, dann immer zum nächstgelegenen PoP geroutet werden, bei O365 zum Beispiel meist Amsterdam oder Frankfurt.

Cloudnative Konvergenz von Netzwerk- und Sicherheitslösungen



xantaro
connecting the world.

Management und Integration in externe Systeme

Cato bietet seinen Kunden eine Self-Service-Management-Anwendung für Ereignisse, Analysen und die Richtlinienkonfiguration. Die Cato-Verwaltungskonsole kombiniert Benutzerfreundlichkeit mit hoher Leistungsfähigkeit. Administratoren definieren granulare Netzwerk- und Sicherheitsrichtlinien ohne lange Lernkurve oder sich wiederholende manuelle Vorgänge. Dabei werden sie von einer kontextsensitiven Benutzeroberfläche unterstützt.

Eine umfassende Netzwerktransparenz liefern Analysen und Berichte in Echtzeit oder für zurückliegende Zeiten. So können IT-Administratoren die wichtigsten Herausforderungen in den Bereichen Zugriffskontrolle, Benutzererfahrung, Fehlerbehebung und Schatten-IT lösen.

Vollständige Netzwerk- und Sicherheits-Ereignisprotokolle können zusammengestellt und an externe SIEM-Lösungen (Security Information and Event Management) übertragen werden, wenn dies benötigt wird. Auf diese Weise müssen Daten von mehreren Geräten und Quellen nicht manuell aggregiert werden, sondern es stehen alle Ereignisse gesammelt über eine einzige Schnittstelle zur Verfügung.

Darüber hinaus bieten Cato sowie zertifizierte Partner eine Reihe von Managed Services an, die bei Bedarf gebucht werden können. Zu den verfügbaren Optionen gehören unter anderem Standortbereitstellung, intelligente Überwachung der letzten Meile, Konfiguration von Änderungen der Netzwerk- und Sicherheitsrichtlinien sowie Managed Detection and Response (MDR).

Positive Einstufung durch Gartner-Analysten

Im Sommer 2024 veröffentlichte Gartner seine Markteinschätzung „Magic Quadrant for Single-Vendor SASE“. In diesem Report landet Cato im Leader-Quadrant. Die Marktanalysten loben den Hersteller für seine umfassende, unkomplizierte Benutzeroberfläche, die über eine einheitliche Plattform bereitgestellt wird. Zudem bescheinigen sie Cato, als Pionier den Markt in einer frühen Phase vorangetrieben zu haben. Zugleich äußern sie die Erwartung, dass das Unternehmen auch künftig dieses Segment mit seinen Innovationen prägen wird. Zudem wird Cato im Rahmen der Studie ein überdurchschnittliches Kundenerlebnis im Vergleich zu anderen Anbietern attestiert.

Zuvor hatten auch andere Marktanalysten bereits positive Einschätzungen publiziert. Unter anderem ist hier der Bericht „Forrester Wave: Zero Trust Edge Solutions Q3/2023“ zu nennen, der Cato als führend einstuft und den Anbieter als „Aushängeschild“ für ZTE und SASE anerkennt. Frost & Sullivan zeichnete Cato als Wachstums- und Innovationsführer im Bereich SASE und im „Product Leadership Award 2023“ für seine Cato SSE 360, eine Schlüsselkomponente der Cato SASE Cloud-Plattform, aus. Positive Auszeichnungen als „Leader“ wurden ebenso von Omdia und GigaOm veröffentlicht.

Fazit

Die Digitale Transformation von Wirtschaft und Gesellschaft schreitet weltweit mit großen Schritten voran. Datenübertragung und -analyse nehmen schnell zu, immer mehr Arbeitsplätze werden digital, und die Kunden erwarten innovative digitale Services. Zugleich beruht der Unternehmenserfolg immer stärker darauf, seine digitalen Assets zu schützen und das Funktionieren der digitalen Infrastruktur – sowohl innerhalb des Unternehmens, als auch gegenüber Lieferanten und Vertriebspartnern, Dienstleistern und Kunden – sicherzustellen.

Netzwerk-Infrastruktur und -management ist dabei nur die eine Seite der Medaille, Cybersecurity ist die andere Seite. Hier steigen Aufwand und Risiko in den vergangenen Jahren steil an – die Gefahr

eines Angriffs nimmt zu, gleichzeitig nehmen die Schäden, die Cyberkriminelle, erboste Mitarbeiter oder „IT-Unfälle“ anrichten, teils bedrohliche Ausmaße an. Man denke nur an den Ransomware-Angriff auf die Reederei Maersk (Schaden: 200-300 Mio. US-Dollar) oder das Update-Fiasko von Crowdstrike, das mutmaßlich eine oder sogar mehrere Mrd. Dollar kostete.

Auch der Gesetzgeber reagiert auf die veränderte Situation. Damit die Versorgung der Bevölkerung und das Funktionieren der Wirtschaft sichergestellt sind, werden bestehende Regelungen zur Cybersecurity beständig verschärft und durch neue Anforderungen ergänzt, wie etwa die ab Oktober 2024 greifende EU-Richtlinie NIS2, die B3S-Branchenstandards oder die ständige Ausweitung des KRITIS-Begriffs, so dass immer mehr Unternehmen als Kritische Infrastruktur gelten und damit verschärften Anforderungen unterliegen.

Der Druck, Unternehmensnetzwerke flexibel und skalierbar, sicher und zukunftsfähig zu gestalten, ist enorm. Mit SASE ist nun eine Technologie verfügbar, die auf der einen Seite die beiden Seiten der Medaille wieder zusammenbringt und dabei gleichzeitig die Komplexität reduziert und damit auch den Aufwand senkt sowie die Anwendbarkeit verbessert. Die Qualität einer SASE-Lösung ist in hohem Maße davon abhängig, dass die verschiedenen Bausteine tatsächlich gut aufeinander abgestimmt sind und ein einheitliches Management zur Verfügung steht. Nur so lassen sich tatsächlich Effizienzgewinne erzielen, die sich in Kostensenkungen und Qualitätsverbesserungen niederschlagen.

Ein Beispiel, wie man das von Gartner definierte Konzept sinnvoll umsetzt, zeigt die Cato SASE Cloud. Sie bietet nicht nur alle relevanten Funktionen zur Optimierung des Netzwerks und einer zuverlässigen Absicherung des Datenverkehrs. Als Lösung aus einer Hand, bei der sämtliche Komponenten aufeinander abgestimmt sind, und zusätzlich mit einer hochintegrierten, einheitlichen Management-Konsole ausgestattet, können sich Anwender sicher sein, dass die Komplexität beim Netzwerk- und Security-Management spürbar reduziert wird.

Liste der verwendeten Security- und Network-Akronyme

AI	Artificial Intelligence -> KI
AIOps	Artificial Intelligence Operations (Künstliche Intelligenz für den IT-Betrieb)
APT	Advanced Persistent Threat
BG	Border Gateway Protocol
CASBP	Cloud Access Security Broker
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMA	Cato Management Application
CRA	Cyber Resilience Act
CSO	Chief Security Officer
CVE	Common Vulnerabilities and Exposure
DC	DataCenter (Rechenzentrum)
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DNS	Domain Name System
DNSSEC	DNS-Sicherheit, Domain Name System Security
DORA	Digital Operational Resilience Act
DPI	Deep Packet Inspection

EDR	Endpoint Detection and Response Solution
EPP	Endpoint Protection Platform (Endpunkt-Schutz)
FW	Firewall
FWaaS	Firewall as a service
Gen-A etc.	Generative Artificial Intelligenz – KI zur Generierung von Bildern, Videos etc.
HA	High Availability (Hochverfügbarkeit)
IaaaS	Infrastructure-as-a-Service
IAM	Identität- & Access-Management
IDS	Intrusion Detection Systems
IoC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IPSec	Internet Protocol Security – Framework zur Absicherung des IP-Datenverkehrs
ISP	Internet Service Provider
KI	Künstliche Intelligenz
KRITIS	Organisationen und Einrichtungen der Kritischen Infrastruktur
LTE/5G Generation	Long Term Evolution/5th Generation -> Mobilfunk der 4. und 5. Generation

MDR	Managed Detection and Response
MNG	Malware Next-Generation
MPLS	Multiprotocol Label Switching
MSSP	Managed Security Service Provider
NGAM	Next Generation Anti-Malware
NGFW	Next Generation Firewall
NIS2	Zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit
NOC	Network Operations Center
NTA	Network Traffic Analysis
PaaS	Platform-as-a-Service
PoP	Point of Presence
QOS	Quality of Service
RBAC	Role-based Access Control (Rollenbasierte Zugriffskontrolle)
RBI	Remote Browser Isolation
SaaS	Software-as-a-Service
SASE	Secure Access Service Edge
SD-WAN	Software-Defined Wide Area Network
SDP	Software-Defined Perimeter
SIEM	Security Information and Event Management

SOAR	Security Orchestration Automation and Responses
SOC	Security Operations Center
SSE	Security Service Edge
SSL	Secure Sockets Layer
SWG	Secure Web Gateway
SWG	Secure Web Gateway
TI	Threat Intelligence
TLS	Transport Layer Security
TSA	Transportation Security Administration
UTM	Unified Threat Management
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network
XBAS	Xantaro Breach & Attack Simulation
XDR	Cross-Layered Detection and Response (Schichtübergreifende Erkennung und Reaktion)
ZTNA	Zero Trust Network Access

Ihr Ansprechpartner

Nils Kammann
Lead Security Consultant
T +49 40 4134980
contact@xantaro.net

Die Xantaro Gruppe

Xantaro ist einer der führenden Solution Provider für High-Performance-Netzwerke und Sicherheitslösungen.

Xantaro unterstützt Unternehmen aller Branchen, Carrier und Service-Provider, Rechenzentren sowie Hosting- und Cloud-Dienstanbieter herstellerübergreifend mit rund 80 zertifizierten Netzwerk-Experten und 60 Kundenberatern.

Xantaro Deutschland GmbH | Jungfernstieg 7 | 20354 Hamburg
T +49 40 4134980 | contact@xantaro.net | www.xantaro.net

xantaro
connecting the world.