WHITEPAPER

CLOUDFLARE

Erste Schritte mit SASE: Ein Leitfaden zur Sicherung und Optimierung Ihrer Netzwerkinfrastruktur

Secure Access Service Edge (SASE) vereinfacht die herkömmliche Netzwerkarchitektur, indem es Netzwerk- und Sicherheitsservices in einem einzigen globalen Netzwerk zusammenführt. In diesem Whitepaper werden die Entwicklungen im Bereich Netzwerksicherheit beschrieben, aus denen schließlich SASE hervorgegangen ist. Außerdem umreißt es die Bandbreite der in einer SASE-Lösung enthaltenen Dienste und bietet einen praktischen Leitfaden zur Einführung von SASE.

+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

EINLEITUNG

Der 2019 von Gartner geprägte Begriff „Secure Access Service Edge“ oder „SASE“ sollte anfangs einen entscheidenden Fortschritt im digitalen Transformationsprozess beschreiben: hochgradig anpassbare und nahtlos in eine globale Cloudplattform integrierte Netzwerk- und Sicherheitsservices. Gartner rechnete mit einer Akzeptanzquote von 20 % bis 2023 und prognostizierte, dass die Nachfrage nach SASE-Funktionen „die Netzwerkdienste und Netzwerksicherheitsarchitektur von Unternehmen neu definieren und die Wettbewerbslandschaft umgestalten“ würde.[1]

Seitdem hat sich der Begriff in der Welt der IT- und Unternehmenssicherheit wie ein Lauffeuer verbreitet. Verschiedene Anbieter von Netzwerksicherheitsdiensten und SD-WAN versuchen nun, sich als SASE-Vorreiter zu positionieren. Das führt allerdings nicht selten dazu, dass sie ihren Unternehmenskunden ein eilig zusammengestelltes Durcheinander von Netzwerk- und Sicherheitsservices vorlegen, das einem echten SASE-Framework oft nur zum Teil entspricht.

Denn zu SASE gehört mehr als nur die Bündelung bestehender Einzellösungen. Es erfordert eine komplette Neubewertung der Netzwerkinfrastruktur von Unternehmen. Ein starrer Netzwerkperimeter am Standort reicht nicht mehr aus, um dezentrale Teams und mobile Mitarbeiter zu schützen. Und das Jonglieren mit mehreren Sicherheitsservices zum Schutz einer hybriden Infrastruktur kann kostspielig werden, die IT-Teams bei der Bereitstellung und Verwaltung überfordern und massive Sicherheitslücken hinterlassen.

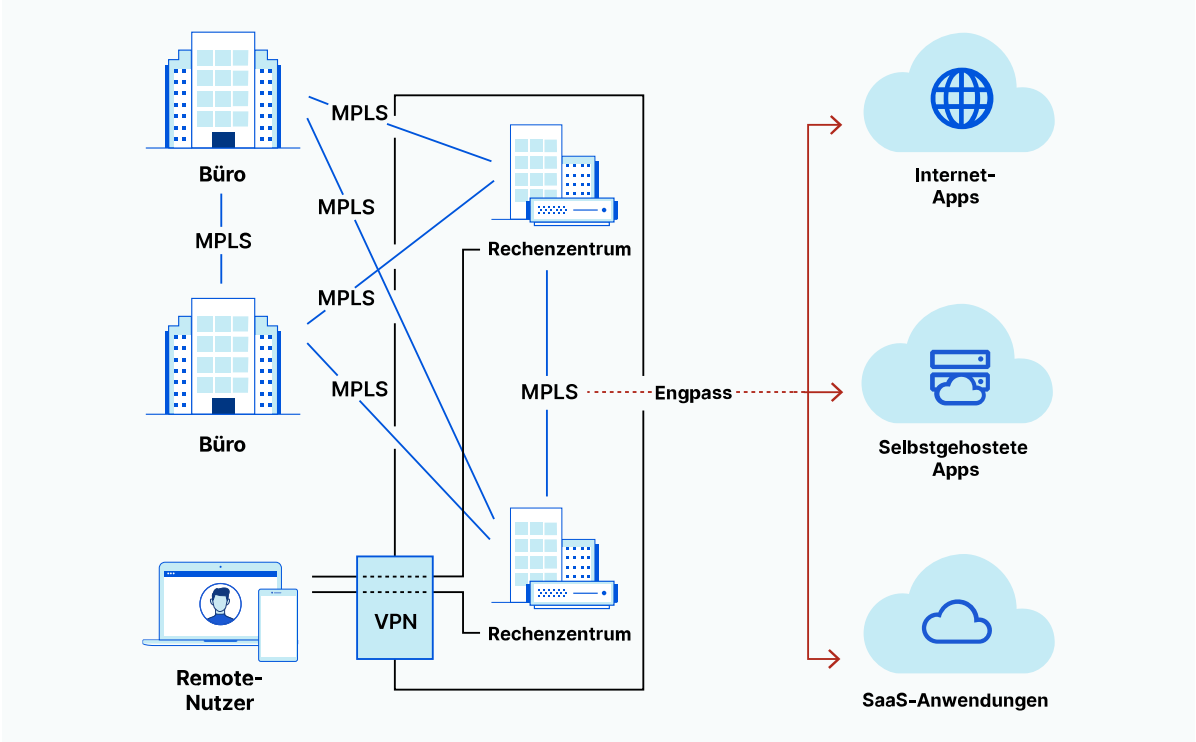
SASE löst diese Probleme durch die Verlagerung des Netzwerkperimeters von zentralisierten Rechenzentren zum Nutzer. Bei diesem Ansatz werden Netzwerkdienste und Netzwerksicherheitsservices gebündelt und nach dem Zero Trust-Prinzip von einer einzigen, cloudnativen Plattform aus bereitgestellt. SASE beseitigt auf diese Weise Sicherheitslücken zwischen den Diensten, verschafft IT-Teams einen besseren Einblick in die Netzwerkaktivitäten und erleichtert die Migration in die Cloud.

DER URSPRUNG VON SASE – DAS ALTE MODELL

SASE stellt einen entscheidenden Wandel dar. Um ihn zu verstehen, müssen wir uns die Entwicklungsgeschichte der Netzwerkinfrastruktur und -sicherheit genauer anschauen.

Vor der großflächigen Einführung von Cloud Computing waren alle Unternehmensressourcen, -daten und -anwendungen am Standort („On-Premise“) untergebracht. Dort wurden sie durch Hardware-Firewalls und DDoS-Geräte geschützt. Die Mitarbeiter in den Firmenbüros griffen über private Verbindungen auf interne Ressourcen zu. Diese Verbindungen wurden dann durch Netzwerk-Firewalls gefiltert. Nutzer, die sich von einem anderen Standort aus einwählen wollten, taten dies in der Regel über ein VPN. Diese Technologie ist allerdings anfällig für Latenz und ein schlechtes mobiles Nutzererlebnis. Außerdem sind die Vermeidung von Überlastungen und die Schließung von Sicherheitslücken dabei mit großem Zeitaufwand verbunden.

Hinter diesem Setup stand die Furcht vor dem offenen Internet – schließlich ging es beim Internet von Anfang an um Widerstandsfähigkeit, während auf die Performance- und Sicherheitsanforderungen von Unternehmen wenig Rücksicht genommen wurde. Da das Internet grundsätzlich anfällig für Angriffe war, richteten viele Organisationen lieber eigene private Netzwerke ein. Dort sicherten sie (oft ineffektiv) Daten, Anwendungen und Unternehmensressourcen mit physischen Firewall-Boxen und DDoS-Geräten und leiteten den gesamten eingehenden Traffic durch zentralisierte Rechenzentren, wo er geprüft und gefiltert wurde.



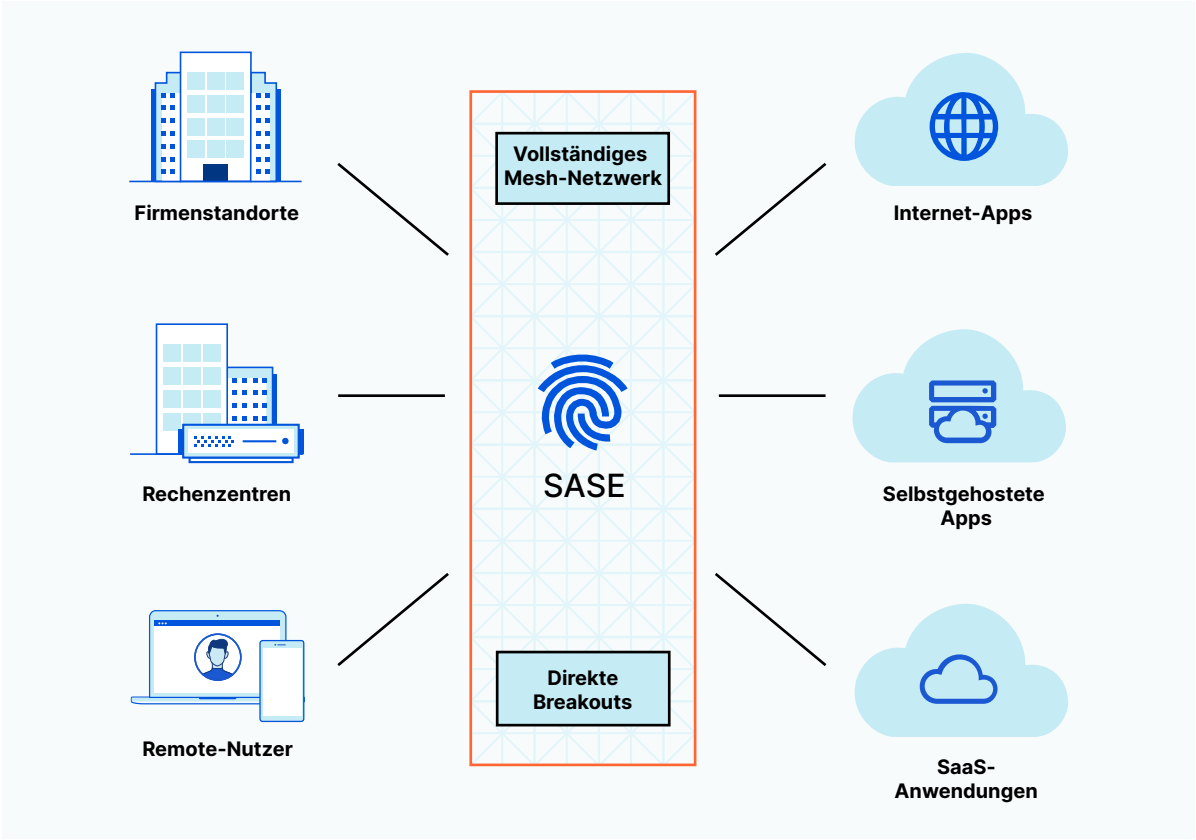
Dieses Netzwerksicherheitsmodell war einerseits teuer und komplex, schaffte andererseits aber die Anfälligkeit von Unternehmen für Datenschutzverletzungen und interne Bedrohungen nicht aus der Welt. Denn sobald ein Angreifer den Netzwerkperimeter durchbrach, konnte er erheblichen Schaden innerhalb einer Organisation anrichten, etwa durch Verbreitung von Ransomware, Übernahme von Nutzerkonten[2] und Diebstahl wertvoller Kundendaten.[3]

Dann kamen die Cloud- und SaaS-Dienste, und mit ihnen mehr Freiheit und Flexibilität bei der Neugestaltung der Netzwerkinfrastruktur von Unternehmen, da sich Anwendungen, Daten und Mitarbeiter nicht mehr ausschließlich vor Ort befinden müssen.

DER URSPRUNG VON SASE – DAS NEUE MODELL

Doch diese Freiheit bringt neue Sicherheitsherausforderungen mit sich: IT-Teams müssen nun eine Mischung aus lokalen und cloudbasierten Diensten schützen und gleichzeitig eine zunehmend mobile Belegschaft und immer mehr Remote-Mitarbeiter absichern.[4] Um dies erfolgreich zu bewerkstelligen, müssen sie oft teure Hardware betreiben und Single-Point-Sicherheitsservices von mehreren Anbietern kombinieren. Hat man ein solches Setup – nicht selten mit hohem Zeitaufwand – implementiert, erweist sich oft auch seine Verwaltung als schwierig.

Mit dem nächsten Schritt in der Entwicklung der Netzwerksicherheit wird man sich wahrscheinlich von der Hardware zum Schutz traditioneller „Hub-and-spoke"-Infrastruktur weitgehend verabschieden, ebenso wie von den komplizierten Zwischenlösungen, die eine hybride Cloud-Architektur erfordert.
Ersetzt werden sie durch Lösungen gemäß einem SASE-Framework, das Netzwerk- und Sicherheitsservices konsolidiert und sie als integrierte Dienstleistung anbietet.



SASE bietet eine optimierte Herangehensweise an Netzwerksicherheit anstelle von ineffektiven Hardware-Appliances oder einem Flickenteppich aus separaten Sicherheitsdiensten. Kompliziertes Backhauling wird dabei durch die Internet-Edge ersetzt. So können Unternehmen den Traffic in einem einzigen Durchgang routen, beschleunigen, verifizieren, filtern, isolieren und prüfen. In Verbindung mit WAN-Konnektivität auf Grundlage eines vollständigem Mesh-Netzwerks, Zero Trust-Zugriffsrichtlinien und Bedrohungsschutz auf Netzwerkebene werden bei SASE weder veraltete VPNs noch MPLS-Leitungen, Hardware-Firewalls, Proxys oder DDoS-Schutz-Geräte mehr benötigt. Dementsprechend können Unternehmen ihre Netzwerksicherheitskonfigurationen besser im Blick behalten und kontrollieren.

DER ANWENDUNGSBEREICH VON SASE – WESENTLICHE FUNKTIONEN

SASE ist ein cloudbasiertes Sicherheitsmodell, das softwaredefiniertes Wide Area Networking mit zentralen Netzwerksicherheitsservices kombiniert und diese an der Cloud-Edge bereitstellt. Die meisten SASE-Angebote zeichnen sich durch fünf primäre Funktionen aus:

Netzwerke aufbauen und verwalten

Mit einem softwaredefinierten Wide Area Network (SD-WAN) können private Unternehmensnetze ohne die Hilfe von Hardware-Routern oder MPLS-Schaltungen (Multiprotocol Label Switching) eingerichtet werden. Diese virtuelle, softwarebasierte Architektur bietet Unternehmen mehr Flexibilität bei der Erstellung und Wartung ihrer Netzwerkinfrastruktur – allerdings weist sie auch einige Sicherheitslücken auf.

Traffic filtern

Ein Secure Web Gateway (SWG) wehrt Cyber-Bedrohungen ab und verhindert Datenschutzverletzungen, indem es unerwünschte Inhalte aus dem Web-Traffic herausfiltert, unbefugtes Nutzerverhalten blockiert und Sicherheitsrichtlinien des Unternehmens durchsetzt. Dazu gehören unter anderem URL-Filterung, Erkennung und Blockierung von Malware und Anwendungskontrolle.

Daten sichern

Ein Cloud Access Security Broker (CASB) führt mehrere Sicherheitsfunktionen für cloudgehostete Dienste aus (z. B. SaaS-, IaaS- und PaaS-Anwendungen). Standard-CASBs sichern vertrauliche Daten durch Zugriffskontrolle und Data Loss Prevention, decken Schatten-IT auf und gewährleisten die Einhaltung von Datenschutzvorschriften.

Verbindung von Nutzern mit Anwendungen

Zero Trust Network Access (ZTNA) erfordert eine Echtzeitverifizierung jedes Nutzers für jede geschützte Anwendung. Dadurch werden interne Ressourcen gesichert und potenzielle Datenschutzverletzungen abgewendet. Bei einem „Zero Trust"-Ansatz wird keiner Entität automatisch vertraut. Selbst wenn sie sich bereits innerhalb des Perimeters des privaten Netzwerks befindet, muss immer zuerst ihre Identität authentifiziert werden.

Anwendungen und Infrastruktur schützen

Cloudbasierte Firewalls (FWaaS) schützen Cloud-Infrastrukturen und Anwendungen vor Cyber-Angriffen durch eine Reihe von Sicherheitsmerkmalen, unter anderem URL-Filterung, Intrusion Prevention und einheitliche Richtlinienverwaltung.

DER ANWENDUNGSBEREICH VON SASE – SPITZENFÄHIGKEITEN

Obwohl eine konventionelle SASE-Lösung die fünf oben beschriebenen Services umfasst, ist diese Liste eher eine erste Orientierungshilfe als ein strenger Anforderungskatalog. SASE vereinigt in seinem Kern zwei grundlegende und getrennte Funktionen – softwarebasierte Netzwerkarchitektur und cloudbasierte Sicherheitsservices. Abgesehen davon können Anbieter je nach Bedarf Dienste hinzufügen oder herausnehmen.

SD-WAN hilft den Kunden beim Zurücklegen der letzten Meile innerhalb des Netzwerks. Auf dem Mittelteil der Strecke, die die Daten zwischen Nutzer und Anwendung zurücklegen müssen, können damit aber Sicherheit, Performance und Zuverlässigkeit nicht gewährleistet werden. Bestenfalls können Ende-zu-Ende-Verbindungen durch die Nutzung mehrerer globaler Netzwerke und die Verkettung verschiedener Sicherheitsdienste optimiert werden, doch das ist kompliziert und kostspielig. Ein SASE-Anbieter, der WAN as a Service – mit oder ohne SD-Wan – von Grund auf aufgebaut hat, gibt seinen Kunden damit die Möglichkeit, sich auf ein einziges globales Netzwerk mit standardmäßig integrierten Sicherheits-, Performance- und Zuverlässigkeitskfunktionen zu beschränken. Werden SWG, CASB und ZTNA gemeinsam eingesetzt, verringern sich die Sicherheitsrisiken dadurch beträchtlich. Lückenlos sind Gefahrenabwehr und Datenschutz deshalb aber in keinem Fall. Diese Lücken lassen sich jedoch schließen, wenn in jedem Rechenzentrum eine Remote-Browser-Isolierung eingesetzt wird, die von einem SASE-Provider von Grund auf entwickelt wurde und über eine native Integration in SWG, CASB und ZTNA verfügt.

VORTEILE DES SASE-ANSATZES

Im Rahmen der weiteren Entwicklung werden sich die SASE-Implementierungen je nach Anbieter und Unternehmen möglicherweise erheblich unterscheiden. Die meisten SASE-Lösungen haben jedoch einige entscheidende Vorteile gegenüber lokalen und hybriden Netzwerksicherheitskonfigurationen gemeinsam:

Optimierte Implementierung

Durch die Konsolidierung von Netzwerk- und Sicherheitsservices erübrigt sich bei SASE das Onboarding von cloudbasierten Diensten, die Einrichtung von Geräten vor Ort sowie die Investition von Zeit, Geld und internen Ressourcen, um den Schutz dieser Instrumente vor aktuellen Bedrohungen auf dem neuesten Stand zu halten.

Reduzierte Latenz

SASE reduziert die Latenz und verbessert die Performance, denn der Netzwerk-Traffic wird über ein ausgedehntes Edge-Netzwerk geroutet. Darin wird der Traffic so nah wie möglich am Nutzer verarbeitet. Routing-Optimierungen helfen, den schnellsten Netzwerkpfad zu bestimmen, basierend auf Netzwerküberlastung und anderen Faktoren.

Vereinfachte Richtlinienverwaltung

Mit SASE können Unternehmen Zugriffsrichtlinien für alle Standorte, Nutzer, Geräte und Anwendungen festlegen, überwachen, anpassen und durchsetzen. Man kann Angriffe und eingehende Bedrohungen von einem einzigen Portal aus identifizieren und abwehren, anstatt sie einzeln zu überwachen und ihnen mit einem Arsenal an spezialisierten Sicherheitswerkzeugen zu begegnen.

Globales Netzwerk

Ein SASE-Framework wird auf einem einzigen globalen Netzwerk aufgebaut und ermöglicht es Unternehmen, ihren Netzwerkperimeter auf jeden beliebigen Remote-Nutzer, jede Zweigstelle, jedes Gerät oder jede Anwendung auszudehnen. So können sie ihre gesamte Netzwerkinfrastruktur besser im Blick haben und kontrollieren.

Identitätsbasierter Netzwerkzugriff

SASE lehnt sich stark an ein Zero-Trust-Sicherheitsmodell an, bei dem Nutzeridentität und Zugriff auf der Grundlage einer Kombination von Faktoren erteilt werden: Standort des Nutzers, Tageszeit, Sicherheitsstandards des Unternehmens, Compliance-Richtlinien und fortlaufende Bewertung von Risiko/Vertrauen. Dieses Sicherheitsniveau schützt sowohl vor externen als auch internen Datenschutzverletzungen und anderen Angriffen – ein bedeutender Fortschritt gegenüber dem allzu permissiven und inhärent anfälligen VPN.

ERSTE SCHRITTE MIT SASE

Viele Unternehmen schrecken vor der SASE-Einführung zurück, wenn sie bereits viel Zeit, Ressourcen und Geld in aufwendige On-Premise-Setups investiert haben, komplexe Netze von cloudbasierten Sicherheitsservices verwalten oder den Wandel hin zur virtuellen Arbeitswelt der Zukunft noch nicht vollständig vollzogen haben. Aber SASE muss nicht kompliziert sein.

Hier sind fünf praktische erste Schritte zum Einstieg in SASE:

1. Schützen Sie Ihre Remote-Teams.

Verabschieden Sie sich teilweise oder sogar ganz von Ihrem VPN, indem Sie eine ZTNA-Lösung implementieren, mit der Sie Unternehmensdaten und -ressourcen vor internen und externen Bedrohungen schützen und die Nutzererfahrung verbessern können. Verlagern Sie Ihr Secure Web Gateway, Ihre Firewall und Geräte-Browser an den Netzwerkrand, denn dann können Sie den Traffic inspizieren, filtern und isolieren, ohne ihn erst durch ein zentrales Rechenzentrum leiten zu müssen.

2. Platzieren Sie Zweigstellen hinter einem Cloud-Perimeter.

Richten Sie eine Zero Trust-Architektur für Zweigstellen ein und verzichten Sie dafür auf Sicherheitsvorrichtungen vor Ort (einheitlicher Bedrohungsschutz usw.) – denn die Instandhaltung dieser Geräte kann teuer werden und angesichts einer sich schnell entwickelnden Bedrohungslandschaft erweisen sie sich möglicherweise als wirkungslos.

3. Verlagern Sie den DDoS-Schutz an den Rand.

Trennen Sie sich von DDoS-Geräten und schützen Sie Unternehmensnetzwerke vor Angriffen, indem Sie auf cloudnativen DDoS-Schutz auf Netzwerkebene setzen, der Bedrohungen in Echtzeit erkennen und bekämpfen kann.

4. Migrieren Sie Anwendungen in die Cloud.

Werden Sie dem Wachstum Ihres Unternehmens gerecht, indem Sie selbstgehostete Anwendungen von ihren Rechenzentren in die Cloud verlagern und dafür sorgen, dass für den gesamten Traffic einheitliche Netzwerk-Sicherheitsrichtlinien gelten.

5. Ersetzen Sie Sicherheits-Appliances vor Ort durch eine einheitliche, cloudnative Richtliniendurchsetzung.

Durch Verlagerung der Richtliniendurchsetzung an den Netzwerkrand reduzieren Sie die Kosten und die Komplexität der Instandhaltung von Netzwerk-Hardwaregeräten. An der Edge können Sie den gesamten Traffic, die Angriffsmuster und die Sicherheitsrichtlinien zentral überwachen und verwalten.

UNSERE SASE HEISST CLOUDFLARE ONE

Cloudflare One ist eine auf dem Zero Trust-Prinzip aufbauende Network as a-Service-Plattform, die Nutzer dynamisch mit Firmenressourcen verbindet. Dabei werden identitätsbasierte Sicherheitskontrollen in der Nähe der User bereitgestellt, wo auch immer sich diese befinden.

Möglichkeiten der Netzwerkdienste von Cloudflare One für Infrastruktur-Teams:	Möglichkeiten der Zero Trust-Dienste von Cloudflare One für IT-Sicherheitsteams:
• Verwendung des globalen Cloudflare-Netzwerks als WAN • Ersetzen älterer Geräte durch eine cloudnative Netzwerk-Firewall • Verbesserung der Anwendungsperformance und Senkung der Latenz für Endnutzer	• Einfacher und sicherer Ressourcenzugriff ohne VPN für Nutzer • Verhindern lateraler Bewegungen; Blockieren von Ransomware, Malware und Phishing • Bescheren Sie den Endnutzern ein besseres Erlebnis und optimieren Sie die Verwaltung, insbesondere im Hinblick auf die Onboarding-Zeit.

Welche Gründe sprechen für Cloudflare?

Einfache Bereitstellung und Verwaltung

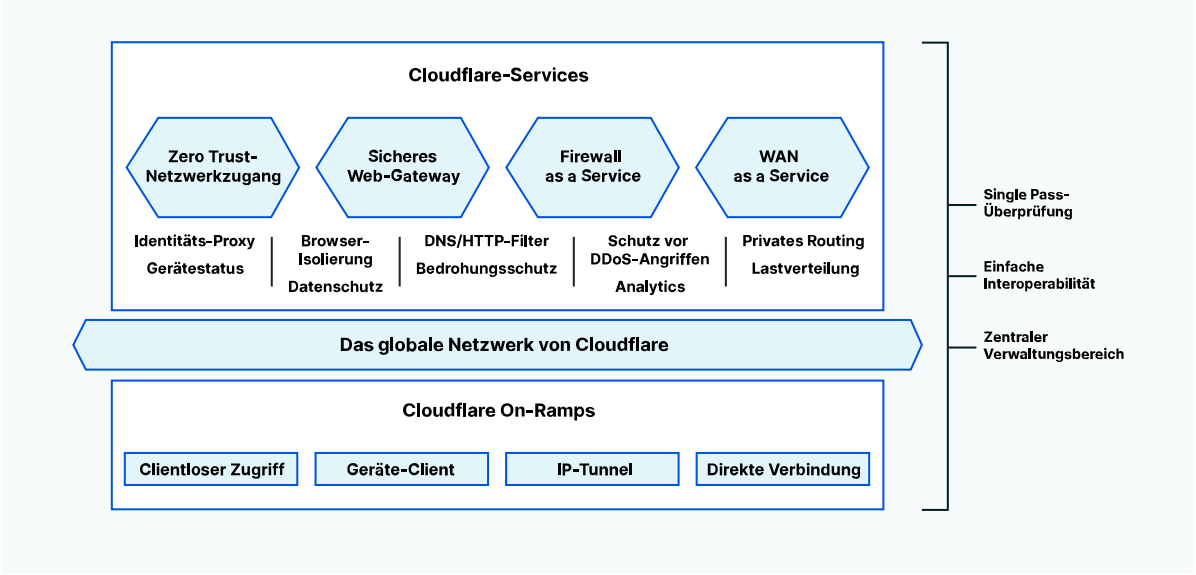
Jeder Cloudflare One-Dienst wird an allen unseren Standorten in über 250 Städten weltweit ausgeführt. Keine Notwendigkeit einer manuellen Integration mehrerer Einzellösungen bei der Umstellung auf ein SASE-Modell.

Einheitliche Sicherheit und Geschwindigkeit überall auf der Welt

Jedes Cloudflare-Rechenzentrum bietet eine Überprüfung des Traffics in einem einzigen Durchgang, sodass Nutzer überall auf der Welt den gleichen Schutz genießen können – ohne Geschwindigkeitsverluste aufgrund von Latenz oder der Umleitung von Daten.

Möglichkeit der Verknüpfung mit bereits genutzten Systemen

Cloudflare betreibt das weltweit leistungsstärkste und am besten überwachte Netzwerk, und Cloudflare One unterstützt die Identitäts-, Endpunkt- und Cloud-Anbieter, die Sie bereits nutzen. Benutzerfreundlich, nur eine einzige Integration erforderlich.



UNSERE SASE HEISST CLOUDFLARE ONE

Cloudflare One bietet die Sicherheits- und Konnektivitätsfunktionen, die Sie benötigen, um Nutzer, Anwendungen und Zweigstellen in einer mobilen Arbeitswelt miteinander zu verbinden.

Cloudflare One

Zero Trust-Netzwerkzugang

Verbinden Sie jeden Benutzer mit jeder Anwendung und jedem privaten Netzwerk schneller und sicherer als ein VPN, indem Sie identitäts- und kontextbasierte Regeln durchsetzen und laterale Bewegungen einschränken.

SASE-Kernfunktionen:

- Verbindung von Nutzern mit Anwendungen
- Datensicherung

WAN as a Service

Ermöglichen Sie Any-to-Any-Konnektivität mit höherer Performance, integrierter Sicherheit und erhöhter Ausfallsicherheit, indem Sie Ihre alte WAN-Architektur durch unser globales privates Backbone ersetzen.

SASE-Kernfunktion:

- Netzwerke aufbauen und verwalten

Secure Web Gateway

Blockieren Sie bekannte und unbekannte Internet-Bedrohungen – und kontrollieren Sie problemlos den Datenfluss. Möglich wird dies, indem Sie DNS-, HTTP-, Netzwerk- und Browser-Isolierungsregeln mit unbegrenzter SSL-Prüfung durchsetzen.

SASE-Kernfunktionen:

- Traffic filtern und kontrollieren
- Datensicherung

Firewall as a Service

Zugriff kontrollieren – und blockieren von DDoS-Angriffen und anderen Bedrohungen – durch Durchsetzung von Stateful-Inspection-Regeln für den gesamten ein- und ausgehenden Traffic bei gleichzeitig hoher Performance.

SASE-Kernfunktion:

- Anwendungen und Infrastruktur schützen

Das globale Netzwerk von Cloudflare

Unser Netzwerk erstreckt sich über mehr als 250 Städte, verfügt über eine Kapazität jenseits von 100 Tbit/s, über 10.000 Verbindungen und ein SLA für 100%ige Verfügbarkeit. Außerdem befindet es sich nur 50 ms von 95 % aller mit dem Internet verbundenden Menschen weltweit entfernt.

Clientloser Zugriff

Onboarden jedes Benutzers oder jedes Gerät innerhalb von Minuten – auch von Drittanbietern und BYOD– mit sicherem browserbasiertem Zugriff auf selbstgehostete und SaaS-Anwendungen, nicht nur über HTTP.

IP-Tunnel

Onboarding ganzer öffentlicher und privater IP-Subnetze über BGP Anycast-Routenankündigungen mit GRE-Tunneln oder unserem eigenen Tunnel-Connector in Cloud- oder On-Premise-Umgebungen.

Geräte-Client

Onboarden von Windows-, macOS-, iOS-, Android-, ChromeOS- und Linux-Geräten für den sicheren clientbasierten Zugriff auf beliebige Anwendungen, private Netzwerke oder Internet-Ziele.

Direkte Verbindung

Binden Sie Ihre Netzwerkinfrastruktur physisch oder virtuell in mehr als 1600 Co-Location-Einrichtungen ein – anstatt über das öffentliche Internet – und profitieren so von einer zuverlässigeren und sichereren Erfahrung.

GESCHÄFTSERFOLGE DANK CLOUDFLARE ONE

↓91 %

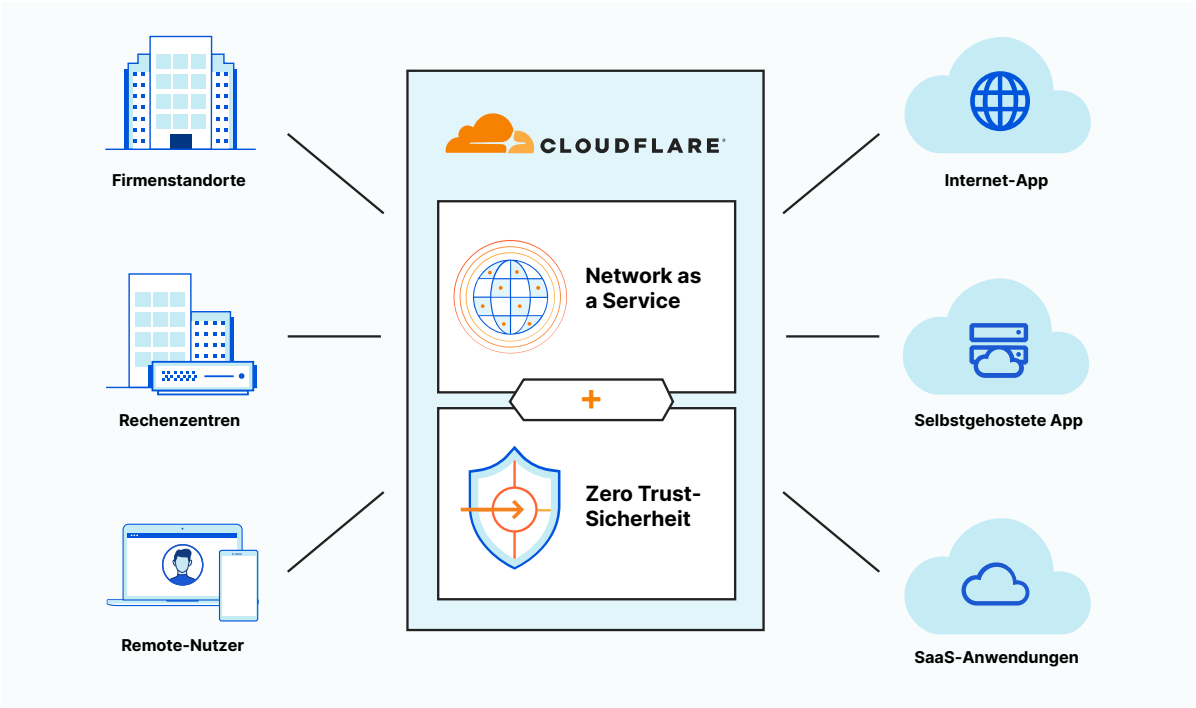
Reduzieren Sie die Angriffsfläche um bis zu 91 %, indem Sie risikoreiches Browsing von Endbenutzersystemen isolieren und den Anwendungszugriff von Netzwerken trennen.

10 → 1

Senken Sie die Gesamtbetriebskosten und kurbeln Sie Ihr Geschäft durch die Konsolidierung von bis zu zehn Einzellösungen zu einer einzigen Plattform an.

↑60 %

Das Onboarding neuer Mitarbeitenden und Auftragnehmenden wird um bis zu 60 % beschleunigt, wenn Sie ihre Nutzer nicht per VPN, sondern über Cloudflare auf Ressourcen zugreifen.



Mehr über Cloudflare One erfahren

Hier klicken

INHALT

1. Gartner, „The Future of Network Security Is in the Cloud.“ Analyst(en): Neil MacDonald, Lawrence Orans, Joe Skorupa. 30. August 2019. Gartner.

2. Twitter Inc., „An update on our security incident.“ Twitter. Zugriff am 27. Oktober 2020.

3. Marriott International News Center, „Marriott International Notifies Guests of Property System Incident.“ Marriott. Zugriff am 27. Oktober 2020.

4. Bursztynsky, Jessica, „Dropbox is the latest San Francisco tech company to make remote work permanent.“ CNBC. CNBC. Zugriff am 27. Oktober 2020.