CLOUDFLARE

E-BOOK

SASE-Einführung: Ein Leitfaden für CISOs

Wie Sie SASE-Plattformen für vorrangige Anwendungsfälle bewerten

Das Streben nach Cyberresilienz

Das National Institute of Standards and Technology (NIST) definiert Cyberresilienz als die Fähigkeit, ungünstige Bedingungen, Belastungen, Angriffe oder Kompromittierungen von Systemen, die Cyberressourcen nutzen oder durch sie ermöglicht werden, zu antizipieren, ihnen standzuhalten, sich von ihnen zu erholen und sich an sie anzupassen.

Die Stärkung der Cyberresilienz – bei gleichzeitiger Senkung der Kosten für die Bekämpfung von Sicherheitsverstößen – bringt jedoch auch einige Herausforderungen mit sich:

- **Cyberkriminelle entwickeln ihre Taktiken ständig weiter:** Da die Angreifer immer ausgefeiltere Tools, Techniken und Verfahren entwickeln, wird es für Unternehmen immer schwieriger, die Bedrohungslandschaft zu schützen
- **IT-Umgebungen werden immer komplexer:** Aufgrund der großen Anzahl von Geräten und Anwendungen, die über Multi-Cloud-Architekturen verbunden sind, ist die Sicherung dieser Umgebungen ein kostspieliger und komplizierter Prozess
- **Interne Teams sind überlastet:** Unternehmen stoßen möglicherweise auf Engpässe bei den Ressourcen, da die Budgets knapper werden und die internen Teams überlastet sind

Um diese Herausforderungen zu meistern, wenden sich viele CISOs einem Secure Access Service Edge (SASE)-Framework zu. Im Unterschied zu früheren Netzwerkansätzen vereint eine SASE-Architektur Sicherheit und Netzwerk auf einer Cloud-Plattform und sorgt so für einheitliche Transparenz und Kontrolle. SASE verlagert die Netzwerkkontrolle an die Cloud-Edge – und nicht in das Rechenzentrum des Unternehmens. So können Unternehmen jedem Benutzer, jeder Anwendung, jedem Gerät und jedem Netzwerk unabhängig vom Standort einen einfachen und sicheren Zugang bieten.

Dieser Leitfaden behandelt einige der häufigsten Anwendungsfälle für SASE und beschreibt die wichtigsten Schritte für den Start Ihrer SASE-Einführung, damit Sie Ihre Cyberresilienz stärken und schnelle Erfolge erzielen können.

Anwendungsfall #1:

Zero Trust-Netzwerkzugang (ZTNA) einführen

Wenn Sie sich bei hybriden Arbeitsformen, Multi-Cloud-Umgebungen und nicht verwalteten Geräten auf die herkömmliche, perimeterbasierte Sicherheit verlassen, haben Unternehmen nur einen begrenzten Überblick, widersprüchliche Konfigurationen und ein zu hohes Risiko. Ein Zero Trust-Ansatz – bei dem präzise Zugriffskontrollen sicherstellen, dass keiner Entität standardmäßig vertraut wird – kann Ihre Sicherheitsstrategie auf folgende Weise modernisieren:

Ersetzen der traditionellen hardwarebasierten Sicherheit

Herkömmliche Kontrollmechanismen des Netzwerkperimeters, wie z.B. virtuelle private Netzwerke (VPNs), lassen sich nur schwer skalieren, beeinträchtigen die Transparenz und erschweren es den Sicherheitsteams, Angriffe zu erkennen und zu beheben. Ein SASE-Modell bietet eine sichere Alternative, indem es den Zero Trust Network Access (ZTNA) implementiert und gleichzeitig den Netzwerktraffic über ein globales Cloud-Netzwerk leitet und verarbeitet – und damit sowohl die Reibung zwischen den Endbenutzern als auch die laterale Bewegung reduziert.

Verwalten des Gerätezugriffs

Dritten Nutzern – wie Auftragnehmern, Agenturen und Lieferanten – Zugang zu gewähren, kann ein Risiko darstellen, wenn Unternehmen versehentlich zu viele Privilegien gewähren oder Zugang zu nicht verwalteten Geräten gewähren. Mit SASE können Unternehmen clientlose Zero Trust-Richtlinien festlegen und so sicherstellen, dass Drittnutzer nur auf das zugreifen können, was sie benötigen.

Verhindern von Ransomware-Angriffen

Ransomware kann sich schnell über ein ganzes Netzwerk verbreiten – und in einigen Fällen sogar über mehrere Netzwerke und Organisationen. SASE trägt dazu bei, die Ausbreitung von Ransomware-Angriffen zu verhindern, indem es den Netzwerk- und Anwendungszugriff sperrt, sobald eine Infektion entdeckt wird. Unterstützt durch das Zero Trust-Prinzip der „Zugriffskontrolle mit geringsten Berechtigungen“ erschwert dieser Ansatz Angreifern die Ausweitung ihrer Berechtigungen und die laterale Bewegung innerhalb eines Netzwerks.

Die Offenlegung von Daten einschränken

Die Offenlegung und das Abfließen von Daten kann für Unternehmen eine ernsthafte Bedrohung darstellen, da Benutzer sensible Informationen über genehmigte und nicht genehmigte Anwendungen hochladen oder verbreiten. SASE Zero Trust-Richtlinien können dazu beitragen, die Offenlegung von Daten zu verhindern, indem sie die Anwendungen, auf die jeder Benutzer Zugriff hat, einschränken und gleichzeitig beliebte SaaS-Suiten auf sensible Daten und Fehlkonfigurationen überprüfen.

KUNDENREFERENZ

Einführung von Zero Trust

Ein Fortune 500-Telekommunikationsanbieter nutzte die SASE-Plattform von Cloudflare, um seine hybride Arbeitsumgebung für mehr als 100.000 Mitarbeitende zu sichern – über Hunderte von Anwendungen hinweg, die auf AWS, Azure und anderen Cloud-Umgebungen gehostet werden. Mit einer identitätsbasierten Zero Trust-Netzwerkarchitektur, einem sicheren Web-Gateway und einheitlichen Zugriffskontrollen konnten sie die Benutzer vor Bedrohungen schützen, ohne mit mehreren richtlinienbildenden Schnittstellen, VPNs und Internet-Filterdiensten jonglieren zu müssen.

Anwendungsfall #2:

Schutz der Angriffsfläche

Der digitale Wandel und die Remote-Arbeit haben die Angriffsfläche vergrößert, da mehr verstreute Benutzer und nicht-verwaltete Geräte Zugriff auf interne Ressourcen benötigen. Die Ausweitung von Firewalls vor Ort auf die Cloud und die Skalierung von Netzwerken über VPNs kann jedoch die Anfälligkeit für externe und interne Bedrohungen erhöhen und gleichzeitig die Transparenz verringern. Mit einer SASE-Architektur können Unternehmen die Sichtbarkeit und die Kontrollmechanismen erweitern, um ein „perimeterloses“ Modell zu unterstützen und einen einheitlichen Schutz auf folgende Weise durchzusetzen:

Vermeiden von Multi-Channel-Phishing

Angreifer starten Phishing-Attacken oft über Kanäle, bei denen die Benutzer dazu neigen, nicht darauf zu achten, wohin sie klicken – insbesondere bei Tools, die normalerweise nicht durch E-Mail-Sicherheitskontrollen geschützt sind. Eine einheitliche SASE-Plattform ermöglicht einen umfassenden Schutz für alle Ihre Umgebungen, um das Risiko des Diebstahls von Anmeldeinformationen, der Übernahme von Konten und der Ausschleusung von Daten zu verringern.

Remote-Mitarbeitende schützen

Remote-Arbeit erfordert, dass sich Benutzer von verschiedenen Standorten und Geräten aus verbinden, oft außerhalb des Zuständigkeitsbereichs der Unternehmen, die sie beschäftigen. Eine SASE-Architektur ermöglicht es Unternehmen, den Zugriff von Mitarbeitenden und Dritten auf kritische Umgebungen und Daten zu sichern und so sicherzustellen, dass von überall aus sicher und produktiv gearbeitet werden kann.

Verbesserung der Nutzererfahrung

Herkömmliche Ansätze zur Bereinigung des Datenverkehrs im Büro erfordern häufig ein Backhauling des Datenverkehrs zu zentralen Rechenzentren des Unternehmens, was zu zusätzlichen Latenzzeiten führen und die Produktivität beeinträchtigen kann. Aber die Alternative – der direkte Zugang zum Internet – birgt Sicherheitsrisiken und schafft uneinheitliche Benutzererfahrungen. SASE verwaltet und optimiert auf intelligente Weise direkte Verbindungen zu jedem Cloud- oder Internet-Ziel und setzt Richtlinien und Schutzmaßnahmen so nah wie möglich am Endbenutzer durch.

Wide Area Networks (WANs) schützen

Einige WANs umgehen die Cloud-Sicherheit für den Traffic zwischen den Zweigstellen, sodass die Ansprüche an die Integration von Sicherheitsdiensten und softwaredefinierten WANs möglicherweise nicht das sind, was sie auf den ersten Blick scheinen. SASE ermöglicht es Unternehmen, ihre WAN-Verbindungen zu vereinfachen und zu sichern, indem es den Datenverkehr zwischen Büros, Rechenzentren, öffentlichen Clouds und anderen Standorten innerhalb und außerhalb des Internets filtert und prüft.

KUNDENREFERENZ

Schutz der sich vergrößernden Angriffsflächen

Werner Enterprises hat die SASE-Services während seiner Cloud-Migration nahtlos eingesetzt – ohne Unterbrechung der kritischen Geschäftsabläufe oder des Kundenservices. Nach der Implementierung reduzierte sich die Anzahl bösartiger E-Mails um mehr als 50 %. Gleichzeitig konnte der manuelle Aufwand für die E-Mail-Sichtung um mehrere Stunden pro Tag reduziert werden, sodass sich das Sicherheitsteam auf strategisch wichtigere Geschäftsziele konzentrieren konnte.

Anwendungsfall #3:

Daten überall schützen

Da sich die Daten über mehrere Umgebungen erstrecken, ist es für Unternehmen oft schwierig, sie im Auge zu behalten. Sensible Daten können durch den unerlaubten Einsatz von generativer KI und Schatten-IT offengelegt werden, was zu Kompromissen oder Sicherheitsverstößen führen kann, deren Behebung teuer sein kann. SASE vereint Datentransparenz und -kontrolle in Web-, SaaS- und privaten Anwendungsumgebungen und hilft Unternehmen dabei, Folgendes zu erreichen:

Vereinfachung der Einhaltung von Datenschutzbestimmungen

Mit dem Aufkommen von Large Language Models (LLMs) und anderen KI-Tools müssen sich die Compliance-Standards weiterentwickeln, um die Daten der Nutzer zu schützen. SASE sorgt für die Sicherheit und Vertraulichkeit von Daten, indem es Datenkontrollen vereinheitlicht, sodass Sicherheitsteams regulierte Datenklassen sperren, das Risiko von Verstößen verringern und die kontinuierliche Einhaltung strenger Datenanforderungen gewährleisten können.

Schatten-IT verwalten

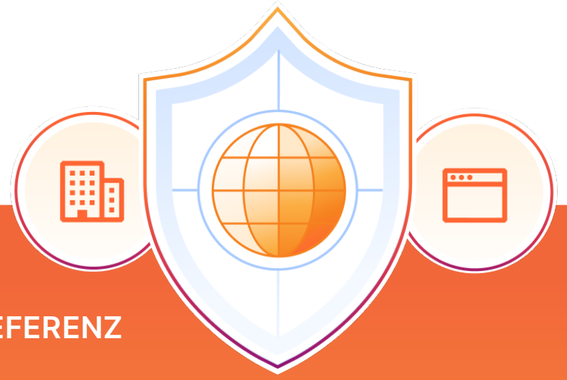
Schatten-IT – nicht genehmigte Anwendungen, die nicht von den Unternehmen, die sie nutzen, verwaltet oder gesichert werden – kann ein Risiko darstellen, wenn sensible Daten in oder durch sie verschoben werden. SASE trägt zur Minimierung dieses Risikos bei, indem es den Datenverkehr durch Inline-Cloud Access Security Broker (CASB) leitet. Diese protokollieren jede Verbindung und jede Anfrage, um das Vorhandensein nicht genehmigter Anwendungen aufzudecken, und ermöglichen es Unternehmen dann, zu kontrollieren, wie auf diese Anwendungen zugegriffen wird.

Generative KI sicher nutzen

Je mehr Unternehmen KI einsetzen, desto größer ist das Risiko, sensible Daten preiszugeben. Dank eines sicheren Web-Gateways und eines Sicherheitsbrokers mit Inline-Cloud-Zugriff können Sicherheitsteams mit einem SASE-Ansatz die Nutzung von KI-Anwendungen erkennen und genehmigen, nach Fehlkonfigurationen suchen, die Datenlecks verursachen, oder KI-Anwendungen in isolierten Webbrowsern ausführen, um die Dateneingabe und -ausgabe zu beschränken.

Sensible Daten schützen

Mit einer SASE-Architektur können Unternehmen erkennen und kontrollieren, wie sensible Daten in ihre IT-Umgebungen eindringen, sich dort bewegen und sie wieder verlassen. Dazu gehören das Scannen von Apps und die Überprüfung des Datenverkehrs auf regulierte personenbezogene Daten und geistiges Eigentum, das Blockieren von Internet-Bedrohungen wie Phishing und Ransomware sowie die Implementierung zusätzlicher Schutzmaßnahmen gegen Datendiebstahl und unbeabsichtigte Lecks.



KUNDENREFERENZ

Daten überall schützen

Applied Systems hat sich für SASE-Services entschieden, um den Zugang zu selbstgehosteten Anwendungen und Infrastrukturen für über 2.500 Mitarbeitende zu sichern. Dieser neue Ansatz gibt dem Sicherheitsteam die Flexibilität, strenge Kontrollen anzuwenden, um den unterschiedlichen Bedürfnissen der Benutzer gerecht zu werden und gleichzeitig zu kontrollieren, wie ihre Daten mit KI-Tools geteilt werden.

Auswahl einer SASE-Lösung:

Konsolidierung mit einem einzigen Anbieter im Vergleich zu mehreren Einzellösungen

Ein SASE-Plattform aus einer Hand führt Netzwerk- und Sicherheitsfunktionen in einem einzigen Cloud-Service zusammen. Dies ermöglicht es Unternehmen, verschiedene Einzelprodukte zu konsolidieren, Appliances zu eliminieren und eine einheitliche Durchsetzung von Richtlinien zu gewährleisten. Eine SASE-Implementierung mit mehreren Anbietern kann zwar ähnliche Ergebnisse erzielen wie ein Single-Vendor-Ansatz, erhöht jedoch häufig die Komplexität und die Kosten und verringert die interne Transparenz und Flexibilität.

Die Konsolidierung dieser Funktionen auf einer einheitlichen Plattform ermöglicht es Ihnen, das wahre Potenzial von SASE zu erschließen: eine vereinfachte, effiziente Netzwerk- und Sicherheitsinfrastruktur, die Ihre Gesamtbetriebskosten senkt und sich problemlos an Ihre sich wandelnden Geschäftsanforderungen anpassen lässt.

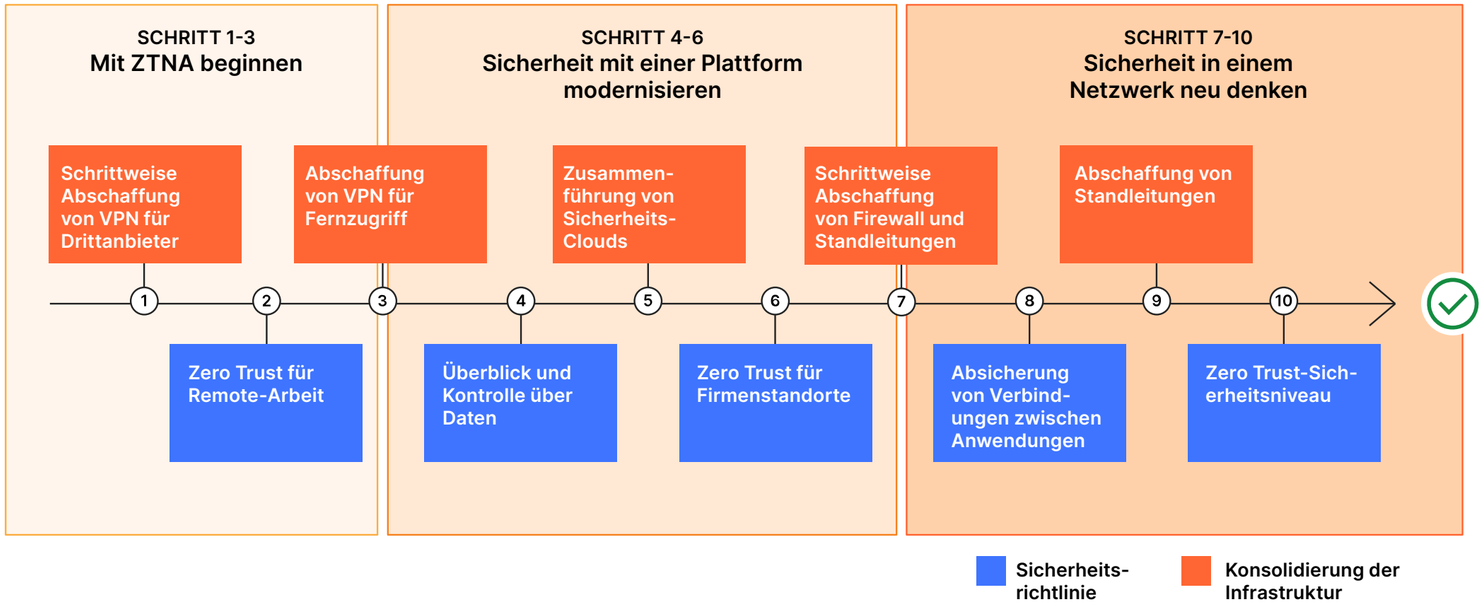
Wenn Sie potenzielle SASE-Anbieter evaluieren, sollten Sie die folgenden Fragen im Hinterkopf behalten:

1. Wird der Anwendungstraffic in einem einzigen Durchgang entschlüsselt und von den Engines zur Erkennung von Bedrohungen und sensiblen Daten überprüft? Gibt es Vorbehalte bei der Implementierung?
2. Sind alle Datenströme und die Kommunikation über SaaS-Suites über alle Kanäle hinweg geschützt (Inline- und Out-of-Band-Web- und E-Mail-Aktivitäten)?
3. Ist die Remote-Browserisolierung für jeden Benutzer und jede Anwendung aktiviert? Wie wirkt sich dies auf die Produktivität aus? Entstehen dadurch zusätzliche Kosten?
4. Werden Sicherheitsfunktionen aufgrund von Netzwerk-On-Ramps umgangen?
5. Ist es möglich, den Kundentraffic in einer mandantenfähigen Cloud-Architektur isoliert und privat zu halten?
6. Welche Möglichkeiten der Datenlokalisierung sind verfügbar? Erhöht die Aktivierung der Datenlokalisierung die Latenz für Remote-Benutzer, die sich außerhalb Ihrer lokalisierten Region verbinden?
7. Können Sie Ihre Threat Intelligence-Feeds in ihre Architektur integrieren? Wie reduziert die Plattform Fehlalarme durch Threat Intelligence-Feeds?
8. Welche Art von Benutzer-/Geräte-Risikobewertungen und Analysen sind verfügbar? Können Risikobewertungen einheitlich für alle Anwendungen durchgesetzt werden?

Wie Cloudflare SASE bereitstellt

Um die Umstellung auf eine einheitliche SASE-Plattform abzuschließen, vertrauen viele Unternehmen Cloudflare. Wir sind der einzige SASE-Anbieter, der mit einer Zero Trust Network-Architektur mit identitäts- und kontextbasierter Konnektivität beginnt, die konsequent in unsere gesamte Plattform integriert ist.

Ihre langfristige Roadmap für eine vollständige SASE-Architektur könnte einen ähnlichen Ablauf haben wie das folgende Beispiel:



Gestützt auf ein globales Netzwerk, das sich über mehr als 310 Städte weltweit erstreckt, hilft Cloudflare CISOs, Sicherheit, Ausfallsicherheit und Performance auf Enterprise-Niveau zu erreichen. Unsere zentrale Steuerungsebene führt Einzellösungen über mehrere Sicherheitsbereiche hinweg zusammen, sodass Unternehmen ihre Sicherheitsabläufe vereinfachen und einen einheitlichen Schutz vor sich weiterentwickelnden Bedrohungen gewährleisten können.

Besuchen Sie unsere Website, um mehr über Cloudflare und die Cloudflare SASE-Plattform zu erfahren.

Telefon: +49 89 2555 2276
E-Mail: enterprise@cloudflare.com
Web: www.cloudflare.com/de-de/