CLOUDFLARE

KURZDARSTELLUNG DER LÖSUNG

Security Service Edge (SSE)

Planen Sie die Konsolidierung von Sicherheitsdiensten und führen Sie SASE ganz in Ihrem eigenen Tempo ein

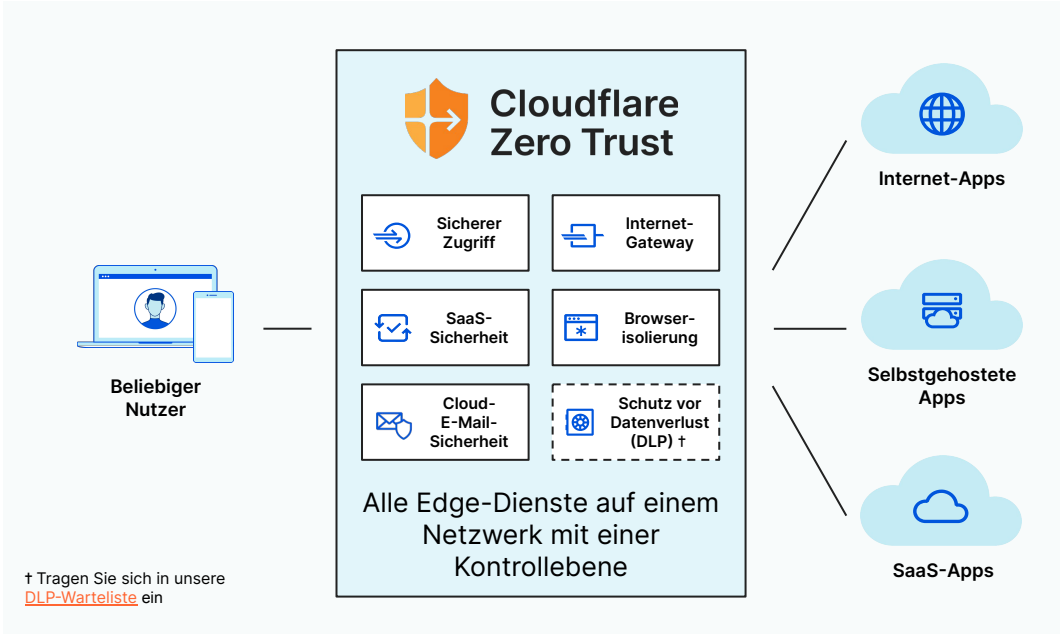
Cloud-zentrierte Konvergenz

Die Komplexität der Verwaltung mehrerer Einzellösungen veranlasst die meisten Unternehmen dazu, ihre bevorzugten Anbieter zusammenzuführen. Heute müssen sich branchenführende Fähigkeiten und umfangreiche Plattformen nicht mehr gegenseitig ausschließen. Da die Mehrheit der IT-Einkäufer zur Konsolidierung neigt, reagieren die Sicherheitsanbieter auf diese Entwicklung, indem sie den Wert ihrer Sicherheitsplattformen über das hinaus steigern, was jeder einzelne Dienst leisten könnte.

Der SSE-Ansatz – der zwischen Einzelprodukten und vollständiger Konsolidierung angesiedelt ist – konzentriert sich stärker auf Sicherheitsfunktionen als die meisten Secure Access Service Edge (SASE)-Produkte, da er nicht an die Netzwerkinfrastruktur gebunden ist. Wir sind der Meinung, dass unsere Zero Trust-Plattform auch der SSE von Gartner entspricht, da die früheren Einzelprodukte ZTNA, VPN, SWG, DNS-Filterung, CASB, RBI und Firewall as a Service (FWaaS) gebündelt werden.

„Konsolidieren Sie die Anbieter und reduzieren Sie die Komplexität und die Kosten, wenn die Verträge für SWGs, CASBs und VPNs erneuert werden (Ersetzen durch einen ZTNA-Ansatz). Nutzen Sie einen zusammenwachsenden Markt, der durch die Kombination dieser Dienste entsteht.“ [1]

Gartner



† Tragen Sie sich in unsere DLP-Warteliste ein

VPN-Ersatz
vereinfacht und sichert die Verbindung zwischen jedem Benutzer und jeder Ressource

SaaS-Sicherheit
Sichtbarkeit und Kontrolle von Anwendungen einschließlich E-Mail

Internetschutz
Schützen Sie Ihre Daten vor Bedrohungen über jeden Port und jedes Protokoll

Modernisierung der Sicherheit
verbesserte Produktivität, einfachere Abläufe, geringere Angriffsfläche

SSE als Brücke zu SASE

Die Zusammenführung von Sicherheits- und Netzwerk-Edge-Services ist das ultimative Ziel von SASE. Dennoch werden einige Unternehmen aufgrund ihrer Geschichte und ihrer aktuellen Infrastruktur vielleicht niemals eine vollständige Konsolidierung bei einem einzigen Anbieter anstreben. Unabhängig von Ihrer langfristigen SASE-Strategie kann Cloudflare Ihnen helfen, die Sicherheit zu modernisieren, Ihr Unternehmensnetzwerk zu transformieren oder beides.

SASE von einem Anbieter
Für Unternehmen, die Sicherheit und Netzwerk-Edge-Services von einem einzigen Anbieter vollständig vereinheitlichen möchten, bietet Cloudflare One, unsere SASE-Plattform, ein Zero Trust Network-as-a-Service, das auf unserem globalen Netzwerk mit über 275 Städten aufbaut.

SASE von mehreren Anbietern
Für Unternehmen mit ausgereiften SD-WAN-Implementierungen oder unzusammenhängenden Sicherheits- und Netzwerkteams kann Cloudflare Zero Trust dabei helfen, die Sicherheit zu modernisieren und eine SSE-Implementierung zu erreichen, indem SD-WAN-Partnerschaften für Multi-Vendor-SASE genutzt werden.

Modulare Einführung von SSE

Die Umstellung auf cloudbasierte SSE soll nicht von heute auf morgen erfolgen. Cloudflare Zero Trust hilft Unternehmen, die Hardware in dem von ihnen gewünschten Tempo abzuschaffen. Viele Unternehmen werden ihre Umstellung auf Zero Trust damit beginnen, ihr VPN mit ZTNA zu ergänzen, um es dann vollständig zu ersetzen. Die Optimierung der SaaS-Sicherheit steht für die meisten an zweiter Stelle der Prioritätenliste, wobei umfassendere Strategien zum Schutz vor Bedrohungen und Daten bald darauf folgen.

Unsere einheitliche, zusammensetzbare Architektur erleichtert die modulare Einführung von Sicherheitsdiensten. Unternehmen können benutzerdefinierte Kombinationen von Diensten einsetzen, die ihren vorrangigen Anwendungsfällen entsprechen. Dies beugt einer „Alles-oder-Nichts"-Mentalität vor.

„Inventarisierung von Geräten und Verträge zur Umsetzung eines mehrjährigen Ausstiegs aus der lokalen Perimeter- und Zweigstellen-Sicherheitshardware zugunsten einer cloudbasierten Bereitstellung von SSE. Ziel ist die Konsolidierung der Geräte vor Ort, idealerweise auf eine einzige Appliance."[1]

Gartner

Integration beflügelt Innovation

Sämtliche Cloudflare-Dienste werden auf allen Servern in jedem Rechenzentrum unseres riesigen globalen Netzwerks betrieben, sodass keine Abdeckungslücken oder Unstimmigkeiten bestehen. So können wir eine Überprüfung in einem einzigen Durchgang durchführen und ein Höchstmaß an Sicherheit, Performance und Zuverlässigkeit gewährleisten.

Nativ integrierte Dienste eröffnen auch kreativere Möglichkeiten, Funktionen über mehrere Dienste hinweg zu kombinieren und die gewünschten Anwendungsfälle unserer Kunden zu erfüllen. Da diese Produktlinien verschwimmen, hilft uns die dienstübergreifende Interaktion, fortschrittlichere Szenarien zu lösen und die Sicherheit wirklich zu modernisieren.

Verstärken Sie die Sicherheit beim Zugriff durch Dritte

- ZTNA und RBI integrieren, um Dritten wie Auftragnehmern und Partnern sicheren Zugang zu gewähren
- Verifizieren Sie kontextbezogene Informationen zur Autorisierung und stellen Sie Anwendungen in isolierten Browsern bereit, um Daten zu schützen
- Clientloser Betrieb für beide Dienste vereinfacht die Einführung, da keine Downloads erforderlich sind

Visualisieren und überprüfen Sie SSH-Sitzungen

- Die Integration von ZTNA und SWG ermöglicht einen Einblick in gesamte SSH-Sitzungen zur Überwachung des privilegierten Zugriffs
- Vereinfachen Sie den SSH-Zugang mit clientlosen, browserbasierten SSH-Sitzungen über ZTNA
- Bieten Sie Sichtbarkeit von SSH-Sitzungen auf Netzwerkebene; protokollieren Sie jeden Befehl, der SWG als Proxy verwendet

Vereinfachen Sie SaaS-Wiederherstellungsabläufe

- SWG und CASB lassen sich integrieren, um einen „Find and Fix"-Workflow zu ermöglichen; blockieren Sie einige oder alle verdächtigen SaaS-Aktivitäten direkt aus den CASB-Sicherheitsergebnissen
- Erweitern Sie die SaaS-Transparenz, um Probleme zu erkennen und zu beheben, die zu Datenlecks oder Compliance-Verstößen führen könnten.

Besserer Schutz vor Phishing

- Integration von E-Mail-Sicherheit und RBI zur Bekämpfung ausgeklügelter Phishing-Angriffe und Kompromittierung von Geschäfts-E-Mails (BEC)
- Keine prädiktive Bedrohungsanalyse ist perfekt. Das Öffnen von E-Mail-Links in einem isolierten Browser bietet eine zusätzliche Schutzschicht.

Wechseln Sie jetzt zu einem schnelleren, zuverlässigeren und sichereren Netzwerk

Jetzt Testen

Sie möchten noch mehr Informationen erhalten, bevor Sie die Lösung ausprobieren? Hier erfahren Sie mehr über Cloudflare One

[1] *Gartner Hype Cycle™ for Network Security, 2021*