Artikel

SASE bewerten: Fünf Anwendungsfälle für Schutz, Sicherung und Modernisierung

Da die Grenzen herkömmlicher Netzwerke immer mehr von Anwendungen, Benutzern und Daten gesprengt werden, evaluieren viele Unternehmen, wie sie ihre Umgebungen verbinden und schützen können. Die Einführung von Cloud-Lösungen, die Nutzung von SaaS und hybride Arbeitsmodelle haben die Datenverkehrsmuster und Zugriffsanforderungen verändert und dabei oft die Grenzen von Architekturen verdeutlicht, die auf festen Standorten, Backhaul-Datenverkehr und voneinander getrennten Tools basieren.

SASE wird bei dieser Evaluierung immer wichtiger. Anstatt Netzwerktechnik und Sicherheit als getrennte Aufgaben zu behandeln, vereint SASE sie mit einem Cloud-basierten Ansatz, der auf die Unterstützung moderner Zugriffsmuster und Sicherheitsanforderungen ausgelegt ist.

SASE ist keine „Entweder-oder"-Entscheidung. Viele Unternehmen betrachten SASE als einen Prozess, bei dem sie die benötigten Fähigkeiten im Laufe der Zeit passend zu ihren Prioritäten, ihrer vorhandenen Infrastruktur und ihrer Risikobereitschaft entwickeln können. Die folgenden Anwendungsfälle stellen übliche Punkte entlang des Entwicklungspfades vor. Sie zeigen, wie Organisationen SASE im Hinblick auf die Praxis bewerten, indem sie auf unmittelbare Herausforderungen eingehen und gleichzeitig im Laufe der Zeit ein einheitlicheres Netzwerk- und Sicherheitsmodell aufbauen.

1. Modernisierung der Vernetzung von Zweigstellen für eine Cloud-First-Welt

Zweigstellennetzwerke wurden ursprünglich für eine Ära konzipiert, in der die meisten Anwendungen im Rechenzentrum angesiedelt waren und der Datenverkehr vorhersehbaren Pfaden folgte. Heutzutage dominieren Cloud- und SaaS-Anwendungen die Datenverkehrsmuster. Das Backhauling von Daten über eine zentralisierte Infrastruktur kann zu Latenz, Komplexität und unnötigen Kosten führen, insbesondere bei verteilten Zweigstellen.

Die Modernisierung der Zweigstellenvernetzung mit einem sicheren SD-WAN ermöglicht es Unternehmen, sich an die Realität einer Cloud-First-Arbeitsweise anzupassen. Durch die Konsolidierung von Netzwerk- und Sicherheitsfunktionen in den Zweigstellen und die Anwendung zentralisierter, anwendungsbezogener Richtlinien können Unternehmen die Leistung für den Cloud- und SaaS-Datenverkehr optimieren und gleichzeitig eine einheitliche Kontrolle über alle Standorte hinweg gewährleisten. Dieser Ansatz verringert die Abhängigkeit von veralteten Zweigstellenarchitekturen und bietet eine flexiblere Grundlage für die fortschreitende Integration umfassenderer SASE-Funktionen.

Daraus resultierende Möglichkeiten

- Direkter, optimierter Zugriff auf Cloud- und SaaS-Anwendungen von den Zweigstellen aus
- Vereinfachte Zweigstellenarchitekturen durch die Konsolidierung von Routing-, Sicherheits- und Verbindungsfunktionen
- Verbesserte Anwendungsleistung durch anwendungsorientierte Datenverkehrssteuerung
- Höhere betriebliche Effizienz bei der Verwaltung verteilter Zweigstellenumgebungen

2. Von VPN zu ZTNA: Sichern des Zugriffs für hybrides Arbeiten

Da hybrides Arbeiten immer mehr zur Norm wird, stellen viele Unternehmen den Zugriff von Remote-Benutzern auf interne Ressourcen auf den Prüfstand. Herkömmliche VPN-basierte Zugriffsmodelle wurden für Umgebungen entwickelt, in denen Anwendungen im Rechenzentrum ausgeführt werden und Benutzer von vorhersehbaren Standorten aus arbeiteten. In den heutigen Cloud-First-Umgebungen können diese Modelle Leistungsengpässe verursachen und einen umfassenderen Netzwerkzugriff gewähren, als für die meisten Benutzer erforderlich ist.

ZTNA verlagert Zugriffsentscheidungen vom Netzwerk auf die Identität. Anstatt Benutzer in das Netzwerk zu lassen, erzwingt ZTNA identitäts- und richtlinienbasierten Zugriff auf Anwendungsebene und unterstützt so das Prinzip der minimalen Berechtigungen für Mitarbeiter, Auftragnehmer und Drittbenutzer. Mit diesem Ansatz können Unternehmen die Sicherheit des Zugriffs auf private Anwendungen gewährleisten, ohne das zugrunde liegende Netzwerk zu gefährden oder auf VPN-Tunnel zurückzugreifen, die für eine andere Ära konzipiert wurden.

Daraus resultierende Möglichkeiten

- Anwendungszugriff statt umfassender Netzwerkkonnektivität
- Umsetzung des Prinzips minimaler Berechtigungen basierend auf Benutzeridentität und Kontext
- Einheitliche Zugriffskontrollen für über remote arbeitende, lokale und externe Benutzer
- Ein praktischer Ausgangspunkt für Unternehmen, die den sicheren Zugriff in Cloud-First-Umgebungen neu überdenken

3. Einheitliche Sicherheitsmaßnahmen für Benutzer, das Internet und SaaS anwenden

Die Sicherung des Zugangs zu privaten Anwendungen stellt nur ein Teil der Herausforderung dar. Da die Nutzung von Cloud-Diensten und SaaS-Anwendungen sich immer mehr durchsetzt, müssen die Sicherheitskontrollen über die Zugriffskontrolle für private Anwendungen hinausgehen. Die Benutzer interagieren mit dem Internet und SaaS-Plattformen von einer Vielzahl von Standorten und Geräten aus, was es schwierig macht, mit herkömmlichen, perimeterbasierten Tools eine einheitliche Transparenz und Durchsetzung von Richtlinien zu gewährleisten.

Ein einheitlicher SSE (Security Service Edge)-Ansatz, der ZTNA um SWG- (Secure Web Gateway) und CASB (Cloud Access Security Broker)-Funktionen erweitert, wendet Sicherheitsrichtlinien einheitlich für alle Benutzerzugriffe, den Internetverkehr und die SaaS-Nutzung an. Wenn diese Kontrollmechanismen gemeinsam verwaltet und nicht als isolierte Instrumente betrachtet werden, können Unternehmen Richtlinienlücken verringern, die Transparenz der Benutzeraktivitäten verbessern und Schutzvorkehrungen einheitlicher durchsetzen, insbesondere in zunehmend verteilten Arbeitsumgebungen. Dieses Modell unterstützt Sicherheitsteams bei der Bekämpfung webbasierter Bedrohungen, beim Management von SaaS-Risiken wie Schatten-IT und Datenverlust sowie bei der Umsetzung des Prinzips der geringsten Berechtigungen, ohne den Betrieb unnötig zu verkomplizieren.

Daraus resultierende Möglichkeiten

- Einheitliche Durchsetzung der Richtlinien für alle Benutzer, den gesamten Internetverkehr und alle SaaS-Anwendungen
- Verbesserte Transparenz der Internetaktivitäten und SaaS-Nutzung
- Verbesserte Sicherheit beim Surfen im Internet und Schutz vor webbasierten Bedrohungen
- Ein skalierbares Sicherheitsfundament für Cloud-First-Umgebungen

4. Schutz von IoT- und nicht verwalteten Geräten mit universellem ZTNA

IoT- und Edge-Geräte stellen nach wie vor eine der hartnäckigsten Sicherheitslücken in modernen Umgebungen dar. Viele dieser Geräte werden nicht verwaltet, sind schwer zu patchen und können keine Endpoint-Agenten ausführen, was die konsequente Anwendung traditioneller Zero-Trust-Kontrollen erschwert. Da sie aber immer häufiger mit Unternehmensnetzwerken und Cloud-Services verbunden werden, erweitern sie die Angriffsfläche auf eine Weise, für die benutzerzentrierte und perimeterbasierte Sicherheitsmodelle nie konzipiert wurden. Universal ZTNA erweitert die identitätsbasierte Zugriffskontrolle über Benutzer hinaus auf IoT-Geräte und andere nicht verwaltete Geräte. Mithilfe von Profilbildung, Segmentierung und globalen Richtlinien werden die Zugriffsmöglichkeiten der einzelnen Geräte eingeschränkt.

KI-basiertes NAC untermauert diesen Ansatz und trägt zum Schutz von nicht verwalteten Geräten und IoT-Geräten bei, indem es die Gerätetransparenz, Verhaltensanalysen und die kontinuierliche Vertrauensprüfungen in allen Umgebungsbereichen verbessert. Nach der erfolgreichen Authentifizierung kann der IoT-Datenverkehr segmentiert und somit vom Datenverkehr geschäftskritischer Anwendungen getrennt werden. Da viele IoT-Geräte Internet- und Cloud-Datenverkehr für Aktivitäten wie Updates und Telemetrie generieren, können Unternehmen mithilfe der Integration von SWG-Funktionen mit sicherem SD-WAN diese Geräte schützen, ohne auf jedem einzelnen Gerät einen SSE-Agenten installieren zu müssen. Dieser Ansatz erweitert die Internetsicherheit auf alle Geräte und bietet Schutz vor schädlichen Websites durch Funktionen wie URL Filtering. Gemeinsam unterstützen diese Funktionen Unternehmen beim Schließen von Sicherheitslücken im IoT-Bereich und ermöglichen gleichzeitig einen einheitlichen Zero-Trust-Schutz für alle Benutzer, Geräte und Datenverkehr.

Daraus resultierende Möglichkeiten

- Transparenz in Bezug auf IoT- und nicht verwaltete Geräte durch Profilbildung und Verhaltensanalysen
- Segmentierte Zugriffsrichtlinien, die die Reichweite von Geräten einschränken und das Risiko lateraler Bewegungen im Netzwerk verringern
- Konsequente Durchsetzung von Zero Trust für Geräte, auf denen keine Agenten ausgeführt werden können
- Schutz vor Gefahren aus dem Internet bei IoT-Datenverkehr ohne zusätzliche Komplexität am Endpunkt

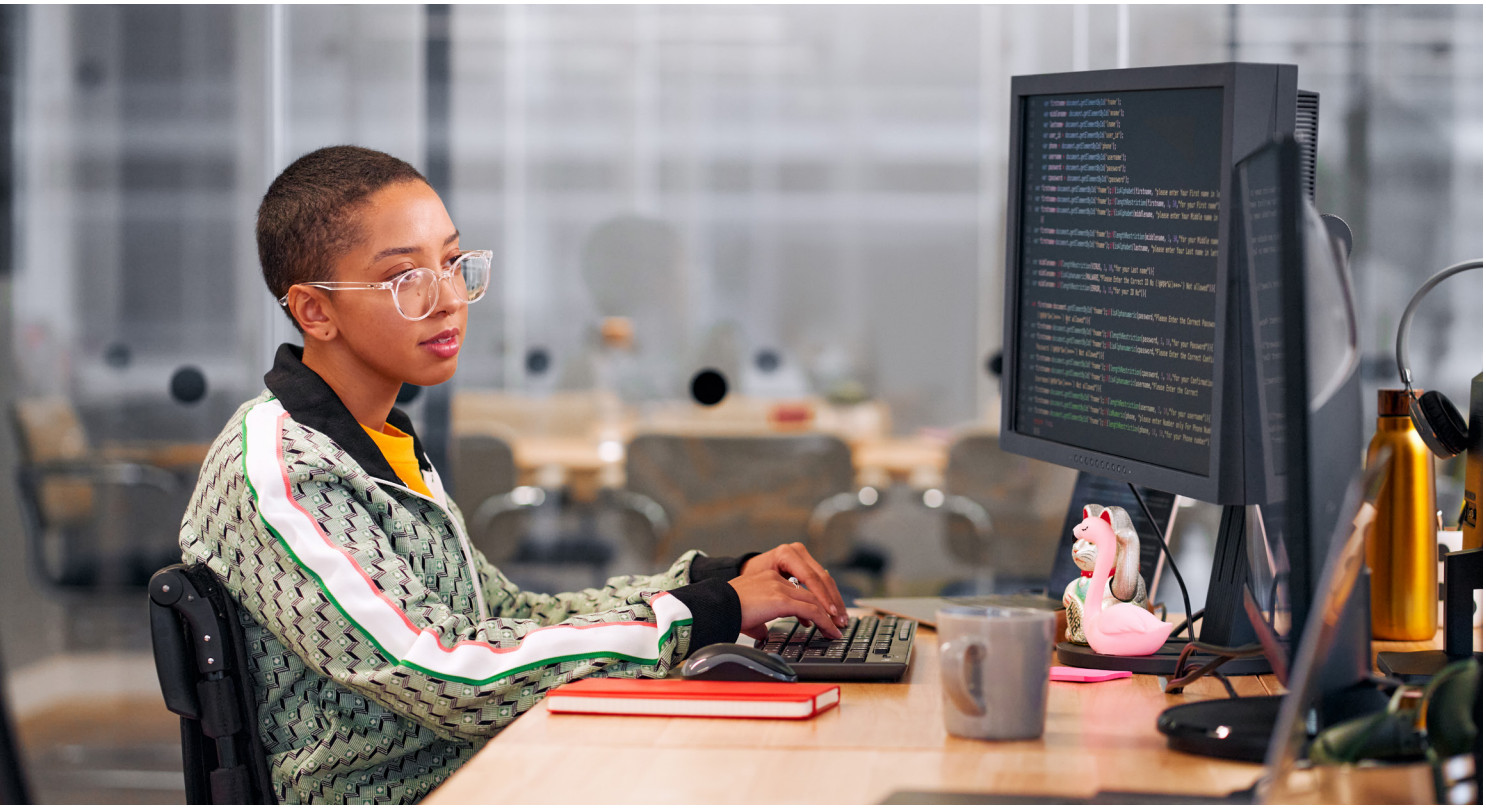
5. Verbinden von Zugriff, Sicherheit und Konnektivität mit einheitlichem SASE

Die Verwaltung von Zugriff, Sicherheit und Konnektivität in Form separater Initiativen kann unnötige Komplexität verursachen. Nicht miteinander verbundene Tools, sich überschneidende Richtlinien und manuelle Integrationsbemühungen verlangsamen oft die Bereitstellung und erschweren die Aufrechterhaltung von Einheitlichkeit in wachsenden Umgebungen. Mit der Zeit kann diese Fragmentierung den betrieblichen Aufwand erhöhen und die Fähigkeit eines Unternehmens einschränken, sich an neue Anforderungen anzupassen.

Eine einheitliche SASE-Architektur vereint diese Funktionen in einem einzigen, über die Cloud bereitgestelltem Modell. Durch die Abstimmung von sicherem Zugriff, Internet- und SaaS-Schutz und modernisierter Zweigstellenkonnektivität aufeinander können Unternehmen die Einführung und das Management von Veränderungen für Benutzer, Anwendungen und Standorte vereinfachen. Dieser einheitliche Ansatz unterstützt schnellere Einführungsprozesse, reduziert den Integrationsaufwand und hilft Teams, mit größerem Vertrauen zu handeln, während sich ihre Umgebungen ständig weiterentwickeln.

Daraus resultierende Möglichkeiten

- Vereinfachung der Nutzung von SASE-Funktionen ohne das Zusammenflicken mehrerer Plattformen
- Reduzierung des Betriebsaufwands durch einheitliche Management- und Richtlinienmodelle
- Schnellere Einführung von Änderungen für alle Benutzer, Anwendungen und Standorte
- Eine zusammenhängende Architektur, die skalierbar ist, ohne unnötige Komplexität zu verursachen



Wir unterstützen Sie auf Ihrem Weg zu Unified SASE

Unternehmen, die SASE evaluieren, betrachten den Ansatz oft als einen allmählichen Prozess und nicht als eine einmalige, umfassende Initiative. Indem Unternehmen zunächst Zugriff, Sicherheit und die Modernisierung von Zweigstellen in Angriff nehmen und diese Funktionen anschließend durch eine einheitliche SASE-Architektur zusammenführen, können sie ein Fundament schaffen, das Flexibilität, Einheitlichkeit und langfristige Skalierbarkeit im Zuge der Weiterentwicklung ihrer Anforderungen unterstützt.

HPE kann Unternehmen in allen Phasen dieses Prozesses kompetent unterstützen. Unsere KI-native, einheitliche SASE-Plattform integriert SD-WAN, SSE und NAC in eine einzige, identitätsgesteuerte Architektur. Durch den Einsatz von AIOps ermöglicht die Plattform fortschrittliche Beobachtbarkeit und Authentifizierung und bietet Unternehmen Echtzeit-Transparenz und kontinuierliche Vertrauensprüfungen für Benutzer, Geräte und Anwendungen, sogar in Umgebungen von Drittanbietern.

Unternehmen können nun unabhängig davon, ob sie ihre ersten Schritte in Richtung SASE unternehmen oder ihre bereits vorhandenen Fähigkeiten vereinheitlichen wollen, mit Vertrauen vorgehen.

Weitere Informationen unter

HPE.com/networking

HPE.com besuchen

Jetzt chatten

a00158357DEE

HEWLETT PACKARD ENTERPRISE

hpe.com