



Unified SASE: Kohärente Konnektivität und Sicherheit

Senken Sie Sicherheitsrisiken und verbessern
Sie gleichzeitig Netzwerkleistung und -management

Sicherheitsexperten haben den Secure Access Service Edge (SASE) unter die Lupe genommen. Sie wissen, dass in den Unternehmen von heute eine „neue Normalität“ herrscht und Sicherheitspraktiken, die einst effektiv waren, heute nicht mehr effektiv sind. Netzwerke, die früher überschaubar waren, sind es nun nicht mehr. Lösungen, die einmal funktioniert haben, funktionieren heute nicht mehr so gut.

Angesichts dieser unbequemen Situation wird es Zeit für einen neuen Ansatz für sicheren Zugriff, bei dem Sicherheit und Konnektivität im Gleichgewicht sind. SASE kombiniert SD-WAN und Security Services Edge (SSE) und bringt damit Sicherheit und Konnektivität zusammen. So entsteht ein überall verfügbarer, sicherer Zugriff für alles und jeden – mit einer einzigen, in der Cloud verwalteten Konsole.

Unified SASE verwirklicht die Versprechen von SASE und noch vieles mehr. Durch die umfangreiche Integration von SSE und SD-WAN werden Netzwerkarchitekturen vereinfacht, ohne die Sicherheit oder Leistung zu beeinträchtigen. So können Unternehmen ihre Bereitstellungen beschleunigen, ihren Betrieb optimieren und gleichzeitig Risiken für die Cybersicherheit senken.

Hohe Leistung und unterbrechungsfreier Zugriff bei geringeren Risiken

Die Implementierung von SASE verlangt nach strategischen Entscheidungen.

Für den Einstieg können Sie entweder alle Elemente gleichzeitig bereitstellen oder auch kleiner anfangen. Beginnen Sie beispielsweise mit der Bereitstellung eines Zero Trust-Netzwerkzugriffs (Zero Trust Network Access, ZTNA), um einen sicheren Zugriff von jedem Ort zu gewährleisten. Damit ersetzen Sie ältere und unsichere VPNs für den Remote-Zugriff. Eine weitere gute Option für den Einstieg ist die Vernetzung aller Ihrer Standorte mithilfe eines sicheren SD-WAN.

Ganz gleich, für welche Option Sie sich entscheiden, kann eine Integration von Sicherheit und Konnektivität in einer einzigen Lösung den Betrieb einfacher machen. Mit Unified SASE können Unternehmen globale digitale Innovationen auf der Grundlage von sicheren Netzwerken effizient und souverän implementieren.

In Kombination mit dieser sicheren Konnektivität unterstützt SASE die dringend benötigte Netzwerkleistung. Eine zentrale Plattform liefert Netzwerk- und Sicherheitsteams netzwerkweite Einblicke in Ereignisse, Sicherheitsvorfälle und Leistungskennzahlen.

Die Vorteile von integrierter Sicherheit und Konnektivität

Ohne Unified SASE kann es schwierig sein, Sicherheits- und Konnektivitätsziele gleichzeitig zu erreichen. Hybride Arbeitsmodelle, zunehmende Digitalisierung und das Wachstum des IoT können die Erreichung von Konnektivitäts- und Sicherheitszielen zum Drahtseilakt machen. Doch Sie können es sich auch einfacher machen.

Oftmals erkennt man die Signale, dass es an der Zeit für Unified SASE ist, damit man hohe Leistung, robuste Sicherheit und einen unterbrechungsfreien Zugriff im Einklang mit den geschäftlichen Anforderungen erzielen kann. Achten Sie auf die folgenden Anzeichen:

- Es fällt Ihnen selbst mit einer vollständigen Auswahl von Sicherheitstools und -Appliances schwer, sichere Anwendungen in Web, Hybrid Cloud und Software-as-a-Service (SaaS) zu unterstützen.
- Um der sich stetig weiterentwickelnden Bedrohungslandschaft einen Schritt voraus zu bleiben, müssen Zero Trust-Prinzipien im gesamten Unternehmen eingeführt werden.
- Remote-Benutzer sind wegen Leistungsproblemen unzufrieden, und ihre VPN-Verbindungen stellen ein Sicherheitsrisiko dar.
- Das Benutzererlebnis mit Cloud- und Rechenzentrumsanwendungen ist inkonsistent.
- Konnektivität und Sicherheit sind so komplex, dass es schwierig ist, Bereitstellungen zu beschleunigen und Ergebnisse zu erzielen.
- Sicherheits- und Netzwerkteams wenden zu viel Arbeitszeit für Fehlerbehebungen auf.
- Die Anwendungsleistung in der Cloud ist so inkonsistent, dass die Benutzer frustriert sind.
- Ein Mangel an Ressourcen und Know-how verhindert bzw. verlangsamt die SASE-Einführung.





59 %

der befragten Cybersicherheitsexperten glauben, dass die Einführung von SASE für ihr Unternehmen äußerst wichtig ist¹

Mit Unified SASE zu kombinierter Konnektivität und Sicherheit

Wenn Ihr Unternehmen wächst und Innovationen einführt, kann Unified SASE Ihnen dabei helfen, überall konsistente Konnektivität und Sicherheit bereitzustellen – und zwar ohne Kompromisse bei der Leistung oder beim Management mehrerer Plattformen, Tools und Steuerungselemente. Halten Sie sich beim Einstieg an die folgende SASE-Checkliste:

- **Grundlage für Ihre SASE-Reise:** Können Sie mithilfe von Richtlinien und Management über dieselbe Konsole SASE vereinheitlichen und Ihr gesamtes Unternehmen vernetzen? Verhindert die Lösung die Abhängigkeit von einem Anbieter und ermöglicht es Ihnen, Unified SASE in Ihrem eigenen Tempo einzuführen?
- **Schnellere Bereitstellungen:** Konsolidiert die SASE-Lösung Ihren gesamten Bestand vom Edge über das Rechenzentrum bis hin zur Cloud?
- **Zusammenarbeit zwischen Netzwerk und Sicherheit:** Können Netzwerk- und Sicherheitsteams mithilfe derselben Tools Ihre Ziele erreichen und die Komplexität verringern?
- **Hervorragendes Benutzererlebnis:** Sind Benutzer vernetzt, geschützt und produktiv?
- **Erstklassiges IT-Erlebnis:** Stehen der IT intuitive Kontrollen zur Verfügung, die ihr bei der Konfiguration, dem Management und dem Betrieb im großen Maßstab helfen, um an jedem Ort sichere Netzwerkverbindungen zu ermöglichen?

¹ „Security Service Edge Adoption Report“, Cybersecurity Insiders, März 2024



Einheitliche Konnektivität und Sicherheit mit Unified SASE von HPE Aruba Networking

Befolgen Sie diese Schritte, um einen einheitlichen SASE zu erzielen und Sicherheit und Konnektivität vom Edge bis zur Cloud an einem Ort zusammenzubringen:

Schritt 1 Sichere Verbindung für alle Benutzer, Geräte und Anwendungen

HPE Aruba Networking EdgeConnect SD-WAN bietet einen überall verfügbaren, einfachen und sicheren Zugriff und ermöglicht Konsistenz bei allen Anwendungen in Private oder Public Clouds oder SaaS. Benutzer und IT profitieren von schnelleren Bereitstellungen und proaktiven Einblicken für den Support. Sicherheit vom Edge bis zur Cloud durch dynamische Segmentierung ermöglicht es Ihnen, Richtlinien für Benutzer und Geräte zu definieren und durchzusetzen. So schützen Sie Ihr Unternehmen vor Bedrohungen aus dem IoT und erreichen mehr, als Ihnen mit typischen SASE-Architekturen möglich wäre.

Schritt 2 Sicherer Zugriff von überall mit SSE

HPE Aruba Networking SSE bietet Benutzern einen sicheren Zugriff auf sämtliche Unternehmensressourcen – ob privat, SaaS oder internetbasiert –, und zwar ohne mehrere Uls oder komplexe Richtlinien. Die hochgradig skalierbare Lösung von HPE Aruba Networking mit mehr als 500 Point-of-Presence-Standorten vereinheitlicht ZTNA, SWG, CASB und DEM und ermöglicht und unterstützt sichere Verbindungen überall dort, wo sie benötigt werden.

Schritt 3 Automatisierung der Netzwerkkonfiguration und -sicherheit im großen Maßstab

Mit HPE Aruba Networking Central kann die IT Netzwerke aller Größenordnungen – Zweigstellen, Remote-Standorte, Campus, Rechenzentrum oder Co-Location – mithilfe KI- und Cloud-basierter Tools verwalten und schützen. Netzwerk- und Sicherheitsteams profitieren von integrierter Unterstützung für Zero-Trust-Sicherheit, automatisierten Workflows mit Selbstreparatur sowie KI-basierter Geräteerkennung und -profilierung, absichtsbasierten Richtlinien und Orchestrierung für eine schnellere Problembehebung und ein besseres Benutzererlebnis.

Schritt 4 Aufbau eines zukunftsfähigen Netzwerks

Leistungsstarke Wi-Fi 6/6E- und Wi-Fi 7-Wireless Access Points verbessern das IT-, Benutzer- und IoT-Erlebnis durch eine intelligente, schnelle und sichere Wireless-Konnektivität im gesamten Unternehmen, die Ihre Zukunftsfähigkeit stärkt.

Warum HPE Aruba Networking am Edge?

Arbeiten Sie auf Ihrem Weg zur digitalen Transformation effizienter, nicht härter. Ein modernes, KI-basiertes Netzwerk, bei dem Sicherheit im Mittelpunkt steht, kann eine solide Grundlage für Ihre Zukunft schaffen. Das moderne Netzwerk kann die Einführung neuer Technologien beschleunigen, das Endbenutzererlebnis verbessern und Cyberrisiken reduzieren.

Ein gemeinsames Netzwerk- und Sicherheitsfundament von HPE Aruba Networking auf der Grundlage von Zero Trust-Prinzipien, das für eine flexible As-a-Service-Nutzung zur Verfügung steht, kann Ihnen dabei helfen, das Benutzererlebnis zu optimieren, eine höhere Leistung zu erzielen und mit der sich stetig weiterentwickelnden Bedrohungslandschaft Schritt zu halten.

Weitere Informationen unter

[HPE Edge-Konnektivität](#)

[HPE GreenLake besuchen](#)

 [Chat mit Vertrieb](#)