HPE GreenLake

Technische Beschreibung

SSE: Schutz von Verbindungen zu Benutzern, Geräten und Anwendungen überall und jederzeit

Mit Security Services Edge ermöglichen Sie den sicheren Zugriff vom Client auf die Cloud

Außergewöhnliche digitale Erlebnisse sind entscheidend, wenn Sie Wachstum beschleunigen, Rentabilität steigern und Kundentreue fördern möchten. Auch Ihre Mitarbeiter erwarten ein außergewöhnliches digitales Erlebnis, wenn sie im Büro, zu Hause oder überall dazwischen ihrer Arbeit nachgehen.

Da Mitarbeiter, Anwendungen, Geräte und Daten immer stärker verteilt sind, wird der Schutz dieser Verbindungen immer mehr zur Herausforderung. Weil sich die traditionelle Sicherheitsgrenze immer weiter auflöst und die riskanten Stellen zunehmen, müssen auch die Sicherheitsfunktionen in die Cloud verlagert werden. Organisationen müssen ihre Netzwerke in Sicherheitslösungen umwandeln, um sicherer arbeiten und Innovationen voranbringen zu können.

Die Vorteile von Security Service Edge

Security Service Edge (SSE) kann Organisationen dabei helfen, ihre Benutzer, Geräte und Anwendungen zu schützen – unabhängig von deren Standort. Eine SSE-Lösung ermöglicht Ihren Benutzern einen konsistenten und sicheren Zugriff auf ihre Anwendungen und Daten über Websites, SaaS-Anwendungen (Software-as-a-Service), Cloud-Services und private Rechenzentren hinweg.

SSE ist ein in der Cloud bereitgestellter Service, der vier zentrale Sicherheitskomponenten in einer einzigen, benutzerfreundlichen Oberfläche integriert:

- Beim **Zero Trust Network Access (ZTNA)** wird davon ausgegangen, dass kein Benutzer vertrauenswürdig für den Zugriff ist, bis das Gegenteil bewiesen ist. Im Gegensatz zu einem VPN, bei dem verbundene Benutzer einen breiten Zugriff auf das Unternehmensnetzwerk erhalten, beschränkt ZTNA den Zugriff der Benutzer nur auf die spezifischen Anwendungen oder Mikrosegmente, die ausdrücklich genehmigt wurden.
- **Secure Web Gateway (SWG)** schützt Benutzer und Organisationen vor webbasierten Bedrohungen mit Sicherheitsinspektionen wie URL-Filterung, Erkennung von bösartigem Code und Web-Zugriffskontrolle.
- **Cloud Access Security Broker (CASB)** identifiziert und erkennt sensible Daten in Cloud-Anwendungen und setzt Sicherheitsrichtlinien wie die Verwendung der Multifaktor-Authentifizierung um.
- **Digital Experience Monitoring (DEM)** unterstützt die IT-Abteilung bei der proaktiven Verbesserung der Netzwerk- und Anwendungsleistung.

Sicherer Zugriff für alle Benutzer, Geräte und Anwendungen

Sichern Sie den Zugriff für Ihre Mitarbeiter, Auftragnehmer und Geschäftspartner auf Ihre SaaS, privaten Anwendungen und das Internet. Verringern Sie Frustration und die Risiken, die mit der Verwendung eines Remote-Access-VPN verbunden sind, und setzen Sie konsistente Sicherheitsmaßnahmen für alle Benutzer, Geräte, Anwendungen, Netzwerkverbindungen und Standorte um. Zero Trust Network Access stellt sicher, dass Benutzer und Geräte schnell und einfach auf die benötigten Anwendungen und Daten zugreifen können – und auf nichts mehr. Benutzer können sich vor Internet-Bedrohungen wie Ransomware schützen. Das Netzwerk überwacht aktiv und prüft kontinuierlich, ob Verbindungen und Geräte den Sicherheitsrichtlinien Ihrer Organisation entsprechen.

Modernisiertes Netzwerk vom Edge zur Cloud

Beschleunigen Sie Ihre Cloud-First-Strategie, um sicheres hybrides Arbeiten zu unterstützen, die digitale Transformation zu beschleunigen und das IoT zu nutzen. SSE ist ein wichtiger erster Schritt zum Aufbau einer SASE-Architektur (Secure Access Service Edge), mit der Sie Zero-Trust-Konnektivität für Ihre Benutzer, Geräte und Anwendungen an Edge-, Campus-, Rechenzentrums- und Cloud-Standorten bereitstellen können. Leiten Sie den gesamten Datenverkehr intelligent weiter, sodass Anwendungen für Ihre Benutzer reaktionsschneller sind und die Ausfallsicherheit des Netzwerks verbessert wird.

Vereinfachte Sicherheitsabläufe

Beseitigen Sie die Komplexität der Verwendung mehrerer Sicherheitstools zur Verwaltung von Richtlinien an verschiedenen Standorten. Mit SSE können Sie mit nur einer Schnittstelle und einer Richtlinie den Zugriff auf alle Unternehmensressourcen sichern. Überwachen Sie die digitale Erfahrung aktiv, um Probleme schnell zu beheben, bevor die Benutzer davon betroffen sind. Reduzieren Sie Inkonsistenzen, die zu Sicherheitslücken führen können – und profitieren Sie von der Sicherheit, dass diese Richtlinien konsequent und kontinuierlich durchgesetzt werden. Durch die Vereinfachung der Abläufe kann sich Ihr IT-Team auf strategische Initiativen konzentrieren.

Lassen Sie sich nicht durch Komplexität und Herausforderungen aufhalten

SSE ist ein entscheidender Schritt bei der Aktivierung der Zero-Trust-Prinzipien zum Schutz Ihrer Benutzer, Geräte und Anwendungen vor den erhöhten Risiken, die durch hybride Arbeit und hybride Clouds entstehen. SSE kann Ihnen dabei helfen, Herausforderungen wie die folgenden zu meistern:

- Silos zwischen Netzwerk- und Sicherheitsteams, die eine Zusammenarbeit verhindern und zu Ineffizienzen in den Abläufen führen
- Schwache Kontrollen des Zugriffs auf Anwendungen und Daten, die zu Datendiebstahl oder der Nichteinhaltung von Vorschriften führen könnten
- Steigende Komplexität und Kosten für den Kauf, die Wartung und die Verwaltung vieler verschiedener Sicherheitsprodukte
- Beschwerden von Benutzern über unzuverlässige Verbindungen und langsame Anwendungen, die ihre Produktivität beeinträchtigen

Effiziente Konnektivität von überall und zu jeder Zeit ist unerlässlich. Verbessern Sie den sicheren Zugang für Ihr Unternehmen, indem Sie VPN durch ZTNA ersetzen: für vereinfachte Sicherheit und eine außergewöhnliche Erfahrung für Ihre Mitarbeiter.

Verbinden und schützen Sie Ihr Unternehmen mit HPE Aruba Networking

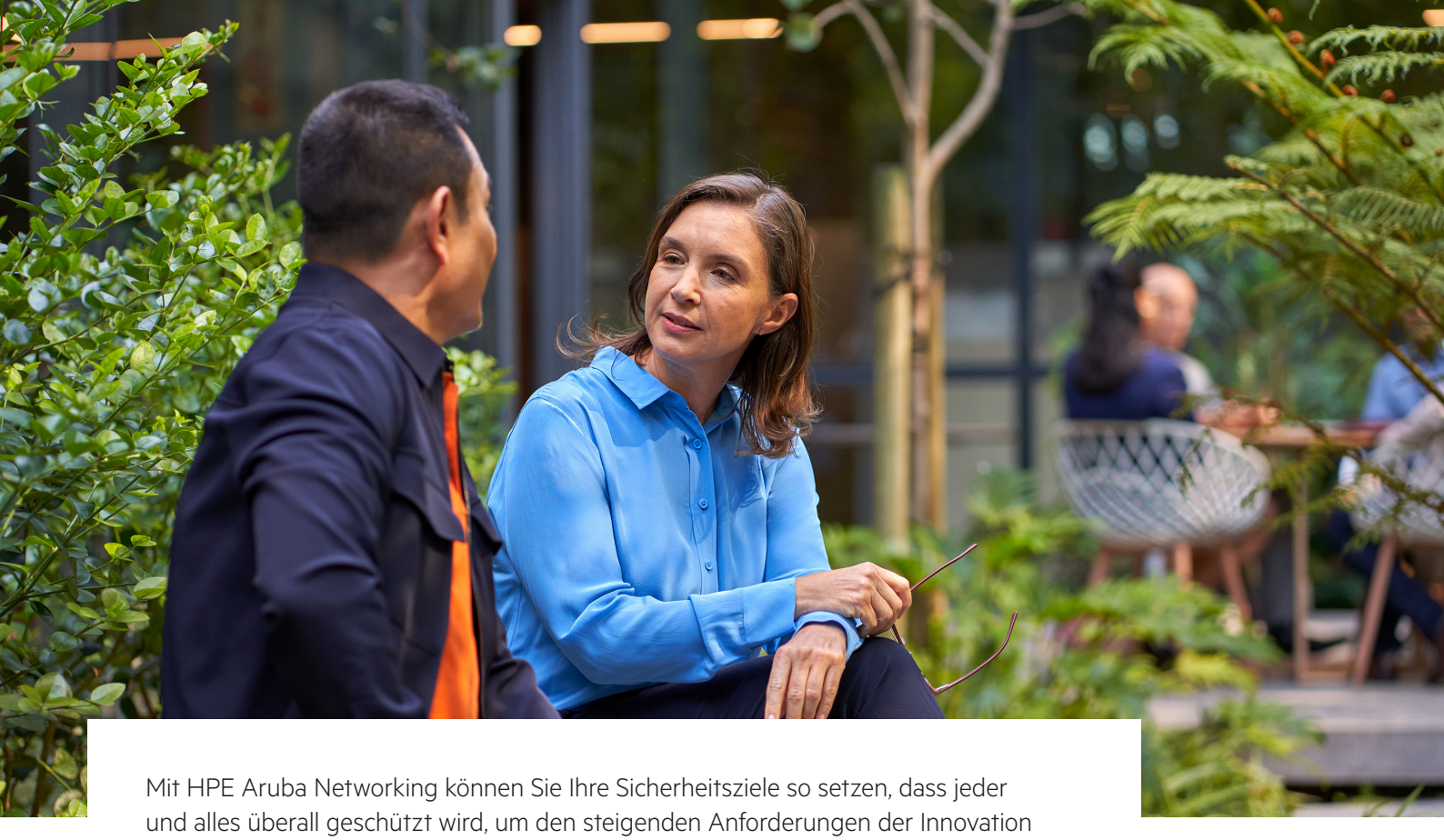
Mit HPE Aruba Networking SSE können Sie Ihre Benutzer, Geräte und Anwendungen vom Edge bis zur Cloud verbinden und schützen. ZTNA, SWG, CASB und DEM sind in eine aus der Cloud bereitgestellte Plattform für Sicherheitsdienste integriert, die Sie über eine einzige Verwaltungsoberfläche und -richtlinie steuern können. HPE Aruba Networking SSE verfügt über mehr als 500 Präsenzpunkte auf der ganzen Welt, sodass Ihre Benutzer eine schnelle und sichere Verbindung zu ihren Geschäftsressourcen haben – egal wo sie arbeiten.

Schritt 1: Konsistenter, sicherer Zugriff auf Anwendungen und Daten mit einer SSE-Lösung

Mit HPE Aruba Networking SSE können Sie allen Mitarbeitern, Auftragnehmern und Kunden einen sicheren Zugriff von deren Geräten – egal ob vom Unternehmen verwaltet oder BYOD – auf deren Anwendungen – egal ob privat, SaaS oder Internet – überall auf der Welt ermöglichen.

Schritt 2: Modernisiertes Netzwerk und beschleunigte Einführung von SASE

HPE Aruba Networking SSE lässt sich mit HPE Aruba Networking EdgeConnect SD-WAN integrieren, um den sicheren Zugriff und die Vernetzung mit einer einzigen, einheitlichen SASE-Plattform zu transformieren, die Anwendungsleistung zu verbessern, die Sicherheit zu stärken und die betriebliche Effizienz zu steigern, während Ihre Organisation immer mehr Anwendungen in die Cloud migriert.



Mit HPE Aruba Networking können Sie Ihre Sicherheitsziele so setzen, dass jeder und alles überall geschützt wird, um den steigenden Anforderungen der Innovation gerecht zu werden. Mit dem sicherheitsorientierten, KI-basierten Netzwerk kann Ihre Organisation außergewöhnliche digitale Erfahrungen bieten, um Wachstum zu beschleunigen, Rentabilität zu steigern und die Kundentreue zu fördern.

Verwandeln Sie Ihr Netzwerk in eine Sicherheitslösung, die Ihre Mitarbeiter dazu befähigt, Innovationen sicherer voranzutreiben.

Weitere Informationen unter

HPE Aruba Networking SSE

HPE Aruba Networking EdgeConnect SD-WAN

HPE GreenLake besuchen

Chat mit Vertrieb

Hewlett Packard Enterprise

a50010358DEE