HPE aruba networking

Business-Whitepaper

Der Architektenleitfaden für das Ersetzen von VPN

HPE GreenLake

Alte Technologie in einer neuen Welt

Während der vergangenen Jahre hat sich die Arbeitsumgebung erheblich verändert. Die Landschaft hatte mit der Erfindung und dem Wachstum der Cloud bereits begonnen, sich zu verändern, doch die COVID-19-Pandemie führte zu einem starken Anstieg von Remote-Arbeit.

Dies verändert, die Art und Weise wie wir unsere Architektur-Designs betrachten. Unsere Benutzer sind nicht mehr durch eine Perimetergrenze geschützt. Die Beschäftigten arbeiten überall. Darüber hinaus sind die Anwendungen, auf die sie täglich zugreifen müssen, nun auf SaaS-, lokale und IaaS-Standorte verteilt.

Die Teams müssen heute eine sichere Konnektivität zu internen und externen Anwendungen für einen Benutzerstamm unterstützen, der sich an jedem Ort befinden kann. Architekten müssen einen sicheren Zugriff auf alle älteren Anwendungen unterstützen und ebenfalls erwägen, wie der Anwendungszugriff in Zukunft gestaltet sein soll.

Die neue Welt der Cloud und der Mobilität verändert, wie wir uns vernetzen und wie wir diese Konnektivität schützen. Außerdem können ältere Lösungen wie herkömmliches VPNs die heutigen Anforderungen nicht angemessen erfüllen. Viele Unternehmen ersetzen ihr VPN durch eine moderne Technologie, die sich auf vielen Security Service Edge (SSE)-Plattformen findet und als Zero Trust Network Access (ZTNA) bezeichnet wird.

Was ist SSE und wofür eignet sich ZTNA?

SSE ist Teil des größeren Secure Access Service Edge (SASE) Frameworks, das Gartner® 2019 eingeführt hat. Als es während der Pandemie 2021 zu einer sprunghaften Zunahme von Remote-Arbeit kam, führte Gartner® SSE ein.

Das SSE-Framework ist eine Sammlung integrierter cloud-zentrierter Sicherheitsfunktionen, die mithilfe folgender Technologien einen sicheren Zugriff auf private Anwendungen, Software-as-a-Service-Anwendungen (SaaS) sowie das Internet ermöglichen: Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB) und Secure Web Gateway (SWG).

- **ZTNA** ermöglicht Zero Trust-Zugriff auf private Anwendungen.
- **CASB** schützt den Zugriff auf alle SaaS-basierten Anwendungen.
- **SWG** gewährleistet, dass der gesamte Zugriff auf das Internet sicher ist.

Eine SSE-Plattform sollte eine zentrale einheitliche Plattform für sämtliche Anwendungszugriffe bieten und gleichzeitig den Anwendungszugriff vom Unternehmens-Netzwerk entkoppeln. Sie sollte als Overlay des vorhandenen Netzwerks dienen und der IT-Abteilung die Möglichkeit bieten, die Konnektivität zu modernisieren und zu vereinfachen, während gleichzeitig die Sicherheit verstärkt wird, ohne komplexe Änderungen an der Netzwerk-Architektur vornehmen zu müssen.

Eine SSE-Plattform aus mehreren Kerntechnologien besteht, die unabhängig implementiert werden können. Wo also beginnen Sie? Wie sollten Sie SSE einführen? Die Antwort auf diese Frage ist dieselbe wie bei allen anderen Sicherheitsprojekten oder -initiativen: in den Bereichen mit dem höchsten Risiko. In der neuen Welt dezentraler Anwendungen und Benutzer ist der beste Start das Ersetzen Ihrer VPN-Technologie und der Schutz des Zugriffs auf Ihre privaten Anwendungen durch ZTNA.

„Bis 2025 werden 70 % der neuen Implementierungen für den Remote-Zugriff hauptsächlich mithilfe von ZTNA-Services umgesetzt, statt mit VPN-Services.“

– **Gartner® Forecast Analysis:** Information Security and Risk Management, Worldwide, September 2022

ZTNA als Alternative zu VPN

Teams müssen die Komplexität bei der Sicherung von Remote-Arbeitsumgebungen bewältigen. Hier bietet ZTNA eine überzeugende Alternative zu traditionellen VPNs. ZTNA beseitigt mehrere Beschränkungen herkömmlicher VPNs und bietet die folgenden Vorteile für moderne Unternehmen.

Sicherheit

- **VPN-Herausforderung:** VPNs setzen Netzwerke Bedrohungen wie Malware, Ransomware und DDoS-Angriffen aus, indem Netzwerk-IP-Adressen offengelegt werden und Angreifern der Zugriff auf das gesamte Netzwerk ermöglicht wird.
- **ZTNA-Lösung:** ZTNA minimiert das Risiko internet-basierter Angriffe durch Verbergen privater Ressourcen vor dem Internet. Rein ausgehende Verbindungen machen Ihr Netzwerk und Ihre Anwendungen unsichtbar und nicht nachverfolgbar, wobei Benutzer niemals Netzwerkzugriff erhalten. Darüber hinaus wird der Zugriff basierend auf einer dynamischen Benutzeridentität sowie Geräte- und Datenkontext gewährt – eine nicht autorisierte laterale Verschiebung wird verhindert.

Skalierbarkeit und Flexibilität

- **VPN-Herausforderung:** Da es sich bei VPNs um physische Appliances handelt, kann die Skalierung der Infrastruktur mühsam und problematisch sein. Durch die Zunahme der mobilen Arbeit müssen viele Unternehmen ihre Investitionen in die VPN-Infrastruktur erheblich ausweiten, um mehr Verbindungen zu unterstützen und ein gestiegenes Datenverkehrs-Aufkommen zu bewältigen.
- **ZTNA-Lösung:** Die Cloud-Architektur von ZTNA ermöglicht eine mühelose Skalierung und eine zentrale Verwaltung per Remote-Zugriff. Zero Trust-Richtlinien können innerhalb von Sekunden auf Benutzer- sowie auf Anwendungsebene angepasst und global durchgesetzt werden.

Produktivität

- **VPN-Herausforderung:** Da der Datenverkehr über das Unternehmens-Netzwerk umgeleitet wird, können VPNs die Verbindungsgeschwindigkeiten und die Anwendungsleistung beeinträchtigen. Dies führt zu Produktivitätsverlusten und einer erhöhten IT-Workloads für die Verwaltung des Zugriffs.
- **ZTNA-Lösung:** ZTNA optimiert das Benutzererlebnis, indem der Zugriff durch globale Cloud-Edge-Standorte so nah wie möglich in die Nähe des Benutzers gebracht wird. Hierbei wird der Datenverkehr automatisch über den schnellsten Zugriffspfad geleitet. ZTNA beseitigt VPN-bezogene Verlangsamungen, Trennungen und Anmeldeprobleme, während gleichzeitig eine nahtlose Integration mit SSO- und Identitätsmanagement-Systemen erfolgt.

Kosten

- **VPN-Herausforderung:** VPNs sind mit hohen Kosten verbunden, da kostspielige lokale Hardware sowie spezielles Personal für die Überwachung und Verwaltung benötigt werden. Hinzu kommt die Notwendigkeit eines erweiterten Stacks für die Sicherheit des eingehenden Datenverkehrs zur Minimierung des Risikos VPN-bezogener Angriffe.
- **ZTNA-Lösung:** ZTNA eliminiert die Kosten in Verbindung mit herkömmlicher VPN-Hardware, DDoS-Schutz sowie Firewalls und vereinfacht die Überwachung, sodass Ressourcen für andere wichtige Projekte freigesetzt werden.

Beginnen Sie Ihre SSE-Einführung mit ZTNA

ZTNA hat sich über die Grenzen eines reinen Remote-Zugriffs hinaus zu einem grundlegenden Konzept für den Anwendungszugriff als Ganzes entwickelt. Es ist mehr als nur ein Gateway. Es handelt sich um einen transformativen Ansatz, der den Weg zu einer umfassenderen Vision ebnet. ZTNA ist ein einzelner, über die Cloud bereitgestellter Service, der alle Ihre Zugriffsanforderungen erfüllt.

Wählen Sie den Einstiegspunkt

Bei der Implementierung von ZTNA ist es wichtig, die treibende Kraft für die Entscheidung zu bestimmen. Ist das primäre Ziel die Verbesserung der Sicherheit, die Optimierung des Benutzererlebnisses oder das Einsparen von Kosten? Die zugrundeliegende Motivation zu kennen, hilft Ihnen bei der Auswahl des am besten geeigneten Startpunkts für Ihre ZTNA-Einführung.

„Bis Ende 2024 führt die Änderung der Arbeitsweise zu einem Anstieg der Remote-Arbeit auf 60 % aller Beschäftigten, statt 52 % im Jahr 2020."

– **Gartner® Forecast Analysis:** Information Security and Risk Management, Worldwide, September 2022

Wenn **Sicherheit** Ihre Priorität darstellt, bestimmen Sie den Bereich mit dem höchsten Risiko und konzentrieren Sie sich auf Lösungen für einen sicheren Zugriff durch bestimmte Gruppen wie Drittnutzer oder Beschäftigte. Wenn das Ziel die **Verbesserung des Benutzererlebnisses** ist, ermitteln Sie, welche Benutzergruppen durch einen unzureichenden Zugriff beeinträchtigt werden (z. B. Führungskräfte oder Remote-Arbeitskräfte) und verbessern Sie deren Zugriff auf private Anwendungen. Wenn **Kosteneinsparungen** das Ziel sind, analysieren Sie, welche älteren Technologien die höchsten Kosten verursachen (z. B. VPNs) und überlegen Sie, wie sie durch ZTNA ersetzt werden können.

ZTNA-Anwendungsfälle

Die Auswahl des ersten Anwendungsfalls kann entmutigend sein. Zu Ihrer Unterstützung haben wir drei vorherrschende Anwendungsfälle bestimmt. Die folgenden Abschnitte beschreiben diese Szenarien und die nahtlose Integration von ZTNA.

Sicherer Remote- und Hybrid-Zugriff für Mitarbeitende

In der mobilen Welt haben herkömmliche VPNs Schwierigkeiten, Schritt zu halten. Wenngleich VPNs ein entscheidender Faktor war, um einen Remote-Zugriff für Mitarbeitende zu ermöglichen, stellen Sie nun erhebliche Sicherheitsrisiken in Bezug auf die Konnektivität dar. Vor dem Hintergrund zu Hause, im Büro oder an einem beliebigen anderen Ort arbeitender Beschäftigter ist ein konsistenter, unauffälliger Zero Trust-Ansatz für den Zugriff entscheidend.

Das nachstehende Diagramm zeigt, wie die ZTNA-Technologie veraltete, üblicherweise in Rechenzentren genutzte VPN-Frameworks ersetzt. ZTNA fungiert als Vermittler zwischen Benutzer und Anwendung, wobei der Zugriff nur autorisierten Benutzern und zugelassenen Anwendungen gewährt wird, unabhängig von deren Standort – ob lokal oder in der Public Cloud.

Dies wird durch einen einfachen Anwendungskonnektor erreicht, der sich innerhalb der Anwendungsumgebung befindet und den Zugriff nur gestattet, wenn er entsprechende kontextuelle Anforderungen erfüllt. Wenn die Kriterien erfüllt sind, wird eine ausgehende Verbindung aufgebaut, die sicherstellt, dass die Benutzer nicht direkt in das Netzwerk gelangen, und lediglich Zugriff auf die gewünschte zulässige Anwendung erhalten.

Darüber hinaus beeinträchtigt der Übergang vom Remote-Zugang zum bürointernen Zugang nicht das Benutzererlebnis, da ZTNA nahtlos im Hintergrund arbeitet. Er schützt sogar das Netzwerk, indem der Zugriff von potenziell kompromittierten Geräten verhindert wird, während diese sich vor Ort innerhalb des Unternehmens befinden.

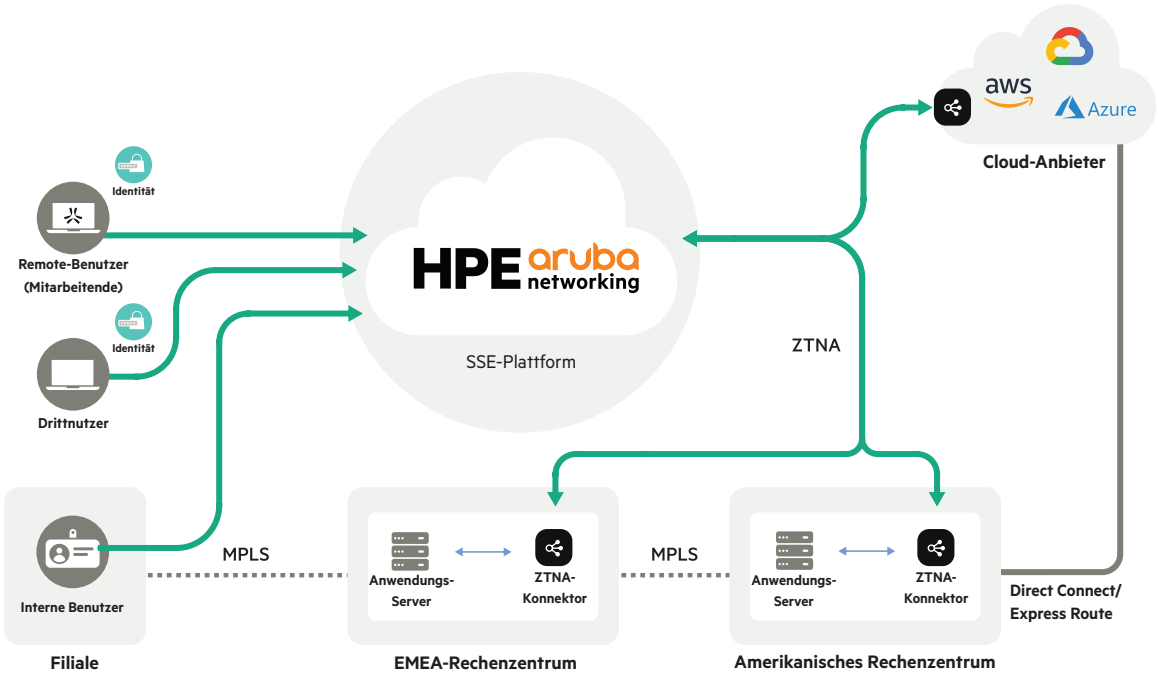

Abbildung 1. Sicherer Remote- und Hybrid-Zugriff

Sicherer Drittpartei- und BYOD-Zugriff

Der herkömmliche Zugriff basierte auf VPN-Technologie für den Remote-Zugriff. Die Benutzer mussten einen Client installieren, auf manuelle Aktualisierungen der ACL- und FW-Richtlinien durch einen Administrator warten und anschließend versuchen, eine Verbindung herzustellen. Erfolgreiche Verbindungen gewährten Zugriff auf sensible Assets und stellten ein erhebliches Risiko für das Netzwerk dar. VPN erweitert den Netzwerkzugriff auf nicht vertrauenswürdige Benutzer oder nicht vertrauenswürdige Geräte aus nicht vertrauenswürdigen Netzwerken. Sobald sich ein Drittnutzer im Netzwerk befindet, erhält er häufig freien Zugriff auf das gesamte Netzwerk.

ZTNA beseitigt das Risiko dieses Ansatzes, indem lediglich ausgehende Verbindungen zulässig sind. ZTNA verbirgt Netzwerk-Infrastruktur, Unternehmensanwendungen und Drittpartei-Portale vor dem Internet und schützt sie vor Standortbestimmungen und DDoS-Angriffen, da sie bei eingehenden Sondierungen nicht gefunden werden können. Private Anwendungen und Drittportale befinden sich sicher hinter einem Anwendungskonnektor, der ausschließlich Datenverkehr über die ZTNA-Cloud zulässt.

ZTNA ermöglicht außerdem die Durchsetzung von Richtlinien für einen Zugriff mit geringstmöglichen Rechten, selbst für BYOD-Nutzer von Drittparteien. Eine nahtlose Integration mit allen wichtigen SSO-Lösungen ermöglicht einen reibungslosen Zugriff auf private Anwendungen über einen einfachen Web-Browser, ohne die Sicherheit zu beeinträchtigen.

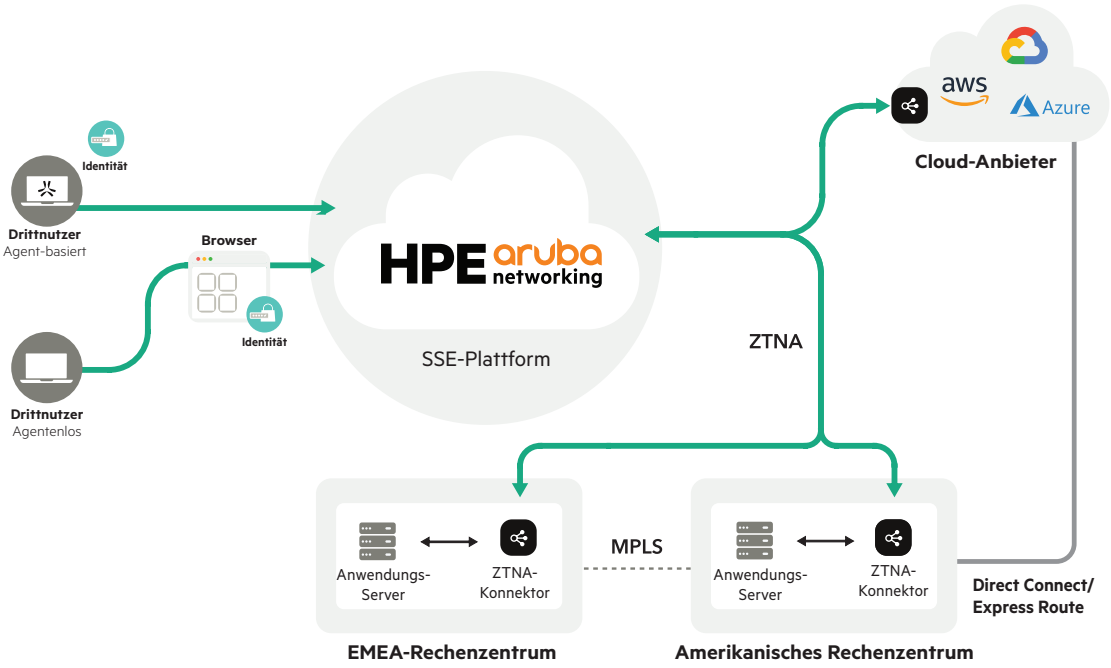

Abbildung 2. Sicherer Drittpartei- und BYOD-Zugriff

Beschleunigung von Fusionen und Übernahmen

Fusionen und Übernahmen (M & A) stellen komplexe Herausforderungen dar, doch ZTNA bietet eine optimierte Lösung für den sofortigen Zugriff auf kritische Anwendungen ab dem ersten Tag. Durch diesen Ansatz wird die Notwendigkeit von VPNs, Netzwerkintegrationen oder Infrastruktur-Änderungen beseitigt. Die Strategie basiert auf einer vordefinierten Liste wesentlicher Anwendungen, wie beispielsweise Personalsysteme, ERP und andere web-basierte Tools, die über die SSE-Plattform zugänglich sind.

ZTNA beinhaltet eine solide Identitätsstrategie, die gewährleistet, dass die Benutzer sich sicher authentifizieren und auf die Anwendungen zugreifen können, sogar noch vor der Konsolidierung von Verzeichnissen, Benutzern und Gruppen in denn fusionierenden Unternehmen. Die SSE-Plattform kann gemeinsam mit zahlreichen Identitätsanbietern integriert werden. Die ist entscheidend, um die vielfältigen Anforderungen für den Anwendungszugriff durch alle Benutzer zu erfüllen.

Die nicht agent-basierten Funktionen von ZTNA beschleunigen den Fusions- und Übernahmeprozess durch sicheren, browser-basierten Zero Trust-Zugriff mit einer erheblich beschleunigten Integration.

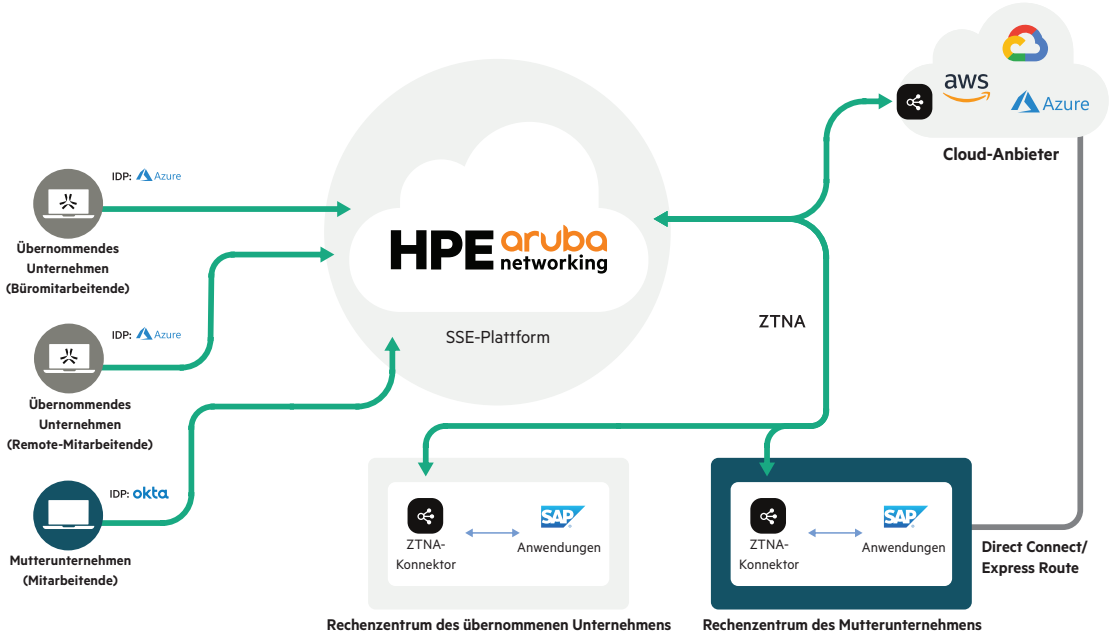

Abbildung 3. Beschleunigung von Fusionen und Übernahmen

HPE Aruba Networking ZTNA: der ultimative VPN-Ersatz

Der Beginn Ihrer Umstellung auf SSE muss nicht schwierig sein. Unsere SSE-Experten helfen Ihnen gerne weiter. Dies sind nur einige wenige Gründe, warum Teams wie Ihre sich entschieden haben, bei ihrer Umstellung auf SSE mit HPE Aruba Networking zusammen zu arbeiten.

- **Vollständiger VPN-Ersatz:** HPE Aruba Networking ZTNA übertrifft dank seiner umfassenden Unterstützung für private Anwendungen den Markt. Die Lösung wickelt den gesamten TCP-/UDP-Datenverkehr ab, einschließlich VoIP und Peer to Peer, und ist mit modernen Web-Anwendungen wie SSH, RDP, Git und Datenbanken kompatibel.
- **Zugriff mit den geringstmöglichen Rechten ohne Segmentierung:** Ohne die Notwendigkeit komplexer Netzwerk-Segmentierungen schränkt unser ZTNA-Service den Zugriff auf bestimmte Ressourcen ein, reduziert die Angriffsfläche und verhindert ein unbefugtes Eindringen in das Netzwerk.
- **Flexibler Zugriff mit oder ohne Agent:** Die Benutzer können von jedem Gerät aus nahtlos auf die Anwendungen zugreifen, mit oder ohne Client. Unsere client-lose Option ermöglicht browser-basierte RDP-Sitzungen und beseitigt die Notwendigkeit einer VDI.
- **Granulare Untersuchung des Datenverkehrs:** Erhalten Sie detaillierte Informationen über den Datenverkehr privater Ressourcen. Verfolgen Sie Benutzeraktionen, Datei-Downloads und Befehlsanwendungen nach und blockieren Sie schädliche Aktivitäten.
- **Adaptive Zugriffssteuerung:** Unsere API-basierte Steuerung passt die Zugriffsrechte basierend auf Benutzerstandort, Identität und Gerätestatus an und verbessert so die Datensicherheit.
- **100-prozentige Cloud-Architektur:** Mit HPE Aruba Networking SSE werden die Verbindungen durch den besten SSE-Edge-Standort verwaltet, sodass eine konsistente Produktivzeit gewährleistet ist, ohne die Notwendigkeit, VPN-Appliances verwalten zu müssen.

Erste Schritte mit HPE Aruba Networking ZTNA

Bewerten Sie die Anforderungen Ihres spezifischen Anwendungsfalls und setzen Sie sich mit unseren erfahrenen Experten in Verbindung, um die Bereiche zu bestimmen, in denen ZTNA erhebliche Vorteile für Ihr Unternehmen bieten kann. Schützen Sie noch heute Ihre wichtigsten Anwendungen mit unseren modernen Sicherheitslösungen.

Weitere Informationen

Einen SSE-Experten kontaktieren

ZTNA 24 Stunden lang kostenlos testen

Besuchen Sie **ArubaNetworks.com**

Entscheiden Sie sich für das richtige Produkt. Kontaktieren Sie unsere Presales-Experten.

Kontakt

Hewlett Packard Enterprise

BWP_Architect-VPN-Replacement_A4_RB_012624 a00137489dee