



Sichern des Zugriffs durch Dritte mit HPE Aruba Networking

Vernetzen Sie Ihr Business-Ökosystem, um die Produktivität zu steigern und gleichzeitig das Risiko zu minimieren



Eine Geschichte über Drittparteirisiken

Im Februar 2022 stellte Toyota seinen Betrieb in Japan vollständig ein, nachdem es bei einem seiner Drittanbieter zu einer schwerwiegenden Datenschutzverletzung gekommen war.

Nicht nur verschaffte sich das Drittunternehmen Kojima Zugang zum Netzwerk und den Fertigungsanlagen von Toyota und beeinträchtigte so die Produktion; die Sicherheitsverletzung hatte auch Auswirkungen auf den Betrieb anderer Tochtergesellschaften von Toyota.

Das Netzwerk, die Daten und die Infrastruktur von Toyota gerieten in Gefahr, was letztlich zu einem Produktionsstopp und damit zu einem negativen Geschäftsergebnis führte.

Dies diente vielen Unternehmen als Warnung. Zwar sollten Unternehmen die Entwicklung ihrer Ökosysteme nicht behindern, doch müssen die Verantwortlichen für IT-Sicherheit bessere und sicherere Wege finden, um Drittanbietern den Zugriff zu ermöglichen, ohne das Unternehmen oder seine kritischen Daten zu gefährden.

Zusammenfassung

- Ältere Zugriffslösungen sind nicht ausreichend für den Schutz vor modernen Cyber-Risiken.
- Zero Trust Network Access (ZTNA) minimiert das Drittparteirisiko und unterstützt die IT gleichzeitig bei der Einführung einer Secure Service Edge (SSE)-Strategie.
- HPE Aruba Networking bietet eine vertrauenswürdige SSE-Plattform mit einem erweiterten ZTNA-Angebot.

92%

der Unternehmen sind über VPN-Risiken besorgt.¹

VPNs gefährden Unternehmen, statt sie zu schützen.

Der herkömmliche Drittparteizugriff birgt enorme Risiken

Bisher war der Zugriff durch Dritte – oder Partner – stark von der VPN-Technologie für den Remote-Zugriff abhängig. Unabhängig davon, ob der Zugriff über ein Partnerportal oder direkt auf eine Rechenzentrumsanwendung erfolgte, musste ein Drittnutzer einen VPN-Client auf sein Gerät herunterladen, warten, bis ein Administrator die ACL- und Firewall-Richtlinien manuell aktualisiert hatte, und konnte dann einen Zugriffsversuch unternehmen.

Darüber hinaus stand das Unternehmensnetzwerk nach dem erfolgreichen Zugriff vollständig offen, was dem Partnerbenutzer nicht nur Zugriff auf das Unternehmensnetzwerk, sondern auch auf potenziell vertrauliche Daten ermöglichte. Das ist das Problem mit VPNs: Sie ermöglichen nicht vertrauenswürdigen Benutzern auf nicht vertrauenswürdigen/nicht unternehmenseigenen Geräten und von nicht vertrauenswürdigen Partnernetzwerken aus einen uneingeschränkten Netzwerkzugriff. Nachdem ein Drittbenutzer im Netzwerk angemeldet ist, kann er häufig ohne nennenswerte Einschränkungen auf Systeme im gesamten Netzwerk zugreifen. Dieses VPN-Problem des offenen Zugriffs ist der Kern des herkömmlichen Drittparteirisikos.

Herkömmliche VPNs bieten umfassenden offenen Netzwerkzugriff auf alle Anwendungen, Server und Ressourcen in einem bestimmten Netzwerksegment.

¹ VPN Risk Report 2024 von Cybersecurity Insiders

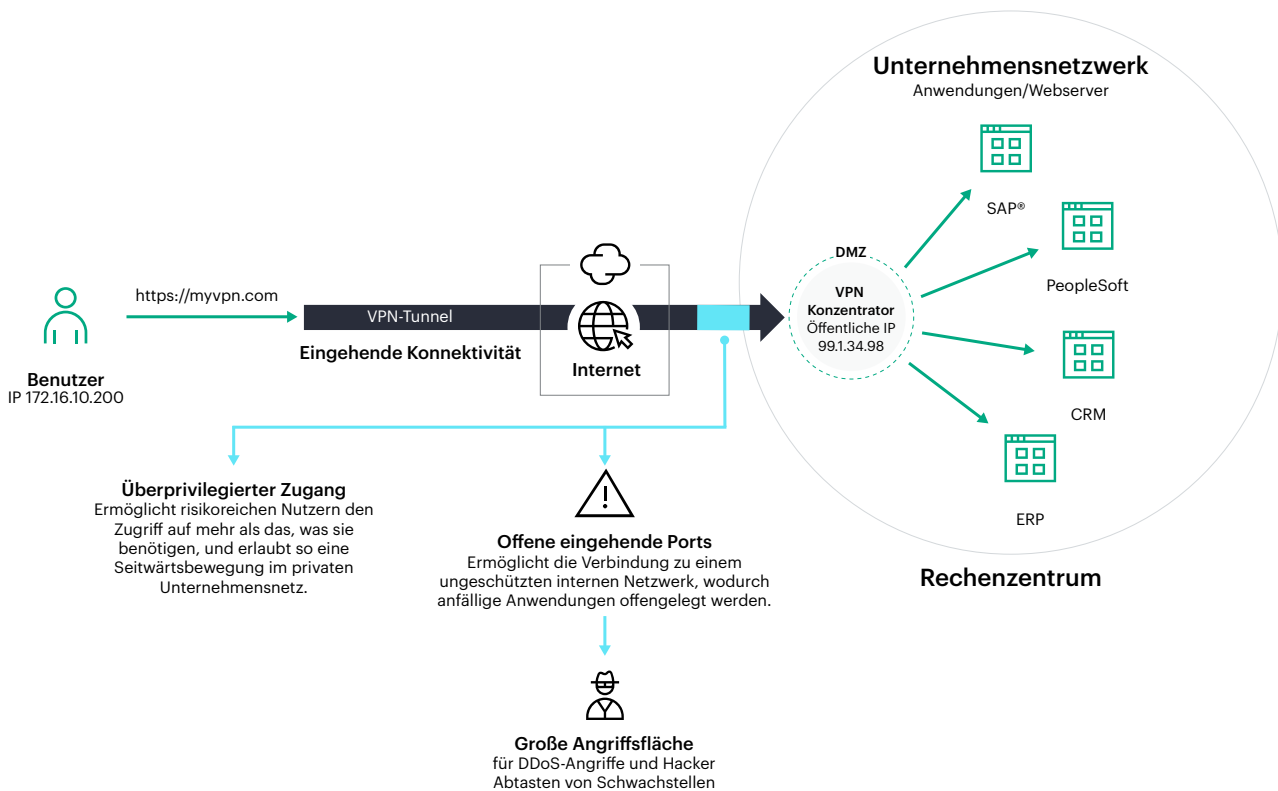


Abbildung 1. Zugriff durch Dritte mit herkömmlichem VPN.

Sichern des Drittparteizugriffs mit einem modernen Ansatz

Unabhängig davon, ob das Risiko durch Dritte durch ein schwaches Passwort, veraltete VPN-Software, BYOD-Systeme, komplexe Cloud-Services oder einfach dadurch entsteht, dass Benutzer die Sicherheitsrichtlinien eines Unternehmens missachten, benötigen IT-Sicherheitsteams zweifellos eine moderne Zugriffslösung, die diese Kernprinzipien berücksichtigt:

— Drittbenuer vom Netzwerk fernhalten

Drittbenuer benötigen nur Zugriff auf bestimmte interne Anwendungen und sollten niemals erweiterten Netzwerkzugriff erhalten. Moderne Drittparteizugriffe müssen berücksichtigen, dass für den Zugriff auf bestimmte Anwendungen kein vollständiger Netzwerkzugriff erforderlich ist. Stattdessen sollte den Benutzern der Zugriff mit den geringstmöglichen Rechten gewährt werden. Dies bedeutet, dass sie nur auf die spezifischen Daten, Ressourcen und Anwendungen zugreifen können sollten, die sie zum Bewältigen einer erforderlichen Aufgabe benötigen.

— Erhöhte Sicherheit durch bessere Sichtbarkeit und Kontrolle

Durch umfassende Transparenz wissen Sicherheitsteams genau, auf welche Ressourcen Benutzer zugreifen, wie sie darauf zugreifen und welche Aktionen sie während des Zugriffs ausführen. Durch echte Kontrolle hat die IT-Abteilung die Möglichkeit, Aktivitäten auf der granularen Ebene von Benutzern, Geräten oder Anwendungen zu autorisieren.

— Optimieren der Produktivität und Minderung des Risikos

Unternehmen wünschen sich sowohl eine starke Sicherheit als auch ein großartiges Benutzererlebnis. Verantwortliche für die IT-Sicherheit müssen Lösungen einführen, die eine enge partnerschaftliche Zusammenarbeit fördern, indem sie einen einfachen, sicheren und unkomplizierten Benutzerzugriff ermöglichen – und gleichzeitig das Risiko von Bedrohungen durch Dritte, wie etwa Datenverlust und -exfiltration, minimieren.

Herkömmliche VPN-Zugriffslösungen können diese Prinzipien nicht erfüllen, eine moderne ZTNA-Lösung als Teil einer größeren SSE-Plattform kann dies jedoch.



Sicherer Drittparteizugriff mit SSE

Moderne Unternehmen arbeiten heute intensiv zusammen und sind integriert. Dies bedeutet, dass ihr Erfolg von den Partnerschaften abhängt, die sie mit Auftragnehmern, Zulieferern, Verkäufern, Partnern und B2B-Kunden eingehen. Das Sicherheitsteam muss sicherstellen, dass diese oft risikoreichen Partner auf Geschäftsressourcen zugreifen können, ohne die Geschäftsintegrität zu gefährden oder das Risiko zu erhöhen. Aus diesem Grund beginnen viele Unternehmen mit der Einführung einer SSE-Plattform.

Als Schlüsselservice einer SSE-Plattform stellt ZTNA insbesondere sicher, dass der Zugriff auf private Anwendungen auf granularer Ebene gewährt wird. Dies trägt dazu bei, Netzwerksicherheitsrisiken wie den Zugriff mit zu umfassenden Rechten, kompromittierte BYOD-Systeme und die laterale Ausbreitung von Bedrohungen zu reduzieren.

Einführung von ZTNA für den sicheren Zugriff durch Dritte

ZTNA von HPE Aruba Networking verwendet eine service-initiierte Architektur, um ausschließlich ausgehende Verbindungen zu nutzen. Diese Art von Verbindung stellt sicher, dass die Netzwerkinfrastruktur und Geschäftsanwendungen vor dem Internet verborgen sind und nicht aufgespürt werden können, weil sie nicht nach eingehenden Signalen suchen. Sie befinden sich hinter unserem ZTNA-Konnektor, der ausschließlich mit unserer SSE-Plattform kommuniziert.

HPE Aruba Networking behandelt das Internet als das neue, sichere Unternehmensnetzwerk und gewährleistet, dass dynamische, internet-basierte, verschlüsselte Mikrotunnel herkömmliche Netzwerkverbindungen wie VPN mit unterbrechungsfreier Verfügbarkeit, MPLS und dedizierte Site-to-Site-Verbindungen für die Public Cloud ersetzen. Dies spart Zeit und Geld, damit sich

Netzwerk- und Sicherheitsteams auf strategischere Projekte konzentrieren können, statt teure Anwendungen zu verwalten, Versionen zu aktualisieren, Hardware bereitzustellen und Modernisierungen zu planen.

1. Der Benutzer fordert Zugriff auf eine interne Anwendung an.

Beispiel-URL: `hr-app-tenant.acme.com`

2. Wenn der Benutzer nicht bei einer mit HPE Aruba Networking verwalteten Anwendung angemeldet ist, wird der Benutzer zum zugehörigen Anwendungs-Identitäts-Anbieter weitergeleitet.
3. Unser ZTNA-Service prüft die Zugriffsanforderung des Benutzers basierend auf den vom Kunden definierten Richtlinien.
4. Der Benutzer wird kontinuierlich gemäß seiner Identität, Gruppe und anderen kontextabhängigen Kriterien überprüft.

Hinweis: ZTNA überprüft aktiv den Datenverkehr und schließt die Sitzung bei Eintreten eines Sicherheitsereignisses.

5. Der ZTNA-Service sucht nach einer bestehenden Verbindung mit der Anwendung, damit sie möglicherweise wiederverwendet werden kann.
6. Wenn keine Verbindung besteht, wird von der Anwendung über einen bestimmten Port eine neue Verbindung zum SSE-Konnektor zur HPE Aruba Networking SSE Cloud hergestellt.
7. Die hergestellte Verbindung wird an das dedizierte Frontend zurückgegeben.
8. Das Frontend-Web stellt eine Verbindung mit der Anwendung her.
9. Die angeforderte Website wird an den Benutzer zurückgegeben.

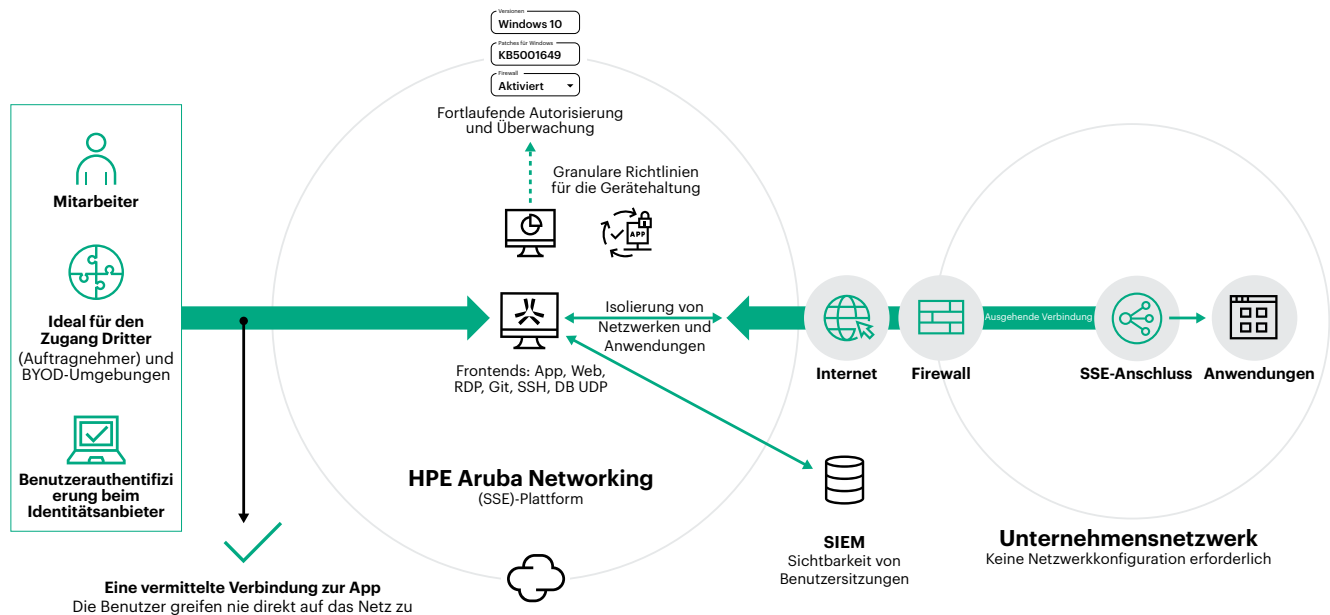


Abbildung 2. Sichern des Zugriffs durch Dritte mit HPE Aruba Networking SSE.

Über ZTNA hinaus: Die Vorteile von HPE Aruba Networking SSE

Die Architektur von HPE Aruba Networking SSE umfasst ZTNA und andere wichtige Sicherheits-Services, um die Sicherheitslage Ihres Unternehmens zu skalieren und zu stärken und gleichzeitig den Zugriff Ihrer Drittparteien sicher zu optimieren.

Universeller Zugang für alle Beteiligten

Unabhängig davon, ob Sie Partner, Lieferanten, Auftragnehmer oder B2B-Kunden (und natürlich Ihre Mitarbeitenden) unterstützen, unsere SSE-Plattform bietet jedem Benutzer universellen sicheren Zugriff. Mit mehr als 500 Edge-Standorten weltweit ist unsere SSE-Plattform eine der zuverlässigsten, verfügbarsten und skalierbarsten Zero-Trust-Lösungen, die für die sichere Konnektivität mit Unternehmensressourcen entwickelt wurde. Wenn Ihre Anforderungen an den sicheren Zugriff steigen, wächst HPE Aruba Networking SSE mit Ihnen.

Granulare und adaptive Zugriffskontrolle ohne Komplexität

Implementieren Sie mühelos den Zugriff mit den geringstmöglichen Rechten für Drittbenutzer mit einfachem, aber dennoch granularem richtlinienbasiertem Zugriff. Passen Sie automatisch Zugriffsrechte basierend auf Änderungen bei Schlüsselkriterien an, einschließlich Benutzerstandort, Identität und Gerätezustand und weiteren. Durch diese anpassungsfähige Risikobewertung werden Ihre sensiblen Geschäftsdaten besser geschützt.

Flexibilität und Skalierbarkeit mit und ohne Agent-Zugriff

Wir bieten die einzige SSE-Architektur, die alle Ports und Protokolle unterstützt, sogar VOIP, ICMP, AS400-Anwendungen sowie RDP, SSH, Git und DG über agent-loses Surfen im Internet – plus gängige SaaS-Anwendungen und Internetprotokolle. Dadurch entfällt für Sie der Zeit- und Arbeitsaufwand, der dadurch entsteht, dass Dritte Clients auf ihre BYOD-Geräte herunterladen müssen, und Sie können den Zugriff vereinfachen.

Verbesserte Überwachung und Bedrohungserkennung

Im Gegensatz zu anderen Angeboten ist HPE Aruba Networking SSE darauf ausgelegt, den gesamten Datenverkehr jederzeit über eine intuitive, einheitliche Management-Konsole anzuzeigen und zu prüfen. Sie erhalten umfassende und kontinuierliche Erkenntnisse über die Zugriffe von Partnern sowie Mitarbeitenden und erkennen Bedrohungen sowie Sicherheitsrisiken an der Quelle, um diese schnell zu beheben.

Was ist Zero Trust-Netzwerkzugriff?

Der im April 2019 von Gartner® geprägte Begriff ZTNA stellt eine neue Technologie-Untergruppe dar, die in eine SSE-Plattform oder -Architektur fällt. Der ZTNA-Bereich von SSE dient speziell der Sicherung des Zugriffs auf alle privaten Anwendungen.

ZTNA-Technologien nutzen granulare Zugriffsrichtlinien, um autorisierte Benutzer mit bestimmten Anwendungen zu verbinden, ohne dass ein Zugriff auf ein Unternehmens-Netzwerksegment erforderlich ist. Sie etablieren eine Segmentierung auf Anwendungsebene mit den geringsten Rechten als Ersatz für die Netzwerksegmentierung – im Gegensatz zu VPN-Konzentratoren, ohne

den Speicherort der Anwendung unbefugten Benutzern oder dem öffentlichen Internet preiszugeben.

Was ist Security Service Edge?

Eine SSE-Plattform ist eine Reihe integrierter, über die Cloud bereitgestellter Sicherheitsdienste, die auf Grundlage von Identität und Richtlinien sichere Verbindungen zwischen autorisierten Benutzern und Unternehmensressourcen vermitteln. Eine SSE-Plattform konsolidiert drei primäre Lösungen in einem einzigen Cloud-Angebot: ZTNA für private Anwendungen, CASB für SaaS-Anwendungen und SWG für den gesamten Webzugriff. Fortschrittlichere SSE-Plattformen umfassen auch Digital Experience Monitoring (DEM)-Funktionen.



Erfahren Sie, wie HPE Aruba Networking SSE Ihr Geschäfts-Ökosystem schützt

44%

planen, die SSE-Implementierung mit der Bereitstellung von Zero Trust Network Access (ZTNA) zu beginnen.²

Insgesamt bietet eine SSE-Plattform eine umfassende Sicherheitslösung, die Unternehmen dabei hilft, die mit Drittbenedutzern und veralteten Zugriffslösungen verbundenen Risiken zu beseitigen, indem sie einen sicheren und konformen Zugriff auf die Unternehmensressourcen ermöglicht und gleichzeitig vertrauliche Daten und Infrastrukturen schützt. **Aus diesem Grund planen 69% der Unternehmen, in den nächsten zwei Jahren eine SSE-Plattform einzuführen.**

² 2024 Security Service Edge Adoption Report by Cybersecurity Insiders.



Weitere Informationen unter

Erfahren Sie, warum Unternehmen von VPNs zu ZTNA wechseln im VPN Risk Report 2024

[Testen Sie SSE mit unserem Test Drive](#)

[HPE.com besuchen](#)

Chat mit Vertrieb

© Copyright 2025 Hewlett Packard Enterprise Development LP. Die hier enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Die einzigen Garantien für Produkte und Services von Hewlett Packard Enterprise sind in den ausdrücklichen Garantieerklärungen enthalten, die diesen Produkten und Services beiliegen. Aus dem vorliegenden Dokument sind keine weiter reichenden Garantieansprüche abzuleiten. Hewlett Packard Enterprise haftet nicht für hierin enthaltene technische oder redaktionelle Fehler oder Auslassungen.

SAP ist eine Marke oder eingetragene Marke von SAP SE (oder einem Tochterunternehmen von SAP) in Deutschland und anderen Ländern. Windows ist in den USA und/oder anderen Ländern eine Marke oder eingetragene Marke der Microsoft Corporation. Alle Marken von Dritten sind Eigentum ihrer jeweiligen Rechteinhaber.

a00141306DEE, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](#)

