HPE aruba networking | Leuchter IT SOLUTIONS

Broschüre

Vier Voraussetzungen für ein KI-gestütztes Netzwerk

Moderne Geschäftsanforderungen führen dazu, dass Netzwerke mehr Anwendungen und IoT (Internet of Things)-Geräte als je zuvor verbinden und gleichzeitig mit der Entwicklung von KI-Workloads Schritt halten müssen. Ist Ihr Netzwerk bereit?

HPE

Hindernisse im Edge-to-Cloud-Zeitalter

Trotz der Tendenz zur Rückkehr ins Büro müssen moderne Unternehmensnetzwerke nach wie vor verteilte Mitarbeiter mit Services verbinden, die überall gehostet werden – von der Cloud bis zu IoT-Geräten am Edge. Darüber hinaus verändert KI die Netzwerklandschaft kontinuierlich. KI-Anwendungen erzeugen eine riesige Datenmenge, die sich nicht auf einen einzigen Standort beschränken lässt – und diese Daten müssen dennoch geschützt und gesichert werden.

Kann die vorhandene Netzwerkinfrastruktur die steigenden Anforderungen durch anspruchsvollere Anwendungen, zusätzliche IoT-Geräte und eine stärkere Nutzung künstlicher Intelligenz bewältigen? Andernfalls wird es schwierig sein, differenzierte Nutzererlebnisse zu schaffen und IoT-Geräte sicher zu verbinden, um KI und andere Geschäftsanforderungen zu unterstützen.

Angesichts des Ausmaßes der Herausforderungen, vor denen die Unternehmen heute stehen, sind Innovationen erforderlich, und diese lassen sich auf drei Kernpunkte reduzieren:

— **Anspruchsvolle, immersive Anwendungen:** Veralteten Netzwerkinfrastrukturen mangelt es an Intelligenz, und sie sind einfach zu komplex und langsam, um digitale Erlebnisse der nächsten Generation bereitzustellen oder die sich entwickelnden KI-Anforderungen zu unterstützen. Drahtlose Konnektivität wird nach wie vor überall benötigt – von traditionellen Campusumgebungen bis hin zu Produktionsanlagen und Außenbereichen. Da die Nutzung von IoT-Geräten und -Anwendungen jedoch in einem beispiellosen Tempo zunimmt, haben Unternehmen Schwierigkeiten, Flexibilität und Skalierbarkeit in ihren bereits ausgedehnten Netzwerken zu erreichen. Ohne Echtzeit-Transparenz über die Nutzung der verschiedenen Anwendungen riskieren Unternehmen zudem eine unzureichende Leistung, die die Benutzer frustriert.

— **Betriebliche Ineffizienzen:** In fragmentierten Umgebungen sind betriebliche Ineffizienzen unvermeidlich. Im Zuge der Digitalisierung von Geschäftsabläufen zur Steigerung der Produktivität und zur Erlangung von Wettbewerbsvorteilen müssen Netzwerkteams flexibler und reaktionsfähiger sein. Ohne eine einheitliche Infrastruktur, die WLAN, private 5G-Netze, kabelgebundenes LAN und SD-WAN umfasst und KI-basierte Automatisierung nutzt, bleibt diesen Teams keine andere Wahl, als jedes Netzwerk auf dem Campus, in Zweigstellen, bei Remote-Mitarbeitern und in Rechenzentren unabhängig voneinander mit domänenspezifischen Tools zu verwalten.

— **Sicherheitslücken:** Ein Patchwork-Setup ist komplex zu verwalten, und manuelle und statische VLAN-basierte Ansätze zur Sicherung von Netzwerken können fehleranfällig sein. Daher müssen Netzwerkbetreiber rollenbasierte Richtlinien in komplexen, sich entwickelnden und geografisch verteilten Netzwerken einheitlich definieren und global durchsetzen. Hinzu kommt, dass IoT-Geräte, die sich in immer größerer Zahl mit dem Netzwerk verbinden, mit herkömmlichen Erkennungs- und Profilerstellungstechniken nur schwer genau identifiziert werden können. Das Ergebnis ist eine mangelnde Transparenz und ein erhöhtes Risiko ungeplanter Ausfallzeiten oder Sicherheitsvorfälle.

Ein zweckmäßiges Netzwerk sollte die erforderliche Leistung, Sicherheit und Abdeckung bieten, um alle Benutzer, Geräte und Workloads zu verwalten – insbesondere datenintensive KI-Workloads, da die Nachfrage hier exponentiell steigen wird. Darüber hinaus sollte ein modernes Netz nicht nur einfach genug sein, um es mit den vorhandenen Ressourcen und ohne Ausfallzeiten verwalten zu können – es sollte auch verwertbare Erkenntnisse liefern können.

Die Netzwerk-Checkliste

Bei der Modernisierung sollte der Schwerpunkt der Netzwerkinvestitionen auf der Bereitstellung einer einheitlichen Infrastruktur liegen, die sich schnell an Veränderungen in den Geschäftsanforderungen anpassen kann. Unternehmen, die diese Flexibilität nutzen wollen, sollten sich vom Einsatz unterschiedlicher Managementkonsolen verabschieden und sich für ein breites und innovatives Netzwerkportfolio entscheiden, das integrierte Sicherheitslösungen, Konnektivität vom Kunden bis zur Cloud sowie wichtige KI-Funktionen bietet, die alle über eine zentrale Ansicht mit Beobachtbarkeit für Elemente von Drittanbietern verwaltet werden, um Zuverlässigkeit und Sicherheit über den gesamten Stack zu gewährleisten.

Im Hinblick auf KI müssen Unternehmen sowohl die aktuellen als auch die zukünftigen Anforderungen im Auge behalten und in eine Architektur investieren, die die Ausweitung von KI sowie die wachsende Zahl von IoT-Geräten unterstützt, die für KI-Training und -Inferenz benötigt werden. Eine solche Infrastruktur muss auch skalierbar sein, um den zunehmenden Netzwerkverkehr bewältigen zu können, der durch KI-Workloads erzeugt wird, die vom Edge über das Rechenzentrum bis zur Cloud laufen.

Ein modernes Netzwerk sollte vier grundlegende Kriterien erfüllen. So können Sie sicherstellen, dass Sie die drei wichtigsten Anforderungen an geschäftliche Flexibilität, IT-Effizienz und verbesserte Sicherheit erfüllen.

1. Ist es nahtlos? Eine moderne Netzwerkinfrastruktur verfügt über Wireless Access Points, unternehmenstaugliche private Mobilfunknetze und programmierbare Switches, um Abdeckungslücken zu vermeiden. Sie unterstützt die nahtlose Integration von IoT-Vorgängen und bietet einfache Verwaltung mit umfassender Transparenz.

2. Ist es KI-basiert? Mit KI-basierter Verwaltung von WLANs, privaten 5G-Netzen, kabelgebundenen LANs und SD-WANs erhalten Sie die nötige Transparenz, Kontrolle und Einblicke, um Ihren IT-Betrieb zu optimieren und zu sichern. Dazu tragen KI-gestützte Fehlerbehebungs- und Optimierungsempfehlungen bei, mit denen Sie zeitaufwändige manuelle Verwaltungsvorgänge und Eingriffe reduzieren und gleichzeitig Bereitstellungen und Updates automatisieren können. Eine Reihe robuster Anwendungsprogrammierschnittstellen (APIs) und Webhooks ermöglicht eine reibungslose Integration mit privaten Tools.

3. Ist die Sicherheit integriert? Integrierte Zero Trust-Sicherheitslösungen sind der Schlüssel zu mehr Sicherheit. Hierzu gehören eine identitätsbasierte Zugriffskontrolle, eine automatische Richtliniendurchsetzung im kabelgebundenen und drahtlosen LAN und SD-WAN sowie eine umfassende Gerätetransparenz über das gesamte Netzwerk. KI-Funktionen erhöhen die Sicherheit zusätzlich, indem sie genaue Kundeneinblicke für die proaktive Problemlösung und die Erkennung von Anomalien zur Vorbeugung und Reaktion auf Bedrohungen liefern.

4. Ist es flexibel? Sie können die Ressourcennutzung (und die Kosten) durch flexible Beschaffungs- und Bereitstellungsmodelle (vor Ort und in der Cloud) optimieren, die vorhersehbare Ausgaben und eine schnellere Time-to-Value ermöglichen. Das Management bietet Beobachtbarkeit im Zusammenhang mit Drittanbietern für Umgebungen mit mehreren Anbietern und einen Satz robuster APIs und Webhooks für eine einfachere Interoperabilität.

Netzwerkinnovation zur Erfüllung der Unternehmensanforderungen

Mit dem einheitlichen Infrastrukturportfolio von HPE Networking können Unternehmen die Hindernisse überwinden, die herkömmliche Netzwerke darstellen. HPE bietet Ihnen ein sicheres, flexibles und KI-basiertes Netzwerk, mit dem Sie Ihren Bedarf an zukunftssicherer Agilität und Effizienz erfüllen können. Was bedeutet das?

1

Moderne Infrastruktur für nahtlose, flächendeckende Konnektivität

HPE bietet ein umfassendes KI-gestütztes Netzwerkportfolio, das Ihnen alles bietet, was Sie zur Unterstützung verschiedener und wachsender Konnektivitätsanforderungen in unterschiedlichen Umgebungen benötigen.

Unser KI-gestütztes Portfolio an WLAN-Zugangspunkte und HPE Aruba Networking Private 5G bietet eine zuverlässige, leistungsstarke Abdeckung, um die wachsende Zahl an Benutzern und Geräten sowie die Anforderungen der KI zu unterstützen.Die Innovation der HPE Aruba Networking Wi-Fi 7 Access Points geht über den Industriestandard hinaus und ermöglicht die Maximierung der Wireless-Leistung, die Stärkung der Netzwerksicherheit, die Verbesserung standortbasierter Dienste und die Nutzung als sichere IoT-Plattform. Dadurch können Unternehmen den Wert ihrer Investitionen in die drahtlose Kommunikation und ihre operative Effizienz steigern. Gleichzeitig erhalten Unternehmen mit unserer Lösung für private 5G-Netze die Möglichkeit, ihre WLAN-Netzwerke ganz einfach um private Mobilfunknetze zu erweitern – mit einer Komplettlösung auf Basis ausgereifter und bewährter Technologien.

Wenn es um die Bereitstellung einer umfassenden Abdeckung geht, sind Switches, die verschiedene Teile des Netzes miteinander verbinden und einen nahtlosen Datenfluss ermöglichen, ebenso wichtig. Legacy-Switches bieten nicht die gleiche hohe Verfügbarkeit und robuste Datenverarbeitungsfunktionen wie CX-Switches. Die HPE Aruba Networking CX Switch Serie erfüllt die Anforderungen vom Zugangs-Edge bis zum Rechenzentrum und bietet einheitliche Kontrollen und Abläufe sowie eine einheitliche Sicht auf die gesamte Switching-Fabric und trägt so zur Steigerung der Effizienz im IT-Betrieb bei.

2

KI-gestütztes Management für betriebliche Effizienz

Im Zeitalter der künstlichen Intelligenz ist es von entscheidender Bedeutung, dass Netzwerke die immer größeren Datenmengen verwalten und mit ihnen wachsen können. HPE Aruba Networking Central ist eine einheitliche Verwaltungslösung für sichere drahtlose und kabelgebundene WAN- und IoT-Netzwerke, die mit einem KI-gestützten, intuitiven Benutzererlebnis die Effizienz der Anwender maximiert. Durch die neue Integration der Überwachungsfunktion für Netzwerkgeräte von Drittanbietern in HPE Aruba Networking Central erhalten Kunden einen Vorteil bei der Kontrolle, Vorhersage und Verwaltung ihrer End-to-End-Netzwerkinfrastruktur.

HPE Aruba Networking Central wird auf einer Cloud-nativen, auf Microservices basierenden Architektur bereitgestellt und bietet Zero-Touch-Provisioning für schnellere Bereitstellungen und Live-Updates. Die Lösung macht manuelle Fehlerbehebungsaufgaben überflüssig, verkürzt die Zeit zur Behebung gängiger Netzwerkprobleme und erhöht die Netzwerkkapazität durch peerbasierte Konfigurationsoptimierung.

Sie bietet IT-Teams eine einfachere Navigation und verbesserte Transparenz vom Endpunkt bis zur Infrastruktur und ist auf eine intuitivere Einbindung von AIOps-Analysen ausgelegt, um ein erstklassiges Benutzererlebnis zu bieten.

Eine nutzbare KI, die handlungsrelevante, vertrauenswürdige Ergebnisse liefert, benötigt drei wesentliche Zutaten: umfangreiche und vielfältige Daten, Domänenexpertise und erfahrene Data Scientists. HPE Aruba Networking AIOps nutzt die Erfahrung aus über 18 Jahren bewährter Netzwerkinnovationen für die Modellierung von Telemetriedaten von mehr als zwei Millionen kabelgebundener, kabelloser und SD-WAN-Geräte, um Anomalien zu identifizieren und präskriptive Empfehlungen zu liefern, auf die sich Netzwerkadministratoren verlassen können.

3

Integriertes Zero Trust für erhöhte Sicherheit

Ein Security-First KI-Netzwerk von HPE Networking erleichtert die Einführung von Zero Trust-Sicherheit und unterstützt die Compliance mit Cybersicherheitsstandards und -vorschriften. Unternehmen erhalten damit die Möglichkeit, das Netzwerk als Sicherheitslösung zu nutzen. Das Netzwerk kann jetzt umfassendere Transparenz und Einblicke, ein zentralisiertes Richtlinienmanagement, Datensicherung, Bedrohungsabwehr und Zugriffssteuerung über eine einzige Plattform bereitstellen.

Zero Trust-Sicherheit beginnt mit Transparenz. HPE Aruba Networking Central nutzt native Infrastruktur-Telemetrie von Access Points, Switches, Gateways und Kunden, um automatisch Fingerabdrücke von verschiedenen IoT-Geräten in der gesamten kabelgebundenen und kabellosen Infrastruktur zu erstellen und zu identifizieren und so eine möglichst detaillierte Profilbildung und Transparenz zu gewährleisten. Cloud-native NAC (Network Access Control)-Funktionen ermöglichen ein reibungsloses Onboarding von Benutzern und Geräten und weisen jedem automatisch Netzwerkzugriff auf der richtigen Stufe zu, die mit seiner Identität und Rolle übereinstimmt. Die dynamische Segmentierung wendet den Zugriff mit geringsten Rechten auf Anwendungen und Daten durch rollenbasierte Zugriffsrichtlinien an, die den Benutzer im gesamten Netzwerk begleiten und einheitlich auf drahtlose, kabelgebundene und Remote-Verbindungen angewendet werden.

Zero Trust-Sicherheitsmodelle basieren auf einer aktuellen Kenntnis des Geräteverhaltens, mit der potenzielle Manipulationen und Angriffe erkannt und im Keim erstickt werden. HPE Aruba Networking Central nutzt KI für die umfassende Analyse der Gerätetelemetrie, um anomales Verhalten zu erkennen und Warnungen zur Untersuchung auszulösen. So können Netzwerk- und Sicherheitsteams potenzielle Gefährdungen von IoT-Geräten mit hohem Risiko leichter erkennen. KI-basierte Tools zur Richtlinienoptimierung innerhalb der innovativen Lösungen von HPE Aruba Networking können Unternehmen auch dabei helfen, ohne manuelle Eingriffe oder Betriebsunterbrechungen schneller auf potenzielle Bedrohungen zu reagieren. Wie? Durch die Empfehlung und Vorschau rollenbasierter Richtlinienänderungen, die auf den Prinzipien von Zero Trust und dem Grundsatz minimaler Zugriffsrechte basieren.

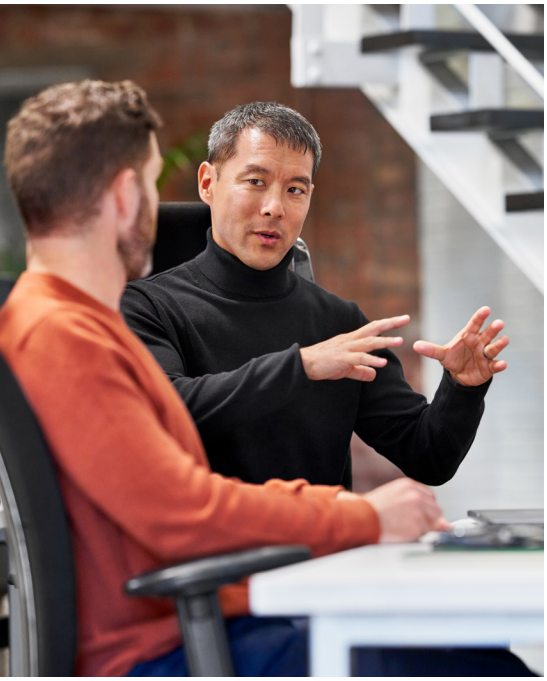
Bleiben Sie zukunftsfähig

Die Modernisierung des Netzwerks ist eine sinnvolle Investition, da sie nicht nur den heutigen Betrieb unterstützt, sondern Ihr Unternehmen auch für die Zukunft rüstet. Um eine Rendite auf diese Investition zu erzielen, ist eine einheitliche, KI-basierte Infrastruktur, bei der die Sicherheit an erster Stelle steht, die einzige wirkliche Antwort.

Mit HPE erhalten Sie nicht nur Zugriff auf ein umfassendes Cloud-natives Portfolio für alle Ihre Anforderungen in den Bereichen WLAN, private 5G-Netze, kabelgebundenes WAN und SD-WAN, sondern können über HPE Aruba Networking Central auch einen zentralen Transparenz- und Kontrollpunkt beibehalten. Auf diese Weise können Unternehmen jeder Größe und Branche ein großartiges Benutzererlebnis und eine sichere IT-Konnektivität über alle Unternehmensstandorte hinweg gewährleisten – vom Homeoffice bis zum Campus, der Filiale und dem Rechenzentrum.

Durch die Kombination von modernster Hardware, KI-basierter Verwaltung und integrierter Sicherheit bietet die Innovation von HPE mehr Leistung und nahtlose Konnektivität auch an den entlegensten Standorten. Sie können mit unseren Lösungen auch die Bandbreite erhöhen, um sie den geschäftlichen Anforderungen anzupassen – ohne den vom Netzwerk angebotenen Service zu unterbrechen.

Die HPE Innovation bietet Ihnen ein umfassendes Netzwerkportfolio, das die Anforderungen aller Szenarien erfüllt und großartige Erfahrungen bietet.



Informationen zu HPE

HPE ist das Edge-to-Cloud-Unternehmen, das Unternehmen weltweit durch eine optimale Wertschöpfung aus allen ihren Daten bei schnelleren Ergebnissen unterstützt. Basierend auf jahrzehntelangem Engagement für eine Neugestaltung der Zukunft und Innovationen, die unsere Lebens- und Arbeitsweise verbessern, bietet HPE einzigartige, offene und intelligente Technologielösungen mit einer konsistenten Erfahrung über alle Clouds und Edges hinweg, um Kunden dabei zu helfen, neue Geschäftsmodelle zu entwickeln, neue Wege zu beschreiten und die operative Leistung zu steigern.

Weitere Informationen finden Sie unter

HPE.com/de/de/networking

HPE.com besuchen

Jetzt chatten

a00148129DEE, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com

Leuchter IT SOLUTIONS