HPE aruba networking

Die wichtigsten Netzwerk- und Sicherheitstrends für 2024

KI-basiertes Networking für Ihr Unternehmen – mit Sicherheit an erster Stelle

Hewlett Packard Enterprise | Bohnen IT®

Nach einem Jahr voller Innovationen, Unterbrechungen und schwieriger Bedingungen auf Makroebene steht das Streben nach einer schnelleren geschäftlichen Transformation bei IT-Abteilungen weiterhin im Vordergrund. Generative künstliche Intelligenz (Generative AI bzw. GenAI), Nachhaltigkeitsinitiativen und weitere strategische Prioritäten verschieben sich vom Early-Adopter-Status zur allgemeinen praktischen Umsetzung. Da sich die Unternehmensarchitektur zunehmend auf hybride datenorientierte Anforderungen konzentriert, wird die Edge-to-Cloud-Sicherheit zu einem der Kernpunkte der Vernetzung im Unternehmen.

„Immer mehr Unternehmen entscheiden sich für programmatische, hybride Arbeitskonzepte, sodass es wahrscheinlicher wird, dass Käufer Firewall-Anbieter auswählen, die Cloud-basierte Sicherheitsservices ohne ernstzunehmende Cloud-Sicherheitsstrategien anbieten.“

– Gartner®, Research Critical Capabilities for Network Firewalls, Hils, Kaur und Lintemuth, Mai 2023.

Die wichtigsten Trends für 2024

1. Das Ende der Standalone-Firewall

Die zunehmende Bedeutung hybrider Arbeit und die umfassende Bereitstellung von IoT-Geräten haben die Grenzen des Netzwerks unumkehrbar zunichte gemacht – und damit stirbt auch die eigenständige Firewall aus. Ein sicheres „Inneres“ lässt sich nicht länger durch einen Kreis aus Firewalls vor einer bösen „Außenwelt“ schützen. Der Versuch, Sicherheitslücken mit weiteren Firewalls innerhalb eines Unternehmens zu stopfen, erhöht die Komplexität, schafft Raum für Fehler und bremst Unternehmen aus, die schnell agieren wollen.

Infolgedessen wird aus der Firewall-Appliance der nächsten Generation schnell die Firewall-Appliance der letzten Generation. Mit seiner Fähigkeit, die Sicherheit für Benutzer zu verwalten, die von überall aus auf Anwendungen zugreifen, ersetzt der Security Service Edge (SSE) einerseits Firewalls und Proxies mit über die Cloud bereitgestelltem Secure Web Gateway, Cloud Access Security Broker und Zero-Trust-Netzwerkzugriff. Andererseits erfordert die IoT-Sicherheit die Segmentierung vor Ort am Edge des Netzwerks. Das wird durch unmittelbar in die Access Points, Switches und SD-WAN-Gateways integrierte Firewall-Services erreicht. Im Rechenzentrum liefern Top-of-Rack-Switches mit L4-7-Sicherheitsfunktionen am Ende des Ganges im Vergleich zu den traditionellen Firewalls der nächsten Generation eine weitaus kosteneffizientere horizontale Segmentierung. In den nächsten Jahren wird der Markt für Firewalls der nächsten Generation weiter zurückgehen. Denn diese neuen Cloud-basierten und integrierten Leistungen leiten eine einfachere Verwaltung sicherer Konnektivität ein.

Wie wir helfen

- Implementierung von Sicherheitsservices für Interaktionen zwischen Benutzer und Anwendung mit HPE Aruba Networking SSE
- Integration der rollenbasierten Richtlinie sowie umfangreiche Anwendungserkennung und -steuerung mit HPE Aruba Networking Central
- Einführung der Security Services Edge (SSE)-Technologie als Overlay zum Netzwerk eines beliebigen Anbieters
- Möglichkeit zur Verwendung vorhandener HPE Aruba Networking Produkte und Services zum Investitionsschutz

Weitere Informationen zum SSE



„96 % der Kunden gaben an, dass Sicherheit und Netzwerk bei der Implementierung des SASE zusammen arbeiteten"

– The Forrester Wave™ Zero Trust Edge Solutions Q3, 2023 (Holmes und Kindness, 2023)

2. Zero-Trust-Prinzipien beschleunigen die Abstimmung der Ziele von Sicherheit und Netzwerk

Obwohl nicht in allen, so werden Netzwerk und Sicherheit doch in den meisten Unternehmen von verschiedenen Teams verwaltet. In vielerlei Hinsicht können deren Ziele im Widerspruch stehen. Im Jahr 2024 werden führende Unternehmen Zero-Trust-Prinzipien einsetzen, um die Interessen beider Teams abzustimmen und so die Endbenutzererfahrung zu verbessern und die Geschäftsergebnisse zu steigern.

In einem typischen Unternehmen sorgt das Netzwerkteam dafür, dass Menschen und Services zuverlässig und mit vorhersehbar guter Leistung verbunden werden und bleiben. Seine Aufgabe besteht darin, den Menschen die Verbindung zu allem zu erleichtern und Komplexität zu vermeiden, die zu Ausfällen, Latenzen oder Verzögerungen führen kann. Andererseits ist die Sicherheit im Unternehmen damit betraut, Risiken zu minimieren und für die Einhaltung von Vorschriften zu sorgen. Benutzer können zwischen die Fronten geraten, da eine übereifrige Sicherheitsimplementierung den Zugriff auf Anwendungen oder Daten, den sie benötigen, möglicherweise verlangsamt oder blockiert. Gleichzeitig kann ein laxes Sicherheits- oder Netzwerkteam, das durch ein Umgehen von Sicherheitsmaßnahmen zufriedenstellen will, Unterwanderung und Ransomware Tür und Tor öffnen.

Führende Unternehmen werden Zero-Trust-Architekturen einführen, bei denen die Aufgabe des Netzwerks nicht darin besteht, alles mit allem zu verbinden, sondern vielmehr darin, als Durchsetzungsebene für Sicherheitsrichtlinien zu agieren. Für Benutzer, die auf Anwendungen zugreifen, können Sicherheitsrichtlinien in der Cloud durchgesetzt werden. Aber für viele Verkehrsflüsse (besonders für IoT-Geräte mit deren zugehörigen Services) ist es effizienter, Sicherheitsrichtlinien in Zugriffsgeräten wie Access Points, Switches und Routern automatisch bereitzustellen. Mit dem richtigen Maß an Transparenz, Automatisierung und einer klaren Beschreibung der Richtlinien und Durchsetzung, können Netzwerk- und Sicherheitsteams ihre Ziele abstimmen und eine bessere Erfahrung bieten.

Wie wir helfen

- Verwendung eines zentralen Transparenz- und Steuerungspunkts mit anpassbarem Zugriff für Netzwerk- und Sicherheitsteams
- Bereitstellung eines einheitlichen Richtlinienrahmens für Netzwerk und Sicherheit mit HPE Aruba Networking Central
- Nahtlose Integration von Cloud-Sicherheitsfunktionen mit vorhandenen Netzwerkmanagementtools

Ihr Einstieg in ein KI-basiertes Netzwerk mit Sicherheit an erster Stelle

„Bis 2027 wird die DEM-Bereitstellung von 60 % auf 90 % ansteigen, da Unternehmen synthetische und Echtzeit-Überwachung einsetzen werden, um die User Journey zu verbessern und Benutzerinteraktion von SaaS-Anwendungen und -Services besser zu verstehen.“

– Gartner®, Market Guide for Digital Experience Monitoring, Bangera, Siegfried und Byrne, November 2023.

3. Die Überwachung der Benutzererfahrung wird für höhere betriebliche Exzellenz unverzichtbar werden

Gängige Endbenutzer-Kennzahlen

- Standortbasierter Netzwerkstatus (Standort A vs. Standort B)
- Serviceleistung (Wi-Fi, DHCP, DNS)
- Interner Anwendungsstatus (VoIP, Workday)
- Externer Anwendungsstatus (Dropbox, Teams, WhatsApp)

Um die Erwartungen von Mitarbeitenden und Kunden zu erfüllen, müssen IT-Organisationen entsprechend der erfassten Benutzererfahrung auf Service Level Objectives (SLOs) und Service Level Agreements (SLAs) umstellen. Eine großartige Benutzererfahrung bereitzustellen, bedeutet, dass Anwendungen reibungslos laufen müssen – und falls das einmal nicht der Fall ist, muss die Problemlösung schnell erfolgen.

Deshalb sorgen Unternehmen für eine umfassende Bereitstellung von Digital Experience Management (DEM)-Tools, die die tatsächliche Erfahrung der Endbenutzer erfassen und synthetische Tests machen, um sicherzustellen, dass die Infrastruktur selbst ohne aktive Benutzer bereit ist. Unternehmen wünschen sich höchstwahrscheinlich eine Mischung aus Messdaten, die von Endpunkt-Agenten (wie einem SSE-Agenten) und von dedizierten Hardware-Sensoren, besonders bei der Überwachung der Wi-Fi-Leistung, erfasst werden. Idealerweise beschicken dieselben Messdaten automatisierte AIOps, die dann Best Practices lernen und in der Folge implementieren können, Probleme schnell einstufen und Fehler automatisch beheben können.

Wie wir helfen

- Automatisierung und Verbesserung von Benutzer- und Client-Erfahrungen mit Plattformen und Tools wie HPE Aruba Networking Central und User Experience Insight
- Anpassung des Netzwerkzugriffs und der Sicherheit an diejenigen, die sie am meisten benötigen – mit rollenbasiertem Zugriff und dynamischer Segmentierung, orchestriert durch NetConductor
- Digital Experience Monitoring (DEM) zum Testen und Beheben von Fehlern bei der Anwendungs- und Netzwerkleistung aus Sicht der Endbenutzer mit HPE Aruba Networking User Experience Insight

Erfahren Sie mehr zum Optimieren des Benutzererlebnis



„HPE Aruba Networking war ein Pioneer bei der Bereitstellung von Wi-Fi 6E und ist branchenweit führend bei der Gesamtauslieferung von Wi-Fi 6E APs für Unternehmen.“

– Siân Morgan, WLAN Analyst Dell'Oro Group, Dezember 2023

4. Die Einführung von 6 GHz Wi-Fi nimmt rasant zu – und bleibt das wichtigste Feature von Wi-Fi 7

Die Hürden, die die Wi-Fi-Bereitstellung im 6-GHz-Spektrum verlangsamen, werden in den meisten Gegenden beseitigt, sodass die Einführung explosionsartig zunehmen wird.

Vor ein paar Jahren brachte der Wi-Fi-6E-Standard die Unterstützung des 6-GHz-Bandes. Dadurch wurde die Wi-Fi-Kapazität mehr als verdoppelt, und mehr Benutzer und schnellere Geschwindigkeiten wurden möglich. In einigen Bereichen wurde der Standard schnell umgesetzt; andere waren zurückhaltender. Im Jahr 2024 wird die letzte verbleibende Hürde für eine breite Einführung beseitigt werden.

Erstens benötigt man für die Verwendung des 6-GHz-Bandes – besonders in Außenbereichen – die Genehmigung der Behörden. Einige Länder wie die Vereinigten Staaten öffneten das Spektrum schnell für Wi-Fi; andere waren dagegen langsamer. Glücklicherweise gab es in diesem Bereich viel Fortschritt und 2024 werden die meisten Unternehmen in einem Großteil der Welt über das 6-GHz-Spektrum verfügen.

Zweitens waren einige Unternehmen zögerlich mit der Einführung von Wi-Fi 6E, da Wi-Fi 7 schon vor der Tür stand. Jetzt, da Wi-Fi 7 zugelassen ist, besteht kein Zweifel mehr, dass Wi-Fi 6E und Wi-Fi 7 vollständig kompatibel sind. Da 6E-Geräte und -Access-Points außerdem in großen Mengen ausgeliefert werden, können 6-GHz-Wi-Fi-Bereitstellungen auf Hochtouren voranschreiten.

Letztlich wird die Akzeptanz dadurch eingeschränkt, ob Support auf Access Points und Client-Geräten besteht. Wir erleben, dass zahlreiche neue Geräte und ein Großteil von 6E-Access-Points Wi-Fi 6E unterstützen. Zusätzlich sind weitere Wi-Fi-7-Geräte absehbar, die das 6-GHz-Band verwenden können, und die mit Wi-Fi-6E- oder Wi-Fi-7-Access-Points eine bessere Benutzererfahrung bieten.

Die Kombination dieser Entwicklungen prognostiziert eine starke Verbreitung des 6-GHz-Spektrums im Jahr 2024 – und damit schnellere Übertragungen und eine bessere Benutzererfahrung.

Wie wir helfen

- Verfügbarkeit eines Portfolios von HPE Aruba Networking Wi-Fi 6E Access Points für Innenbereiche und Remote, die den Zugriff auf das 6-GHz-Spektrum freischalten
- Integration einer Vielzahl beliebter IoT-Anwendungen durch ein Dashboard für IT-Abläufe, um die Rolle der AP-Infrastruktur über die interne Konnektivität hinaus zu erweitern und IoT-Overlay-Implementierung zu unterstützen
- Entwicklung eines branchenweit ersten, in Wi-Fi 6E Access Points integrierten GPS-Empfängers, der ein standortfähiges Netzwerk zur Unterstützung aufkommender Anwendungsfälle – wie automatischer AP-Zuordnung und Turn-by-Turn-Navigation – bietet

Entdecken Sie die Vorteile von 6 GHz und Wi-Fi 6E

„Bis 2026 wird die Technologie der generativen künstlichen Intelligenz (GenAI) bei anfänglichen Netzwerkkonfigurationen 20 % ausmachen, was im Vergleich zu nahezu null im Jahr 2023 eine Steigerung bedeutet.“

– Gartner®, Research Strategic Roadmap for Enterprise Networking. Brown, Munch, Leibovitz und Lerner, Oktober 2023.

5. KI wird IT-Administratoren befreien

Manchmal wird zitiert, dass man seinen Job nicht an KI verlieren wird, sondern an jemanden, der KI effektiv einsetzt. Für IT-Administratoren trifft das immer mehr zu.

Die zunehmende Belastung, neue Technologie implementieren und die Cybersicherheit mit gleich bleibendem oder weniger Personal aufrecht erhalten zu müssen, bedeutet, dass jeder Administrator mehr bewältigen muss. Glücklicherweise entwickeln sich KI und die Automatisierung schnell weiter, sodass sich dieses Aufgabe von der Verwaltung und Konfiguration einzelner Geräte zur Festlegung von Richtlinien für ganze Umgebungen und der automatischen und einheitlichen Implementierung dieser Richtlinien verschiebt. KI kann auch große Datenmengen durchforsten, um Anomalien zu erkennen und Maßnahmen vorzuschlagen (und sogar zu implementieren). Inzwischen ist erwiesen, dass eine KI nur so gut ist wie ihr Datensatz. Daher sind umfassendere, hochwertige Datensätze von entscheidender Bedeutung. Führende Anbieter ziehen KI-Erkenntnisse aus Data Lakes, die Millionen verwalteter Geräte und Hunderte Millionen Endpunkte repräsentieren. Letztlich beschleunigen Large Language Models (LLMs) vorhandene Sprachoberflächen und bieten Administratoren eine bequemere Möglichkeit, die Informationen abzurufen, die sie benötigen.

Fazit ist, dass Unternehmen ihren IT-Teams die KI-Leistungen bereitstellen müssen, die diese Administratoren benötigen, um wettbewerbsfähig zu bleiben.

Wie wir helfen

- Zugriff auf einen der größten Netzwerk-Data-Lakes, um Ihr Netzwerk mit einzigartigen Erkenntnissen, Empfehlungen und Maßnahmen zu unterstützen, die die Leistung und Stabilität steigern
- Verwendung eines KI-basierten Netzwerks mit Sicherheit an erster Stelle für einen vereinfachten Backend-Betrieb – von der Suche über Firmware-Upgrades bis hin zu sonstigen Wartungs- und Support-Funktionen
- Implementierung eines einheitlichen Frameworks für die konsistente Erstellung von Netzwerk- und Sicherheitsrichtlinien
- Nahtlose Integration von Cloud-Sicherheitsfunktionen mit unseren vorhandenen Netzwerkmanagementtools

Entmystifizieren Sie das KI-basierte Netzwerk

Unsere Lösungspartner

Bohnen IT®

Bohnen IT ist ein inhabergeführtes IT-Unternehmen mit Sitz in Wuppertal. Vor gut 36 Jahren als Systemhaus gestartet, steht bei Bohnen IT heute die Entwicklung und Umsetzung komplexer Software-Lösungen für den Mittelstand im Mittelpunkt. Das Unternehmen realisiert strategische IT-Konzepte und unterstützt damit die unternehmerischen Ziele ihrer Kunden nachhaltig.

www.bohnen.it
+49 (202) 24755 28
Hastener Strasse 2
D-42349 Wuppertal

Sie brauchen einen KI-basierten Netzwerk-Ansatz mit Sicherheit an erster Stelle

Die sicherheitsbezogenen Aspekte des Edge-to-Cloud-Zeitalters sind eine häufige Herausforderung für jede IT-Organisation, egal wie Ihre Strategie für das Jahr 2024 aussieht. Und egal wann die Implementierungen sicherer Netzwerke in Betracht gezogen werden, wird es für Unternehmen immer deutlicher, dass die Benutzererfahrung ein kritischer Aspekt bleibt. Steht in Ihrem Netzwerk die Sicherheit an erster Stelle? Erfahren Sie mehr darüber, was uns 2024 erwartet.

Kontakt

BR_TopNetworkingAndSecurityTrends2024_CT_122023 a00136590dee

Hewlett Packard Enterprise