



EBOOK

Das Wichtigste miteinander verbinden

Ohne Modernisierung Ihres Netzwerks kann Ihre Digitale Transformation nicht gelingen

5 wichtige Prinzipien, um Netzwerke von heute
für die Herausforderungen von morgen zu wappnen

aruba
a Hewlett Packard
Enterprise company

 **TEAM-IT**
Systemhaus GmbH



Inhaltsverzeichnis

EINFÜHRUNG

Wenn Netzwerke nicht mithalten können 3

ABSCHNITT 1

Umgang mit zunehmender Komplexität 4

SEKTION 2

5 Möglichkeiten, Ihr Netzwerk jetzt zu modernisieren 5

Prinzip Nr. 1: Konnektivität und Skalierung 6

Prinzip Nr. 2: KI-gestützte Automatisierung 8

Prinzip Nr. 3: Sicherheit 10

Prinzip Nr. 4: Flexibilität und Agilität 12

Prinzip Nr. 5: Beschäftigung als Dienstleistung 14

SEKTION 3

Warum sich die Modernisierung von Netzen lohnt 16

SEKTION 4

Wie Aruba helfen kann 17





Wenn Netzwerke die Geschwindigkeit nicht beibehalten können

Das Netzwerk ist gewissermaßen das zentrale Nervensystem der heutigen digitalen Unternehmen. Bei den meisten Unternehmen ist es aber der Aufgabe nicht gewachsen, das steigende Volumen und die zunehmende Diversität von Datenimpulsen zu lenken, die physische und virtuelle Assets sowie Mitarbeitende verbinden. Das führt dazu, dass:

- Remote-Mitarbeitende quasi Bürger zweiter Klasse sind
- neue Geschäftsmodelle zum Stillstand kommen
- Ihre Mitarbeitenden und Kunden unterdurchschnittliche Erfahrungen haben
- ein enormer IT-Ressourcenaufwand für archaische, manuelle Prozesse verschwendet wird
- Gefährliche Sicherheitslücken

Indem Sie Ihre Netzwerke modernisieren, können Unternehmen Herausforderungen bei Architektur, Betrieb und Sicherheit überwinden und die digitale Transformation beschleunigen. Modernisierung ist notwendig, um neuen Geschäftsmodellen, dynamischen Belegschaftstrends und der Forderung nach besseren Erfahrungen für Mitarbeitende und Kunden zu entsprechen. Eine Netzwerkmodernisierung bietet folgende Vorteile:

- Die Bereitstellungsdauer für neue Netzwerklösungen verkürzt sich von Tagen und Wochen auf Minuten
- Ein starkes Sicherheitsfundament auf Basis von Zero Trust und SASE
- Netzwerkskalierung stellt kein Problem mehr dar
- Neue Nutzungsmodelle entlasten strapazierte Budgets und Mitarbeitende
- Konsistente Benutzererfahrungen vom Edge zur Cloud

Dieses E-Book betrachtet die wesentlichen Punkte, die eine Netzwerkmodernisierung erforderlich machen, und stellt anhand von Beispielen fünf wichtige Funktionsprinzipien für die weitere Vorgehensweise vor, damit das Netzwerk den Unternehmensanforderungen gerecht werden kann.






Mit wachsender Komplexität umgehen

Netzwerke von gestern ähnelten starren, mehrstufigen Hierarchien und können nur unter hohen Kosten neu konfiguriert und verwaltet werden. Heute erwarten Unternehmen von Netzwerken Unterstützung für ausgesprochen dezentrale Edge-Umgebungen mit immer mehr Remote-Mitarbeitenden, eine schnell steigende Zahl verbundener IoT-Geräte und den weiter bestehenden Bedarf an sicheren Verbindungen mit den in der Cloud und im Rechenzentrum gehosteten Anwendungen, Diensten und Daten.

Die Netzwerke von gestern an diese neue Umgebung anzupassen, schafft jedoch auf mehreren Ebenen betriebliche Herausforderungen:

- **Die Skalierung von Netzwerken** mit potenziell hunderttausenden Benutzern und Geräten über verschiedenste Standorte und Verbindungstypen hinweg muss manuell erfolgen und erfordert spezifische Konfigurationen. Leistungseinbußen sind unvermeidlich und die Erfüllung von SLAs wird zunehmend schwerer.
- **Knappe IT-Belegschaften** und die überwiegend manuellen Prozesse, die für die Einrichtung und Konfiguration von Netzwerken erforderlich sind, haben zur Folge, dass zu viel Zeit und Energie für sehr grundlegende Vorgänge aufgewendet werden und nur wenige Ressourcen verbleiben, um sich auf strategische Geschäftsinitiativen zu konzentrieren.
- **Ohne ein starkes Netzwerksicherheitsfundament sind Sicherheitslücken wahrscheinlicher.** Netzwerk- und Sicherheitsteams müssen bei der Abwehr von Cyberangriffen zusammenarbeiten und branchenweit anerkannte Sicherheits-Frameworks wie Zero Trust und Secure Access Service Edge (SASE) implementieren. Neue Netzwerkinfrastrukturen erfordern häufig einen **vollständigen Austausch der bestehenden Infrastruktur**. Das führt zu vorzeitiger Obsoleszenz und Herstellerbindung.
- Mit herkömmlichen Kauf- und Servicebereitstellungsmodellen ist es **schwierig, schnell neue Netzwerklösungen zu kaufen, verwalten und finanzieren.**



„Herkömmliche Netzwerke, die aus mehreren Produktlinien, Tools und Schnittstellen bestehen, sind starr und komplex im Management. Netzwerkprobleme jeglicher Art – Konfiguration, Bereitstellung, Fehlerbehebung, Problemlösung, Sicherheit, Optimierung – schränken geschäftliche Flexibilität und Mitarbeiterproduktivität ein.“

Enterprise Software Group

Sie bekommen vielleicht das Geld, aber liefern Sie auch Ergebnisse?

Unternehmen erkennen den Wert der Stärkung von Technologie-Assets. **Der Bericht 2022 State of the CIO stellte fest, dass 59 % der IT-Entscheidungsträger höhere Budgets erwarten und nur 10 % von einer Verringerung ausgehen.**

Die Top-3-Gründe für steigende Tech-Budgets sind:

- 57%: Bedarf an verbesserter Sicherheit
- 48%: Notwendige Upgrades veralteter Infrastruktur
- 48%: Investitionen in neue Fachkräfte/Nachwuchs



5 Möglichkeiten, wie Sie Ihr Netzwerk sofort modernisieren können

Die Herausforderung, die sich Netzwerk-Entscheidungsträgern stellt, ist es, ein Netzwerk für die Zukunft aufzubauen, wenn die Erwartungen höchstwahrscheinlich stark von unseren heutigen abweichen. Daher ist die Netzwerkmodernisierung kein Ziel, sondern ein fortwährender Prozess. Deshalb ist es entscheidend, Cloud-native Dienste – ob in der Cloud oder vor Ort – zu nutzen, die die Agilität bieten, um sich an dynamische Unternehmensanforderungen anpassen zu können.

Ein modernisiertes Netzwerk muss den Anforderungen von Remote-Mitarbeitenden, Zweigstellen, Campus, Rechenzentrum und Cloud entsprechen und alle ideal integrieren; gleichzeitig muss es einen neuen Architekturansatz bieten, der Edge-zentrisch, Cloud-fähig und datengestützt ist und dem Unternehmen Einfachheit, Geschwindigkeit und Sicherheit in einem flexiblen Nutzungsmodell bietet.

Netzwerkmodernisierung kann wie ein sehr großes Projekt aussehen. Unternehmen können mit den fünf grundlegenden Prinzipien für mehr Leistung, Automatisierung, Sicherheit und Agilität einfach und effizient ihre Aktivitäten und Investitionen zur Modernisierung verwalten und priorisieren.





Prinzip 1: Konnektivität und Skalierbarkeit

Remote-Arbeit, IoT und neue Geschäftsmodelle haben außerordentlich verteilte Umgebungen zur Folge. Netzwerke auf Basis herkömmlicher VLAN-Architekturen können potenziell hunderttausende Benutzer und Geräte über verschiedenste Standorte und Verbindungstypen hinweg nur schwer bewältigen.

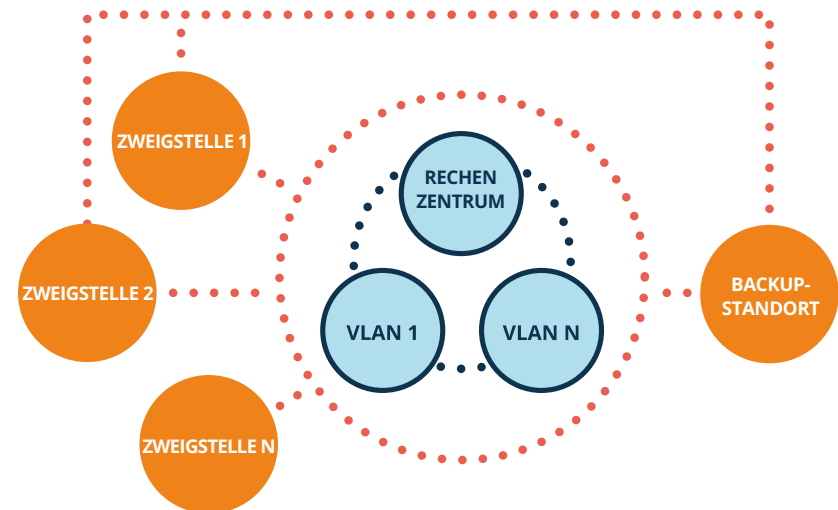
Daher sind neue Protokolle und Architekturen für Skalierbarkeit und Konnektivität essenziell. Beispielsweise ermöglicht es EVPN-VXLAN (Virtual eXtended LAN) Unternehmen, geografisch weit verteilte Standorte und isolierte VLANs mithilfe von Layer 2 Virtual Bridging über ein Layer-3-Netzwerk zu verbinden. Der erweiterte Adressraum von EVPN-VXLAN ermöglicht die Erstellung von bis zu 16 Millionen separaten Netzwerken. Dadurch kann eine wesentliche Beschränkung von VLANs überwunden werden, die maximal 4094 separate Netzwerke erstellen können, und die Möglichkeit zur Erstellung detaillierter Richtlinien zur Segmentierung des Datenverkehrs erheblich erweitert werden.

Zudem ist das Zusammenfügen von VLANs über eine stark verteilte Umgebung hinweg eine manuelle Aufgabe und mit erheblichem Aufwand für spezifische Switch- und Gateway-Konfiguration verbunden. Das bedeutet üblicherweise, dass der Datenverkehr über ineffiziente Routen läuft und die Netzwerksegmente ständig umsortiert und gepflegt werden müssen, was die Fehleranfälligkeit erhöht. Wenn das Netzwerk wie vorgesehen funktioniert, sind auch die tägliche Verwaltung, Fehlersuche und Optimierung manuelle und ineffiziente Aufgaben, die zur Folge haben, dass die IT weder SLAs noch die Erwartungen der Benutzer erfüllen kann.

Das modernisierte Netzwerk bietet zudem einen einzigen, Cloud-nativen Kontrollpunkt, mit dem Administratoren Einblick und einfache Verwaltbarkeit über Wireless LANs (WLANs), LANs und SD-WANs erhalten, die am Campus, in Zweigstellen, bei Remote-Mitarbeitenden, in Rechenzentren und an Cloud-Standorten eingesetzt werden.



Layer-2-Overlay (z. B. EVPN/VXLAN)



Layer-2-Netzwerkoverlays wie EVPN/VXLAN schaffen einen „Superhighway“ für effizienteren Datenverkehr und umfassende Durchsetzung von Sicherheitsrichtlinien



Das können Sie jetzt gleich tun:

- Stellen Sie mit Cloud-basierten Diensten schnell und kostengünstig ein sicheres Netzwerk bereit. Wählen Sie eine Cloud-native Lösung, die die Agilität und Pünktlichkeit der Cloud bietet, unabhängig davon, ob Sie sie in der Cloud oder vor Ort nutzen. Beginnen Sie mit einem Projekt wie der Aktualisierung eines Campus, einem neuen Standort oder mit Zweigstellen, damit das IT-Team selbst erfahren kann, wie einfach drahtlose Access Points (APs), Switches und Gateway-Infrastruktur aktiviert werden können, während gleichzeitig das Netzwerk und Sicherheitsrichtlinien zentral über einen einzelnen Sichtbarkeits- und Steuerungspunkt konfiguriert werden.
- Führen Sie Netzwerk-Overlays wie EVPN/VXLAN neben bestehender Infrastruktur ein, um zu erfahren, wie diese Protokolle auf aktuelle und zukünftige Umgebungen angepasst werden können. Es geht darum, einen Ansatz auszuwählen, der mit dem aktuellen Ansatz koexistieren kann und keinen vollständigen und radikalen Austausch Ihrer aktuellen Investition erfordert. Stellen Sie für zukünftiges Wachstum sicher, dass Verwaltung und Architektur für kabelgebundene drahtlose und WAN-Verbindungen gleich sind.
- Modernisieren Sie Ihre WAN-Lösungen mit SD-WAN (Software-definiert). Mit größerer Flexibilität, Effizienz und Kostenersparnis ist Breitbandinternet die bevorzugte Wide-Area-Zugriffsmethode mit Blick auf die Prävalenz Cloud-basierter Workloads und die wirtschaftlichen Aspekte der Internetverbindung. Suchen Sie eine SD-WAN-Lösung, die mit der gewählten Netzwerk-Overlaystruktur funktioniert und über integrierte Unterstützung für Sicherheitsframeworks wie SASE verfügt.





Prinzip 2: KI-basierte Automatisierung

Die Größe moderner Netzwerke übersteigt bereits die Möglichkeiten des Menschen zur Überwachung, Fehlerbehebung und Optimierung der Konnektivitäts-Assets von Unternehmen. Fachkräfte sind zunehmend rar, weswegen es nicht nur nicht wünschenswert, sondern auch schwer ist, das Problem einfach mit mehr Händen zu beheben.

Unternehmen müssen den für die Planung, Bereitstellung, Verwaltung und Optimierung von stark verteilten Netzwerken erforderlichen Zeit- und Ressourcenaufwand erheblich reduzieren. Automatisierung ist die einzige Antwort, und für eine erfolgreiche Umsetzung ist die KI-basierte Automatisierung von Abläufen (AIOps) erforderlich.

AIOps ist eine Hilfstechnologie, die es Administratoren ermöglicht, Aufgaben mit höherem Mehrwert zu übernehmen, indem wiederkehrende Aufgaben wie die Konfigurationsverwaltung, RF-Optimierung und Fehlerbehebung automatisiert werden. KI-basierte Lösungen erfassen und analysieren automatisch und sicher Daten aus verschiedenen Quellen, um Probleme vorherzusagen, spezifische Aufgaben unter Betreiberkontrolle zu automatisieren und die Netzwerkleistung insgesamt zu optimieren.

AIOps verbessert die Effizienz und Effektivität des Netzbetriebs von der Planung bis zur Bereitstellung an Tag Null und die laufende Verwaltung an Tag N. Nachdem ein Netzwerk eingerichtet ist, bietet AIOps die Möglichkeit, Probleme mit Auswirkungen auf das Netzwerk automatisch zu erkennen und zu diagnostizieren. Dazu verwendet es dynamische, standortindividuelle Basisdaten, die bei sich ändernden Bedingungen kontinuierlich angepasst werden, ohne dass eine manuelle Einrichtung oder eine Anpassung von Schwellenwerten auf Service-Ebene erforderlich ist. Die integrierte Erkennung von Anomalien gibt die Schwere und Auswirkungen von Problemen an, während sie auftreten, und hilft der IT-Abteilung dabei, die zugrunde liegende Ursache und geeignete Abhilfemaßnahmen genau zu ermitteln.

AIOps kann die Fehlerbehebung um bis zu 90 % schneller erledigen und reduziert dabei die Störungstickets um 50 %, indem es Probleme ganz einfach vor dem Benutzer erkennt.



Das können Sie jetzt gleich tun:

- Die Verwendung von AIOps ist ein Kulturwandel, der bei einigen Mitarbeitenden Sorgen um den Arbeitsplatz wecken wird. Diese Sorgen sind unbegründet. Arbeiten Sie mit Ihrem Team zusammen und verdeutlichen Sie den Idealzustand, in dem KI Zeit und Mühen für banale Aufgaben einspart, die Ihre Mitarbeitenden dann für interessantere und strategisch bedeutendere Projekte nutzen können.
- Fangen Sie klein an, um zu testen, wie KI-Lösungen in Ihrer Umgebung funktionieren. KI-Lösungen sollten eine ausfallssichere Schaltfläche haben, über die der Netzwerkadministrator Änderungen vor der Umsetzung annehmen muss, sowie eine Rückgängig-Option für Empfehlungen, die sich nicht bewährt haben. KI ist in vielen Situationen sehr gut, aber nicht perfekt.
- Lernen Sie, kühne Behauptungen von Anbietern zu den Fähigkeiten der KI („AI-Washing“) zu erkennen. Die erste Frage, die Sie stellen sollten: „Wie viele Daten werden in Ihre KI-Modelle gefüttert und woher kommen sie?“ Die korrekte Antwort beginnt mit einem Kundenstamm von 100.000 oder mehr. Achten Sie dann auf Fachkenntnisse, bewährte Leistung und Anwendbarkeit in allen Unternehmensgrößen. Ist das nicht gegeben, ist die KI nicht vertrauenswürdig.



Vorsicht vor „AI-Washing“. Fünf Kriterien zur Bestimmung der Vertrauenswürdigkeit von KI für den Netzbetrieb

Prinzip 3: Sicherheit

Strategien für die Cybersicherheit müssen eine sich stets wandelnde Benutzer- und Gerätebasis berücksichtigen, die sich mit dem Netzwerk verbindet. Die Verwaltung veralteter Netzwerke mit manuellen Verfahren ist nicht nur ineffizient und unpraktisch, sondern führt auch zu Lücken in der Sichtbarkeit sowie zu potenziellen Sicherheitsschwachstellen. Sie ist anfällig für menschliche Fehler. Latenz führt zu nicht akzeptablen Verzögerungen bei der Reaktion auf potenzielle Sicherheitsvorfälle.

Entlastung für IT und Netzwerkmanager kommt durch die zunehmende Integration von Netzwerk- und Sicherheitsfunktionen. Zero-Trust- und SASE-Frameworks bieten die Vorlage für ein sicheres Netzwerkfundament, das in das Netzwerk integrierte identitätsbasierte Zugriffskontrolle verwendet, um das Unternehmen zu schützen.

Heute muss die IT davon ausgehen, dass kein Benutzer, Gerät oder Netzwerksegment von Haus aus vertrauenswürdig ist. Zero-Trust-Architekturen stellen sicher, dass alle Geräte und Benutzer, die versuchen, auf das Netzwerk zuzugreifen, identifiziert und authentifiziert werden, bevor sie über eine vordefinierte Sicherheitsrichtlinie den minimal erforderlichen Zugriff gewähren.

Ein grundlegendes Prinzip von Zero Trust und SASE ist, dass Zugriffsberechtigungen von der Verbindungsmethode unabhängig sind. Wenn validierte Geräte und Benutzer im Netzwerk sind, müssen sie durchgehend überwacht werden, damit eine vollständige Sichtbarkeit darüber besteht, wer und was im Netzwerk ist und welche Aktivitäten durchgeführt werden.

Es gibt fünf wesentliche Funktionen, die für die Implementierung von identitätsbasierter Zugriffskontrolle zur Unterstützung von Zero Trust und SASE erforderlich sind:

1. Beseitigen Sie blinde Flecken. Verwenden Sie KI-basierte Techniken, um IoT-Geräte zu sehen, die sich außerhalb der Reichweite von Netzwerk- und Sicherheitsteams mit dem Netzwerk verbunden haben.
2. Authentifizieren Sie alle Benutzer und Geräte mit einer Kombination aus 802.1x, Multi-Faktor-Techniken, Geräte-Fingerabdrücken usw.
3. Autorisieren Sie Zugriffsberechtigungen basierend auf der Benutzer- und

Geräteidentität, der von der IT zugewiesenen Rolle und den mit dieser Rolle verbundenen Zugriffsprivilegien.

4. Setzen Sie Regeln durch und überwachen Sie sie. Segmentieren Sie Datenverkehr basierend auf Zugriffsrichtlinien und überwachen Sie Endpunkte in Zusammenarbeit mit der allgemeineren Sicherheitsumgebung kontinuierlich, um Änderungen des Sicherheitsstatus zu erkennen, die auf eine Gefährdung hinweisen.
5. Reagieren Sie auf Angriffe durch die dynamische Änderung von Rollen und Zugriffsprivilegien. Das kann von Bandbreitendrosselung über Quarantäne bis zur direkten Blockierung reichen. Zusammen sorgen Zero Trust und SASE dafür, dass für Mitarbeitende im Homeoffice oder in Telearbeit mit LAN-, WLAN- und WAN-Verbindungen dieselben Zugriffskontrollen gelten wie für Campus- oder Zweigstellennetzwerke.



Zero Trust und SASE beruhen auf identitätsbasierter Zugriffskontrolle, die vom Netzwerk durchgesetzt wird

Das können Sie jetzt gleich tun:

- Sofern nicht bereits der Fall, suchen Sie nach Wegen, wie das Netzwerkteam und das Sicherheitsteam zusammenarbeiten und dieselben Tools verwenden können, um die Konfigurations- und Datenverkehrsrichtlinien sowie die Sicherheitsrichtlinien zu konfigurieren und zu verwalten. Das Netzwerkverwaltungssystem sollte die UX/UI-Tools bereitstellen, die diese Integration ermöglichen.
- Bestehen Sie darauf, dass Zero Trust und SASE in Netzwerklösungen integriert und nicht nachträglich angebaut werden. Diese Lösungen sollten konsistente Richtlinien und Kontrollen ermöglichen, mit denen das Netzwerk Geräte und Benutzer entdecken, identifizieren und authentifizieren kann, die Zugriff erlangen möchten, Konfigurationskonformität und rollenbasierte Zugriffskontrolle durchsetzen kann sowie den Netzwerkverkehr basierend auf Berechtigungen segmentieren kann, die in der Zugriffsrichtlinie enthalten sind.
- Die Netzwerk- und Sicherheits-Ökosysteme müssen zusammenarbeiten, damit Unternehmen ihre Investitionen mit führenden Lösungen optimieren können. Beispielsweise gewinnen SASE-basierte Lösungen an Verbreitung, je mehr Workloads in die Cloud verlagert werden; Netzwerkfunktionen wie SD-WAN müssen sich daher nahtlos in eine breite Palette von Cloud-basierten Sicherheitservices integrieren lassen, um insgesamt bestmögliche Netzwerk- und Sicherheitsergebnisse zu erzielen.

Zero Trust und SASE auf dem Vormarsch

- 57 % der Befragten geben an, dass ihre Organisationen Zero Trust entweder implementiert haben oder einsetzen werden
- 49 % der Befragten geben an, dass ihre Organisationen SASE-Architekturen entweder bereits bereitgestellt haben oder bereitstellen werden– **Umfrage des Ponemon Institute**

Was steckt hinter Zero Trust?

„Endpunktschutz stoppt bösartige Aktivitäten; Erkennung und Reaktion am Endpunkt findet alles, was übersehen wurde; Mikrosegmentierung verhindert die Verbreitung und das mit Experten besetzte Sicherheitszentrum verwendet Automatisierung zur Behebung.“ — **Forrester**



Prinzip 4: Flexibilität und Agilität

Sich rasch ändernde Unternehmensziele erfordern ein Netzwerk, das sich schnell – und automatisch – an neue oder veränderte Bedingungen anpassen kann.

Leider sind viele Unternehmen heute durch einen Flickenteppich an getrennten Lösungen für die Verwaltung von WAN-, LAN- und WLAN-Netzwerken für Remote-Mitarbeitende und Campus-, Zweigstelle- und Rechenzentrums-Standorte eingeschränkt. Dieser Silo-Ansatz erfordert den Einsatz von mehreren domänenspezifischen Netzwerk-Management-Tools. Eine Fragmentierung dieser Größenordnung schafft Reibungspunkte im Betrieb, die sehr viel manuelle und ineffiziente Arbeit erfordern.

Die Agilität eines sich fortwährend modernisierenden Netzwerks zeigt sich auf unterschiedliche Weise. Zunächst bieten Cloud-native Netzwerklösungen einen einzelnen Sichtbarkeits- und Kontrollpunkt für LAN, WLAN und WAN sowie Konsistenz in Workflow und Benutzeroberfläche, die Domänensilos auflöst. Cloud-native Lösungen liefern von Haus aus kontinuierlich neue Updates und Funktionen, mit der Unternehmen immer auf dem aktuellsten Stand bleiben.

„Cloud-nativ“ heißt jedoch nicht notwendigerweise „in der Cloud bereitgestellt“. Zwar ist das eine zunehmend verbreitete Wahl, jedoch entscheiden sich viele Unternehmen, wichtige IT-Lösungen aus verschiedenen Sicherheits- und Kontrollgründen weiterhin lokal umzusetzen. Daher ist ein wesentliches Prinzip der Agilität die Fähigkeit, dieselbe Funktionalität in beiden Szenarien zu bieten.

Ein weiteres Prinzip der Netzwerkgilität ist die Fähigkeit, neue Architekturen und Topologien einzuführen, ohne aktuelle Investitionen obsolet zu machen. Wie oben erwähnt, sollten neue Sicherheitsparadigmen oder die Verwendung von Netzwerk-Overlaystrukturen keinen vollständigen und radikalen Austausch der aktuellen Infrastruktur erfordern, um von den Verbesserungen bei Funktion und Leistung zu profitieren. Das bedeutet, einen Migrationspfad einzuschlagen, der neue Lösungen in einem Tempo einbringt, das für das Unternehmen geeignet ist.

Anbieterbindung ist eine weitere Bedrohung für die Agilität. Häufig weichen scheinbar normbasierte Produkte letztendlich von weit verbreiteten Protokollen ab, um

sicherzustellen, dass der Kunde nach der Implementierung keine andere Wahl hat, als bei der Lösung zu bleiben. Das Resultat ist eine „geschützte Umgebung“, in der Interoperabilität mit Lösungen von Drittanbietern sehr schwer ist. Modernisierende Netzwerke sind offen und lassen führende Integrationen, die die Lösung insgesamt ergänzen und verbessern, problemlos zu.

Abschließend kommt Agilität von den Tools und Hilfsmitteln, die das Netzwerkteam nutzen kann, um Änderungen rasch und sicher vorzunehmen. Werden Workflows von grafischen Benutzeroberflächen gestützt, die den Business Intent widerspiegeln, ohne dass Kenntnis der zugrunde liegenden Infrastruktur erforderlich ist? Anders gesagt: Können sie die Welt der Befehlszeilenschnittstellen hinter sich lassen? Erkennen WLAN Access Points bei der Bereitstellung ihren Standort selbstständig oder muss das Personal Pläne heranziehen und jedes Gerät einzeln aufzeichnen? Passen sich die Gerätepläne bei physischen Änderungen automatisch an? Netzwerkmanagementlösungen, die diese Art von Multiplikatoren bieten, steigern die Effizienz des Unternehmens enorm.



Ob in der Cloud oder lokal, Cloud-native Netzwerkdienste liefern die Agilität, die modernisierte Netzwerke benötigen



Das können Sie jetzt gleich tun:

- Wenn Sie den Weg zur Cloud für die Netzwerkverwaltung und identitätsbasierte Zugriffskontrolle noch nicht begonnen haben, wählen Sie ein Projekt oder einen Teil Ihres Netzwerks, das oder der von zentralisierter Kontrolle und Sichtbarkeit in der Cloud profitieren könnte. Ein guter Startpunkt sind Umgebungen für die Telearbeit, bei der Zero-Touch-Provisioning, KI-basierte Kontrolle und konsequent durchgesetzte Sicherheitsrichtlinien zu Hause dieselbe Erfahrung wie im Büro ermöglichen. Wenn Sie bereits Cloud-natives Netzwerkmanagement einsetzen, stellen Sie sicher, dass es auf Ihre Bedürfnisse skalierbar ist und die Funktionen bietet, die Sie benötigen. Viele Cloud-Lösungen begannen als Tools für kleine Unternehmen und versuchen, „erwachsen zu werden“ und in die Unternehmensklasse aufzusteigen, ohne die zugrunde liegende Architektur aufzuweisen, die für größere Umgebungen erforderlich ist.
- Bestehen Sie auf Cloud-nativen Diensten, die entweder in der Cloud oder lokal bereitgestellt werden können, um Einrichtung, Konfiguration und Verwaltung für ideale Sichtbarkeit und Kontrolle in einer zentralen Benutzeroberfläche zu integrieren. Sie sollten in der Lage sein, die manuelle Konfiguration statischer VLANs und Zugriffskontrolllisten durch Business-Intent-Richtlinien zu ersetzen, die Netzwerktopologien, Datenverkehrsfluss und ordnungsgemäße Zugriffsrechte für Mitarbeitende, Gäste, Dienstleister und andere Benutzergruppen definieren.
- Achten Sie genau auf Lizenzbedingungen. In manchen Fällen binden Lizenzbedingungen Kunden an aktuelle Geräte oder zwingen Sie zu einem Upgrade, bevor sie dazu bereit sind.





Prinzip 5: Employ-as-a-Service

Viele Unternehmen sind mit schwierigen, häufig scheinbar unüberwindbaren Herausforderungen bei der schnellen Beschaffung, Implementierung, Verwaltung und Finanzierung neuer Netzwerklösungen konfrontiert. Einschränkungen durch langfristige CAPEX und Abschreibungen, knappe Mitarbeiterressourcen und Fachkräftemangel können häufig zu langen Lebenszyklen für Produkte führen und eine schnelle Umstellung bei Änderungen in der Geschäftsdynamik behindern. Heute würden sich so gut wie alle Organisationen lieber auf Unternehmensergebnisse fokussieren, statt Neuanschaffungen zum bevorstehenden Ende der Produktlebensdauer zu planen.

Alternative Nutzungs- und Bereitstellungsmodelle, einschließlich selbst bereitgestellter oder selbst verwalteter Dienste, flexible Finanzierung und neue Technologien bieten mehr Optionen, mehr Agilität und eine kürzere Produkteinführungszeit als traditionelle Kauf- und Bereitstellungsmodelle.

Auf dieselbe Art, wie Unternehmen Begrenzungen bei Rechenleistung und Speicher durch die Einführung öffentlicher und hybrider Cloud-Infrastruktur überwinden konnten, können Sie nun Network-as-a-Service (NaaS)-Nutzungsmodelle verwenden. Dieser Ansatz liefert schnelle neue Netzwerklösungen und optimiert dabei Budgetressourcen durch einfachere Skalierbarkeit und Flexibilität nach oben oder unten.

NaaS bietet die Flexibilität, um Netzwerkinfrastrukturen auf Unternehmensniveau auf eine Art zu nutzen, die es Unternehmen ermöglicht, mit technischen Innovationen Schritt zu halten, hochdynamischen Geschäftsanforderungen gerecht zu werden und die Netzwerkleistung und Benutzererfahrung durch Wahl zwischen einem CapEX oder einem Cloud-ähnlichen Abomodell zu optimieren, selbst bei Infrastruktur on-premises.

In einem Modell kann NaaS die Belastung durch langfristige Netzwerkplanung und -budgetierung verringern, indem alle Hardware, Software und Dienste über ein einzelnes monatliches Abonnement bereitgestellt werden und keine Kapitalinvestitionen im Vorfeld erforderlich sind. Unternehmen können die neuesten Technologien nutzen und entlasten gleichzeitig ihre Mitarbeitenden in der IT. So können sie sich schnell unternehmenswichtigen Herausforderungen zuwenden und Netzwerklösungen rasch bereitstellen – und ihr Budget gleichzeitig optimieren.



NaaS ist laut neuer Umfrage angekommen. 1/3 hat schon bereitgestellt, weitere 25 % planen dies für das kommende Jahr

- 60 % sagen, dass Langzeitplanungszyklen nun nur noch 2 Jahre umfassen
- Treiber Nr. 1: Schnellere Bereitstellung neuer Technologien rasch ermöglichen
- 41 % entscheiden sich für OpEx statt CapEx
- Für 82 % sind Vorteile bei der Nachhaltigkeit wichtig

Source: 2022 IDC NaaS Global Survey, gesponsert von Aruba



Das können Sie jetzt gleich tun:

- Beurteilen Sie das Potenzial, das ein flexibler Finanzierungs- und Abonnementansatz Ihrem Unternehmen bieten kann, und ob Ihr Anbieter über die Ressourcen verfügt, ein As-a-Service-Modell in signifikantem Maßstab zu unterstützen.
- Fragen Sie Ihre Anbieter, ob sie NaaS-Optionen für alternde, bestehende Lösungen anbieten und ob sie ein Standard-Serviceangebot haben oder jeder Vertrag individuell ist. Erfahrene NaaS-Anbieter wissen, wie Kunden Services nutzen möchten, und können den Bestell- und Bereitstellungsvorgang vereinfachen.
- Ermitteln Sie, ob Ihr Unternehmen NaaS-Optionen benötigt und ob Ihr Anbieter oder Partner diese liefern kann, um die tägliche Netzwerküberwachung, die Administration und den Betrieb auszugliedern und interne Ressourcen so für Aktivitäten mit höherem Mehrwert freizugeben.

So viel outsourcen, wie Sie möchten

„NaaS-Modelle ermöglichen es Unternehmen, Planung, Bereitstellung, tägliche betriebliche Verwaltung, Upgrades, Überwachung und Fehlerbehebung von Unternehmensnetzwerken sowie die Außerbetriebnahme und den Support von Geräten am Ende der Produktlebensdauer auszulagern.— IDC





Was modernisierende Netzwerke leisten

Netzwerkmodernisierung bedeutet nicht einfach nur aktuelle Infrastruktur umzurüsten, um mit der neuen Technologiegeneration Schritt zu halten. Es ist ein wesentlicher und andauernder Prozess zur Schaffung eines agilen Netzwerkfundaments, das die Fähigkeit des Unternehmens zur raschen Implementierung von Initiativen zur digitalen Transformation durch Nutzung neuer Ansätze für Architektur, Sicherheit, Verwaltung und Bereitstellung stärkt.

Ein modernisiertes Netzwerk ist aber keine Zukunftsmusik mit schwerer Umsetzung. Mit den oben stehenden Vorschlägen können schon heute dringende Unternehmensfragen ideal mit dem Wechsel zu einer modernen Netzwerkbasis adressiert werden:

- Leichte Ausweitung der Erfahrung am Campus auf kleine Büros sowie Benutzer im Homeoffice und an Mobilgeräten
- Entwicklung standortbezogener Dienste für nahtlose Erfahrungen im Innen- und Außenbereich
- Nutzung der Daten, die durch rasches Wachstum bei IoT-Geräten generiert werden
- Entlastung des Fachkräftemangels durch Automatisierung des Netzwerkbetriebs
- Effiziente Bereitstellung von konsistentem, sicherem Zugriff auf Cloud-basierte Anwendungen unabhängig vom Standort der Benutzer
- Automatisierung der Konfiguration und Verwaltung von komplexen Netzwerk- und Sicherheitsprozessen mit Workflows, die an den Business Intent geknüpft sind
- Verringerung des Zeit- und Ressourcenaufwands für die Planung und Implementierung von Änderungen mit neuen Nutzungs- und Bereitstellungsmodellen
- Nutzung von KI-basierten Analysen, um die erforderliche Zeit für die Fehlerbehebung zu verkürzen, das Ticketaufkommen signifikant zu verringern und Best Practices aus der Community zur Optimierung des Netzwerkbetriebs zu nutzen
- Bereitstellung von neuen digitalen Erfahrungen für Kunden, Mitarbeitende und Gäste





So kann Aruba Sie unterstützen

Aruba ermöglicht die Netzwerkmodernisierung in jeder Phase Ihrer Reise vom Edge zur Cloud.

Aruba wurde mehrfach von externen Analysten als führender Anbieter bei allen Netzwerkkonnektivitätsoptionen hervorgehoben: WLAN, Switches und SD-WAN. Die Welt verlässt sich auf Aruba, eine Hewlett Packard Enterprise Company mit hunderttausenden Kunden von kleinen und mittelständischen Unternehmen bis hin zu weltweit tätigen Organisationen, um eine sichere, KI-basierte Edge Services Plattform für alle Netzwerkkumgebungen zu erhalten.

Seit Gründung 2002 ist Aruba in Sachen Innovation ganz vorn dabei und bietet mit der Aruba Edge Services Plattform (ESP) Lösungen für die Netzwerkmodernisierung über alle fünf Prinzipien hinweg.

Mit Aruba ESP nutzt das Unternehmen einen Cloud-nativen Ansatz, um Kunden bei der Erfüllung Ihrer Konnektivitäts-, Sicherheits- und Budgetanforderungen für Campus-, Zweigstelle-, Rechenzentrums- und Homeoffice-Umgebungen zu unterstützen. ESP bietet alles in höherer Geschwindigkeit – Verbindungen für Benutzer, IoT-Onboarding, Skalierung von sicheren Standorten, Problembhebung und Erkenntnisse zum Betrieb in einer einzigen Architektur.

Als Kernkomponente von Aruba ESP vereinfacht und verbessert Aruba Central IT-Abläufe mit einem einzelnen, Cloud-nativen Sichtbarkeits- und Kontrollpunkt für LAN, WLAN und SD-WAN. Dies umfasst KI-gestützte Erkenntnisse, Workflow-Automatisierung und robuste Sicherheit, die der IT-Abteilung die Verwaltung und Optimierung von Campus-, Zweigstelle-, Remote-, Rechenzentrums- und IoT-Netzwerken über ein einziges Dashboard ermöglicht.

Und aufgrund der Rolle des Netzwerks bei der Erstellung von Zero-Trust- und SASE-Frameworks bietet Aruba Central Unternehmen vollständige Sichtbarkeit, Kontrolle und Durchsetzung von identitätsbasierter Zugriffskontrolle und Datenverkehrssegmentierung in der gesamten Infrastruktur.

Egal, welche Anforderungen Sie an das Netzwerk und die digitale Transformation haben, bietet der Ansatz von Aruba zur Netzwerkmodernisierung auf dieser Grundlage die notwendigen Lösungen für heute und morgen.





Um mehr zu erfahren, besuchen Sie:
www.arubanetworks.com/connectwhatmatters

© Copyright 2022 Hewlett Packard Enterprise Development LP. Die hierin enthaltenen Informationen können ohne Vorankündigung geändert werden. Die nur Garantien für Produkte und Dienstleistungen von Hewlett Packard Enterprise sind in den beigefügten ausdrücklichen Garantieerklärungen aufgeführt Produkte und Dienstleistungen. Nichts hierin sollte als zusätzliche Garantie ausgelegt werden. Hewlett Packard Enterprise ist dies nicht haftet für hierin enthaltene technische oder redaktionelle Fehler oder Auslassungen.

ebook_aruba_network-modernization_031522

aruba
a Hewlett Packard
Enterprise company