

Vergleich von SD-WAN-Lösungen. Vom Client bis zur Cloud







SD-WAN-Lösungen, die Unternehmen heute zur Verfügung stehen, sind nicht alle gleich. Viele Vergleiche konzentrieren sich auf einige wenige Schwerpunkte und vernachlässigen das Gesamtbild aus Nutzererfahrung, simplifizierten Abläufen und übergreifendem Schutz vom Client bis zur Cloud. Ihr SD-WAN sollte die Geschäftsabläufe unterstützen, auch jenseits des WAN, und das gesamte Unternehmen mit einbinden.

Vergleich* der Funktionsbreite und -tiefe der einzelnen Lösungen









Artificial Intelligence for Network Operations (AIOps)

Die Netzwerkbranche steht vor einem Paradigmenwechsel vom traditionellen, veralteten CLI-Netzwerkbetrieb zu einem automatisierten AIOps-Ansatz. Angesichts der unterschiedlichen Geräte, Nutzer, Anwendungen, Bandbreiten, IoT usw. ist es schlichtweg unmöglich, sich bei der Fehlerbehebung und dem Gewinnen von Einblicken in Netzwerkprobleme auf Protokolldateien zu verlassen. Mit AIOps stützen Sie sich auf künstliche Intelligenz und maschinelles Lernen, um die Nadel im Heuhaufen zu finden und mit der Komplexität der aktuellen Digitalisierung Schritt zu halten.

Mehrwertversprechen						
Funktionen mit AIOps	<p>● ● ● ● ●</p> <ul style="list-style-type: none"> - Juniper WAN Assurance, Visibilität der Endbenutzererfahrung und kürzere MTTR - Virtueller Netzwerkassistent MARVIS 	<p>● ○ ○ ○ ○</p> <p>Nyansa-Produkt soll für Absicherung sorgen</p>	<p>○ ○ ○ ○ ○</p> <p>Kein KI/AIOps</p>	<p>○ ○ ○ ○ ○</p> <p>Kein KI/AIOps</p>	<p>○ ○ ○ ○ ○</p> <p>Kein KI/AIOps</p>	<p>○ ○ ○ ○ ○</p> <p>Keine ESP-Integration mit Silver Peak-Produkt</p>
WAN Servicelevel-Erwartungen (SLE): Überwachung und Durchsetzung von SLE für wichtige Benutzer- und Gerätekenzzahlen im gesamten WAN KI-gestützte Überwachung des Zustands von WAN-Verbindungen, Anwendungen und Geräten	<p>● ● ● ● ●</p> <ul style="list-style-type: none"> - SLE-Framework stellt KI/ML-gestützt die Funktionen bereit - KI zur Steuerung des Datenverkehrs - SLE für Zustand der WAN-Verbindung, Zustand des Gateway und Nutzererfahrung 	<p>● ○ ○ ○ ○</p> <p>Nyansa-Produkt soll SLE erfüllen</p>	<p>○ ○ ○ ○ ○</p> <p>Kein KI/AIOps</p>	<p>○ ○ ○ ○ ○</p> <p>Kein KI/AIOps</p>	<p>○ ○ ○ ○ ○</p> <p>Kein KI/AIOps</p>	<p>○ ○ ○ ○ ○</p> <p>Keine ESP-Integration mit Silver Peak-Produkt</p>
KI-gesteuerte Einblicke und unterstützte Aktionen	<p>● ● ● ● ●</p> <ul style="list-style-type: none"> - Einblicke in Zustand des WAN-Edge - Umfassende Einsichten in jeden Aspekt des WAN 	<p>● ○ ○ ○ ○</p> <p>Planungsphasen mit Nyansa</p>	<p>○ ○ ○ ○ ○</p> <p>Kein KI/AIOps</p>	<p>○ ○ ○ ○ ○</p> <p>Kein KI/AIOps</p>	<p>○ ○ ○ ○ ○</p> <p>Kein KI/AIOps</p>	<p>○ ○ ○ ○ ○</p> <p>Keine ESP-Integration mit Silver Peak-Produkt</p>
Virtueller AIOps-Netzwerkassistent (Virtual Network Assistant, VNA)	<p>● ● ● ● ●</p> <p>Integration in Marvis und Juniper Mist KI zur Absicherung von WAN, WLAN und WAN</p>	<p>● ○ ○ ○ ○</p> <p>Hier muss Nyansa noch liefern</p>	<p>○ ○ ○ ○ ○</p> <p>Kein KI/AIOps</p>	<p>○ ○ ○ ○ ○</p> <p>Kein KI/AIOps</p>	<p>○ ○ ○ ○ ○</p> <p>Kein KI/AIOps</p>	<p>○ ○ ○ ○ ○</p> <p>Keine ESP-Integration mit Silver Peak-Produkt</p>

Sicherheit und SASE in Aktion

Sie müssen Ihr gesamtes Unternehmen schützen, auch über das WAN hinaus. Die Sicherheit muss integriert sein, sie darf nicht nachträglich eingebaut werden. Von Zero-Trust bis hin zum Schutz vor der lateralen Verbreitung von Bedrohungen muss das SD-WAN die Sicherheitsrichtlinien auf einfache und effiziente Weise umfassend durchsetzen.

Mehrwertversprechen						
In eine Netzwerkschicht integrierte Zero-Trust-Sicherheit	● ● ● ● ● - Die einzige Zero-Trust-Fabric, die Zugangskontrolle, Segmentierung und Direktionalität simplifiziert (verfolgt die Richtung nach und setzt Unternehmensrichtlinien durch) - Integrierte(s) Richtlinie und Routing auf Grundlage von SASE	○ ○ ○ ○ ○ Es gibt keine Zero-Trust-Sicherheit auf der Netzwerkschicht	○ ○ ○ ○ ○ Es gibt keine Zero-Trust-Sicherheit auf ihrer Netzwerkschicht	○ ○ ○ ○ ○ Es gibt keine Zero-Trust-Sicherheit auf ihrer Netzwerkschicht	○ ○ ○ ○ ○ Es gibt keine Zero-Trust-Sicherheit auf ihrer Netzwerkschicht	○ ○ ○ ○ ○ Es gibt keine Zero-Trust-Sicherheit auf ihrer Netzwerkschicht
Benutzerschutz, Arbeitsauslastungsschutz und Schutz vor lateralen Bedrohungen	● ● ● ● ● Vollständiges Portfolio, einschließlich Benutzersicherheit, IoT-Sicherheit, Zero-Day-Bedrohungsschutz und Schutz vor Phishing	○ ○ ○ ○ ○ Sicherheit hängt von Zusatztechnologien und -geräten von Partnern ab, die zunehmend mit VMware konkurrieren; Sicherheitsrichtlinie wird nicht über die Software von VMware gesteuert	● ● ● ○ ○ Sicherheitsfunktionen hängen stark davon ab, welche Zweigstellenplattformen zum Einsatz kommen (DNS-Weiterleitung von vEdge an die Cisco Umbrella Cloud)	● ● ○ ○ ○ Keine KI/AIOps	● ● ● ● ● Keine KI/AIOps	● ○ ○ ○ ○ Sicherheit hängt von Zusatztechnologien und Geräten der Partner ab, die zunehmend mit Silver Peak konkurrieren
Zentrales Richtlinienmanagement der Enterprise-Klasse	● ● ● ● ● Komplette Portfoliolösungen mit zentraler Richtlinien- und Edge-Durchsetzung	○ ○ ○ ○ ○ Planungsphasen mit Nyansa	● ● ● ○ ○ Keine KI/AIOps	● ● ● ● ● Keine KI/AIOps	● ● ● ● ● Keine KI/AIOps	○ ○ ○ ○ ○ Keine ESP-Integration mit Silver Peak-Produkt
Bedrohungsvisibilität und Analyse von Anwendungen, Benutzern, Geräten	● ● ● ● ● Vollständige Benutzervisibilität mit KI- und ML-Anwendungen, mit Live-Feed zu Bedrohungen und Benutzervisibilität	○ ○ ○ ○ ○ VMware verlässt sich auf externe Sicherheitslösungen	● ● ● ○ ○ Beschränkte Zero-Day-Funktionen zum Erlernen und Vermeiden komplexer Bedrohungen und Sicherheitsfunktionen mit LAN-Integration. (Der aktuelle NSS Labs-Bericht hat Cisco-Sicherheit nicht empfohlen)	● ● ● ○ ○ Beschränkte Zero-Day-Funktionen zum Erlernen und Vermeiden komplexer Bedrohungen	● ● ● ● ● Keine integrierte Sicherheit	○ ○ ○ ○ ○ Keine integrierte Sicherheit
Integration hochentwickelter Bedrohungsinformationen und -abwehr am WAN-Edge	● ● ● ● ● Vernetzte Sicherheit in der gesamten Netzwerkinfrastruktur mit Kabel, ohne Kabel und mit WAN	○ ○ ○ ○ ○	○ ○ ○ ○ ○	○ ○ ○ ○ ○	● ● ● ○ ○	○ ○ ○ ○ ○







Funktionen und Performance des WAN-Edge

SD-WANs müssen sich weiterentwickeln. Aktuell verlassen sich die meisten Angebote auf arbeits- und kostenintensive Tunnel, die wenig Sicherheit bieten, teuer sind und viel Bandbreite verbrauchen. Junipers Session Smart™ ist jedoch tunnelfrei und gewährleistet durch Sitzungen mit großem Datengehalt und -detailreichtum eine hochwertige Benutzererfahrung. In Kombination mit Juniper Mist KI erhalten Sie ein wahrhaft benutzerfreundliches SD-WAN der dritten Generation.

Mehrwertversprechen	JUNIPER NETWORKS	vmware®	CISCO	VERSA NETWORKS	FORTINET®	Hewlett Packard Enterprise
Benutzerfreundliches, auf Benutzererfahrung ausgelegtes Design	● ● ● ● ● - Mehr Benutzerfreundlichkeit durch sitzungsbasierte Technologie - Umfassende sitzungsbasierte Visibilität und Einblicke, fein abgestimmtes App-fähiges Routing - Bis zu 60 % weniger Latenz	○ ○ ○ ○ ○ Herkömmlicher Ansatz, im Zentrum steht das Netzwerk, nicht die Sitzung des Benutzers	○ ○ ○ ○ ○ Herkömmlicher Ansatz, im Zentrum steht das Netzwerk, nicht die Sitzung des Benutzers	○ ○ ○ ○ ○ Herkömmlicher Ansatz, im Zentrum steht das Netzwerk, nicht die Sitzung des Benutzers	○ ○ ○ ○ ○ Herkömmlicher Ansatz, im Zentrum steht das Netzwerk, nicht die Sitzung des Benutzers	○ ○ ○ ○ ○ Herkömmlicher Ansatz, im Zentrum steht das Netzwerk, nicht die Sitzung des Benutzers
Wirtschaftlichkeit/Eingesparte Bandbreite des SD-WAN	● ● ● ● ● Tunnelfreie Architektur/SVR entfernt Overhead, ermöglicht bis zu 75 % geringere Infrastrukturkosten und 30-50 % geringere Bandbreitenkosten	○ ○ ○ ○ ○ Bandbreitenintensiver, tunnelbasierter Ansatz	○ ○ ○ ○ ○ Bandbreitenintensiver, tunnelbasierter Ansatz	○ ○ ○ ○ ○ Bandbreitenintensiver, tunnelbasierter Ansatz	○ ○ ○ ○ ○ Bandbreitenintensiver, tunnelbasierter Ansatz	○ ○ ○ ○ ○ Bandbreitenintensiver, tunnelbasierter Ansatz
Intelligente Verschlüsselung: Standardmäßig sind die meisten Anwendungen verschlüsselt, beispielsweise der HTTPS-Datenverkehr (doppelte Verschlüsselung möglichst vermeiden)	● ● ● ● ● Anpassungsfähige Verschlüsselung berücksichtigt Sitzungen und spart Bandbreite: Bereits verschlüsselter Datenverkehr muss nicht erneut verschlüsselt werden	○ ○ ○ ○ ○ Unintelligente Verschlüsselung	○ ○ ○ ○ ○ Unintelligente Verschlüsselung	○ ○ ○ ○ ○ Unintelligente Verschlüsselung	○ ○ ○ ○ ○ Unintelligente Verschlüsselung	○ ○ ○ ○ ○ Unintelligente Verschlüsselung
Universelles CPE	● ● ● ● ● NFX-Serie von Juniper bietet gesamtes Spektrum an Konnektivität und Skalierbarkeit; weithin anerkannt und verbreitet	● ● ● ● ○ Dell EMC Edge	● ● ● ● ○ Cisco 5000 ENCS	○ ○ ○ ○ ○ Kein Portfolio mit universellem CPE	○ ○ ○ ○ ○ Kein Portfolio mit universellem CPE	○ ○ ○ ○ ○ Kein Portfolio mit universellem CPE
SD-WAN-Edge für jede Umgebung (unterstützt kleine/mittlere/große Bereitstellungen)	● ● ● ● ● Junipers breites Portfolio reicht von Desktop-Formfaktoren bis zu großen Campus-/Unternehmen	● ● ○ ○ ○ WAN-Edge-Gerät mit begrenzten Routing-Funktionen	● ● ● ● ○ Großes Produktsortiment, aber getrennte Produktreihen mit unterschiedlichen Managementlösungen	● ● ○ ○ ○ Begrenztes Zweigstellenangebot mit White-Box-Optionen	● ● ● ● ● Kundenspezifisches ASIC-Design bietet hohe Leistung	● ● ○ ○ ○ Begrenzte Routing-Funktionen
Zustandsmessungen von Verbindungen und Anwendungen	● ● ● ● ● Erweiterte Funktionen mit Juniper Paragon (Netrounds)	● ● ● ○ ○ Passiv	● ● ● ○ ○ Aktiv	● ● ● ○ ○ Aktiv	● ● ● ○ ○ Aktiv	● ● ● ○ ○ Aktiv
Ausfallsicheres Design des WAN-Edge	● ● ● ● ● Redundanz auf jeder Ebene (aktiv/aktiv, aktiv/Backup, Datacenter-Hub, Control Plane und Data Plane)	● ● ● ● ●	● ● ● ● ●	● ● ● ● ●	● ● ● ● ●	● ● ● ● ●

Architektur

Aktuell basieren viele Lösungen auf veralteten Architekturen, die an vorhandene Technologien gebunden sind. Eine moderne Lösung für die Cloud-Ära von heute muss auch auf einer modernen Cloud-Architektur mit Microservices aufbauen. So bleibt das Unternehmen flexibel, und das Netzwerk hält mit dem Geschäftsbetrieb Schritt.

Mehrwertversprechen						
Für die Cloud-Ära entwickelte Architektur	<p>● ● ● ● ●</p> <p>Zeitgemäße Microservices auf Grundlage der Cloud-Architektur</p> <ul style="list-style-type: none"> - Servicecontainerisierung - Schnelle Updates mit geringem Risiko - Bugfixes nahezu in Echtzeit ohne Netzwerkunterbrechung 	<p>● ● ○ ○ ○</p> <p>Cloud der ersten Generation</p>	<p>● ● ○ ○ ○</p> <p>Meraki:</p> <ul style="list-style-type: none"> - Cloud der ersten Generation - Gemeinsam genutzte Legacy-Datenbank in gehosteter Datenbank-„Cloud“ - Virtuell, Controller-basiert <p>Cisco:</p> <ul style="list-style-type: none"> - Controller-basierte monolithische Legacy-Softwarearchitektur - Fehlen einer zuverlässigen Cloud-Lösung, beschränkt auf SMB - Viel Hardware und Boxen, alle benötigen die richtigen Versionen - Mehrere voneinander isolierte Produkte und Betriebssysteme (10+) 	<p>● ● ○ ○ ○</p> <p>Cloud der ersten Generation</p>	<p>● ○ ○ ○ ○</p> <p>Fragmentiertes Cloud-Angebot</p>	<p>● ● ○ ○ ○</p> <p>Aruba ESP ist das überarbeitete Design von Aruba Central mit Management-Funktionen</p> <ul style="list-style-type: none"> - Controller-basierte Architektur mit vier verschiedenen Clouds - Benutzer müssen die gesamte Software aktualisieren, pflegen und integrieren - Monolithische Codebasen sind aufwendig zu skalieren und schwer zu verwalten - Begrenzte API-Unterstützung
Skalierbarkeit: die Fähigkeit, viele Mandanten, Standorte, Geräte zu unterstützen	<p>● ● ● ● ●</p> <p>3-fache Skalierbarkeit im Vergleich zu jeder SD-WAN-Lösung</p> <ul style="list-style-type: none"> - Elastische vertikale und horizontale Skalierbarkeit - Keine teure Hardware erforderlich - Single-Software-Image simplifiziert Versionsplanung und Upgradepfad 	<p>● ● ● ○ ○</p> <p>Skalierung für mehrere Mandanten und Standorte erfordert zusätzliche Orchestrierung und Gateways</p>	<p>● ● ● ● ○</p> <ul style="list-style-type: none"> - Komplexe Skalierung, benötigt vManage, vBond und vSmart für die Verwaltung in der Management und Control Plane - Cisco empfiehlt Meraki für Lean IT: Wechsel zur SD-WAN-Vollversion nur mit kostspieliger Aufrüstung der Software und Hardware möglich 	<p>● ● ● ● ○</p> <p>Unterstützt derzeit angeblich 5.000 CPEs</p>	<p>● ● ● ● ●</p> <p>Unterstützt laut FortiManager 100.000 Standorte</p> <ul style="list-style-type: none"> - Wurde nicht öffentlich getestet und bestätigt - Gilt nur für Management Plane der Lösung 	<p>● ● ● ● ○</p> <p>Skalierung basierend auf Cloud-VPC-Leistung</p>
Vielseitige Automatisierung (APIs, Plugins für die Erweiterung)	<p>● ● ● ● ●</p> <ul style="list-style-type: none"> - Einfach, 100 % API-gestützt - API und Konfigurationsvorlagen - Kunden können mit eigenen Plugins für Erweiterbarkeit sorgen - Integration in Splunk und ServiceNow 	<p>● ● ○ ○ ○</p> <p>Grundlegende APIs für Velocloud Orchestrator</p>	<p>● ● ● ● ○</p> <p>REST-APIs verfügbar mit DevNet-Support</p>	<p>● ● ● ● ○</p> <p>REST-APIs</p>	<p>● ● ● ● ○</p> <p>Komplexität durch Abhängigkeit von mehreren Python-Modulen</p>	<p>● ● ● ● ○</p> <p>RESTful APIs verfügbar</p>

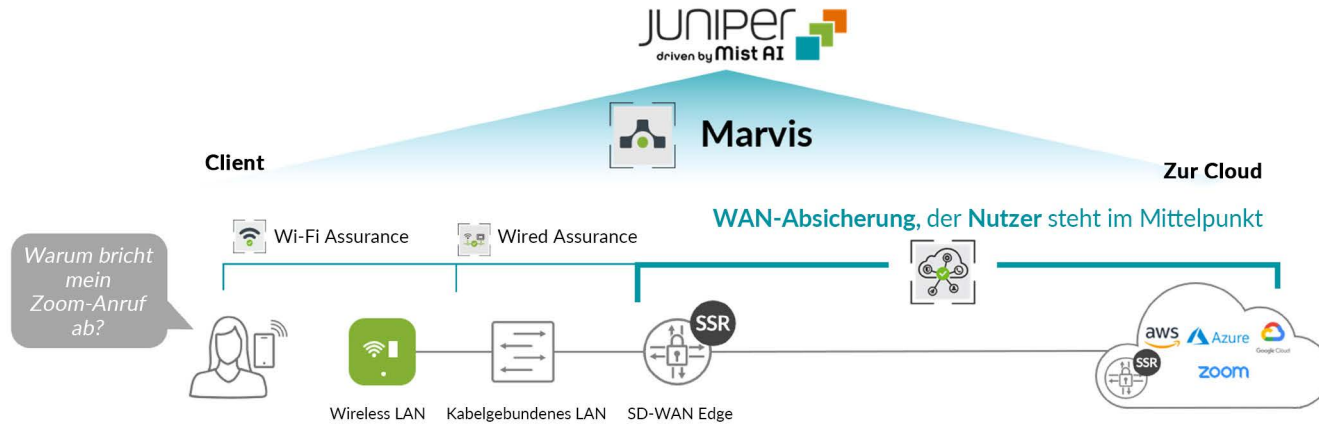
Mehrwertversprechen



Mehrwertversprechen	JUNIPER NETWORKS	vmware®	CISCO	VERSA NETWORKS	FORTINET®	Hewlett Packard Enterprise
Agilität	<p>● ● ● ● ●</p> <ul style="list-style-type: none"> - Zeitgemäße Cloud auf Grundlage von Microservices anstatt monolithischer Codebasis - Schnelle Updates ohne Netzwerkunterbrechung 	<p>● ● ○ ○ ○</p> <ul style="list-style-type: none"> - Cloud der ersten Generation - Keine auf Microservices basierende Cloud-Architektur 	<p>● ● ○ ○ ○</p> <p>Meraki:</p> <ul style="list-style-type: none"> - Cloud der ersten Generation mit VMs und Hypervisors - Langsame Updates, da keine zeitgemäße Microservices-Architektur vorhanden <p>Cisco:</p> <ul style="list-style-type: none"> - Monolithische (spröde) Software mit umständlichen Updates für neue Geräte/ Apps/Fixes - Erhöhtes Update-Risiko 	<p>● ● ○ ○ ○</p> <ul style="list-style-type: none"> - Cloud der ersten Generation - Keine auf Microservices basierende Cloud-Architektur 	<p>● ○ ○ ○ ○</p> <p>Fragmentiertes Cloud-Angebot</p>	<p>● ● ○ ○ ○</p> <ul style="list-style-type: none"> - Monolithische (spröde) Software mit umständlichen Updates für neue Geräte/ Apps/Fixes - Erhöhtes Update-Risiko
Flexibilität bei der Bereitstellung	<p>● ● ● ● ●</p> <ul style="list-style-type: none"> - Skalierung von den größten bis zu den kleinsten Unternehmen für schnelle Updates - Aktivierung mit einem Klick für optimierte Rollouts - LAN-, Wi-Fi- und WAN Assurance ermöglicht umfassendes Lebenszyklus-Management 	<p>● ● ● ○ ○</p>	<p>● ● ● ○ ○</p> <p>Virtuelle Controller, die in Co-Location-Datencentern gehostet werden</p>	<p>● ● ● ● ○</p> <p>Viele Implementierungsoptionen</p>	<p>● ● ● ○ ○</p>	<p>● ● ● ○ ○</p> <ul style="list-style-type: none"> - Controller/Gateway für Großkunden - Aruba Central für kleine bis mittlere Unternehmen - Monolithische Architektur - Bietet On-Premise- und Cloud-Lösungen - Wird mit verschiedenen Anwendungen angeboten.
Mehrfachmandantenfähigkeit	<p>● ● ● ● ○</p> <ul style="list-style-type: none"> - Hierarchisch für mehrere Anbieter, Unternehmen und Abteilungen, alles über ein Conductor-Konto mit konfigurierbarer RBAC - Wechsel zwischen Umgebungen ist mit einer Benutzeranmeldung möglich - Wi-Fi- und Assurance-Leistungen von Juniper Mist sind auch mit einer Anmeldung mehrmandantenfähig 	<p>● ● ● ○ ○</p> <ul style="list-style-type: none"> - Cloud-Gateways für mehrere Mandanten und Orchestratoren (Skalierungs-Rating, bei dem die Unterstützung mehrerer Mandanten viele On-Premise-Softwareinstanzen erfordert) - LAN nicht verfügbar 	<p>● ● ● ○ ○</p> <ul style="list-style-type: none"> - Ein vSmart pro Kunde und begrenzte Anzahl von Kunden pro vBond und vManage - Alternativ angebotene Option Meraki ist nicht mehrmandantenfähig 	<p>● ● ● ● ○</p> <ul style="list-style-type: none"> - Auf Mehrfachmandantenfähigkeit bei Service Providern ausgelegt - Keine Hierarchie - LAN nicht verfügbar 	<p>● ● ● ● ○</p> <ul style="list-style-type: none"> - Bereitstellung von administrativen Domänen (ADOMs) und Verwendung mit FortiManager - Eine mehrmandantenfähige Ebene für Anbieter und Kunden, Wechsel zwischen beiden Ansichten erfordert aber separate Anmeldung 	<p>● ○ ○ ○ ○</p> <p>Eingeschränkte RBAC und keine mehrschichtige Mandantenverwaltung</p>

Vom Client bis zur Cloud

Ihre SD-WAN Lösung sollte einen kompletten Überblick über die Benutzererfahrung bereitstellen, vom Client bis zur Cloud. Daher muss eine Komplettlösung Einblicke und Fehlerbehebungsmöglichkeiten von dem Moment an bieten, in dem sich Benutzer mit dem WLAN verbinden und ihr Datenverkehr durch das LAN und dann hinaus ins WAN geführt wird. Sie sollte über alle diese Verbindungen hinweg Korrelationen mit dem Netzwerk herstellen und Probleme lösen, wie zum Beispiel: „Warum stürzt mein Zoom-Gespräch ab?“ Diese Tabelle enthält einen ganzheitlichen Überblick über AIOps, Benutzererfahrung und Sicherheit im gesamten Netzwerk – vom Client bis zur Cloud.



Mehrwertversprechen	JUNIPER NETWORKS	vmware®	CISCO	VERSA NETWORKS	FORTINET®	Hewlett Packard Enterprise
AIOps, vom Client bis zur Cloud Vereinfacht Operationen und ermöglicht IT-Teams die Verbesserung der Benutzerfreundlichkeit	<p>● ● ● ● ●</p> <p>Einblicke und automatisierte Fehlerbehebung mit Juniper Mist KI korreliert über alle Punkte im Netzwerk hinweg</p> <p>Was ist AIOps? KI und ML</p>	<p>● ○ ○ ○ ○</p> <p>Nyansa-Produkt soll für Absicherung sorgen</p>	<p>○ ○ ○ ○ ○</p> <p>Keine KI/AIOps</p>	<p>○ ○ ○ ○ ○</p> <p>Keine KI/AIOps</p>	<p>○ ○ ○ ○ ○</p> <p>Keine KI/AIOps</p>	<p>● ○ ○ ○ ○</p> <ul style="list-style-type: none"> - Basisfunktionen: eher Empfehlungen als Abhilfe, mit vielen Dashboards, sodass der Benutzer Netzwerkprobleme selbst lösen muss - Kein VNA, fehlende Zeit für effektives ML
Rundum-Benutzererfahrung vom Client bis zur Cloud KI sorgt für eine großartige Erfahrung des Benutzer sicher, vom Client zur Cloud	<p>● ● ● ● ●</p> <ul style="list-style-type: none"> - Wi-Fi-, LAN- und WAN-Assurance mit Juniper Mist KI garantiert jederzeit optimale Benutzerfreundlichkeit - Juniper Mist Cloud Services - Juniper WAN Assurance 	<p>● ○ ○ ○ ○</p> <p>Nyansa-Produkt soll für Absicherung sorgen</p>	<p>● ○ ○ ○ ○</p> <p>Sehr beschränkte Einblicke in die Benutzererfahrung</p>	<p>● ○ ○ ○ ○</p> <p>Keine KI/AIOps</p>	<p>○ ○ ○ ○ ○</p> <p>Keine KI/AIOps</p>	<p>● ○ ○ ○ ○</p> <ul style="list-style-type: none"> - Sehr beschränkte Einblicke in die Benutzererfahrung - Viele Funktionen erfordern CLI-Vorlagen

Mehrwertversprechen



<p>Sicherheit vom Client bis zur Cloud</p> <p>Jenseits des Perimeter, für alle Geräte und Clouds, Schutz gegen Zero-Day-Bedrohungen</p>	<p>● ● ● ● ●</p> <p>Durch Juniper Connected Security und Zero-Trust-Funktionen sind alle Anwendungen, Benutzer Geräte, und Daten geschützt und sicher vor allen Bedrohungen</p>	<p>● ○ ○ ○ ○ ○</p> <ul style="list-style-type: none"> - Kein etablierter Sicherheitsanbieter - Muss sich für vollständige, moderne Sicherheit auf externe Technologien verlassen 	<p>● ● ● ● ● ○</p> <p>ISE und Stealthwatch Integration mit OpenDNS</p>	<p>● ○ ○ ○ ○ ○</p> <ul style="list-style-type: none"> - Kein etablierter Sicherheitsanbieter - Muss sich für vollständige, moderne Sicherheit auf externe Technologien verlassen 	<p>● ● ● ● ● ●</p>	<p>● ○ ○ ○ ○ ○</p> <ul style="list-style-type: none"> - Kein etablierter Sicherheitsanbieter - Muss sich für vollständige, moderne Sicherheit auf externe Technologien verlassen
<p>Integriertes verdrahtetes Access Switching</p>	<p>● ● ● ● ● ●</p> <p>Jupiter Mist KI konfiguriert und orchestriert alle Aspekte des WAN der EX-Serie, unterstützt alle Campus-Architekturen einschließlich Virtual Chassis, ESI-LAG, MC-LAG oer EVPN-VXLAN</p>	<p>○ ○ ○ ○ ○ ○</p> <p>Kein LAN-Management</p>	<p>● ● ● ● ● ○</p> <p>Kunden müssen zwischen zwei Lösungstypen wählen: Softwaredefinierter oder Cloud-basierter Zugang</p>	<p>○ ○ ○ ○ ○ ○</p> <p>Kein LAN-Management</p>	<p>● ● ● ○ ○ ○ ○</p> <p>Beschränkte Switching-Plattformen mit leistungsschwacher Stacking-Lösung</p>	<p>● ● ● ● ○ ○</p> <ul style="list-style-type: none"> - Controller/Gateway mit sehr begrenzten Einblicken in WAN-Erfahrung - Viele Funktionen erfordern CLI-Vorlagen - Dynamische Port-Konfiguration erfordert ClearPass und Mobilitäts-Controller mit herstelleregebundenen Architekturen - Port-Profilen erfordern viele manuelle Konfigurationen
<p>Integriertes WLAN</p> <p>Unter mist.com/compare-wlan-solutions/ werden die anderen WLAN-Aspekte (außer Integration) im Detail verglichen.</p>	<p>● ● ● ● ● ●</p> <p>Erstklassiger Betrieb KI-gestützter WAN- und BLE-Standorttechnologien, Konfiguration mit Juniper Mist KI, KI-Unterstützung bei Einblicken, Überwachung und Fehlerbehebung</p>	<p>○ ○ ○ ○ ○ ○</p> <p>Kein LAN- oder WLAN-Management</p>	<p>● ● ● ● ● ○</p> <ul style="list-style-type: none"> - Trennung zwischen Meraki und DNA - Keine echte AIOps-Lösung für Einblicke, Überwachung und Fehlerbehebung 	<p>○ ○ ○ ○ ○ ○</p> <p>Kein LAN- oder WLAN-Management</p>	<p>● ● ● ● ○ ○</p> <ul style="list-style-type: none"> - Integriertes WLAN-Management, aber keine starke Position im WLAN-Marktsegment - Keine echte AIOps-Lösung für Einblicke, Überwachung und Fehlerbehebung 	<p>● ● ● ● ○ ○</p> <p>Keine echte AIOps-Lösung für Einblicke, Überwachung und Fehlerbehebung</p>



Hauptsitz und Sitz des Vertriebs
 Juniper Networks, Inc.
 1133 Innovation Way
 Sunnyvale, CA 94089 USA
Telefon: +1 888 586 4737
oder +1 408 745 2000
Fax: +1 408 745 2100
www.juniper.net/de/de

Hauptniederlassung für die Regionen APAC und EMEA
 Juniper Networks International B.V.
 Boeing Avenue 240
 1119 PZ Schiphol-Rijk
 Amsterdam, Niederlande
Telefon: +31 0207 125 700
Fax: +31 0207 125 701

Copyright 2021. Juniper Networks, Inc. Alle Rechte vorbehalten. Juniper Networks, das Juniper Networks Logo, Juniper und Junos sind eingetragene Marken von Juniper Networks, Inc. in den USA und anderen Ländern. Alle anderen Marken, eingetragenen Marken, Servicemarken und eingetragenen Servicemarken sind Eigentum ihrer jeweiligen Inhaber. Eine Haftung durch Juniper Networks für fehlerhafte Angaben in diesem Dokument wird ausgeschlossen. Juniper Networks behält sich das Recht vor, diese Veröffentlichung ohne Ankündigung zu ändern, zu übertragen oder anderweitig zu überarbeiten.