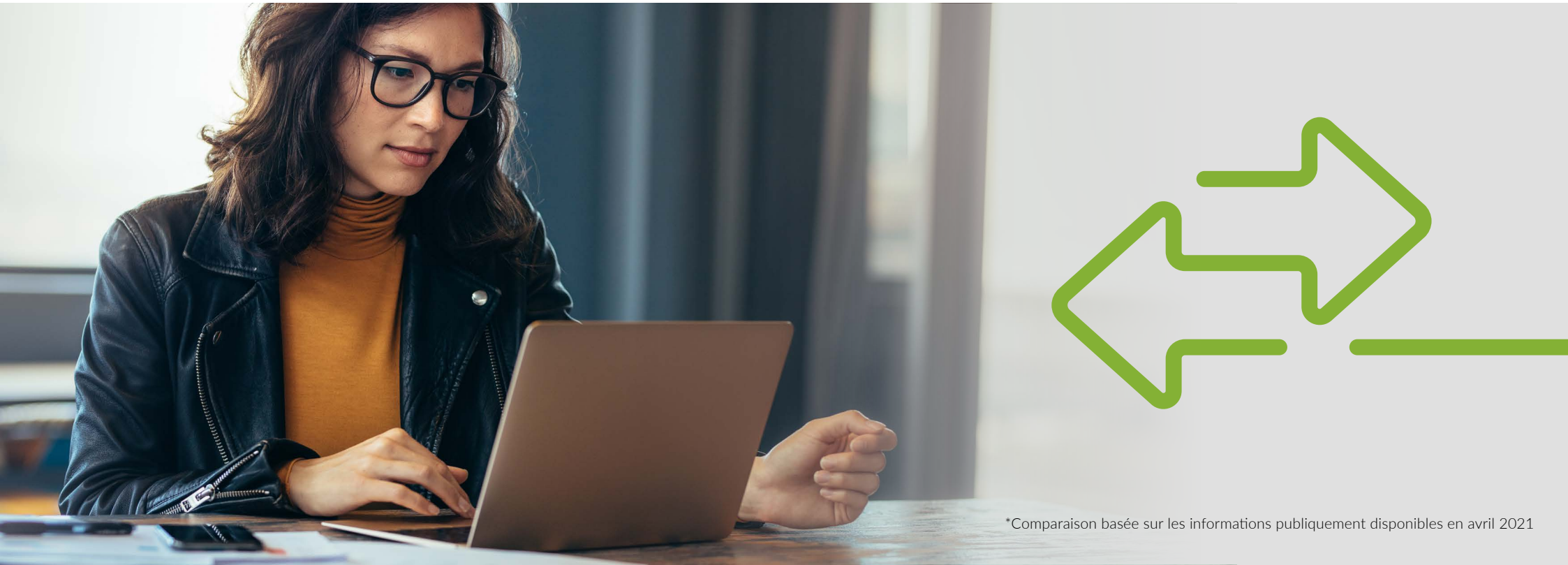
JUNIPER NETWORKS | Engineering Simplicity

Comparaison des solutions SD-WAN, du client jusqu'au cloud

Toutes les solutions SD-WAN proposées aux entreprises ne se valent pas. De nombreuses comparaisons de SD-WAN se focalisent sur quelques caractéristiques seulement, et passent à côté de leur finalité principale, qui vise à offrir une meilleure expérience utilisateur, à simplifier les opérations et à protéger l'ensemble de vos sites, du client jusqu'au cloud. Le SD-WAN que vous choisirez doit prendre en charge vos activités au-delà du WAN, et reposer sur une structure qui consolide l'ensemble de l'entreprise.

Après ces précisions, comparons ces solutions selon la diversité et l'efficacité de leurs fonctionnalités*



*Comparaison basée sur les informations publiquement disponibles en avril 2021

Intelligence artificielle pour les opérations réseau (AIOps)

L'industrie du réseau est en train de changer de paradigme : elle abandonne petit à petit l'exploitation CLI des réseaux, traditionnelle et dépassée, pour une approche AIOps automatisée. Avec la prolifération des équipements, des utilisateurs, des applications, de la bande passante, de l'IoT et autres, il n'est tout simplement plus possible de se référer aux fichiers journaux seuls pour comprendre et dépanner les problèmes réseau. Avec l'AIOps, vous vous appuyez sur l'intelligence artificielle et le machine learning pour détecter et résoudre les problèmes difficilement identifiables tout en suivant le rythme de la numérisation d'aujourd'hui.

Proposition de valeur	Juniper Networks	VMware	Cisco	Versa Networks	Fortinet	Hewlett Packard Enterprise
Fonctionnalités AIOps	●●●●● – WAN Assurance de Juniper Mist, visibilité sur l'expérience des utilisateurs finaux et MTTR plus court – Assistant de réseau virtuel MARVIS	●○○○○ La solution Nyansa vise à apporter une assurance	○○○○○ Pas d'IA/d'AIOps	○○○○○ Pas d'IA/d'AIOps	○○○○○ Pas d'IA/d'AIOps	○○○○○ ESP non intégré avec la solution Silver Peak
Niveaux de service WAN attendus (SLE) : possibilité de surveiller et d'appliquer les SLE pour les mesures clés des utilisateurs et des équipements sur le WAN **Surveillance de l'état des équipements, applications et liaisons WAN gérée par l'IA**	●●●●● – Le système SLE piloté par IA/ML assure cette fonctionnalité – IA exploitée pour guider le trafic – SLE pour l'état des liaisons WAN et des passerelles, et les expériences applicatives	●○○○○ La solution Nyansa cherche à adopter les SLE	○○○○○ Pas d'IA/d'AIOps	○○○○○ Pas d'IA/d'AIOps	○○○○○ Pas d'IA/d'AIOps	○○○○○ ESP non intégré avec la solution Silver Peak
Analyses pilotées par l'IA et actions assistées	●●●●● – Insights sur l'état de la périphérie WAN – Insights approfondis sur tous les aspects du WAN	●○○○○ Fonctionnalité naissante avec Nyansa	○○○○○ Pas d'IA/d'AIOps	○○○○○ Pas d'IA/d'AIOps	○○○○○ Pas d'IA/d'AIOps	○○○○○ ESP non intégré avec la solution Silver Peak
Assistant réseau virtuel (VNA) AIOps	●●●●● Intégration de Marvis et de l'IA de Mist pour l'assurance filaire, sans fil et WAN.	●○○○○ Nyansa n'a pas encore atteint cet objectif	○○○○○ Pas d'IA/d'AIOps	○○○○○ Pas d'IA/d'AIOps	○○○○○ Pas d'IA/d'AIOps	○○○○○ ESP non intégré avec la solution Silver Peak

La sécurité et le SASE en action

Vous devez sécuriser l'ensemble de votre entreprise, y compris sur le WAN. La sécurité doit faire partie intégrante de l'infrastructure et non pas être ajoutée ultérieurement. Qu'il s'agisse d'une approche zero-trust ou de la protection contre la propagation latérale des menaces, votre SD-WAN doit appliquer des stratégies de sécurité sur l'ensemble du réseau de manière simple et efficace.

Proposition de valeur	Juniper Networks	VMware	Cisco	Versa Networks	Fortinet	Hewlett Packard Enterprise
Sécurité zero-trust incorporée à la couche réseau	●●●●● – La seule structure zero-trust qui simplifie le contrôle des accès, la segmentation et la directivité (suivi des directions et mise en application des stratégies d'activité) – Stratégie axée sur le SASE et routage intégré	○○○○○ Pas de sécurité zero-trust sur leur couche réseau	○○○○○ Pas de sécurité zero-trust sur leur couche réseau	○○○○○ Pas de sécurité zero-trust sur leur couche réseau	○○○○○ Pas de sécurité zero-trust sur leur couche réseau	○○○○○ Pas de sécurité zero-trust sur leur couche réseau
Protection des utilisateurs, des charges de travail, et contre la propagation latérale des menaces	●●●●● La gamme complète comprend la sécurité des utilisateurs, la sécurité IoT, la protection contre les menaces zero-day et contre le phishing.	○○○○○ La sécurité repose sur l'ajout de technologies et d'équipements provenant de partenaires qui sont de plus en plus en concurrence avec VMware. La stratégie de sécurité n'est pas contrôlée par le logiciel VMware.	●●●○○ Les fonctionnalités de sécurité dépendent fortement des plates-formes de site distant utilisées [vEdge est un redirecteur DNS vers le cloud Cisco Umbrella]	●●○○○	●●●●●	●○○○○ La sécurité repose sur l'ajout de technologies et d' équipements provenant de partenaires qui, de plus en plus souvent, sont en concurrence avec Silver Peak.
Gestion centralisée des stratégies de classe entreprise	●●●●● Gamme complète de stratégies centralisées et mise en application à la périphérie	○○○○○ Fonctionnalité naissante avec Nyansa	●●●○○ Pas d'IA/d'AIOps	●●●●● Pas d'IA/d'AIOps	●●●●● Pas d'IA/d'AIOps	○○○○○ ESP non intégré avec la solution Silver Peak
Visibilité sur les menaces et analyse des applications, utilisateurs et équipements	●●●●● Visibilité totale sur les utilisateurs grâce aux applications d'IA et de ML, avec un flux en temps réel sur les menaces et les utilisateurs	○○○○○ VMware s'appuie sur des solutions de sécurité tierces	●●●○○ Fonctionnalités LAN d'apprentissage, de prévention et de sécurité limitées pour les menaces zero-day avancées. [Un rapport récent de NSS Labs déconseille la sécurité Cisco]	●●●○○ Fonctionnalités limitées d'apprentissage et de prévention pour les menaces zero-day avancées	●●●●●	○○○○○ Pas de sécurité intégrée
Renseignements sur les menaces avancées et prévention intégrés au niveau du WAN de périphérie	●●●●● Sécurité connectée sur l'ensemble de l'infrastructure réseau sans fil, filaire et WAN	○○○○○	○○○○○	○○○○○	●●●○○	○○○○○

Capacités et performances de la périphérie WAN

Les SD-WAN doivent évoluer. La plupart des offres actuelles reposent sur des tunnels encombrants et coûteux qui manquent de sécurité, augmentent les coûts et consomment votre bande passante. La technologie Session Smart™ de Juniper est pour sa part sans tunnel, et elle s'appuie sur les sessions pour extraire des données détaillées et granulaires, au service de l'expérience utilisateur. Combinée à l'IA de Mist, elle offre un SD-WAN troisième génération, pour une expérience utilisateur optimale.

Proposition de valeur	Juniper Networks	VMware	Cisco	Versa Networks	Fortinet	Hewlett Packard Enterprise
Une conception focalisée sur l'utilisateur, optimisée pour l'expérience utilisateur	●●●●● – Technologie basée sur les sessions, pour une meilleure expérience utilisateur – Une visibilité approfondie de chaque session, des insights et un routage granulaire précis, en fonction des applications – Réduit la latence jusqu'à 60 %	○○○○○ Les approches traditionnelles se concentrent sur le réseau, et non sur la session de l'utilisateur	○○○○○ Les approches traditionnelles se concentrent sur le réseau, et non sur la session de l'utilisateur	○○○○○ Les approches traditionnelles se concentrent sur le réseau, et non sur la session de l'utilisateur	○○○○○ Les approches traditionnelles se concentrent sur le réseau, et non sur la session de l'utilisateur	○○○○○ Les approches traditionnelles se concentrent sur le réseau, et non sur la session de l'utilisateur
Économies SD-WAN/de bande passante	●●●●● Une architecture sans tunnel/ SVR pour une réduction des coûts, ce qui permet d'économiser 30 à 50 % de la bande passante et de réduire jusqu'à 75 % les frais d'infrastructure.	○○○○○ Approche basée sur les tunnels, grosse consommation de bande passante	○○○○○ Approche basée sur les tunnels, grosse consommation de bande passante	○○○○○ Approche basée sur les tunnels, grosse consommation de bande passante	○○○○○ Approche basée sur les tunnels, grosse consommation de bande passante	○○○○○ Approche basée sur les tunnels, grosse consommation de bande passante
Chiffrement intelligent : la plupart des applications sont chiffrées par défaut, comme le trafic HTTPS (évitez le double chiffrement si possible)	●●●●● Le chiffrement adaptatif de Session Smart préserve la bande passante : si le trafic de l'application est déjà chiffré, il n'est pas nécessaire de le chiffrer à nouveau	○○○○○ Chiffrement non intelligent	○○○○○ Chiffrement non intelligent	○○○○○ Chiffrement non intelligent	○○○○○ Chiffrement non intelligent	○○○○○ Chiffrement non intelligent
CPE universels	●●●●● Le NFX Series de Juniper propose une connectivité et une évolutivité complètes, largement reconnues et exploitées	●●●●○ Dell EMC Edge appliance	●●●●○ Cisco 5000 ENCS	○○○○○ Pas de portefeuille CPE universel	○○○○○ Pas de portefeuille CPE universel	○○○○○ Pas de portefeuille CPE universel
Périphérie SD-WAN pour tout déploiement (prise en charge de déploiements de petite et moyenne tailles)	●●●●● La vaste gamme de Juniper comprend aussi bien des équipements de bureau que des équipements pour grands campus/ entreprises.	●●○○○ Équipement de périphérie WAN avec capacités de routage limitées	●●●●○ Large éventail de produits, mais différentes lignes de produit avec des solutions de gestion différentes	●●○○○ Offre limitée pour les filiales, quelques options whitebox	●●●●● Une conception ASIC sur mesure apporte de hautes performances	●●○○○ Capacités de routage limitées
Mesure de l'intégrité des liaisons et des applications	●●●●● Capacités avancées avec Juniper Paragon (Netrounds)	●●●○○ Passif	●●●○○ Actif	●●●○○ Actif	●●●○○ Actif	●●●○○ Actif
Conception robuste de la périphérie WAN	●●●●● Redondance à tous les niveaux (actif/actif, actif/de secours, hub de centre de données, plan de contrôle et plan de données)	●●●●●	●●●●●	●●●●●	●●●●●	●●●●●

Architecture

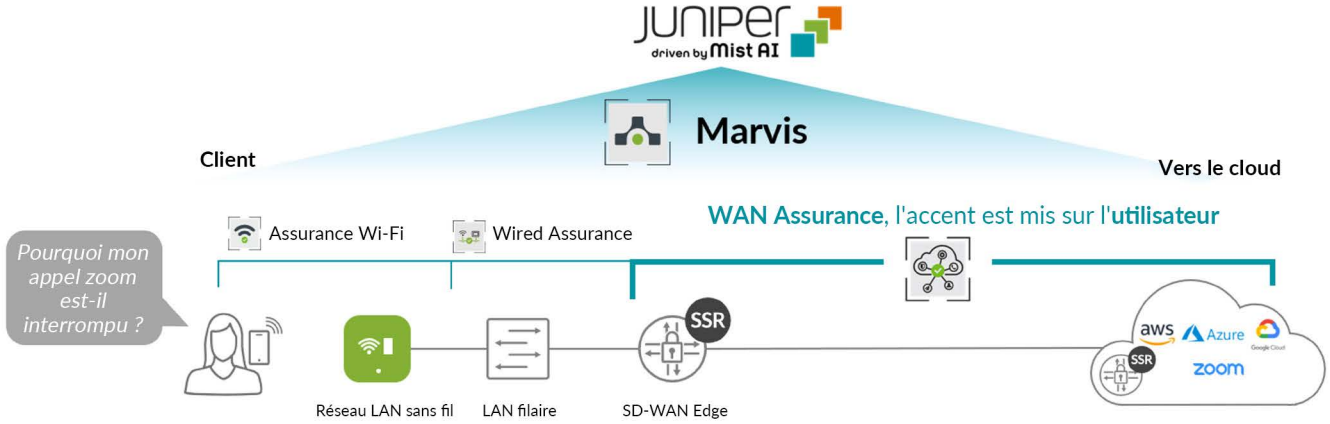
De nombreuses solutions actuelles reposent sur des architectures obsolètes, entachées par la dette technique. Une solution durable, adaptée à l'ère actuelle du cloud, doit notamment reposer sur une architecture cloud de microservices moderne. L'agilité nécessaire à votre entreprise est ainsi assurée et votre réseau peut s'adapter à vos opérations commerciales.

Proposition de valeur	Juniper Networks	VMware	Cisco	Versa Networks	Fortinet	Hewlett Packard Enterprise
Une architecture conçue pour l'ère du cloud	●●●●● Une architecture cloud de microservices moderne – Conteneurisation des services – Mises à jour des fonctionnalités rapides et à faibles risques – Correctifs de bogues en temps quasi-réel, sans interruption du réseau	●●○○○ Cloud première génération	●●○○○ **Meraki :** – Cloud première génération – Base de données héritée partagée dans un « cloud » de base de données hébergé – Basé sur un contrôleur virtuel **Cisco :** – Architecture logicielle monolithique héritée basée sur un contrôleur – Absence de solution cloud robuste, limité aux PME – De nombreux équipements/ boîtes, chacun nécessitant des versions qui leur sont propres – Plusieurs produits et systèmes d'exploitation non intégrés (+ de 10)	●●○○○ Cloud première génération	●○○○○ Offre de cloud fragmentée	●●○○○ Aruba ESP est une refonte d'Aruba Central intégrant des fonctions de gestion – L'architecture basée sur un contrôleur comporte quatre clouds différents – Les utilisateurs doivent mettre à niveau, maintenir et intégrer tous les logiciels – Les bases de code monolithiques sont difficiles à gérer et leur évolutivité est coûteuse – Prise en charge limitée des API
Évolutivité : les bases de code monolithiques sont difficiles à gérer et leur évolutivité est coûteuse	●●●●● 3 fois plus évolutif que toute autre solution SD-WAN – Évolutivité flexible, tant horizontalement que verticalement – Pas d'équipement coûteux requis – Une seule image logicielle simplifie la planification des déploiements et les processus de mise à niveau	●●●○○ L'évolutivité multi-utilisateur et multi-site nécessite d'ajouter beaucoup d'orchestrateurs et de passerelles.	●●●●○ – L'évolutivité est complexe et nécessite vManage, vBond et vSmart pour être gérée dans les plans de gestion et de contrôle. – Cisco recommande Meraki pour le Lean IT : son SD-WAN complet demande une refonte logicielle et matérielle	●●●●○ Affirme actuellement pouvoir prendre en charge 5 000 CPE	●●●●● Affirme que FortiManager prend en charge 100 000 sites – Cela n'a pas été publiquement testé et corroboré – Ne concerne que le plan de gestion de la solution	●●●●○ Évolutivité basée sur les performances de cloud VPC
Polyvalence de l'automatisation (API, plugins d'extension)	●●●●● – Simple, 100 % piloté par API – API et modèles de configuration – Les clients peuvent créer leurs propres plugins à des fins d'extensibilité – Intégration avec Splunk et ServiceNow	●●○○○ API basiques pour Velocloud Orchestrator	●●●●○ API Rest disponibles avec le support DevNet	●●●●○ API Rest	●●●●○ Complexité causée par la dépendance à plusieurs modules Python	●●●○○ API RESTful disponibles

Proposition de valeur	Juniper Networks	VMware	Cisco	Versa Networks	Fortinet	Hewlett Packard Enterprise
Agilité	●●●●● – Cloud moderne basé sur des microservices plutôt que sur un codebase monolithique – Mises à jour rapides sans perturbation du réseau	●●○○○ – Cloud première génération – Pas d'architecture basée sur les microservices	●●○○○ **Meraki :** – Cloud première génération avec des machines virtuelles et des hyperviseurs – Mises à jour lentes en raison d'une absence d'architecture de microservices moderne **Cisco :** – Logiciel monolithique (fragile) avec une capacité de mise à jour réduite pour les nouveaux équipements/applications/correctifs – Mises à jour risquées	●●○○○ – Cloud première génération – Pas d'architecture basée sur les microservices	●○○○○ Offre de cloud fragmentée	●●○○○ – Logiciel monolithique (fragile) avec une capacité de mise à jour réduite pour les nouveaux équipements/applications/correctifs – Mises à jour risquées
Flexibilité des déploiements	●●●●● – S'adapte aux besoins des entreprises de toutes tailles pour des mises à jour rapides – Activation en un clic pour des déploiements simplifiés – Assurance filaire, Wi-Fi et WAN pour une gestion du cycle de vie complet	●●●○○	●●●○○ Contrôleurs virtuels hébergés dans des centres de données colocalisés	●●●●○ Plusieurs options pour le déploiement	●●●○○	●●●○○ – Contrôleur/passerelle pour les grandes entreprises – Aruba Central pour les PME – Architecture monolithique – Offre des solutions sur site et cloud – Disponible sur diverses applications
Mutualisation	●●●●○ – Hiérarchique pour plusieurs fournisseurs, entreprises et services, tous à partir d'un compte conducteur géré dans le cloud avec RBAC configurable – Possibilité de passer d'un environnement à l'autre avec une seule connexion utilisateur – Le Wi-Fi et les services d'assurance Mist sont également multi-utilisateurs avec une connexion unique	●●●○○ – Passerelles et orchestrateurs cloud mutualisés (voir la notation « Évolutivité » : l'accueil de plusieurs locataires nécessite plusieurs instances logicielles sur site) – LAN : S/O	●●●○○ – Un vSmart par client et nombre limité de clients par vBond et par vManage – Avec l'option alternative Meraki, la mutualisation n'est pas possible	●●●●○ – Conçu pour la mutualisation des fournisseurs de services – Pas de hiérarchie – LAN : S/O	●●●●○ – Fournit des domaines administratifs (ADOM) et utilisé avec Fortimanager – Un niveau unique de mutualisation fournisseur et client, mais passer de l'une à l'autre de ces vues nécessite une reconnexion	●○○○○ RBAC limité et pas de gestion d'utilisateur multi-niveau

Du client jusqu'au cloud

Votre solution SD-WAN doit vous permettre d'avoir une visibilité complète sur l'expérience de vos utilisateurs, du client jusqu'au cloud. C'est pourquoi il vous faut une solution complète, capable de fournir des analyses et d'assurer le dépannage dès que vos utilisateurs se connectent au Wi-Fi, qui transmet le trafic à votre réseau filaire, puis au WAN. Elle doit pouvoir établir des relations entre toutes ces connexions réseau et résoudre des problèmes comme « Pourquoi mon appel Zoom a-t-il été interrompu ? ». Ce tableau offre une vue globale de l'AIOps, de l'expérience utilisateur et de la sécurité sur l'ensemble du réseau. Du client jusqu'au cloud.



Proposition de valeur	Juniper Networks	VMware	Cisco	Versa Networks	Fortinet	Hewlett Packard Enterprise
AIOps, du client jusqu'au cloud **Simplifie les opérations et donne aux équipes informatiques les moyens d'offrir une expérience utilisateur de qualité.**	●●●●● L'IA Mist vous offre un dépannage et des insights automatisés qui mettent en corrélation tous les points du réseau Qu'est-ce que l'AIOps ? IA et machine learning	●○○○○ La solution Nyansa vise à apporter une assurance	○○○○○ Pas d'IA/d'AIOps	○○○○○ Pas d'IA/d'AIOps	○○○○○ Pas d'IA/d'AIOps	●○○○○ – Capacités de base : des recommandations plutôt que des mesures correctives, avec de nombreux tableaux de bord permettant à l'utilisateur de résoudre lui-même les problèmes de réseau – Pas d'assistant réseau virtuel et manque de temps pour un machine learning efficace
Expérience utilisateur, du client jusqu'au cloud **Une IA qui garantit que vos utilisateurs bénéficient d'une excellente expérience, du client jusqu'au cloud**	●●●●● – Les assurances Wi-Fi, filaire et WAN pilotées par l'IA de Mist garantissent une expérience optimale pour chaque utilisateur, à chaque instant. – Services Mist Cloud de Juniper – Assurance WAN de Juniper Mist	●○○○○ La solution Nyansa vise à apporter une assurance	●○○○○ Visibilité très limitée sur l'expérience des utilisateurs	●○○○○ Pas d'IA/d'AIOps	○○○○○ Pas d'IA/d'AIOps	●○○○○ – Une visibilité très limitée sur l'expérience des utilisateurs – De nombreuses fonctionnalités exigent des modèles CLI

Proposition de valeur	Juniper Networks	VMware	Cisco	Versa Networks	Fortinet	Hewlett Packard Enterprise
Sécurité, du client jusqu'au cloud **Au-delà du périmètre, vers tous les équipements/clouds ; protection contre les menaces de type zero-day**	●●●●● Les fonctionnalités Juniper Connected Security et zero-trust garantissent que toutes les applications, tous les utilisateurs, tous les équipements et toutes les données sont sécurisés et protégés contre toutes les menaces.	●○○○○ – Fournisseur de sécurité non établi – Technologie tierce nécessaire pour une sécurité avancée complète	●●●●○ Intégration ISE et Stealthwatch avec OpenDNS	●○○○○ – Fournisseur de sécurité non établi – Technologie tierce nécessaire pour une sécurité avancée complète	●●●●●	●○○○○ – Fournisseur de sécurité non établi – Technologie tierce nécessaire pour une sécurité avancée complète
Commutation d'accès filaire intégrée	●●●●● L'IA de Mist configure et exploite tous les aspects du réseau d'accès filaire de la gamme EX Series, en prenant en charge toutes les architectures de campus, y compris Virtual Chassis, ESI-LAG, MC-LAG, ou EVPN-VXLAN	○○○○○ Pas de gestion LAN	●●●●○ Les clients doivent choisir entre deux types de solutions : accès défini par logiciel ou basé sur le cloud	○○○○○ Pas de gestion LAN	●●○○○ Plates-formes à commutation limitée avec une solution de pile inférieure	●●●○○ – Contrôleur/passerelle pour une analyse étendue mais limitée de l'expérience filaire – De nombreuses fonctionnalités exigent des modèles CLI – Configuration de port dynamique nécessitant le contrôleur ClearPass et de mobilité, avec des architectures de dépendance – Les profils de ports exigent une longue configuration manuelle
Wi-Fi intégré Consultez **mist.com/compare-wlan-solutions/** pour une comparaison plus détaillée du sans fil au-delà de l'intégration	●●●●● IA Mist pour exploiter et configurer la technologie de géolocalisation BLE sans fil, avec des analyses, une surveillance et des mesures correctives pilotées par l'intelligence artificielle.	○○○○○ Pas de gestion LAN ou sans fil	●●●●○ – Partagé entre Meraki et DNA – Absence d'une véritable solution AIOps pour l'analyse, la surveillance et les mesures correctives	○○○○○ Pas de gestion LAN ou sans fil	●●●○○ – Gestion Wi-Fi entièrement intégrée, mais pas de proposition de mise en réseau sans fil sérieuse – Absence d'une véritable solution AIOps pour l'analyse, la surveillance et les mesures correctives	●●●○○ Absence d'une véritable solution AIOps pour l'analyse, la surveillance et les mesures correctives

Juniper Networks | Engineering Simplicity

Siège social et commercial
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089, États-Unis
Téléphone : 888.JUNIPER (888.586.4737) ou +1.408.7452000
Fax : +1.408.745.2100

www.juniper.net
Siège EMEA et APAC
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Pays-Bas
Téléphone : +31 0 207 125 700
Fax : +31.0.207.125.701

PN : 7400122- 002-FR