

**aruba**

a Hewlett Packard  
Enterprise company

# Aruba Edge Services Platform (ESP)

Le réseau sécurisé  
pour l'ère du Cloud !

# Introduction

Avec une distribution toujours plus grande du réseau, les solutions de sécurité périmétrique ne sont plus suffisantes. L'avènement du télétravail ou l'adoption croissante d'objets connectés (IoT) dans bon nombre de pans de l'économie, ont changé la donne et les services hébergés dans le Cloud continuent de séduire toujours plus d'entreprises.

Ces évolutions rendent impérieuse la révision des schémas de transport traditionnels, qui consistent à transiter tout le trafic des succursales vers le siège, en utilisant des MPLS et des VPN, pour tendre vers une architecture Service d'Accès Sécurisé Edge (SASE) cloud native, qui dynamise les services réseaux et les sécurise de bout en bout.

Pour exploiter tout le potentiel du cloud et de la transformation numérique, les entreprises ont besoin d'une nouvelle périphérie WAN qui combine la sécurité sur site et dans le cloud, en protégeant les utilisateurs, physiques ou logiques, qui se connectent à des plateformes SaaS et cloud, et en appliquant une stratégie de sécurité ZeroTrust basée sur le profil d'utilisation et le contexte.

Grâce à Aruba ESP, les entreprises ont désormais la possibilité d'appliquer une politique de sécurité granulaire basée sur l'identité, du Edge au cloud, afin de connecter et de protéger les utilisateurs ainsi que les appareils de bout en bout.

## Sommaire

✓ **Aruba ESP, la plateforme cloud-native d'Aruba pour l'Intelligent Edge**  
p. 3

✓ **Avec EdgeConnect, Aruba ESP offre une sécurité réseau complète, combinant Zero Trust et SASE**  
p. 7

✓ **3 questions à... Fernando Rynne, Field and Channel Marketing Manager, HPE**  
p. 10

# 1 Aruba ESP, la plateforme cloud-native d'Aruba pour l'Intelligent Edge

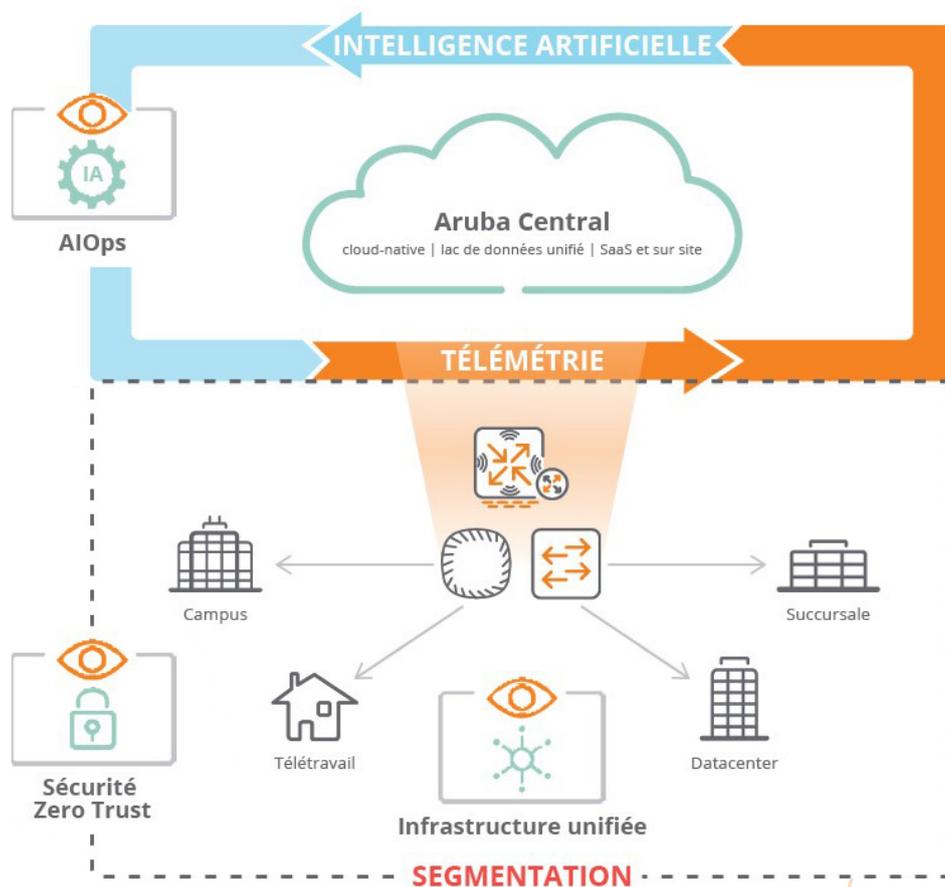
Dans des environnements Edge de plus en plus distribués et, de fait, complexes, les enjeux de performances, de visibilité et de sécurité des réseaux ont drastiquement augmenté. Aruba ESP permet aux entreprises de gérer le réseau à l'aide d'une plateforme cloud-native, en simplifiant les opérations réseau grâce à l'automatisation pilotée par l'IA et ainsi rendre dynamique et véritablement exploitable la puissance de l'Edge.

## Edge Services Platform

Aruba ESP est conçu pour unifier, automatiser et sécuriser l'Edge. Combinant des AIOps (l'intelligence artificielle au service des opérations), une sécurité Zero Trust et une infrastructure unifiée, Aruba ESP offre une grande flexibilité de consommation.

ESP aide les entreprises et leurs services IT à : identifier et résoudre rapidement les problèmes de façon proactive, protéger l'entreprise face aux

menaces dans un périmètre de sécurité toujours plus diffus, surveiller et gérer des milliers de dispositifs filaires, sans fil et WAN partout, déployer rapidement des services réseau à grande échelle, afin de suivre l'évolution des besoins de l'entreprise et autoriser des investissements continus en infrastructure pour affronter les incertitudes financières.



Aruba ESP (Edge Services Platform).

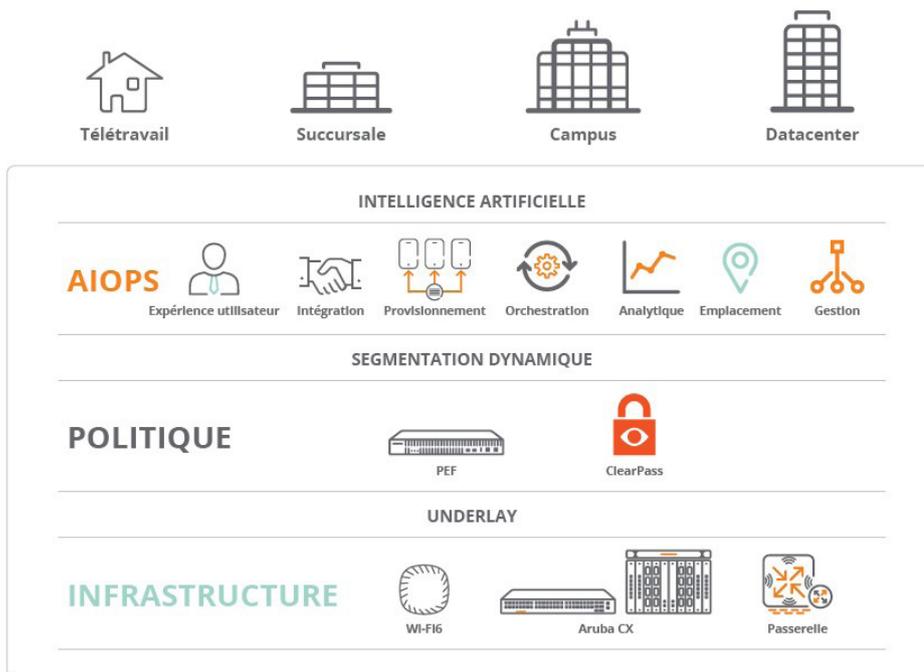
# Infrastructure unifiée

Aruba ESP offre la capacité de fournir une infrastructure unifiée qui réunit la gestion des réseaux filaires, sans fil et WAN.

Une vue unifiée et un OS identique du DC aux télétravailleurs, offre plusieurs avantages. Une meilleure efficacité grâce à une résolution des problèmes jusqu'à 90% plus rapide, une expérience utilisateur optimisée grâce à l'IA, une sécurité renforcée et dynamique, des coûts adaptés, une flexibilité, ainsi qu'une accélération

de l'innovation grâce à une intégration simplifiée, permettent de tenir les engagements qu'impliquent les enjeux modernes.

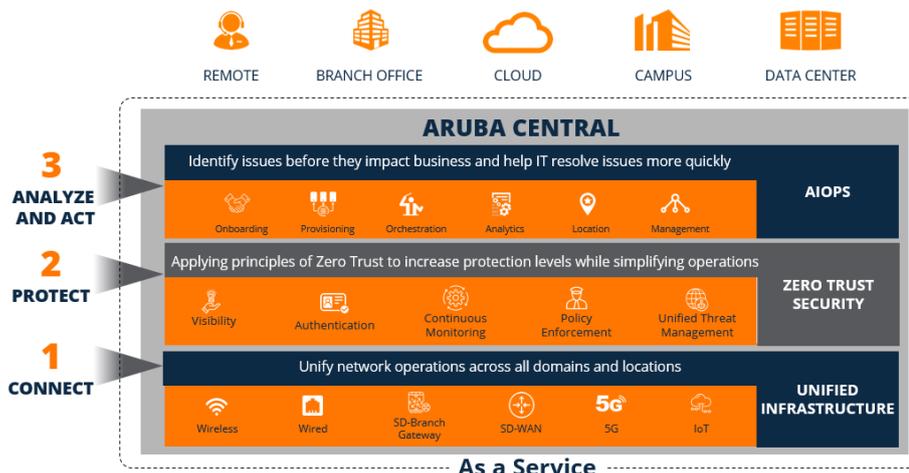
L'infrastructure unifiée d'Aruba est gérée à l'aide d'Aruba Central, une plateforme cloud-native basée sur des microservices qui fournit l'évolutivité, la disponibilité et la résilience requises pour les environnements stratégiques à travers l'Edge distribué.

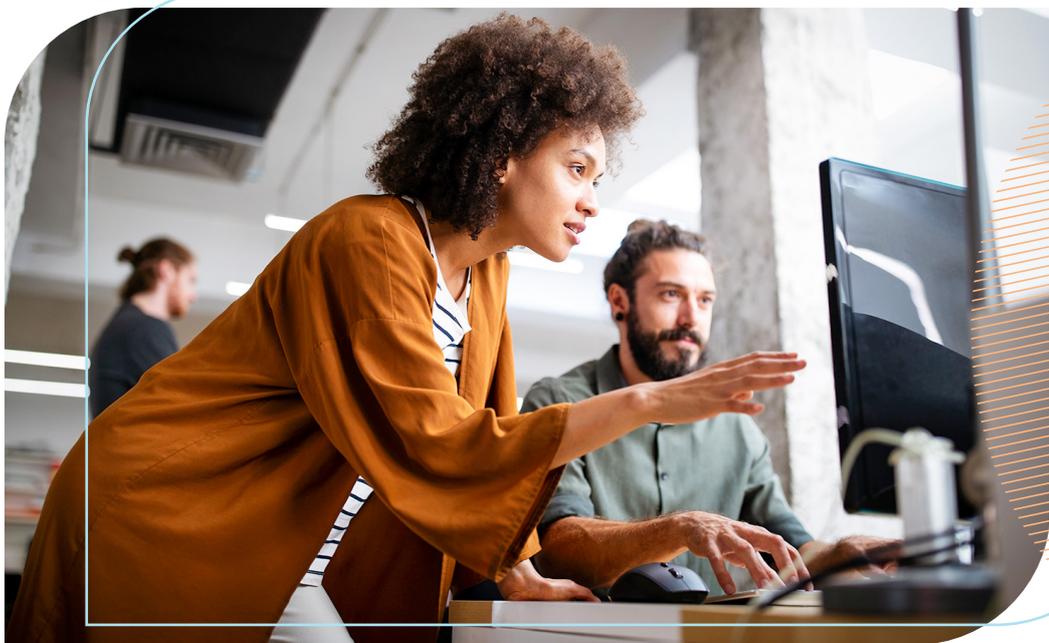


Infrastructure unifiée d'Aruba.

## ARUBA ESP ARCHITECTURE

CONNECTIVITY, SECURITY AND AIOPS CONVERT DATA INTO BUSINESS OUTCOMES



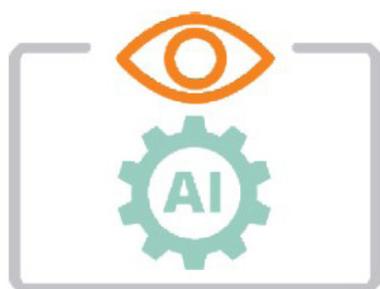


## ZeroTrust Security

Face à des attaques réseau toujours plus pernicioises dans des environnements toujours plus décentralisés et axés sur l'IoT, la solution Zero Trust est apparue comme un modèle efficace et résilient, dont les technologies matures permettent un déploiement simple.

Aruba ESP et la sécurité Zero Trust incluent une visibilité complète, une micro-segmentation du trafic et des contrôles avec accès restreints, ainsi qu'une surveillance continue. Avec l'adoption croissante de l'IoT, la visibilité totale de tous les appareils et utilisateurs sur le réseau est devenue essentielle.

La solution ClearPass d'Aruba détecte le spectre complet de ce qui se connecte ou tente de se connecter au réseau et de créer des politiques d'accès basées sur les rôles ou sur une reconnaissance via l'IA. Son ouverture lui permet d'échanger avec l'écosystème de sécurité potentiellement déjà présent et ainsi augmenter la pertinence de chacun de ces éléments stratégiques, tout en garantissant la cohérence et l'application de la politique d'accès au réseau, quel que soit le vecteur, 24 heures sur 24 et 7 jours sur 7.



### AIOps

AI Insights | Moteur d'analyse des réseaux  
User Experience Insight | Device Insight



### Infrastructure unifiée

Wi-Fi | Commutation | SD-WAN  
Cloud | 5G | Lac de données communes



### Sécurité Zero Trust

Segmentation dynamique | Application des politiques  
Pare-feu | ClearPass | Device Insight

La sécurité Zero Trust est un pilier essentiel d'Aruba ESP.

## AIOps

Aruba AIOps, intégré à Aruba Central, supprime les tâches de dépannage manuelles, réduit jusqu'à 90 % le délai moyen de résolution des problèmes réseau courants et augmente jusqu'à 25 % la capacité du réseau en monitorant des centaines de critères, à fin d'optimisation.

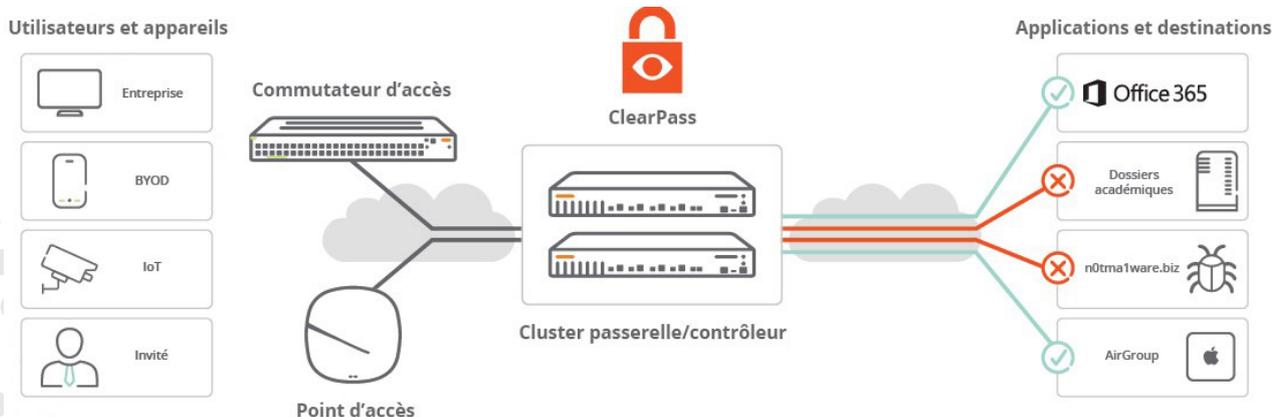
Avec Aruba AIOps, la périphérie est pilotée par l'IA, pour identifier les problèmes liés à la connectivité et à l'authentification, mais aussi déterminer la cause profonde des incidents et fournir des recommandations prescriptives avec une

précision supérieure à 95 %, et ce avant qu'ils n'aient une incidence réelle sur l'entreprise, tout en optimisant continuellement la performance grâce à l'analyse des données de déploiements et appareils réseau Aruba.

Aruba AI Ops est un outil d'aide à la prise de décision intégré à la console de management Aruba Central, permettant de faciliter la visualisation et le déploiement, sur la base d'analyses d'usage du réseau pilotées par IA, le tout mis à disposition dans une vue unifiée et personnalisable.



La sécurité en périphérie.

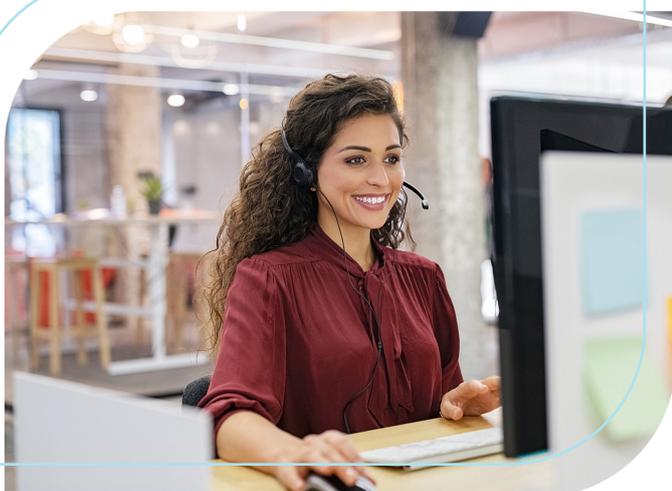


La sécurité Zero Trust est un pilier essentiel d'Aruba ESP.

# 2 Avec EdgeConnect, Aruba ESP offre une sécurité réseau complète, combinant Zero Trust et SASE

L'offre ESP d'Aruba permet donc d'avoir une vue unifiée pour les réseaux, avec une sécurité Zero Trust et une maintenance automatisée. Pour étendre son service et permettre de déployer une approche SD-WAN, ESP intègre désormais EdgeConnect, issu du rachat récent de Silver Peak.

## Contexte



### Qu'est-ce que SASE ?

**SASE (prononcez « Sassi ») ou Secure Access Service Edge (service d'accès sécurisé Edge) est une architecture qui combine des fonctionnalités WAN Edge de succursale telles que SD-WAN, routage, segmentation, pare-feu basé sur une zone et optimisation WAN à des services de sécurité cloud complets, fournis et gérés dans le cloud.**

**SASE permet d'améliorer les performances applicatives et de renforcer la sécurité du réseau à mesure que le nombre d'utilisateurs distants augmente, en intégrant la dimension Cloud.**

La transformation de la périphérie réseau continue de s'accélérer. L'architecture SASE est un modèle de plus en plus prisé par les entreprises. Si celles-ci veulent accélérer leur transformation numérique et bénéficier de toutes les possibilités du cloud, l'architecture et la sécurité doivent être liées.

Transformer les architectures WAN et de sécurité devient un impératif stratégique pour les entreprises, qui vont devoir réaliser (ou poursuivre) avec succès le passage d'une sécurité périphérique traditionnelle basée sur les datacenters à une architecture SASE centrée sur le cloud. Avec les nouveaux besoins de travailler « à partir de n'importe où », l'adoption de services hébergés

dans le cloud va continuer à s'accélérer. Les entreprises devront dès lors abandonner leur modèle traditionnel dans lequel les applications étaient hébergées dans leur datacenter et dont le trafic traversait des services MPLS privés pour y être vérifié.

Cette évolution montre la nécessité pour les entreprises de devoir, à terme, modifier les schémas de transport traditionnels et de mettre en place une architecture SASE native du cloud. Pour améliorer l'expérience utilisateur, l'adoption d'un SD-WAN Edge intelligent sera un passage obligatoire, le tout porté par une automatisation des services de sécurité

...

fournis dans le cloud. Afin de garantir la meilleure expérience utilisateur possible, le SASE met en œuvre le SD-WAN pour le routage intelligent des applications vers l'internet ou le datacenter, tout en offrant une sécurité maximale.

Il faut ajouter à cela une croissance constante des appareils IoT se connectant au réseau, qui

sont autant de défis de sécurité que le cloud n'aborde pas. Les appareils IoT étant sans agent, les services informatiques ne peuvent pas installer de clients de sécurité ou rediriger le trafic des appareils vers des services de sécurité dans le cloud. La sécurité Zero Trust doit donc être appliquée à la périphérie du WAN.

## Solution



La plateforme de contrôle d'accès ClearPass Policy Manager est désormais intégrée à EdgeConnect (la plateforme SD-WAN anciennement Silver Peak). Cela permet d'augmenter l'intelligence des applications en ajoutant la connaissance des identités des utilisateurs, des appareils IoT, des rôles et de la posture de sécurité pour former la base d'une périphérie WAN SASE et ainsi contextualiser la sécurité. La combinaison de l'intelligence des rôles et de la posture de sécurité avec des capacités avancées de segmentation dynamique élimine la complexité associée à la mise en œuvre de centaines de VLAN pour chaque classe d'utilisateurs, d'usages et d'appareils, ce qui simplifie considérablement l'administration et la gestion du réseau. L'intégration de ClearPass

### Aruba EdgeConnect

La plateforme SD-WAN EdgeConnect d'Aruba alimente un réseau WAN autonome destiné aux entreprises de type « cloud-first ». Aruba EdgeConnect est la brique SD-WAN d'ESP. Créé pour les réseaux Edge-to-cloud des entreprises d'aujourd'hui, Aruba EdgeConnect fournit une expérience de la plus grande qualité aux utilisateurs et services informatiques, quel que soit le lieu de résidence des applications.

Grâce à une approche SD-WAN de bout en bout, Aruba, avec l'intégration de Silver Peak présente ainsi une solution réseau exhaustive Edge-to-cloud prenant en charge tous les aspects des réseaux filaires, des réseaux locaux sans fil et des réseaux étendus (WAN).

**Intégration au niveau du backend : aujourd'hui, le backend pour piloter EdgeConnect est Orchestrator (anciennement Silver Peak Unity Orchestrator). EdgeConnect sera intégré à Aruba Central, qui devient l'outil de management unifié des solutions.**

Policy Manager à EdgeConnect permet de définir de manière cohérente et automatisée les rôles qui peuvent être appliqués à l'ensemble du réseau, depuis l'appareil de l'utilisateur, en passant par le LAN et le WAN.



Aruba Threat Defense est désormais également intégré à EdgeConnect afin d'enrichir les capacités de détection et de préventions des intrusions de la plateforme. Cette dernière va ainsi profiter de l'infrastructure de lutte contre les menaces d'Aruba. L'intégration de ClearPass permet également d'ajouter une brique de sécurisation, par exemple de l'IoT, lorsque l'on va connecter l'Edge au cloud. Ce partage d'informations essentielles de sécurité

entre Aruba Central et EdgeConnect promet parallèlement d'offrir une visibilité totale sur le réseau et donc d'améliorer la compréhension des comportements du cloud à l'Edge. Ces deux intégrations concrétisent finalement la transformation de EdgeConnect d'une plateforme SD-WAN en une vraie plateforme SASE adaptée à l'Edge. Sécurisée, économe, et limpide.

## Bénéfices

En utilisant SASE pour transformer les architectures de réseau WAN et de sécurité, les entreprises peuvent garantir un accès sécurisé contextuel aux applications et services sur les environnements multicloud, quels que soient l'utilisateur, l'emplacement ou l'appareil pour y accéder.

L'intégration d'EdgeConnect permet également, par exemple, d'optimiser les besoins applicatifs en fonction des environnements et des utilisateurs ou d'étendre les bénéfices de l'entreprise en étendant simplement le SI jusqu'aux télétravailleurs, pour garantir une qualité de service et une expérience utilisateur qui soient tout aussi performantes qu'au sein des bâtiments de l'entreprise.

Les entreprises pourront à la fois prendre en charge leur architecture de sécurité existante, naviguer vers le SASE pour une meilleure expérience utilisateur et relever les défis de sécurité qu'implique le déploiement massif d'IoT. Elles pourront également s'orienter vers des systèmes « best-of-breed », en choisissant une stratégie de partenariat multifournisseurs, car l'écosystème de partenaires de sécurité d'Aruba ESP offre aux entreprises la liberté de déployer les composants de sécurité de leur choix ou tout simplement d'intégrer ESP dans leurs existants.



La console de gestion Aruba Orchestrator, anciennement Silver Peak Unity Orchestrator, comprend désormais des informations préconfigurées par défaut concernant les services de sécurité dans le cloud de proximité du fournisseur de sécurité. Les administrateurs réseau peuvent associer rapidement et facilement les succursales Aruba aux points de présence (POP) et aux datacenters cloud du partenaire. Ils peuvent également créer des règles extrêmement dynamiques, contextualisées, autour de l'utilisateur et plus seulement autour de l'application.

Enfin, en tirant parti d'une infrastructure et de flux de menaces communs à l'ensemble d'Aruba ESP, les responsables réseau et sécurité peuvent appliquer et mettre en œuvre de manière centralisée des politiques de gestion des menaces à l'échelle de l'entreprise.

# 3 questions à... Fernando Rynne,

Field and Channel Marketing Manager, HPE Aruba



## Quels sont les partenaires sécurité dans l'écosystème de partenaires de sécurité d'Aruba ESP ? Comment cet écosystème évolue-t-il ?

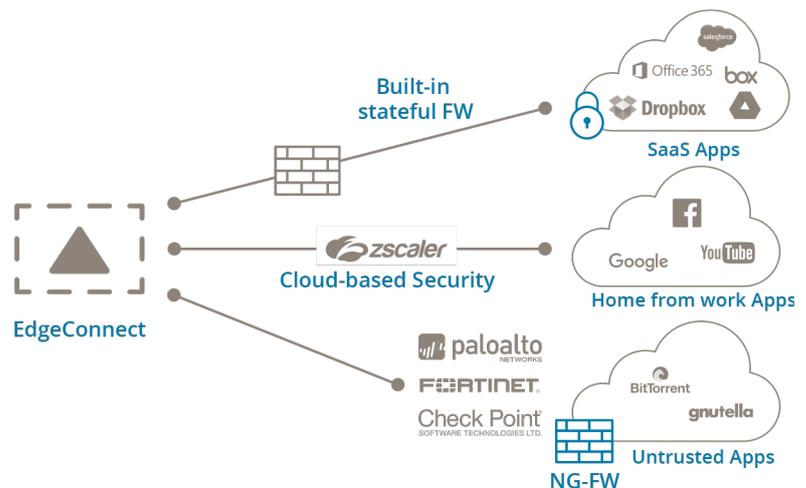
**Fernando Rynne.** En plus de la sécurité intrinsèque de la plateforme EdgeConnect, qui offre des fonctions de Firewall – et bientôt d'IDS et IPS ainsi que de NAC grâce à l'ajout de ces fonctions en 2021 – il existe en effet tout un écosystème de partenaires sécurité avec lequel EdgeConnect s'interface.

Il existe 2 grandes catégories de solutions. D'abord, les NG-FW et les solutions de sécurité Cloud native dits CASB (Cloud Access Security Broker). Les NG-FW de Palo Alto, Fortinet ou Check Point, entre autres,

s'interfaçent facilement à EdgeConnect par une méthode dite de 'Service Chaining' et permettent aux entreprises de continuer à utiliser leurs investissements existants lors de leur migration SD-WAN. Néanmoins la solution plus courante est l'adoption d'une solution de sécurité de type Cloud, soit de filtrage web avec Symantec, Forcepoint et McAfee ou des solutions CASB de ZScaler, Netskope, Check Point ou Palo Alto qui, grâce à une intégration et automatisation poussée, assurent une plus grande agilité et une maintenance réduite.

### Simplified Security Model

- 1 Simple**  
Drag-and-drop approach drastically reduces IT time required to configure and manage security policies
- 2 Intelligent**  
App-driven security policy model that reduces error, increases efficiencies and reduces cost
- 3 Easy to Manage**  
Single dashboard for orchestrating and maintaining policies resulting in accelerated deployment of apps



## Quelles sont les fonctionnalités majeures de la plateforme Aruba EdgeConnect ?

**Fernando Rynne.** Il existe de nombreuses solutions SD-WAN sur le marché mais elles ne se valent pas toutes ! La performance et l'automatisation sont les principaux différenciateurs d'EdgeConnect. EdgeConnect améliore la qualité de l'expérience des services informatiques en leur offrant un SD-WAN offrant des performances

applicatives régulières et fiables, grâce à des fonctionnalités telles que le path conditioning, l'agrégation des tunnels, le lissage du trafic, l'optimisation WAN et l'évasion cloud intelligente. De plus, les différentes applications présentent des exigences diverses en matière de QoS et d'expérience de l'utilisateur final. Par exemple,

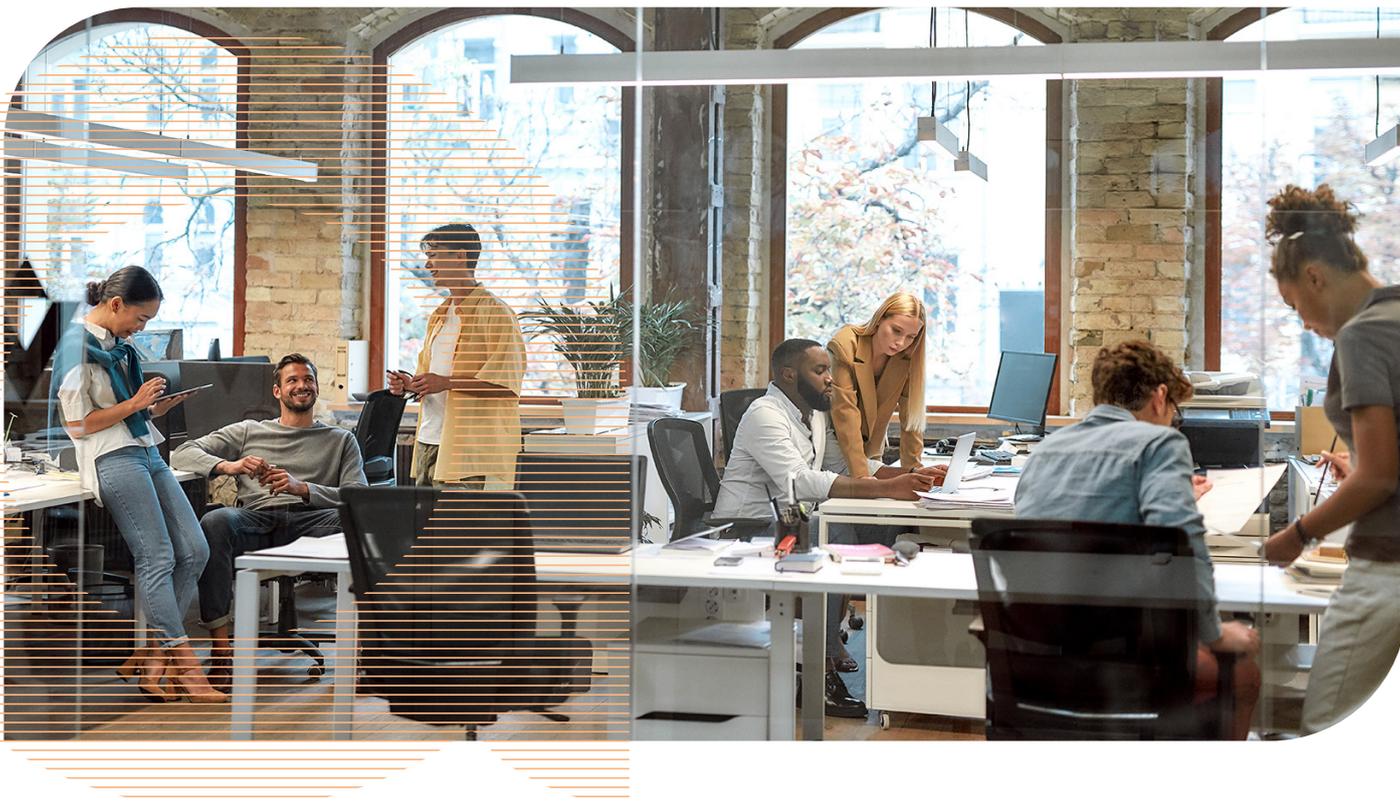


le trafic vocal et vidéo exige que l'on ait zéro perte de paquet et des délais extrêmement faibles, tandis que les transferts de fichiers imposent de larges bandes passantes mais peuvent tolérer des délais plus élevés. Aruba EdgeConnect permet

aux responsables réseaux de définir des business intent overlays, ou overlays de WAN virtuels, qui reflètent les exigences des applications en matière de QoS pertinentes pour l'entreprise.

### Les fonctionnalités de performances applicatives d'EdgeConnect incluent :

- Le path conditioning
- Le dynamic path control
- L'agrégation des tunnels
- Les mises à jour d'applications quotidiennes
- L'évasion internet locale intelligente et adaptative
- L'intégration de l'API REST Microsoft O365



### En quoi Boost permet d'optimiser le WAN et d'accélérer les performances applicatives ?

**Fernando Rynne.** Avec l'option Boost™, EdgeConnect intègre les fonctionnalités d'optimisation WAN éprouvées de Silver Peak en une solution SD-WAN unique.

Les applications TCP/IP telles que le traitement des transactions ou la sauvegarde de données utilisent une fenêtre de données dynamique et l'établissement de liaisons ou des confirmations entre les terminaux avant l'envoi de données supplémentaires. Quelle que soit la bande passante

WAN disponible, la latence engendrée par la distance est une réalité physique : la distance entre San Francisco et Londres ne varie pas entre une bande passante d'un mégaoctet par seconde ou une bande passante de 10 gigaoctets par seconde. L'accélération TCP contourne l'établissement de liaison, ce qui entraîne de meilleurs temps de réponse des applications et améliore à terme la productivité des utilisateurs et de l'entreprise.



Les techniques de déduplication et de compression des données minimisent la transmission répétitive des données au travers du WAN. Cela permet aux services informatiques de réaliser les sauvegardes dans leur fenêtre de temps allouée ou de récupérer les données perdues rapidement dans le cadre d'une application

---

## Conclusion

ARUBA Edge Services Platform, avec l'intégration d'EdgeConnect, permet ainsi de dynamiser et de sécuriser le réseau, du campus au datacenter, jusqu'au Cloud. Aruba ESP propose l'offre la plus complète du marché en matière de solutions sécurisées filaires, sans fil et WAN, qui permet à ses clients de s'adapter aux nouvelles contraintes d'aujourd'hui et aux incertitudes de demain.

de sauvegarde. Ensemble, les technologies d'accélération TCP et de gestion des données améliorent encore davantage les performances applicatives et l'efficacité du WAN, permettant à l'IT de maximiser le retour sur leurs investissements dans le WAN.

### Cette offre WAN Edge inclut :

- **Virtual Intranet Access Client (VIA)** – mobilité maximale pour les utilisateurs qui travaillent depuis n'importe où, qu'ils se connectent via des réseaux privés ou publics.
- **Points d'accès distants (RAP)** – encombrement minimal pour les espaces de travail mobiles, distants et temporaires, offrant une connectivité sécurisée au réseau de l'entreprise.
- **SD-Branch** – intégration maximale et gestion unifiée simple à travers le WLAN, le LAN et le SD-WAN avec une sécurité Zero Trust.
- **EdgeConnect** – Expérience optimale du Edge au cloud avec une plateforme SD-WAN avancée et des composants SASE unifiés.

---

**aruba**  
a Hewlett Packard  
Enterprise company