Présentation générale de la solution

HPE aruba networking

Visibilité et informations pour les réseaux d'aujourd'hui pilotés par l'IoT

Une approche pilotée par l'IA pour sécuriser les points de terminaison du réseau avec Client Insights

HPE GreenLake

Dans un contexte d'expansion et de complexité croissantes et effrénées des clients de terminaux sur le réseau, de nombreuses entreprises ont du mal à gérer l'augmentation de la surface d'attaque. Avec l'omniprésence croissante de l'Internet des objets (IoT) et les nouveaux cas d'utilisation générés par les initiatives de transformation numérique, l'adoption de l'IoT a mis de côté les meilleures pratiques critiques en matière de sécurité et de conformité au profit d'une efficacité opérationnelle et de résultats commerciaux améliorés.

Avec cette évolution, il est fréquent que les équipes informatiques et de sécurité ne sachent pas quand, où et quels types de nouveaux clients sont connectés au réseau. Ce manque de visibilité les empêche de mettre en œuvre en temps opportun des mesures de sécurité et de conformité. Les meilleures pratiques exigeraient que chaque nouveau client soit identifié avec précision, intégré et doté d'une politique, mais le service informatique est souvent pris au dépourvu.

Lacune des méthodes actuelles

Les outils de visibilité du réseau existants se concentrent sur une sélections de clients facilement identifiés à l'aide de techniques de découverte et de profilage de base. Ils incluent la recherche d'éléments tels que des smartphones et des ordinateurs portables populaires exécutant des systèmes d'exploitation de bureau ou mobiles courants. À l'aide de ces techniques, l'identification d'un smartphone fonctionnant sous Android™ à partir d'un ordinateur portable fonctionnant sous Windows est commune.

L'identification des clients tels que les devices IoT est particulièrement difficile pour plusieurs raisons, notamment :

- De nombreux devices IoT fabriqués par des fournisseurs émergents ne sont pas compatibles avec les techniques de découverte et de profilage standard, ce qui les rend difficiles à profiler avec précision.
- Il est également courant de voir des devices IoT fabriqués avec du matériel et des logiciels génériques, comme Raspberry Pi, qui remplit différents rôles, ce qui complique son déchiffrage.
- Conséquence directe d'un profilage imprécis ou partiel, les clients sont souvent identifiés en tant que clients génériques Windows ou Linux®. Il est alors plus difficile d'appliquer les politiques adéquates.
- La plupart des solutions de visibilité du réseau nécessitent des collecteurs ou agents et elles ne peuvent pas toujours déployer des collecteurs sur des sites à grande échelle.

L'importance du contexte

Cette évolution nécessite l'adoption d'une méthode globale de visibilité sur l'ensemble de l'infrastructure sans fil et filaire, sans avoir à utiliser d'agents ou à se connecter aux clients pour identifier leur emplacement. Il faut pour cela comprendre le comportement réel d'un device : quels protocoles sont utilisés ? À quelles applications et URL accède-t-il ? Et en fin de compte, quelle est la fonction de ce client sur le réseau ? Dans le cas de nombreux devices IoT spécialement conçus pour le milieu hospitalier ou les usines de production, ce contexte détaillé est le seul moyen de définir précisément leur empreinte.

La solution HPE Aruba Networking : Client Insights intégrant une IA

La solution de gestion de réseau HPE Aruba Networking Central Cloud inclut désormais Client Insights intégrant une IA, qui propose un profilage et une visibilité parmi les plus précis du secteur. Client Insights exploite la télémétrie native de l'infrastructure à partir des points d'accès, des commutateurs et des passerelles, ainsi que des clients, sans aucune installation de collecteurs ni d'agents physiques. Des modèles de classification reposant sur le machine learning (ML) sont utilisés pour prendre les empreintes digitales et identifier et profiler avec précision une grande variété de clients sur l'ensemble de l'infrastructure filaire et sans fil.

La Figure 1 montre comment Client Insights utilise le ML et le crowdsourcing pour identifier les types de clients.

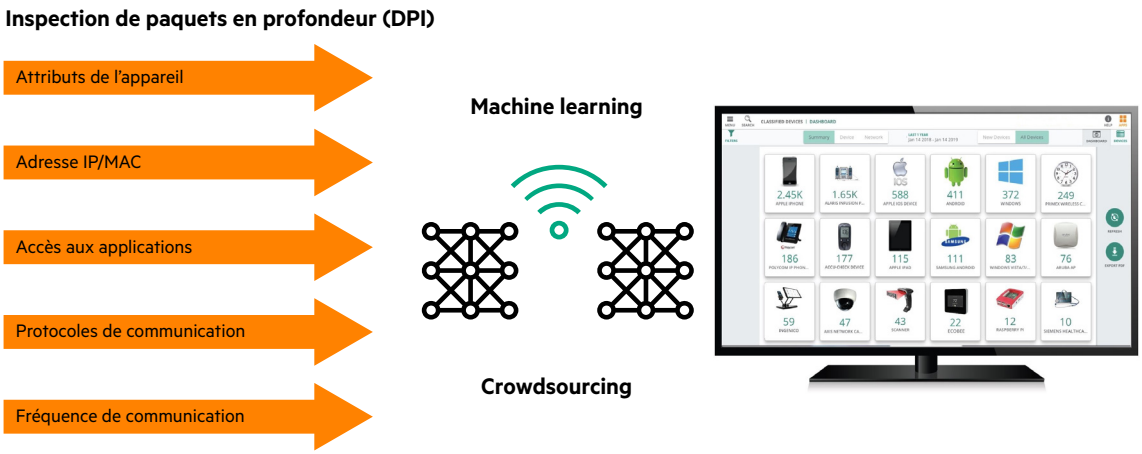


Figure 1. Client Insights utilise le machine learning avancé et le crowdsourcing pour identifier avec précision tout type de client.

Ces fonctionnalités sont encore renforcées grâce à l'inspection de paquets en profondeur (DPI), qui ajoute du contexte et des informations concernant le comportement afin d'identifier avec précision des devices IoT difficiles à détecter. En exploitant la DPI, Client Insights peut utiliser un ensemble plus large d'attributs d'appareil pour une identification plus précise. Les attributs de clients qui incluent des modèles de communication et de comportement sont analysés pour créer des clusters d'appareils similaires de façon dynamique.

Des modèles ML sont utilisés pour approfondir en permanence les connaissances et mettre à jour ces attributs afin d'actualiser de façon dynamique les empreintes digitales et de proposer des recommandations de classification. Une technologie de crowdsourcing est utilisée pour valider les empreintes digitales sur plusieurs sites de clients avant de les ajouter à la base de données de classification HPE Aruba Networking. Le moteur de classification bénéficie ainsi d'une précision accrue et complète.

La Figure 2 montre comment Client Insights utilise la télémétrie des devices d'infrastructure HPE Aruba Networking pour identifier les clients.

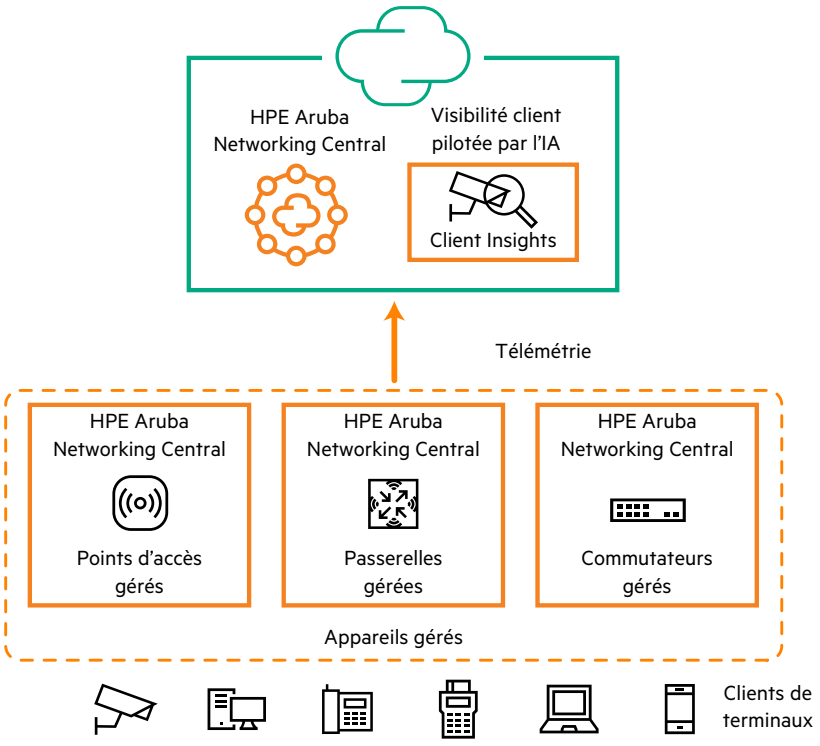


Figure 2. La télémétrie native de l'infrastructure HPE Aruba Networking est utilisée pour identifier avec précision les clients connectés à l'aide d'une classification s'appuyant sur le machine learning.

La Figure 3 montre le tableau de bord de Client Insights avec différents devices répertoriés sous différentes catégories.

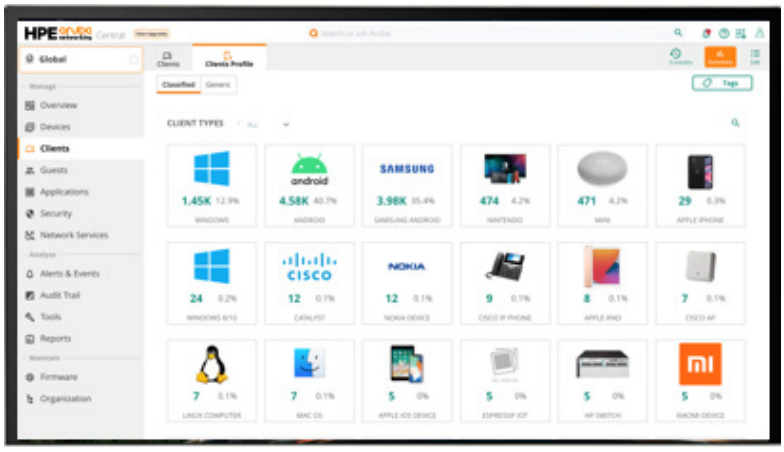


Figure 3. Le tableau de bord HPE Aruba Networking Central Cloud Client Insights affiche tous les devices connectés par catégorie.

Pour les appareils auparavant considérés comme génériques, des modèles de ML sophistiqués sont utilisés pour analyser les attributs et regrouper des clients similaires. Une fois les clients regroupés, ceux-ci peuvent être facilement étiquetés en fonction d'attributs clés. Après cela, les nouveaux clients se connectant au réseau sont automatiquement ajoutés à leur cluster spécifique et étiquetés en conséquence.

Pour les environnements qui ne sont pas actuellement gérés par HPE Aruba Networking Central Cloud ou pour des environnements avec des devices réseau tiers, HPE Aruba Networking ClearPass Device Insight peut être exploité pour l'identification et le profilage des clients en s'appuyant sur le machine learning. HPE Aruba Networking ClearPass Device Insight nécessite l'installation d'un collecteur physique ou virtuel et fait l'objet d'une licence distincte.

La valeur de l'application automatisée des politiques

Sans un contrôle adapté, la visibilité ne permet pas aux entreprises de se prémunir des risques de sécurité et de conformité. Client Insights permet une surveillance continue des clients qui, lorsqu'elle est associée à HPE Aruba Networking ClearPass Policy Manager, fournit un contrôle d'accès de bout en bout en boucle fermée. Il offre une visibilité et une application automatisée des politiques, et réduit considérablement le besoin d'intervention manuelle sur l'ensemble du réseau filaire et sans fil multifournisseur. HPE Aruba Networking ClearPass Device Insight s'intègre également de manière transparente à HPE Aruba Networking ClearPass Policy Manager.

L'application automatisée des politiques répond à plusieurs cas d'utilisation différents, depuis le moment où des clients rejoignent le réseau pour la première fois jusqu'au déclenchement d'un événement indésirable nécessitant la suppression d'un client pour des questions de sécurité et de conformité. Par exemple, lorsqu'une nouvelle caméra se connecte pour la première fois au réseau, elle peut automatiquement être segmentée dans la catégorie des clients inconnus afin de ne pas compromettre l'infrastructure ou les serveurs critiques. Si un client a été compromis ou agit de manière suspecte, il peut être mis en quarantaine complète pour être testé, réparé ou remplacé.

La Figure 4 montre comment Client Insights collabore avec HPE Aruba Networking ClearPass Policy Manager pour une segmentation et une application automatisées.

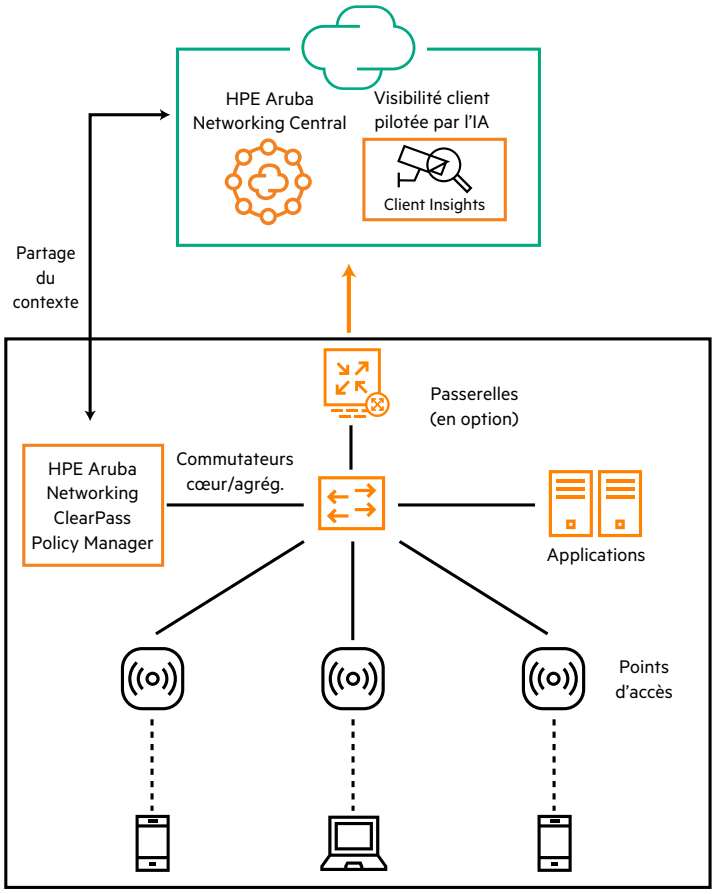
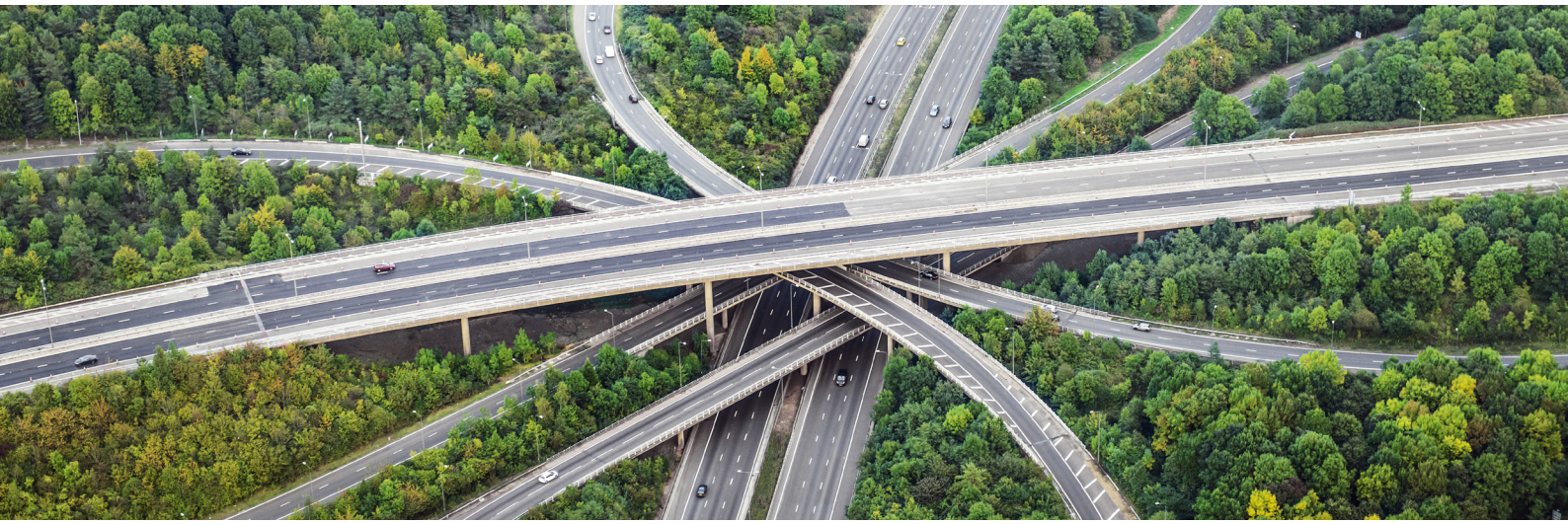


Figure 4. Client Insights s'intègre à HPE Aruba Networking ClearPass Policy Manager pour une segmentation et une application automatisées

HPE Aruba Networking Central Cloud avec Client Insights : Délais de rentabilisation accélérés

La gestion d'applications stratégiques dans des environnements de plus en plus distribués suscite des attentes en matière de disponibilité, de performances et de sécurité améliorées. HPE Aruba Networking Central Cloud offre des fonctions modernes et évolutives de gestion et d'orchestration qui incluent des fonctionnalités avancées d'IA/de ML et de sécurité, permettant aux services informatiques d'offrir des expériences utilisateur supérieures avec une simplicité étonnante, quelle que soit leur taille.

Client Insights exploite ces fonctionnalités uniques et la télémétrie native de l'infrastructure réseau pour réduire le temps et les coûts de déploiement, accélérant ainsi le délai de rentabilisation. Cette approche permet une découverte et une surveillance centralisées et ininterrompues des points de terminaison du réseau sur les déploiements distribués, tout en augmentant votre visibilité et votre politique de sécurité.



Résumé

Avec l'adoption accélérée des devices IoT, le nombre de clients sur les réseaux clients continue de croître, créant de nouveaux cas d'utilisation tout en élargissant la surface d'attaque. Une visibilité complète est essentielle pour que la sécurité et la conformité aux meilleures pratiques évoluent au même rythme que les gains d'efficacité opérationnelle qui accompagnent l'adoption de l'IoT.

Identifier et profiler avec précision les clients pour des politiques reposant sur des rôles précis et garantir que chacun dispose du bon niveau de contrôle d'accès pour réduire les niveaux de risque globaux n'est plus un avantage, c'est une exigence.

En savoir plus

HPE.com/fr/fr/Aruba-Central.html

Rendez-vous sur **HPE.com**

Live Chat Ventes

a00069032FRE, Rév. 1

Hewlett Packard Enterprise