HPE aruba networking

Brochure

Faciliter l'adoption de la sécurité zero trust

Accélérez votre parcours zero trust avec un réseau intégrant une IA et axé sur la sécurité

Commencer >

HPE GreenLake

Table des matières

Le changement de paradigme

L'innovation revêt une importance cruciale pour les organisations. Dans notre monde tourné vers le numérique, c'est la qualité des expériences qui incarne véritablement l'innovation.

La création d'expériences exceptionnelles permet aux entreprises de se démarquer sur un marché compétitif, d'attirer des talents venus des quatre coins du globe et de prospérer malgré l'incertitude, les changements et les perturbations.

Ces expériences prennent vie grâce à une connectivité optimale : celle qui relie les individus entre eux, les commerçants à leurs clients, les médecins à leurs patients, les employés aux applications, les appareils au cloud et les données aux algorithmes.

Cette connectivité ne connaît aucun répit. Elle est toujours présente et accessible où que l'on se trouve.

Elle promet une meilleure personnalisation, des expériences utilisateur et employé satisfaisantes, un avantage concurrentiel indéniable et, en fin de compte, une croissance florissante.

Cependant, elle peut également apporter son lot de complexité pour les services informatiques.

Les équipes réseau et sécurité jouent un rôle de plus en plus stratégique à mesure que la connectivité et les initiatives technologiques, telles que l'intelligence artificielle générative, prennent place parmi les principales priorités. Parallèlement, les environnements dans lesquels ces équipes opèrent deviennent de plus en plus complexes à appréhender.
Les mesures de sécurité, de confidentialité, de gouvernance et de conformité évoluent en permanence, nécessitant une meilleure coordination et mettant à rude épreuve des équipes déjà contraintes de faire plus avec moins.

Qu'est-ce que le zero trust ?
Le zero trust repose sur le principe selon lequel les utilisateurs et les appareils doivent prouver leur légitimité afin d'obtenir l'accès aux ressources dont ils ont besoin pour accomplir leurs tâches ou remplir leurs fonctions. Cette notion d'accès restreint est au cœur des pratiques de sécurité zero trust.

La sécurité zero trust exige également une surveillance continue des utilisateurs et des appareils. Leur légitimité est évaluée en permanence, et si un utilisateur ou un appareil adopte un comportement suspect ou agit de manière incompatible avec son rôle, son accès peut être limité ou révoqué. Ce contrôle restreint et dynamique contribue à minimiser, voire à prévenir, la propagation latérale des attaques.

Pourquoi adopter la sécurité zero trust ?
Les approches traditionnelles de sécurité du réseau qui se concentrent principalement sur la protection du périmètre ne sont plus efficaces. Avec la montée en puissance de l'IoT, la dissolution des frontières de l'entreprise due au télétravail et l'évolution des menaces de plus en plus sophistiquées qui exploitent les utilisateurs et les appareils « de confiance », il devient primordial d'adopter une approche de sécurité plus rigoureuse.

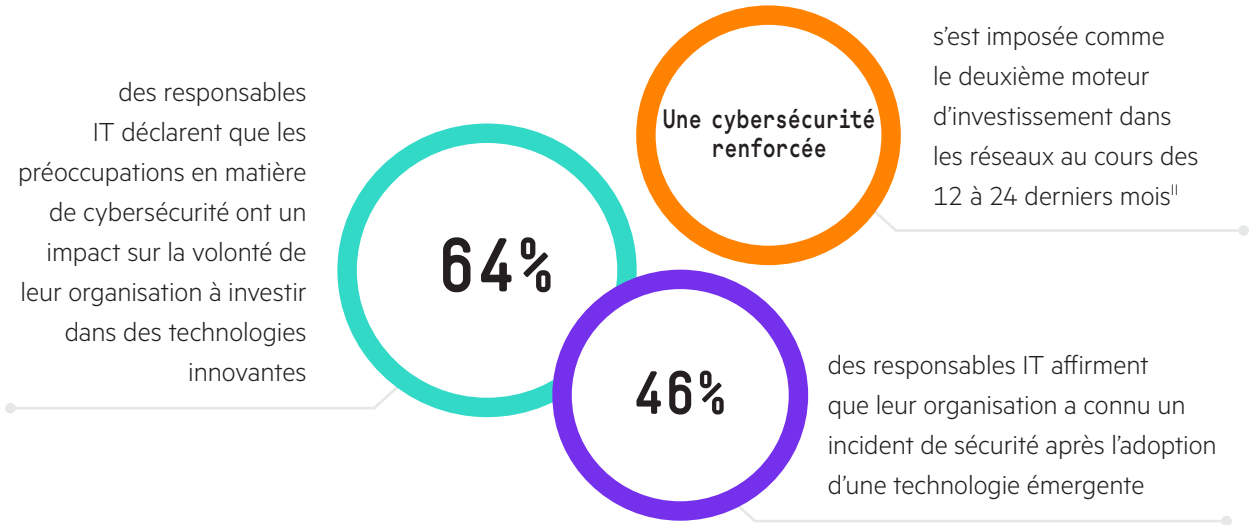
La sécurité zero trust : une nécessité

La connectivité est la clé de l'innovation, et le réseau en est le pilier central. Que ce soit au bureau, lors d'un achat en magasin, en surfant depuis un café ou en connectant une caméra de surveillance à une application cloud, le réseau est omniprésent.

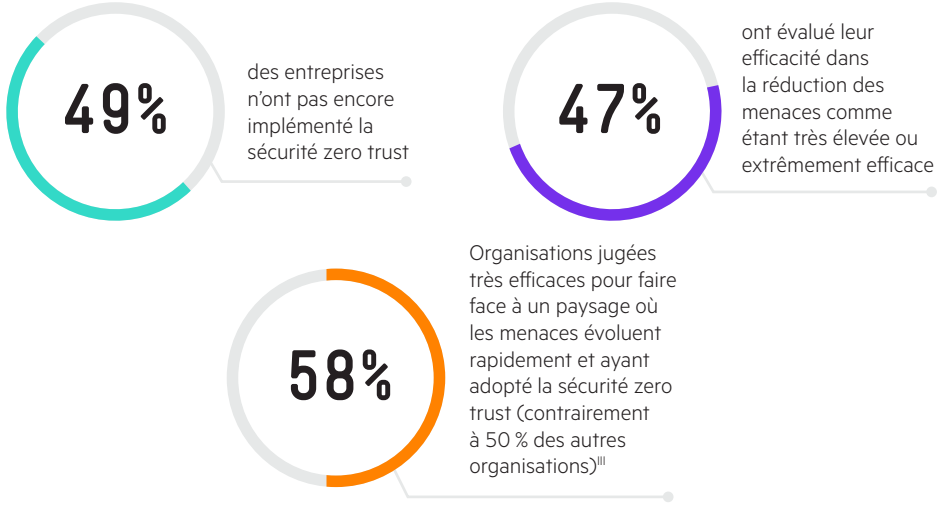
Que peut-on attendre d'autre ? Des menaces qui passent inaperçues.

Cette perspective est si répandue qu'elle a donné naissance à un nouveau modèle d'architecture de sécurité : le zero trust. Les modèles de sécurité zero trust partent du principe qu'une personne malveillante est présente dans l'environnement, ce qui signifie que la sécurité d'un réseau propriétaire n'est pas plus élevée que celle d'un réseau externe.[I]

Comment les entreprises parviennent-elles à concilier la nécessité d'une performance optimale et d'une disponibilité constante de leur réseau, tout en assurant une sécurité efficace ?



Les défis de la sécurité zero trust



Bien que l'adoption du zero trust ait augmenté ces dernières années, sa mise en œuvre reste un défi pour de nombreuses organisations. Plusieurs raisons expliquent cette situation.

1. **Un paradigme plutôt qu'un produit**. Le zero trust ne se résume pas à une simple solution ou un simple produit prêt à l'emploi. C'est un ensemble de principes architecturaux directeurs qui nécessitent une constante amélioration et une implémentation cohérente lors des décisions liées à l'infrastructure et aux politiques. Il ne s'agit pas d'une initiative unique, mais d'un processus continu. Atteindre une maturité avancée dans le cadre d'une sécurité zero trust prend du temps, car les mentalités en matière de sécurité évoluent et les processus s'adaptent en conséquence.

2. **Des exigences interdomaines.** La sécurité zero trust englobe plusieurs domaines technologiques au sein d'une organisation, concernant non seulement les réseaux, mais également les utilisateurs, les appareils, les applications et les charges de travail réparties sur différents sites, filiales, datacenters, et sur le cloud. Assurer une coordination, un contrôle et une cohérence efficaces est crucial, mais cette tâche peut s'avérer complexe en raison de la diversité des environnements à prendre en compte.
3. **Capacités fragmentées.** Les capacités de contrôle d'accès qui soutiennent les architectures zero trust sont généralement réparties entre différentes solutions technologiques, et leur intégration peut souvent être réalisée de manière disjointe. Au fil du temps, cette approche fragmentée complexifie non seulement l'architecture et les opérations, mais expose également l'organisation à des failles de sécurité, des incohérences dans les politiques et leur application, ainsi qu'à des risques potentiels de cybersécurité.[IV]
4. **Collaboration en équipe.** Pour réussir à innover en respectant les exigences de sécurité zero Trust, les équipes réseau et sécurité doivent travailler en étroite collaboration pour atteindre des objectifs et des résultats communs. Cette coopération permettra de fournir des expériences utilisateur exceptionnelles tout en protégeant l'entreprise contre des attaques de plus en plus sophistiquées. L'utilisation d'outils disparates et le manque de contrôles et de partage de données peuvent donner lieu à des opérations cloisonnées qui entravent les efforts déployés pour atteindre les objectifs commerciaux communs.

Le nouveau rôle du réseau

L'intégration des principes zero trust à l'innovation est essentielle, car cette dernière repose sur la connectivité offerte par le réseau. Celui-ci occupe ainsi une place centrale au sein de l'écosystème de sécurité zero trust.

Il est temps pour les responsables IT de considérer le réseau comme une solution de sécurité zero trust.

Bien qu'aucun fournisseur ou solution ne soit à même de couvrir tous les besoins d'une entreprise en matière de cyberprotection, le fait de partir d'un réseau intégrant les fondements de la sécurité zero trust permet de faciliter la mise en place des exigences de sécurité, tout en ajoutant une couche de protection supplémentaire aux points d'entrée numériques critiques. Grâce à sa double fonction en tant que pilier de la connectivité et garant de la cybersécurité, le réseau est un lieu propice à la collaboration et à la coopération entre les équipes réseau et sécurité.

Le réseau que vous choisissez est un élément clé pour assurer une protection efficace de votre entreprise.

Faciliter l'adoption de la sécurité zero trust

Le réseau IA axé sur la sécurité

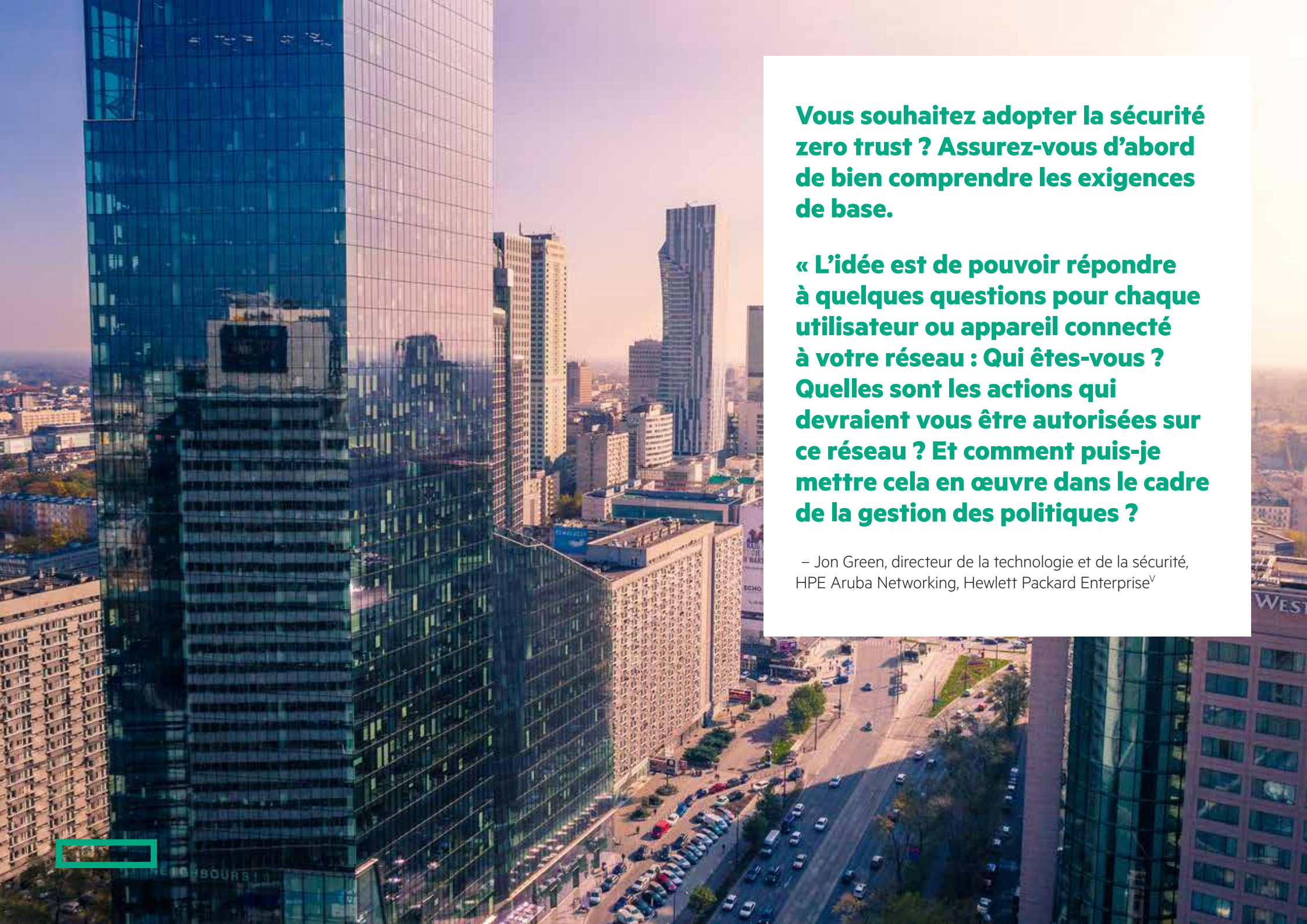
Accélérez l'adoption de la sécurité zero trust grâce à un réseau IA axé sur la sécurité HPE Aruba Networking. Les solutions réseau HPE Aruba Networking, conçues selon les principes du zero trust, offrent une base commune aux équipes réseau et sécurité pour créer des expériences uniques et obtenir des résultats commerciaux innovants, sans compromettre la cybersécurité.

Le réseau IA axé sur la sécurisé de HPE Aruba Networking facilite l'adoption de la sécurité zero trust et favorise la conformité aux normes et réglementations de cybersécurité en permettant aux équipes d'utiliser le réseau comme une solution de sécurité. Désormais, le réseau offre une visibilité avancée, une gestion centralisée des politiques, une protection des données, une défense contre les menaces et un contrôle d'accès, le tout sur une plateforme unique. Ces fonctionnalités intégrées de sécurité zero trust font du réseau une ligne de défense essentielle, qui s'intègre aux éléments de l'écosystème de sécurité pour renforcer la protection, sans les complications supplémentaires liées à l'utilisation de multiples outils disparates, et sans qu'il soit nécessaire d'entreprendre un remplacement intégral de l'infrastructure existante (une opération coûteuse et longue).

De plus, le réseau piloté par l'IA décuple la capacité humaine au sein de l'organisation, un aspect essentiel à mesure que les réglementations se renforcent, les disparités de compétences se creusent et les cybermenaces augmentent. Grâce au réseau IA axé sur la sécurisé de HPE Aruba Networking, les équipes bénéficient d'une automatisation intelligente qui réduit les tâches manuelles, améliore la visibilité et la détection des anomalies, ainsi que la surveillance et les diagnostics, réduisant ainsi les risques inutiles auxquels l'entreprise est exposée.

Comment le réseau IA axé sur la sécurité facilite-t-il l'adoption de la sécurité zero trust ?

1. Offre une **visibilité commune** et fournit une source de vérité pour les équipes et les outils
2. Permet une **gestion globale des politiques**, simplifiant ainsi la définition et l'application des politiques
3. Permet une **mise en application de l'edge au cloud**, garantissant des performances optimales et un contrôle cohérent
4. Utilise **l'intelligence artificielle** pour améliorer à la fois l'efficacité et la sécurité

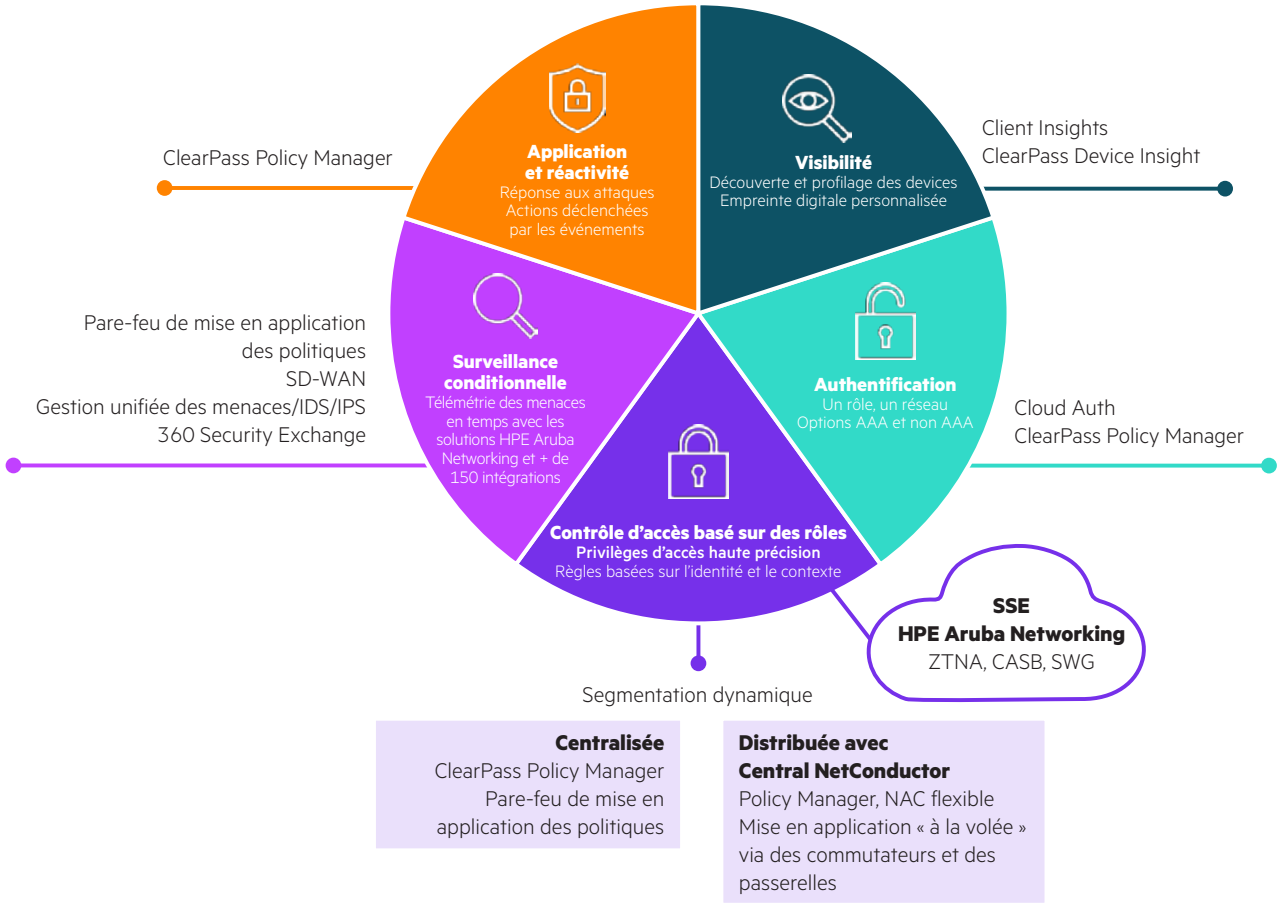


Vous souhaitez adopter la sécurité zero trust ? Assurez-vous d'abord de bien comprendre les exigences de base.

« L'idée est de pouvoir répondre à quelques questions pour chaque utilisateur ou appareil connecté à votre réseau : Qui êtes-vous ? Quelles sont les actions qui devraient vous être autorisées sur ce réseau ? Et comment puis-je mettre cela en œuvre dans le cadre de la gestion des politiques ?

– Jon Green, directeur de la technologie et de la sécurité, HPE Aruba Networking, Hewlett Packard Enterprise[V]

Dispositif de sécurité Zero Trust HPE Aruba Networking

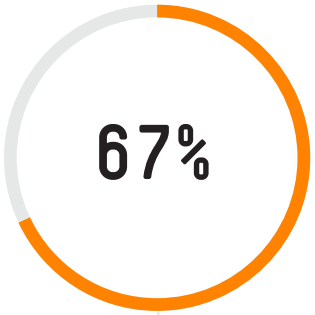


Contrairement à d'autres approches pour lesquelles il est nécessaire d'ajouter une multitude de solutions de sécurité disjointes à l'infrastructure réseau, HPE Aruba Networking adopte une stratégie axée sur la sécurité et s'appuyant sur l'IA, qui propose des solutions Zero Trust intégrées qui sont planifiées, conçues et mises en œuvre comme faisant partie intégrante d'une implémentation réseau standard. Les solutions réseau HPE Aruba Networking s'intègrent parfaitement avec le reste de l'écosystème de sécurité pour à la fois informer et agir en fonction des informations issues de l'environnement de sécurité. Cette approche permet de renforcer la protection tout en simplifiant les opérations.

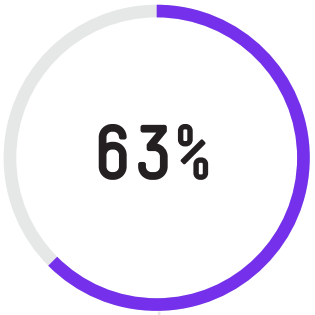
Une visibilité commune

Opérer à partir d'une vérité commune

La sécurité zero trust commence par la visibilité des utilisateurs et des appareils connectés. Malheureusement, de nombreuses organisations manquent encore de visibilité et de contrôle sur les activités de leurs utilisateurs et de leurs appareils, ce qui compromet sérieusement leur sécurité. Cette situation est principalement causée par la prolifération des appareils IoT connectés aux réseaux d'entreprise, qui entraînent une augmentation significative de la surface d'attaque de l'organisation. Ces appareils IoT sont d'ailleurs souvent installés et gérés par d'autres services de l'entreprise, ce qui contribue encore plus à cette perte de visibilité.



des personnes interrogées soulignent l'importance de l'identification et de l'authentification des devices IoT accédant à leur réseau dans le cadre de la stratégie de sécurité de leur entreprise



des personnes interrogées estiment que leurs équipes de sécurité manquent de visibilité et de contrôle sur l'ensemble des activités des appareils connectés à leur infrastructure IT [VII]

L'adoption d'un réseau axé sur la sécurité et intégrant une IA facilite la mise en place des contrôles de sécurité zero trust en offrant aux équipes une visibilité et un contrôle partagés. En fondant leurs décisions sur une source de données combinée, cette approche permet de simplifier les opérations de réseau et de sécurité, conférant ainsi aux équipes la capacité de prendre des décisions éclairées en matière de surveillance et de gestion des risques.

Les avantages d'une visibilité commune

- Avoir une connaissance précise des utilisateurs et des équipements connectés sur votre réseau, et surveiller en continu leur comportement et leur statut
- Partager des données avec d'autres éléments de l'écosystème de sécurité, tels que les outils de gestion des informations et des événements de sécurité (SIEM), pour fournir des alertes et des informations provenant de l'ensemble de l'infrastructure
- Tirer parti des fonctionnalités intégrées d'analyse du trafic réseau et des références comportementales afin de détecter rapidement les attaques, les arrêter ou les prévenir

Solutions HPE Aruba Networking

La solution de gestion de réseau basée sur le cloud HPE Aruba Networking Central inclut une visibilité et un profilage pilotés par l'IA avec Client Insights. Client Insights analyse la télémétrie de l'infrastructure native à partir des points d'accès, des commutateurs, des passerelles et des clients, sans nécessiter l'installation de collecteurs ou d'agents physiques. Cette solution fournit un profilage précis des appareils assisté par IA/ML, avec une précision pouvant atteindre 99 % pour les clients connus et un taux d'appareils inconnus inférieur à 5 %, sur une grande variété de terminaux qui se connectent au réseau[VIII], y compris un ensemble diversifié de devices IoT sur l'ensemble de l'infrastructure filaire et sans fil. Pour les environnements non gérés par HPE Aruba Networking Central basé sur le cloud ou avec des appareils réseau tiers, HPE Aruba Networking ClearPass Device Insight offre une identification et un profilage des clients basés sur l'IA et le machine learning.

Profitez d'une précision de profilage avoisinant les 99 % pour les dispositifs connectés au réseau, y compris les appareils IoT

Comment les politiques basées sur les rôles simplifient-elles l'adoption des frameworks de sécurité zero trust ?
En attribuant des rôles, les politiques peuvent être appliquées sur l'intégralité du réseau, indépendamment de l'emplacement ou du point de connexion sur le réseau. Les utilisateurs et les appareils peuvent ainsi bénéficier des politiques appropriées tout au long de leurs déplacements au sein de l'entreprise, qu'ils soient sur le campus, dans une succursale, dans un bureau à domicile ou dans d'autres lieux.

Une politique globale

Des politiques alignées sur les profils des utilisateurs

Après avoir identifié et profilé un utilisateur ou un appareil, la prochaine étape inscrite dans un framework de sécurité zero trust consiste à authentifier son identité à chaque connexion et à lui assigner les politiques de contrôle d'accès appropriées. Toutefois, la définition et la gestion de ces politiques peuvent poser un défi en raison des évolutions des dynamiques d'entreprise, des employés qui se connectent depuis différents endroits et de l'intégration de nouveaux devices IoT. Les méthodes qui reposent sur des critères liés à l'emplacement ou au réseau, tels que les adresses IP ou les sous-réseaux, peuvent entraîner une complexité et une rigidité de l'infrastructure réseau, ainsi qu'un risque de sécurité dû aux incohérences dans la définition et l'application des politiques.

En intégrant des fonctionnalités de politique globale au sein d'un réseau axé sur la sécurité et intégrant une IA, les organisations sont en mesure d'élargir leur champ d'action en définissant et en appliquant des politiques de haut niveau qui reposent sur l'identité et les rôles. Les rôles sont définis pour l'ensemble de l'entreprise, ce qui permet d'éliminer la gestion fastidieuse des contrôles d'accès pour chaque appareil connecté au sein de l'organisation. La possibilité d'exprimer les politiques en termes d'intention métier vous permet de simplifier les workflows de politiques en isolant celles-ci de la complexité et des variations du réseau physique sous-jacent. Cette approche permet aux équipes réseau et sécurité de procéder à une gestion du réseau basé sur l'intention.

Les avantages d'une politique globale

- Définir une politique une seule fois et l'appliquer à tous les niveaux, éliminant ainsi la gestion fastidieuse des contrôles d'accès et les incohérences qui augmentent les risques
- Surveiller et appliquer en continu les politiques pour les utilisateurs, les appareils, les données et les applications, en veillant à ce qu'il n'y ait aucune faille, peu importe leur emplacement ou ce à quoi ils sont connectés
- Fournir aux équipes réseau et sécurité une « boîte à outils commune » pour optimiser les performances du réseau et appliquer des politiques de sécurité granulaires

Les solutions HPE Aruba Networking

HPE Aruba Networking ClearPass authentifie l'identité des utilisateurs ou des appareils en la confrontant à un large éventail de sources d'identité, comme Active Directory. Grâce à un moteur de politiques avancé, ClearPass offre un contrôle précis des privilèges d'accès en déterminant quels utilisateurs et appareils peuvent accéder à quelles ressources. Les politiques suivent de manière transparente l'utilisateur et l'appareil, qu'ils se trouvent sur des réseaux étendus, filaires ou sans fil, et ce, même dans des environnements multifournisseurs.

Pour les réseaux gérés par HPE Aruba Networking Central, la solution de contrôle d'accès réseau (NAC) cloud-native Cloud Auth permet une intégration fluide des utilisateurs finaux et des appareils clients, soit via une authentification basée sur l'adresse MAC, soit via des intégrations avec des fournisseurs d'identité cloud courants pour attribuer automatiquement le bon niveau d'accès au réseau.

La technologie HPE Aruba Networking SSE Zero Trust Network Access (ZTNA) restreint l'accès, par l'intermédiaire d'un courtier de confiance, aux applications spécifiques ou micro-segments approuvés pour les utilisateurs hybrides, distants et les tiers, tels que les sous-traitants et les intérimaires, conformément aux règles définies via une interface de politique globale unique. Grâce à une surveillance continue, les règles s'adaptent automatiquement en fonction des changements d'identité, de lieu et d'état des appareils, ce qui simplifie le respect des principes zero trust à chaque accès.

Mise en application Edge to Cloud

Une application cohérente des politiques pour les utilisateurs, les applications, les données et les appareils

Les frameworks de sécurité zero trust reposent sur l'application de politiques visant à instaurer la confiance et à garantir que les utilisateurs et les appareils n'accèdent qu'aux ressources dont ils ont besoin, tant qu'ils ne sont pas soupçonnés de planifier une attaque.

Avec la solution réseau axée sur la sécurité et pilotée par l'IA de HPE Aruba Networking, les organisations peuvent mettre en œuvre une application des politiques zero trust basée sur les rôles à chaque point de contrôle. Le réseau IA sécurisé applique la politique basée sur les rôles à l'ensemble des utilisateurs, des appareils et des applications, indépendamment de leur emplacement ou de ce à quoi ils sont connectés. L'application des règles en ligne au sein de l'infrastructure de commutation permet d'éviter le hairpinning du trafic pour implémenter les politiques de sécurité. Cela se traduit par une amélioration des performances, une expérience utilisateur renforcée et une consommation réduite des ressources, tout en préservant l'accès et la protection des systèmes.

Les avantages de la mise en application Edge to Cloud

- Application des politiques à tous les niveaux, y compris pour les terminaux, les points d'accès, les commutateurs d'accès, les passerelles SD-WAN, les commutateurs Top-of-Rack de datacenters, le campus ou le cloud
- Favorise la coopération et la collaboration entre les équipes réseau et sécurité, car les politiques contribuent à assurer des performances réseau optimales tout en protégeant l'entreprise
- Réduction du nombre de solutions de sécurité externes nécessaires pour appliquer les contrôles d'accès requis par les frameworks zero trust et la conformité, ce qui contribue également à diminuer la complexité associée

Les solutions HPE Aruba Networking

La segmentation dynamique de HPE Aruba Networking permet de séparer le trafic réseau en fonction de l'identité et des permissions d'accès associées, octroyant ainsi un accès zero trust selon le principe du « moindre privilège » aux applications et aux données, de l'edge au cloud. Elle prend en charge plusieurs modèles de mise en application ; une application centralisée et distribuée, ce qui permet au service informatique de choisir le ou les modèles adaptés à leur environnement. La mise en application centralisée des politiques est assurée par le pare-feu d'application des politiques intégré à l'infrastructure réseau HPE Aruba Networking. La mise en application distribuée des politiques au sein de l'infrastructure de passerelle et de commutation est quant à elle assurée par HPE Aruba Networking Central NetConductor, une solution full stack qui utilise une technologie largement adoptée telle que EVPN/VXLAN pour produire un overlay de réseau intelligent adapté au déploiement rapide de réseaux d'entreprise et à la mise à l'échelle massive de l'automatisation réseau et de la sécurité.

Les organisations peuvent également utiliser HPE Aruba Networking EdgeConnect SD-WAN pour appliquer des politiques de sécurité cohérentes sur l'ensemble des réseaux WAN et LAN, grâce à des fonctionnalités de pare-feu de nouvelle génération intégrées de bout en bout, conjuguant technologies IDS/IPS, protection contre les attaques par déni de service (DDoS) et microsegmentation à l'échelle de l'entreprise. Les services NGFW intégrés permettent aux organisations de consolider les fonctions réseau et sécurité des succursales en éliminant les pare-feux et les routeurs hérités dans les succursales.

Au sein du datacenter, HPE Aruba Networking Fabric Composer facilite la mise en œuvre de la sécurité zero trust en simplifiant et en automatisant le processus de micro-segmentation grâce à une interface utilisateur conviviale et intuitive. Le commutateur HPE Aruba Networking CX 10000 offre une micro-segmentation distribuée, un pare-feu est-ouest, des services de chiffrement et de télémétrie intégrés, fournis en ligne, sur tous les ports, au plus près des applications d'entreprise critiques et sans nécessiter de pare-feux supplémentaires.

« Les plus grandes entreprises se tournent vers des architectures zero trust, dans lesquelles le rôle du réseau n'est pas d'assurer la connexion entre utilisateurs et ressources, mais d'être une couche de mise en application des règles de sécurité. Pour les utilisateurs qui accèdent aux applications, les règles de sécurité peuvent être appliquées dans le cloud, mais pour de nombreux flux en revanche (notamment ceux des devices IoT et de leurs services connexes), il s'avère plus efficace de mettre en œuvre automatiquement ces règles au niveau des appareils permettant l'accès au réseau, comme les points d'accès, les commutateurs et les routeurs. »

– David Hughes, responsable des produits et de la technologie, HPE Aruba Networking, Hewlett Packard Enterprise[IX]

Qu'est-ce qu'un réseau IA ?
Apparu récemment, le terme « réseau IA » désigne la façon dont l'intelligence artificielle pour les opérations informatiques (AIOps) s'applique aux environnements Wi-Fi, de commutation et WAN.

Opérations automatisées par l'IA

Assurer une gestion et une protection à grande échelle

Le monde des affaires d'aujourd'hui est devenu un environnement complexe et exigeant, où les entreprises doivent faire face à de multiples défis.

Pour maintenir et sécuriser un réseau zero trust, les entreprises doivent disposer d'une visibilité permanente et de fonctionnalités d'automatisation. Grâce à l'IA, elles peuvent exploiter pleinement le potentiel humain, réduire les risques à grande échelle, renforcer la sécurité et libérer les équipes pour générer un avantage concurrentiel.

Les réseaux axés sur la sécurité et pilotés par l'IA permettent aux équipes d'exploiter le machine learning et la télémétrie complète centrée sur le réseau et les utilisateurs, qui capture les données de chaque utilisateur, appareil et réseau. En utilisant ces données, les équipes de sécurité peuvent soutenir la mise en œuvre de la sécurité zero trust, assurer une surveillance continue, tout en prévenant et contenant efficacement les attaques. Grâce à l'automatisation, les équipes réseau peuvent automatiser des tâches fastidieuses telles que l'intégration, la provision et l'orchestration des politiques.

Les avantages des opérations automatisées par l'IA

- Automatisation des tâches de gestion réseau et des tâches relatives aux opérations de sécurité visant à réduire la quantité de travail manuel nécessaire à la protection et à la gestion du réseau
- Amélioration de la visibilité et du contrôle des utilisateurs et des appareils sur le réseau, et détection des anomalies pour améliorer la détection et la prévention des attaques
- Renforcement de la surveillance et des diagnostics afin de fournir des informations pertinentes et exploitables pour les équipes réseau et de sécurité

Opérations HPE Aruba Networking automatisées par l'IA

HPE Aruba Networking Central est une console cloud-native de gestion du réseau et de la sécurité conçue pour l'ensemble de l'infrastructure HPE Aruba Networking. Faisant office de point de contrôle et de visibilité unique pour Aruba ESP (Edge Services Platform), Central offre une solution AIOps, une automatisation de workflow et des fonctionnalités de sécurité avancées, permettant d'unifier les opérations dans divers environnements, qu'il s'agisse du campus, des succursales, des datacenters ou des environnements de télétravail.

Central tire parti de l'intelligence artificielle et de l'analyse avancée pour automatiser les tâches de gestion et d'exploitation courantes du réseau et de la sécurité. Il assure également une surveillance intelligente 24 h/24 et 7 j/7 des réseaux, des applications et des appareils qui composent le lac de données. Ces fonctionnalités reposent sur des modèles ML constamment entraînés à partir des données de performance réseau issues de la base de clients mondiale HPE Aruba Networking. Les fonctionnalité IA de Central comprennent :

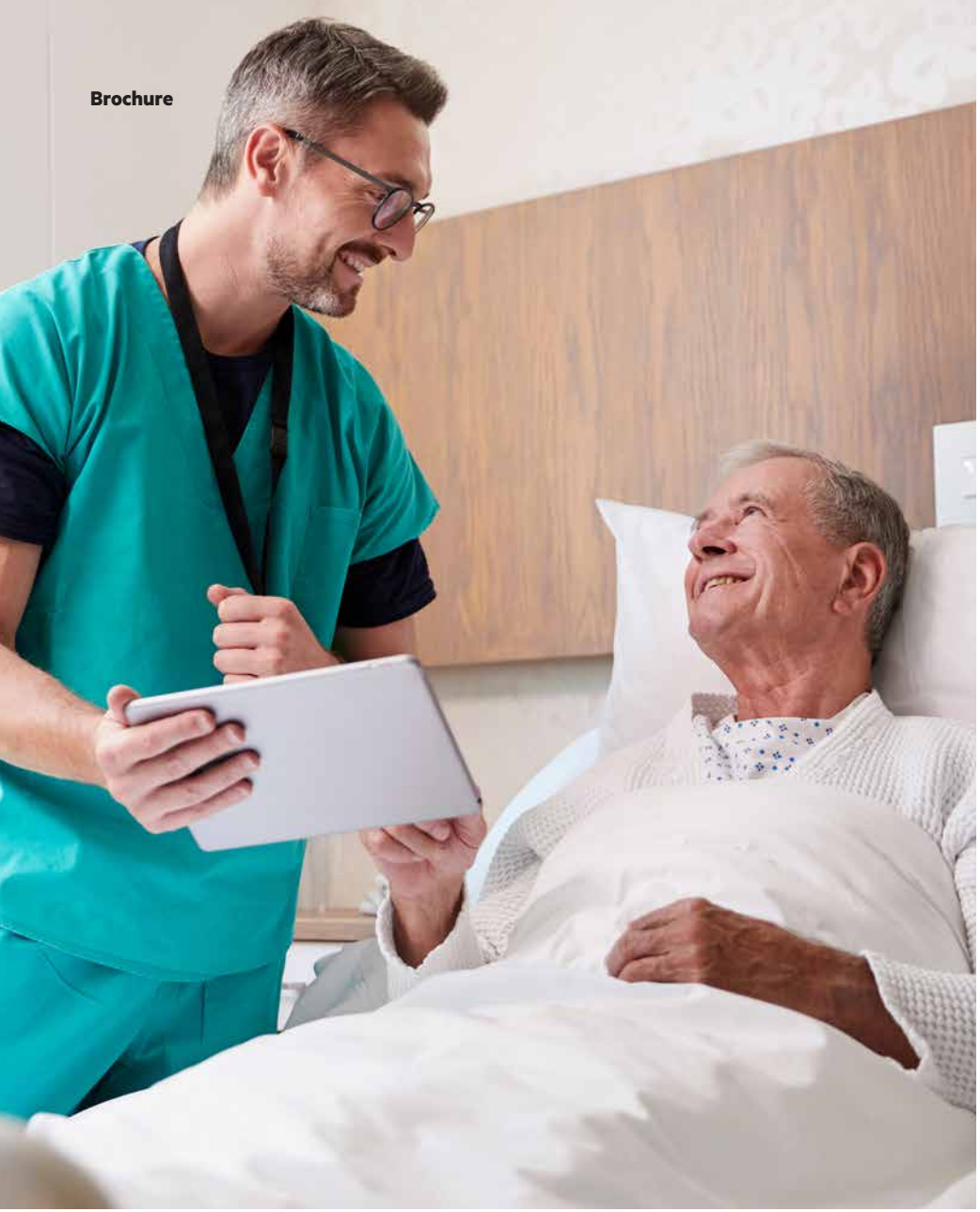
- La détection automatique et le diagnostic des problèmes, grâce à des références dynamiques et une détection des anomalies intégrée, permettant une identification précise des problèmes, de leurs causes et leur résolution, avec une précision proche de 95 %[X]
- Des modèles ML associés à une inspection de paquets en profondeur, permettant d'identifier et de profiler avec précision les clients connectés aux infrastructures sans fil et filaires, sans nécessiter l'utilisation de collecteurs ni d'agents physiques
- Des recommandations du micrologiciel qui permettent de se décharger du suivi manuel des mises à niveau du micrologiciel et réduisent les risques de non-conformité liés aux failles de sécurité

Les fonctionnalités IA de HPE Aruba Networking Central s'appuient sur le plus grand lac de données de l'industrie

2,7
millions d'appareils

200
millions de clients

+ de 30
secteurs d'activité



Bethesda Health Group

L’efficacité du réseau IA axé sur la sécurité

Témoignage client

Depuis 135 ans, Bethesda Health Group s’est forgé une solide réputation en tant que ressource de confiance pour les personnes âgées et leurs familles. Il propose des lieux de vie pour retraités dynamiques et variés qui reflètent fidèlement l’identité des quartiers du Grand St. Louis, ainsi qu’un service de soins à domicile hautement personnalisé. Comptant sur une équipe de 1 100 employés dévoués, l’organisation s’engage à prodiguer des soins de haute qualité, personnalisés, innovants et toujours empreints de compassion dans chacun de ses 16 établissements.

Afin de faire face aux demandes croissantes de ses équipes et de ses résidents, tous adeptes de technologie, Bethesda a décidé d’entreprendre une transformation opérationnelle en adoptant une stratégie axée sur le cloud. En tirant parti d’une connectivité haute performance, la société propose des services de meilleure qualité, fournit l’accès à une multitude d’applications et facilite la communication des résidents avec l’équipe soignante, leur famille et leurs amis. Cette transformation a également exigé des améliorations en matière de cybersécurité, ainsi que l’adoption d’une approche de sécurité zero trust.

Grâce à son partenariat bien établi avec HPE Aruba Networking pour les réseaux filaires, sans fil et SD-WAN (WAN software-defined), Bethesda a décidé de renforcer son infrastructure en adoptant la plateforme Secure Access Service Edge (SASE) entièrement déployée dans le cloud, ainsi que le service HPE Aruba Networking Security Service Edge (SSE).Ce service cloud facile à utiliser regroupe plusieurs fonctionnalités d’accès sécurisé en une seule plateforme, capable d’ajuster automatiquement les politiques en fonction des changements contextuels des utilisateurs, des appareils et des applications.

Suite au déploiement du SD-WAN, Bethesda a cherché à renforcer la sécurité des accès et à se conformer aux exigences d'audit. Grâce à HPE Aruba Networking ClearPass, Bethesda a pu moderniser son contrôle d'accès en adoptant une solution granulaire fondée sur une politique pour ses réseaux filaires et sans fil. Sa petite équipe informatique a rapidement pris en main cette solution, la trouvant intuitive et facile à utiliser.

Bethesda a également été séduit par HPE Aruba Networking Central, une solution qui propose une gestion basée sur le cloud et intégrant une IA, qui a permis une unification encore plus forte de son infrastructure sans fil et filaire.

« Nous avons réussi à mettre en place une infrastructure réseau complète et sécurisée qui nous permet de gérer efficacement nos réseaux filaires, Wi-Fi et SD-WAN, même avec une équipe IT restreinte, et sans nous ruiner. »

– Michael Keller, directeur informatique, Bethesda Health Group[XII]

Lire **l'intégralité de l'article**

Implémentation de la sécurité zero trust

L'adoption d'un modèle de sécurité zero trust est une démarche progressive. Vous ne savez pas par où commencer ? Voici une série de questions axées sur les fonctionnalités qui vous aideront à hiérarchiser vos prochaines étapes :

- ✓ Disposez-vous d'une visibilité totale sur chaque appareil connecté sur votre réseau, même si vous n'en avez pas la gestion directe ?
- ✓ Mettez-vous en place des méthodes cohérentes pour l'attribution des privilèges aux utilisateurs et aux appareils ?
- ✓ Vérifiez-vous la conformité aux normes de sécurité avant d'autoriser un appareil à accéder au réseau ?
- ✓ Appliquez-vous de manière uniforme des politiques de sécurité basées sur les rôles pour l'ensemble du réseau ?
- ✓ Êtes-vous en mesure de surveiller en permanence l'état de sécurité d'un sujet en utilisant toutes les données disponibles ?

Pour en savoir plus sur les réseaux HPE Aruba Networking axés sur la sécurité et intégrant une IA, rendez-vous sur

arubanetworks.com/fr/products/security

[I] Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology. Août 2020.

[II] Équilibrer innovation et risque. Hewlett Packard Enterprise. 2023

[III] Étude globale 2023 sur les moyens de combler les lacunes de sécurité informatique : Combler les failles de cybersécurité de l'edge au cloud. Ponemon Institute. Mars 2023.

[IV] Étude globale 2023 sur les moyens de combler les lacunes de sécurité informatique : Combler les failles de cybersécurité de l'edge au cloud. Ponemon Institute. Mars 2023.

[V] Quelle est la place de la sécurité zero trust dans les entreprises ? HPE Aruba Networking. Avril 2023.

[VI] Étude globale 2023 sur les moyens de combler les lacunes de sécurité informatique : Combler les failles de cybersécurité de l'edge au cloud. Ponemon Institute. Mars 2023.

[VII] Étude globale 2023 sur les moyens de combler les lacunes de sécurité informatique : Combler les failles de cybersécurité de l'edge au cloud. Ponemon Institute. Mars 2023.

[VIII] Infrastructure réseau pilotée par l'IA : La clé de l'efficacité informatique. 2022.

[IX] Hughes, D. Five top networking and security trends for 2024 (Les cinq principales tendances en matière de réseaux et de sécurité en 2024). Janvier 2024.

[X] HPE Aruba Networking Central : Mise en réseau pilotée par l'IA, gérée sur le cloud pour les réseaux de campus, de filiales, distants et de datacenter. 2023.

[XI] HPE Aruba Networking Central : Mise en réseau pilotée par l'IA, gérée sur le cloud pour les réseaux de campus, de filiales, distants et de datacenter. 2023.

[XII] Bethesda Health Group. 2024. https://www.arubanetworks.com/resources/case-studies/bethesda-health-group/

Faites le bon achat.
Contactez nos spécialistes.

Nous contacter

Visiter **ArubaNetworks.com**

Hewlett Packard Enterprise

BR_EasingZeroTrustSecurityadoption_DT_020124 a00137590fre