Aujourd'hui, le réseau est une solution de sécurité

Le réseau piloté par l'IA et axé sur la sécurité de HPE Aruba Networking

Lorsqu'il s'agit de sécurité, les entreprises sont dans l'incertitude et redoutent les menaces imminentes. S'attendent-elles également à un conflit entre les réseaux et les rôles de sécurité ?

Les équipes de réseau et de sécurité peuvent donner une impression trompeuse d'objectifs concurrentiels : l'ouverture de l'accès aux ressources informatiques pour favoriser l'innovation technologique se fait au dépens de l'entreprise en l'exposant à des risques inutiles.

D'après nos clients, si la relation entre les équipes de réseau et de sécurité est faite de négociations, l'innovation et la protection ne peuvent souffrir d'aucune compromission. Les deux sont impératives.

L'opportunité réside dans l'importance croissante du rôle que joue le réseau dans le développement de l'entreprise. Que ce soit par le biais d'une connectivité sur site traditionnelle, ou de l'Internet et du cloud, la mission du réseau est de collecter, sécuriser et fournir des données et ressources informatiques aux utilisateurs, appareils et applications, à tout moment et partout. Étant donnée la nature omniprésente du réseau, il est naturel qu'il soit considéré comme un pont entre la connectivité et la sécurité.

En d'autres termes, le réseau est aujourd'hui une solution de sécurité. Et ce changement de paradigme offre des avantages aux équipes chargées de la sécurité et du réseau.

Dans l'environnement de menaces actuel, chaque ressource doit contribuer à la cybersécurité. Ainsi, le réseau devient la base des architectures telles que Zero Trust et SASE. Grâce à sa double fonction en tant que pilier de la connectivité et garant de la cybersécurité, le réseau devient naturellement un lieu propice à la collaboration et à la coopération entre les équipes de réseau et de sécurité.

Mais tous les réseaux ne sont pas capables de mener à bien ces deux missions.

Un réseau doit satisfaire 4 prérequis pour soutenir les objectifs de connectivité et de sécurité.

- **Des solutions Zero Trust et SASE intégrées dans l'infrastructure réseau.** Cela implique de concevoir et mettre en œuvre l'approche « ne faire confiance à rien ni personne » tout en appliquant les politiques de contrôle d'accès basé sur le « moindre privilège » qui sont utilisées en toute transparence de l'edge au cloud. Cette démarche est à l'opposé de l'utilisation de composants additionnels de sécurité externes pour combler les lacunes de la sécurité du réseau.

- **Un cadre de politiques commun pour le réseau et la sécurité.** Les équipes utilisent toutes deux des politiques pour exprimer des résultats escomptés, que ce soit du point de vue de la sécurité ou de la connectivité. Les solutions réseau Zero Trust et SASE intégrées simplifient l'expression et la mise en œuvre des politiques afin que les deux équipes puissent définir leurs résultats escomptés et se fier aux résultats.
- **L'intégration avec l'écosystème de sécurité.** Le réseau est le point de contact central de toute activité informatique. Les flux de paquets sont la source de vérité du fonctionnement du réseau et de la fourniture d'informations relatives à la sécurité à d'autres solutions de sécurité, telles que les pare-feux, les SIEM, etc. Les paquets de données peuvent être résumés ou livrés bruts pour une analyse en amont. Par ailleurs, étant donné que le réseau est le gardien de l'accès informatique, il peut intercepter et bloquer les attaques détectées par d'autres parties de l'écosystème.
- **L'analytique pilotée par l'IA.** Oui, l'IA est un mot à la mode, mais appliquer le réseau IA aux problèmes de sécurité est le seul moyen d'offrir une cyberprotection complète. Par exemple, les équipes de réseau et de sécurité sont hantées par les appareils malveillants qui parviennent à pénétrer le réseau. Ils sont non seulement une source de vulnérabilité, mais ils ne sont soumis à aucune politique de contrôle d'accès. En appliquant l'IA à la télémétrie du réseau, les appareils sont découverts et consignés avec un haut niveau de précision, ce qui permet d'appliquer automatiquement des politiques de contrôle d'accès.

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

Ces capacités de connectivité et de sécurité n'apparaissent pas comme par magie dans les réseaux dont la sécurité est externalisée avec des produits tiers rajoutés. Qu'il s'agisse de pare-feu à états de couche d'application intégré, de NAC natif pour le cloud ou de découverte et profilage d'appareils, HPE Aruba Networking est un leader historique dans les solutions réseau pilotées par l'IA, axées sur la sécurité.

Le réseau piloté par l'IA et axé sur la sécurité de HPE Aruba Networking est conçu selon les principes du Zero Trust, offre une base commune aux équipes de réseau et de sécurité pour créer des expériences uniques et obtenir des résultats commerciaux innovants, sans compromettre la cybersécurité. Grâce aux solutions HPE Aruba Networking, votre 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. Notre réseau piloté par l'IA aide aussi vos équipes à bénéficier 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.

Faites le bon achat.
Contactez nos spécialistes.

Nous contacter

Visitez **ArubaNetworks.com**

SB_SecuritySolution_RVK_020624 a00137647fre

Hewlett Packard Enterprise