Les pirates s'infiltrent dans votre entreprise. Ils exploitent l'IoT, la mobilité et la complaisance pour pirater votre entreprise.

Aruba ClearPass apporte de la visibilité, du contrôle et de la sécurité à l'entreprise qui est n'importe où, n'importe quand avec n'importe quel appareil

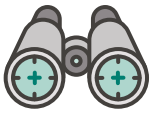
aruba
a Hewlett Packard Enterprise company

SEQUENCE INFORMATIQUE

Selon l'étude de **2016 de Ponemon sur le coût de la violation des données**, les spécialistes malveillants continuent à représenter le vecteur d'attaque le plus important, coûteux et efficace, tandis que 76 % des entreprises restent sans protection contre ces menaces.[1] En même temps, la croissance exponentielle de l'IoT, des appareils d'entreprise et personnels a réduit encore davantage la visibilité, alors que les ressources n'ont pas été accrues en proportion pour la sécurité.

Les entreprises adoptent de plus en plus la pratique de la « connectivité en tout temps et en tous lieux », mais souvent sans se préoccuper de la nécessité d'un système sécurisé de contrôle des accès au réseau (NAC). Nombreuses sont celles qui adoptent une philosophie *d'accès au réseau décontractée* de type « connectez-vous maintenant, sécurisez plus tard ». D'autres choisissent simplement le même fournisseur pour l'infrastructure du réseau et leurs solutions de sécurité. Ces deux approches donnent l'illusion de la sécurité, et même de la conformité, mais en réalité, elles laissent apparaître de graves déficits de sécurité.

Le besoin de visibilité, de contrôle et de réaction



La visibilité est un problème critique pour les équipes d'exploitation et de sécurité en sous-effectif. **Une étude de Gartner** démontre que chaque employé utilise en moyenne trois appareils mobiles,[2] et maintenant, les objets connectés à internet doivent également être pris en considération. Il faut prendre en compte les invités de l'entreprise, les sous-traitants et les employés temporaires, et le nombre d'appareils filaires et sans fil qui se connectent au réseau augmente encore. Sans données précises sur ces objets connectés, les failles de sécurité apparaissent et sont exploitées. La visibilité est la première étape pour refermer ces failles.

Le contrôle des appareils est essentiel à la sécurité d'entreprise. Le fait de s'assurer que seuls les appareils autorisé et/ou authentifiés se connectent à votre réseau filaire ou sans fil réduit sensiblement les risques et libère des ressources.

Réaction. Vos outils de sécurité existants — y compris les systèmes de gestion des événements et informations de sécurité, les pare-feux et les antivirus — fournissent des données hétérogènes difficilement exploitables sur les événements. Des outils de sécurité trop nombreux fournissent trop de possibilités de remèdes de sécurité. Lorsque les données relatives à la menace sont unifiées, vous pouvez prendre des mesures simples et nuancées pour suspendre ou déconnecter les appareils malveillants au niveau de la couche du réseau, et par conséquent limiter la perte—sans nécessiter de ressources ou processus supplémentaires.

Appliquez la sécurité à l'échelle de votre entreprise

Avec un contrôle des accès au réseau sécurisé, votre entreprise peut avoir une stratégie de sécurité robuste sans ressources supplémentaires. La solution appropriée fournit à votre équipe informatique :

- **Visibilité** sur tous les appareils connectés ou en cours de connexion, filaires et sans fil
- **Contrôle** de l'IoT, des appareils personnels et d'entreprise, à travers de multiples fournisseurs de réseaux
- **Capacité de réaction** grâce à l'intégration transparente d'outils de sécurité pour une détection automatisée des menaces, l'escalade et la mise en œuvre d'une stratégie unifiée

La solution de contrôle des accès au réseau d'Aruba, ClearPass, fournit une protection sur un rayon de sécurité unique et des points de vérification pour les réseaux, les applications, l'IoT, les employés, les sous-traitants et les invités qui utilisent des appareils filaires et sans fil. Aruba ClearPass permet aux organisations de créer, définir et mettre en vigueur une politique d'accès cohérente de ce qui peut se connecter et à quels éléments de l'entreprise, selon le type d'appareil, de qui l'utilise, d'où et quand il est utilisé, du type de connexion et de son état.

Seul Aruba ClearPass peut assurer une connectivité sécurisée dans un environnement où la sécurité et l'infrastructure reposent sur plusieurs fournisseurs. Plus de 7 000 entreprises dans le monde utilisent Aruba ClearPass pour garantir un environnement mieux sécurisé et plus productif.

Pourquoi Aruba ClearPass ?

Sécurisez tous les objets—d'entreprise, personnels et IoT—filaires et sans fil

- Identifiez tous les appareils, sécurisez l'accès et assurez-vous que seuls les appareils authentifiés, autorisés ou sains puissent se connecter—à la fois filaires et sans fil—indépendamment du fournisseur du réseau
- Utilisez une solution de confiance, déployée sur les plus grands réseaux, dans plus de 7 000 organisations, couvrant plus de 28 marchés sectoriels différents
- Assurez-vous que votre contrôle d'accès soit prêt pour l'analytique comportementale des utilisateurs et des entités—sécurisez l'accès, puis surveillez et sécurisez l'utilisation



Mettez en vigueur une politique filaire et sans fil

- Définissez ce que les appareils peuvent et ne peuvent pas faire, et l'infrastructure, les applications et les données auxquelles ils peuvent accéder
- Bloquez la faille entre les ports sans fil chiffrés et les ports filaires ouverts
- Renforcez la sécurité des appareils personnels tout en simplifiant l'authentification des applications et des périphériques

Rationalisez la gestion de la sécurité des réseaux

- Unifiez la réaction aux violations potentielles et aux menaces avec les meilleurs fournisseurs de sécurité, le tout à partir d'une même console de gestion
- Renforcez votre périmètre en connaissant et en contrôlant tout ce qui se connecte au sein de l'entreprise
- Automatisez la réaction aux attaques et unifiez les actions face aux menaces avec plus de 100 fournisseurs de sécurité et d'infrastructure

Améliorez la sécurité de bout en bout avec Aruba ClearPass

Découvrez comment Aruba ClearPass peut mettre en œuvre la sécurité à l'échelle de votre entreprise.

EN SAVOIR PLUS

RÉFÉRENCES

[1] *Étude sur le coût d'une violation de sécurité des données en 2016 : Analyse mondiale*, rapport de recherche de l'Institut Ponemon, juin 2016.

[2] *Gartner Says Demand for Enterprise Mobile Apps Will Outstrip Available Development Capacity Five to One*, Gartner, 16 juin 2015.

aruba
a Hewlett Packard Enterprise company

SEQUENCE INFORMATIQUE