FORESCOUT

Visibilité sur les appareils : la clé pour réduire le risque et renforcer votre sécurité

Un plan en six points pour améliorer la sécurité avec une visibilité totale sur les appareils

Sécuriser l'infrastructure réseau devient un peu plus compliqué chaque jour. Cette complexité grandissante est due à la multiplication phénoménale des appareils de l'Internet des objets (IoT), à la diversification des plateformes, à l'adoption du cloud ainsi qu'à la convergence de l'IT et de l'OT. La grande majorité des nouveaux appareils qui rejoignent vos réseaux ne sont pas conçus pour prendre en charge les agents de gestion, ce qui augmente sérieusement votre niveau de risque et votre déficit de visibilité. Et cette situation s'aggrave à mesure que le cloud s'étend aux confins du réseau distribué.

Une chose est sûre : l'invisible peut être un ennemi fatal. Vous avez donc besoin d'une fonction permettant la découverte des appareils, qu'ils soient dotés d'un agent ou non, qu'ils soient physiques ou virtuels, et peu importe où ils se trouvent. Ces appareils doivent en outre faire l'objet d'une surveillance continue en temps réel, mais aussi pouvoir être profilés et classés au moment où ils se connectent à votre réseau. Combler ce déficit de visibilité est le moyen le plus efficace d'influencer positivement vos initiatives de sécurisation des réseaux et de réduction des risques. Les six points ci-dessous expliquent comment y parvenir grâce à une visibilité optimale.

1 Obtenir une visibilité sur tous les systèmes, y compris BYOD, IoT et OT, sans utiliser d'agent

La sécurité passe avant tout par la visibilité. Il est évident qu'une solution n'a de réel intérêt que si elle fournit une vue précise et en temps réel de tous les terminaux du réseau.

Les traditionnelles solutions de sécurité avec contrôle d'accès au réseau (NAC) sont capables de détecter uniquement les appareils pourvus d'un agent. Or, il est impossible de charger des agents sur tous les appareils BYOD et non traditionnels qui se connectent à votre réseau, qu'il s'agisse des smartphones, tablettes ou technologies vestimentaires appartenant au personnel ou encore des appareils IoT, systèmes OT et ordinateurs portables des sous-traitants, sans compter les appareils non approuvés de provenance inconnue. Tous mettent votre entreprise en péril.

Vous avez besoin d'une visibilité sans agent pour identifier tout appareil, quel qu'il soit, à l'instant même où il se connecte à votre réseau. De plus, la simple détection d'une adresse IP ou MAC ne suffit pas : des informations détaillées sur chaque appareil sont nécessaires, pour déterminer sa finalité, son propriétaire et son niveau de sécurité.

2 Unifier la visibilité et le contrôle sur les environnements de réseau de campus, de centre de données et cloud

Il n'y a pas si longtemps, protéger votre centre de données suffisait. Mais dans un monde beaucoup plus complexe, la donne a changé. De nombreuses architectures à un seul centre de données ont été transformées en déploiements à centres de données multiples connectés à des réseaux de campus distribués pouvant s'étendre à l'échelle du globe. Et puis, il y a le cloud.

Vous ne pouvez plus vous contenter de contrôler le périmètre réseau (ou ce qu'il en reste aujourd'hui). Vous avez besoin d'un accès instantané et en temps réel à tous les terminaux, au niveau du centre de données, du réseau de campus et du cloud. Il est désormais inconcevable de tenter de gérer et de sécuriser les appareils et les charges de travail à l'aide d'interfaces et d'outils ponctuels disparates. **Pour être viable, la solution doit offrir une vue consolidée des systèmes traditionnels, terminaux mobiles et appareils IoT, ainsi que des machines virtuelles et instances cloud, et ce quel que soit leur emplacement**. Ce n'est pas tout : la solution mise en place doit offrir une évolutivité sans précédent, de façon à répondre à vos besoins croissants en matière de réseaux.

Ce nouveau modèle indépendant, tant vis-à-vis des technologies que de l'emplacement, exige de repenser l'interopérabilité des solutions (et de se montrer moins tolérant à l'égard de l'enfermement propriétaire). À l'heure actuelle, la valeur d'une technologie s'accroît lorsqu'elle offre une visibilité partagée entre systèmes par le biais de mécanismes de contrôle et de tableaux de bord communs. Le nouveau modèle requiert la flexibilité nécessaire pour déployer une architecture à la fois centralisée et distribuée en fonction de l'évolution des besoins de l'entreprise.

3 Respecter les obligations de conformité des appareils et de conformité réglementaire

L'échec cuisant… De nombreux tests d'intrusion ou audits de conformité réglementaire se soldent aujourd'hui par un tel résultat, notamment en raison d'appareils IoT non détectés ou d'autres actifs à risque mal segmentés. D'où l'importance d'une stratégie de sécurité efficace, laquelle exige avant tout une visibilité continue sur les appareils et des inventaires complets de ces actifs. Vous éviterez ainsi de mettre votre entreprise en danger — sur le plan juridique et financier.

Des données inexactes dans votre système de gestion des actifs informatiques (ITAM) peuvent vous mettre en situation de non-conformité aux réglementations, notamment le RGPD, les lois HIPAA et FISMA, ou la norme PCI. Votre entreprise pourrait alors se voir infliger de lourdes amendes.

Quels que soient les types d'actifs que vous sécurisez (financiers, médicaux, industriels ou autres), la première étape vers une gestion performante du risque et de la conformité est de s'assurer une visibilité absolue. Vous devez pouvoir *voir et classer les appareils, puis automatiser leur contrôle et limiter leur accès* à des zones spécifiques du réseau en fonction des niveaux d'autorisation, des politiques de sécurité d'entreprise et des obligations réglementaires.

Étant donné que bon nombre des réglementations actuellement en vigueur, au niveau local, national ou international, exigent qu'une violation de sécurité soit rendue publique dans les heures qui suivent l'incident, il est crucial que les plateformes de sécurité agissent de concert pour garantir une correction et une riposte à la fois rapide et efficace.

4 Automatiser l'inventaire des appareils et leur gestion

Pour gérer et sécuriser les actifs de l'entreprise de façon efficace, vous avez besoin d'un inventaire qui recense avec précision tous les appareils de votre réseau. N'oubliez pas qu'il suffit d'un appareil ne figurant pas dans votre inventaire ou dont les informations de configuration sont obsolètes ou erronées pour que les pirates se jettent sur l'occasion et s'introduisent dans votre réseau. Cela dit, la découverte des appareils à l'aide d'approches traditionnelles peut s'avérer difficile. Gartner estime que d'ici 2020, 30 % des actifs d'entreprise demeureront non détectés en l'absence de découverte active.

L'exécution manuelle de la découverte des actifs peut aboutir à une base de données de gestion de la configuration (CMDB) incomplète et inexacte, qui compromettrait vos initiatives de gestion de la sécurité. Le suivi de l'inventaire au moyen de feuilles de calcul Excel ou d'autres méthodes manuelles engendre des erreurs, sans compter que les données d'inventaire deviennent rapidement obsolètes. Un inventaire des appareils parfaitement à jour permet aux équipes du centre d'assistance d'être plus réactives.

De plus, *pouvoir accéder immédiatement à des informations exactes sur les appareils est essentiel pour les équipes des opérations de sécurité chargées de neutraliser des attaques ciblées lancées spécifiquement contre certains systèmes d'exploitation de terminaux ou des types d'appareils IoT*. Par ailleurs, à moins d'effectuer un suivi rigoureux des logiciels, vous vous exposez à une surutilisation des licences et au non-respect des accords de licence, ce qui peut se traduire par des sanctions sévères.

L'automatisation de l'inventaire des appareils et de leur gestion vous permet de partager des données contextuelles avec des outils ITAM, tels que ServiceNow®, afin de bénéficier d'une base de données CMDB parfaitement à jour en temps réel. Votre inventaire à jour peut en outre gérer de façon efficace le cycle de vie des appareils, vous aidant à planifier les budgets d'investissement en actifs.

5 Mettre en œuvre la segmentation de réseau sensible au contexte

En général, les professionnels des réseaux et les experts en sécurité s'accordent à dire que, lors de la sécurisation du réseau, sa segmentation doit être la priorité absolue. Grâce à l'évaluation des appareils et leur répartition en segments, vous pouvez automatiser l'affectation et l'application, basées sur des politiques, de listes de contrôle d'accès et de VLAN, mais aussi attribuer dynamiquement les appareils à des segments pour contrôler l'accès et limiter celui-ci aux seules ressources autorisées dans ces segments. Cette stratégie est efficace pour, d'une part, empêcher les membres du personnel de s'aventurer dans des zones du réseau qui sortent du champ de leurs responsabilités et, d'autre part, limiter la propagation d'une attaque par logiciel malveillant.

L'ajout d'informations contextuelles en temps réel sur les appareils aux affectations de segments améliore de façon substantielle la sécurité de plusieurs façons. Par exemple, une solution dotée de cette fonctionnalité est capable de valider l'état de conformité d'un appareil avant de l'attribuer à un groupe de segmentation. De plus, elle peut surveiller en continu le niveau de sécurité et le comportement des appareils pour réaffecter rapidement tout équipement non autorisé ou non conforme au segment adéquat ou à un VLAN à accès restreint si nécessaire (il peut s'agir par exemple d'une imprimante qui tente d'accéder à une base de données des ressources humaines ou d'une caméra de surveillance qui essaie d'accéder à un composant autre qu'un enregistreur vidéo numérique). *Cette nouvelle méthode de segmentation à la fois intelligente et dynamique simplifie en outre considérablement la modification du réseau et offre une plus grande souplesse sur le plan de l'architecture en permettant le partage de données contextuelles et l'orchestration avec les pare-feux de nouvelle génération.*

Pour mener à bien cette étape, vous avez besoin d'une solution NAC qui s'intègre facilement avec les commutateurs, les réseaux privés virtuels (VPN), les systèmes de gestion cloud et les pare-feux de nouvelle génération.

6 Réduire votre période d'exposition grâce à une intervention sur incident orchestrée

Les équipes chargées de la sécurité du réseau *gèrent jusqu'à 15 outils en moyenne*, ce qui signifie que les entreprises consacrent beaucoup d'argent — et de temps — à l'achat de ces outils, ainsi qu'à l'apprentissage et à la coordination de leur utilisation. Ce n'est pas tout… La plupart de ces solutions de sécurité excellent lorsqu'il s'agit d'envoyer des alertes, mais sont incapables d'appliquer les mesures qui s'imposent. Par conséquent, les équipes de sécurité sont submergées par une foule d'alertes qu'elles doivent évaluer et résoudre manuellement.

Pour accélérer l'intervention sur incident, les outils doivent exécuter les actions requises de façon hautement automatisée en cas d'alerte, réagir automatiquement face aux situations connues et fournir aux analystes en sécurité des renseignements priorisés lors de l'apparition de nouvelles menaces.

Afin que vous en tiriez le meilleur parti, ces outils doivent vous offrir une interopérabilité clé en main des flux de travail et vous permettre d'exécuter une découverte et une classification automatisées des appareils. Les solutions choisies doivent en outre être prêtes à fonctionner instantanément avec vos outils réseau existants pour orchestrer le partage de données en temps réel, les alertes et l'intervention sur incident avec d'autres outils ITAM et de sécurité.

Tout nouvel outil doit prendre en charge les réseaux où se côtoient les produits de plusieurs fournisseurs de même que leurs actifs, qu'ils soient physiques ou virtuels, et dans tous les environnements : réseau de campus, centre de données et cloud.

La solution Forescout

La plateforme Device Visibility and Control proposée par Forescout vous aide à mener à bien ces six étapes, et elle offre bien plus. Elle assure la découverte en continu de tous les appareils IP, sans nécessiter d'agent, au moment où ils se connectent à votre réseau. Elle garantit une visibilité en profondeur sur ces appareils grâce à la combinaison de techniques de découverte active et passive, de profilage et de classification. Et elle bénéficie d'une évolutivité exceptionnelle, qui lui permet de prendre en charge jusqu'à deux millions d'appareils dans une simple appliance CounterACT® Enterprise Manager.

Notre approche unique sans agent offre une visibilité sur les appareils les plus variés : peu importe qu'ils soient gérés ou non, câblés ou sans fil, la propriété de l'entreprise ou privés, ou encore qu'il s'agisse d'appareils IoT, d'équipements non approuvés, de commutateurs, de serveurs ou de systèmes BYOD personnels.

Forescout va beaucoup plus loin en matière de visibilité et de contrôle sur les appareils, afin de réduire les risques ainsi que la surface d'attaque et d'automatiser l'intervention sur incident à l'échelle du réseau d'entreprise étendu — ***votre*** réseau.

Glossaire des acronymes

ACL: Access Control List (liste de contrôle d'accès)

BYOD: bring your own device (prenez vos appareils personnels)

CMDB: configuration management database (base de données de gestion de configuration)

FISMA: Federal Information System Management Act

HIPAA: Health Insurance Portability and Accountability Act

IoT: Internet of Things (Internet des objets)

IP: Internet Protocol (Protocole Internet)

ITAM: information technology asset management (gestion des actifs informatiques)

MAC: Media Access Control (Contrôle d'accès au support)

NAC: network access control (contrôle d'accès au reseau)

OT: operational technology (technologies d'exploitation)

PCI: Payment Card Industry (Industrie des cartes de paiement)

VLAN: virtual local area network (réseau local virtuel)

VPN: virtual private network (réseau privé virtuel)

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 (États-Unis)

Email info-france@forescout.com
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591