Contrôle d'accès au réseau

Bénéficiez d'une visibilité en temps réel et contrôlez les appareils dès leur connexion à votre réseau

Défis organisationnels

- Améliorer la sécurité globale du réseau
- Protéger les données sensibles contre les menaces externes
- Ne pas entraver l'accès des employés, sous-traitants et clients
- Respecter les politiques internes et les réglementations externes
- Préserver la valeur des investissements en sécurité existants

Défis techniques

- Détecter sur le réseau les appareils inconnus qui ne sont pas dotés de logiciels d'agent
- Identifier le type et l'emplacement de l'appareil, l'identité et le rôle de l'utilisateur, ainsi que le degré de conformité
- Empêcher les appareils infectés ou non conformes de propager des logiciels malveillants
- Empêcher les attaques ciblées de voler des données ou de rendre le réseau indisponible
- Trouver une solution NAC capable de répondre automatiquement à chaque situation de manière appropriée, sans aucune intervention humaine
- Mesurer l'efficacité des contrôles de sécurité et démontrer le respect des règlementations

ForeScout Technologies, Inc. fournit des solutions uniques pour contrôler et gérer le nombre croissant d'appareils et de types d'appareils qui accèdent chaque jour aux réseaux. Notre produit phare, ForeScout CounterACT®, vous offre une visibilité en temps réel, en vous permettant de détecter instantanément les appareils autorisés *et* non autorisés, et de contrôler leur accès à votre convenance.

Le défi

Aujourd'hui, les réseaux d'entreprise servent un vaste ensemble d'appareils traditionnels et non traditionnels et d'autres points d'extrémité, depuis les PC, tablettes et smartphones jusqu'aux contrôles industriels, serveurs virtualisés, points d'accès sans fil et applications basées sur le Cloud. Et il ne fait aucun doute que les défis en matière de gestion des appareils ne cesseront de s'amplifier avec le développement des environnements informatiques BYOD*, IoT* et hybrides et la plus grande sophistication des attaques. Votre solution de contrôle d'accès au réseau (NAC) doit donc être capable de gérer les appareils connus appartenant à l'entreprise ou aux employés, ainsi que les appareils inconnus non autorisés et « discrets » de plus en plus nombreux.

Les faits exposés ci-après attestent de la nécessité d'une solution de sécurité NAC complète et hautement intelligente :

- 26 milliards d'appareils connectés et en réseau seront utilisés d'ici 2020.[1]
- 75 % des applications mobiles ne satisfont pas les tests de sécurité de base.[2]
- En 2014, 98,7% des enregistrements compromis l'ont été suite à une attaque externe.[3]

En tant que responsable des systèmes d'information ou de sécurité, vous devez être en mesure de savoir si les appareils et systèmes qui tentent d'accéder ou qui sont déjà connectés à votre réseau respectent les normes de sécurité de votre entreprise.

La solution ForeScout

ForeScout CounterACT® offre notamment des fonctionnalités NAC complètes, basées sur la visibilité en temps réel des appareils dès leur connexion au réseau. La solution analyse en continu le réseau et surveille l'activité des appareils connus détenus par l'entreprise, ainsi que des périphériques inconnus, tels que les dispositifs détenus à titre personnel et les points d'extrémité malveillants. Elle vous permet aussi d'automatiser et de mettre en œuvre un contrôle d'accès au réseau, une conformité des points d'extrémité et une sécurité des appareils mobiles basés sur des politiques. En fait, ForeScout CounterACT fournit une large gamme de contrôles automatisés qui préservent l'expérience des utilisateurs et améliorent la performance des entreprises.

Les fonctionnalités de base de CounterACT peuvent se résumer en trois mots :

Voir CounterACT offre la possibilité unique de détecter des appareils dès leur connexion à votre réseau sans aucun agent logiciel ou aucune connaissance préalable des équipements. Il crée des profils et classe les appareils, utilisateurs, applications et systèmes d'exploitation tout en surveillant en permanence les appareils gérés, les appareils détenus à titre personnel et les autres points d'extrémité.

Contrôler CounterACT peut accorder, refuser ou limiter l'accès au réseau en fonction du niveau de sécurité des appareils et des politiques de sécurité. En évaluant et en isolant les points d'extrémité malveillants ou à haut risque, il atténue les risques de vol des données et d'attaques de logiciels malveillants qui pourraient nuire à votre entreprise. En outre, en surveillant en permanence les appareils de votre réseau et en les contrôlant conformément à vos politiques de sécurité, CounterACT vous aide à garantir le respect des normes et des réglementations de l'industrie.

Orchestrer CounterACT s'intègre avec plus de 70 produits de gestion du réseau, de la sécurité, de la mobilité et des SI ** via l'architecture ForeScout ControlFabric®. Cette capacité à partager les informations de sécurité en temps réel entre les systèmes et à appliquer une politique unifiée de sécurité réseau permet de réduire les fenêtres de vulnérabilité en automatisant la réponse aux menaces à l'échelle du système. En outre, il vous permet d'augmenter la rentabilité de vos outils de sécurité existants tout en gagnant du temps grâce à l'automatisation des flux de travail.

ForeScout CounterACT recueille des informations contextuelles détaillées sur le point d'extrémité, son emplacement, son propriétaire et son contenu. Il peut garantir que :

- votre réseau ne comporte pas d'appareils non autorisés ou d'applications illégitimes ;
- les appareils autorisés sont configurés avec les systèmes d'exploitation les plus récents, qu'un logiciel antivirus à jour est installé et en cours d'exécution, et que les vulnérabilités sont corrigées ;
- les agents de chiffrement et de prévention contre la perte de données fonctionnent ;
- les utilisateurs ne peuvent pas exécuter des applications ou appareils périphériques non autorisés sur le réseau.

Lorsque les points d'extrémités ne sont pas conformes aux normes de l'entreprise, CounterACT lance automatiquement une ou plusieurs actions de remédiation basées sur des politiques qui vont de l'envoi par e-mail d'une notification de non-conformité à la remédiation obligatoire (par exemple une mise à jour du logiciel), en passant par la mise en quarantaine ou l'interdiction d'accès pure et simple. La gestion de l'accès des invités, la localisation des systèmes, l'ouverture et la fermeture des ports réseau ne nécessitent aucune intervention humaine ou tâche manuelle. L'accès au réseau est contrôlé conformément à la politique.

ForeScout fournit à plus de 2 000 entreprises réparties dans plus de 60 pays** un contrôle d'accès au réseau intelligent, rentable et conforme aux normes de sécurité et réglementations les plus strictes, ainsi qu'une facilité d'utilisation et de déploiement. CounterACT est commercialisé sous forme de boîtier virtuel ou physique qui se déploie dans votre infrastructure existante et ne nécessite en général aucune modification de la configuration réseau. Le boîtier CounterACT s'installe physiquement hors bande, ce qui évite la latence ou les problèmes liés au risque de défaillance du réseau. Il peut être administré de manière centralisée afin de gérer dynamiquement des dizaines, des centaines voire même des milliers de points d'extrémité à partir d'une seule console.

Pour en savoir plus, visitez le site **www.ForeScout.com**

ForeScout®

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 (États-Unis)

Numéro gratuit (depuis les États-Unis) 1-866-377-8771
Tél. (depuis les autres pays) +1-408-213-3191
Assistance technique 1-708-237-6591
Fax 1-408-371-2284

1 Recherche de Gartner, http://www.gartner.com/newsroom/id/2636073
2 Recherche de Gartner, septembre 2014 http://www.scmagazine.com/gartner-75-percent-of-mobile-apps-will-fail-security-tests-through-end-of-2015/article/372424/
3 Recherche de Privacy Rights Clearinghouse, http://www.securityweek.com/data-breaches-numbers

*BYOD (Apportez vos appareils personnels), IoT (Internet des objets)
** En janvier 2016