FORESCOUT

HAWORTH®

Haworth

Le fabricant international choisit Forescout pour sécuriser ses réseaux IT et OT et rentabilise son investissement de façon impressionnante

SECTEUR D'ACTIVITÉ

Industriel

ENVIRONNEMENT

12 000 appareils filaires et sans fil répartis sur 20 sites de production et dans 55 bureaux commerciaux à travers le monde ; effectif de 6 200 personnes

DÉFI

- Manque de visibilité sur l'ensemble des appareils du réseau, notamment les appareils IoT et OT
- Visibilité insuffisante sur le niveau de sécurité/d'intégrité des appareils des sociétés récemment rachetées
- Nécessité d'une disponibilité ininterrompue dans l'environnement OT
- Petite équipe de sécurité dont le temps et les ressources sont limités

SOLUTION

- Plateforme Forescout
- Forescout Enterprise Manager
- Forescout eyeExtend pour Palo Alto Networks Next-Generation Firewall (anciennement module avancé)

CAS D'UTILISATION

- Visibilité sur les appareils
- Conformité des appareils
- Contrôle de l'accès au réseau
- Segmentation réseau
- Intervention sur incident

Présentation

Spécialiste de l'innovation et de la productivité, Haworth Inc. conçoit et fabrique des espaces de travail adaptables, proposant notamment des planchers techniques, des parois amovibles, des systèmes d'aménagement, des sièges, ainsi que les espaces technologiques de collaboration en temps réel Workware™ en versions câblée et sans fil. Cette entreprise internationale possédant des bureaux à Paris et Lyon emploie 6 200 personnes réparties dans 20 sites de production et 55 agences commerciales à travers le monde. À la suite de plusieurs rachats récents dans les secteurs du design et de l'art de vivre, Haworth devait se doter d'une solution de contrôle d'accès au réseau (NAC) qui limite l'accès à son réseau d'entreprise aux seuls appareils autorisés respectant ses normes de sécurité.

Pour répondre à ses besoins en matière de contrôle d'accès au réseau et combler d'autres failles dans son dispositif de sécurité (notamment au niveau de la détection et de l'isolement des appareils non approuvés), Haworth a implémenté la plateforme Forescout. Offrant une visibilité et un contrôle granulaires, la solution Forescout a fortement amélioré le niveau de sécurité des environnements IT et de production. Son intégration aux pare-feu de l'entreprise a en outre permis l'automatisation de diverses tâches de sécurité, faisant gagner un temps précieux à l'équipe de sécurité informatique de Haworth. Enfin, la plateforme Forescout a fait ses preuves dans des domaines autres que celui de la sécurité puisque des équipes opérationnelles comme celle chargée de la gestion du réseau en tirent également profit.

Défi pour l'entreprise

« Pour ces cas d'utilisation et d'autres, nous avions besoin non seulement d'une plus grande visibilité et d'un meilleur contrôle, mais nous devions également pouvoir classifier les appareils, segmenter les réseaux par type d'appareil et rechercher les indicateurs de compromission — le tout en temps réel. »

— Joseph Cardamone, analyste en sécurité informatique et responsable de la protection de la vie privée pour l'Amérique du Nord, Haworth

Joseph Cardamone, analyste en sécurité informatique et responsable de la protection de la vie privée pour l'Amérique du Nord chez Haworth, supervise la stratégie de sécurité informatique de l'entreprise. En compagnie des collègues avec qui il forme l'équipe de sécurité informatique, constituée de trois personnes seulement, il s'efforce de protéger les environnements réseau commerciaux et de production de l'entreprise internationale Haworth. Les récents rachats de plusieurs sociétés gérées de façon autonome ont ajouté à la difficulté.

S'agissant de la nécessité d'améliorer la visibilité et le contrôle, les appareils appartenant aux nouvelles sociétés n'étaient pas les seuls actifs concernés. Par exemple, l'équipe avait besoin d'une méthode plus efficace et plus rapide

RÉSULTATS

- Retour sur investissement rapide : 97 % des terminaux découverts et catégorisés seulement sept heures après l'implémentation
- Visibilité en temps réel sur tous les appareils au moment où ils se connectent au réseau
- Protection plus aisée des appareils OT et qui se déplacent continuellement grâce à la segmentation dynamique du réseau
- Contrôle de l'accès réseau pour les appareils des sociétés nouvellement acquises lors de leurs tentatives de connexion au réseau d'entreprise
- 20 heures par semaine gagnées grâce à l'automatisation de tâches de sécurité
- Gain de temps supplémentaire grâce à l'automatisation de processus manuels de recherche et d'isolement des appareils à haut risque
- Productivité optimisée pour l'équipe de sécurité informatique (trois personnes seulement)
- Visibilité granulaire utile pour différentes équipes : sécurité, IT et gestion de réseau
- Découverte d'un nombre d'appareils 60 % plus élevé que prévu

pour localiser les appareils IoT à haut risque et les empêcher de recevoir ou de transmettre des communications non autorisées. Elle devait en outre pouvoir identifier et sécuriser facilement les espaces de collaboration numérique Workware — produits technologiques propriétaires de l'entreprise —, qui sont constamment déplacés d'un site à un autre et dont les composants matériels et logiciels sont fréquemment mis à jour.

Pourquoi avoir choisi Forescout ?

Une mine précieuse d'informations, une grande facilité de déploiement et d'utilisation

Joseph Cardamone et son équipe ont réalisé des preuves de concept de la plateforme Forescout et d'une solution d'un fournisseur déjà bien implanté au sein de l'entreprise et soutenu par l'équipe réseau de Haworth. Forescout s'est clairement imposé comme le meilleur choix. « La plateforme Forescout est une véritable mine d'informations et, contrairement à l'autre solution, elle est rapide à déployer et très simple à utiliser », affirme M. Cardamone. « À partir d'une console unique, je vois tout notre environnement, en long et en large, dans ses plus infimes détails, et je peux gérer la protection facilement, avec le bouton droit de ma souris. L'interface graphique est très intuitive et les informations sont si claires que même de nouvelles recrues dans l'équipe ou d'autres départements, pas seulement la sécurité mais aussi la gestion de réseau par exemple, peuvent utiliser la plateforme et en tirer profit. »

Impact de l'implémentation

Déploiement rapide et rentabilité instantanée

Le déploiement de la plateforme Forescout a nécessité moins d'une journée. « Nous avons commencé l'implémentation à la pause déjeuner et quand j'ai démarré mon ordinateur le soir même, 97 % de notre environnement avait déjà été découvert et classifié », se souvient M. Cardamone. « En sept heures à peine, nous avions une visibilité détaillée sur notre environnement à l'échelle mondiale. Impressionnant. »

Démonstration immédiate des avantages offerts par la visibilité complète et granulaire

D'une grande précision, la visibilité offerte par la plateforme Forescout a fait ses preuves aussitôt celle-ci implémentée. « Nous pensions que 7 500 appareils étaient connectés à nos réseaux, mais la plateforme Forescout a découvert plus de 12 000 adresses IP », souligne M. Cardamone. « Nous avons également mis au jour des problèmes de sécurité dont nous n'avions pas connaissance, par exemple une dizaine de points d'accès sans fil installés dans nos showrooms. La visibilité ainsi acquise nous a permis de bloquer ces appareils, ainsi que de contacter les administrateurs locaux pour qu'ils appliquent les mesures de correction voulues. »

« Mais c'est seulement la partie émergée de l'iceberg », poursuit M. Cardamone. « La quantité d'informations que nous recevons de la plateforme Forescout est incroyable. Cette solution se distingue des nombreux autres outils qui recherchent les adresses IP des appareils, et de toutes celles que j'ai utilisées. C'est de loin la meilleure pour détecter, identifier et contrôler les systèmes. Elle s'est avérée un outil inestimable pour nous. »

« La plupart du temps, nous pouvons automatiser une action sur un terminal, mais quand une intervention manuelle est nécessaire, un simple clic droit suffit », explique M. Cardamone. « Je peux aussi autoriser du personnel de niveau 1 ou 2 à effectuer

> **La quantité d'informations que nous recevons de la plateforme Forescout est incroyable. Cette solution se distingue des nombreux autres outils qui recherchent les adresses IP des appareils, et de toutes celles que j'ai utilisées, c'est de loin la meilleure pour détecter, identifier et contrôler les systèmes. Elle s'est avérée un outil inestimable pour nous. »**
>
> **— Joseph Cardamone, analyste en sécurité informatique et responsable de la protection de la vie privée pour l'Amérique du Nord, Haworth**

des actions de niveau 3 en situation de crise sans pour autant lui accorder l'accès à des fonctions nécessitant des privilèges. La plateforme Forescout possède de puissantes fonctionnalités prêtes à l'emploi, mais elle est aussi très personnalisable. Elle nous offre des possibilités illimitées, ou presque. »

Visibilité sur l'état d'intégrité des appareils des sociétés acquises

La plateforme Forescout a apporté à l'équipe une visibilité sur les sociétés rachetées et sur le niveau d'intégrité des appareils au sein de chacune d'elles. « Si leurs appareils n'ont pas reçu les derniers correctifs depuis un long moment, nous le savons désormais, et nous pouvons prendre les mesures appropriées », déclare M. Cardamone. « La plateforme Forescout vérifie également les versions de correctifs et l'état de protection antivirus ainsi que le système d'exploitation de tout appareil qui tente de se connecter au réseau d'entreprise à partir d'une société affiliée et le bloque s'il ne respecte pas nos critères. »

Segmentation de réseau plus simple, mais aussi plus personnalisable

Grâce à Forescout eyeExtend pour Palo Alto Networks® Next-Generation Firewall, M. Cardamone a rapidement intégré la plateforme Forescout aux pare-feu de l'entreprise pour permettre une segmentation de réseau à la volée, en fonction des informations contextuelles précises et en temps réel fournies par la solution Forescout. « Grâce à l'intégration entre les produits de Forescout et de Palo Alto Networks, nous ne sommes plus limités à la segmentation par des identificateurs élémentaires, comme l'adresse IP ou le VLAN », explique M. Cardamone. « Nous disposons d'un choix beaucoup plus large que si nous nous étions limités à l'implémentation 802.1X car nous pouvons baser la segmentation sur un profil d'appareil bien plus riche et minutieux. »

Par exemple, dans l'environnement de fabrication de Haworth, M. Cardamone se sert de la plateforme Forescout pour identifier et classifier tous les appareils IoT à haut risque, c'est-à-dire principalement ceux qui ne sont plus pris en charge par le fabricant. C'est par exemple le cas des équipements dotés du système d'exploitation Windows® XP ou Windows 2000. Ensuite, la fonction de segmentation dynamique du réseau empêche automatiquement ces appareils de recevoir ou de transmettre des informations, sauf dans des circonstances très spécifiques où ces opérations sont autorisées.

Gain de temps immense et quantifiable grâce à l'intégration et à l'automatisation

L'intégration entre les solutions Forescout et Palo Alto Networks a permis à Haworth d'automatiser des processus manuels laborieux. Prenons comme exemple les espaces de travail technologiques Workware de Haworth. Présents au siège de l'entreprise comme dans ses showrooms à travers le monde et en service sur des VLAN de production, ils se voyaient auparavant attribuer une adresse IP statique via laquelle ils étaient ensuite autorisés à communiquer avec le réseau invité situé derrière le pare-feu. Sachant que le siège à lui seul compte non moins de 130 de ces dispositifs, que leur matériel et leurs logiciels sont constamment actualisés et modifiés, et que chacun de leurs déplacements physiques entraîne une modification de leur adresse IP, un processus manuel était tout simplement trop lent pour permettre un contrôle d'accès au réseau performant.

Aujourd'hui, la plateforme Forescout détecte ces appareils, les classifie et les place dans un groupe d'accès dynamique lié à une politique de pare-feu qui permet aux adresses IP de ce groupe de communiquer avec le réseau invité via les ports et applications nécessaires. « Peu importe que l'appareil se retrouve en Chine ou en Allemagne, Forescout le retrouve et le pare-feu sait quoi faire », se réjouit M. Cardamone. « Une tâche autrefois manuelle, sans fin et pratiquement impossible est à présent entièrement automatisée. »

« Si l'on additionne tous les gains de temps de nos différents cas d'utilisation depuis l'installation de la plateforme Forescout et son intégration avec nos pare-feu, j'estime l'économie à environ 20 heures par semaine, soit la moitié d'un équivalent temps plein », déclare M. Cardamone. « Notre petite équipe de sécurité peut sécuriser notre environnement avec plus d'efficacité et moins d'efforts. »

Les avantages de la visibilité offerte par Forescout dépassent le cadre de la sécurité

Le personnel opérationnel de Haworth tire également avantage de la plateforme Forescout. L'équipe d'assistance technique l'utilise pour localiser physiquement les appareils. Les responsables des logiciels s'en servent pour identifier les applications non conformes. Même l'équipe chargée du réseau y recourt chaque semaine pour rechercher des informations sur les ports et les commutateurs. Et l'entreprise réfléchit constamment à de nouveaux usages. Ainsi, Forescout jouera un rôle crucial lors de la mise en place future d'une politique BYOD au sein de Haworth.

Pour en savoir plus, consultez le site **www.forescout.fr**

FORESCOUT

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

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