Toujours plus haut : le Groupe ADP renforce sa sécurité réseau grâce à Forescout

10 000
appareils de plus que prévu identifiés sur le réseau d'ADP

50 %
d'amélioration de l'efficacité opérationnelle grâce à des données complètes sur les appareils

1 jour
pour obtenir une visibilité totale sur les appareils connectés au réseau

Secteur d'activité

- Transport aérien/ exploitation aéroportuaire

Environnement

- Plus grand groupe aéroportuaire en nombre de passagers
- Plus de 35 000 appareils identifiés sur son réseau
- Des milliers de collaborateurs répartis sur différents sites dans le monde entier

Défi

- Se protéger contre les éventuelles cybermenaces sans entraver l'exploitation
- Manque de visibilité sur l'ensemble des appareils connectés
- Environnement réseau étendu, hétérogène et complexe
- Système de sécurité

Présentation

Le Groupe ADP (Aéroports de Paris) est l'un des premiers groupes aéroportuaires au monde. Il gère des millions de passagers chaque année au sein d'un vaste portefeuille qui comprend l'exploitation des trois principaux aéroports de la région parisienne ainsi que des participations dans différents aéroports internationaux, de Santiago à New Delhi. ADP recherchait une solution à même de sécuriser son infrastructure réseau tentaculaire, englobant un grand nombre d'appareils IT et OT. En choisissant Forescout, le Groupe ADP a fait un grand pas dans sa démarche de cybersécurité.

« Avec un réseau en pleine expansion et des défis croissants en matière de visibilité, nous recherchions une solution offrant clarté et contrôle. Forescout nous a procuré non seulement une visibilité totale sur notre vaste réseau, mais aussi la possibilité d'appliquer des politiques de sécurité sans perturber l'exploitation – le partenaire idéal pour l'environnement complexe du Groupe ADP. »

— Éric Vautier, RSSI du Groupe ADP

Défis pour l'entreprise

Les aéroports s'apparentent à des mini-villes, abritant un ensemble de réseaux complexes et hétérogènes. Le Groupe ADP présente trois réseaux distincts :

- Le réseau informatique de l'entreprise, utilisé pour les RH, la messagerie et autres activités d'exploitation
- Le réseau de l'aéroport, où la haute disponibilité est primordiale, avec ses guichets d'enregistrement, ses portes d'embarquement et ses écrans d'informations de vol
- Le réseau OT/IoT, un treillis complexe de systèmes de manutention des bagages, d'éclairage, de contrôle de sécurité et de nombreux capteurs

inefficace, basé sur des certificats

- Évolution rapide des réseaux, au-delà des capacités de surveillance
- Difficulté à classer les différents types d'appareils
- Sécuriser des systèmes OT vieillissants dans les terminaux
- Répondre aux exigences croissantes de la numérisation

Solution de sécurité

- Forescout eyeSight
- Forescout eyeControl
- Forescout eyeRecover

Cas d'utilisation

- Contrôle d'accès réseau
- Conformité des appareils
- Gestion des actifs
- Intervention sur incident

Résultats

- 35 000 appareils identifiés – 10 000 de plus que prévu – en un seul jour
- Efficacité opérationnelle améliorée, temps d'interruption réduits
- Meilleure communication entre les équipes internes du Groupe ADP
- Efficacité accrue grâce à la prévention des failles de sécurité
- Sécurité garantie sans faille grâce à l'évolutivité de la solution

Dans cet environnement complexe, le Groupe ADP était confronté à un double défi.

Tout d'abord un défi de place, l'espace étant limité. Le Groupe ADP ne pouvait pas construire de terminaux plus grands pour des raisons environnementales et autres. Cependant, le nombre de personnes à prendre l'avion n'avait jamais été aussi élevé. Comme Éric Vautier, RSSI du groupe, le fait remarquer, « nos limites physiques nous ont poussés à penser digital. »

En se tournant vers des solutions technologiques évoluées, le Groupe ADP a pu améliorer son efficacité opérationnelle dans l'espace existant d'un aéroport. Cette transformation numérique lui a permis de mieux gérer les flux de passagers, de planifier les vols de manière plus efficace et d'optimiser la manutention des bagages. Le groupe a ainsi pu accueillir davantage de passagers sans s'agrandir. Mais les efforts de modernisation ont amené un deuxième défi : la cybersécurité. L'intégration par le Groupe ADP de davantage d'appareils connectés (OT/IoT) pour être plus efficace a également multiplié les vulnérabilités potentielles. L'entreprise ajoutait des points de contact qui, sans sécurisation adéquate, pouvaient être exploités.

« Les réseaux du Groupe ADP évoluent rapidement, et même notre équipe réseau n'avait pas de visibilité totale sur les appareils connectés », ajoute M. Vautier. Auparavant, le Groupe ADP avait tenté de renforcer la sécurité réseau à l'aide de certificats, mais cette approche n'a pas abouti. La solution n'offrait pas la visibilité globale nécessaire, elle était incompatible avec plusieurs systèmes et appareils propres aux aéroports et exigeait un important effort de supervision manuelle.

« Les seuls certificats ne nous permettent pas d'avoir une vue d'ensemble ; ils ne nous disent rien sur la conformité, la posture de sécurité actuelle ni même ce que fait activement un appareil », explique M. Vautier. La grande préoccupation, c'est qu'il était de plus en plus difficile de résoudre les problèmes sans pouvoir vérifier l'intégrité d'un appareil.

Pourquoi avoir choisi Forescout ?

Reconnaissant le besoin d'une solution plus dynamique, Éric Vautier et l'équipe du Groupe ADP se sont tournés vers Forescout. Laissant de côté les méthodes classiques basées sur des certificats, ils ont opté pour une solution mettant l'accent sur une visibilité complète de tous les appareils connectés. Cette étape logique avec Forescout a non seulement répondu aux défis uniques du Groupe ADP, mais l'a également positionné à l'avant-garde de la sécurité réseau en matière d'exploitation à grande échelle.

Rapidement, la nécessité d'une meilleure collaboration au sein de l'entreprise est apparue. « Dans notre environnement complexe, la confiance et le travail d'équipe sont primordiaux », fait remarquer M. Vautier. « Les outils de Forescout ont fourni un socle commun aux équipes réseau, informatique et de cybersécurité du Groupe ADP. » Cette approche a permis d'aligner toutes les parties prenantes, de renforcer la confiance et de faciliter la prise de décisions éclairées.

De plus, l'approche « crawl, walk, run » (littéralement : ramper, marcher, courir) de Forescout a trouvé un écho auprès du Groupe ADP. Pour Éric Vautier et les équipes qu'il supervise et avec lesquelles il interagit, il était essentiel de procéder à une implémentation progressive et ordonnée. Il voulait s'assurer que tout fonctionnait correctement à chaque étape, sans interrompre l'exploitation de l'aéroport, celle-ci dépendant d'une disponibilité 24 heures/24, 7 jours/7 des systèmes.
Le Groupe ADP a commencé par déployer Forescout dans le bâtiment informatique. Lorsque les équipes réseau, informatique et sécurité ont constaté

que tout fonctionnait comme prévu, elles ont étendu la procédure au réseau informatique de l'aéroport et implémenté Forescout, étape par étape, dans chaque terminal. Selon Éric Vautier, « le fait de commencer par notre bâtiment informatique nous a permis de tâter le terrain, de nous assurer que le système était robuste et fiable avant de le déployer dans nos terminaux d'aéroport, vitaux.»

Impact pour l'entreprise

Visibilité sur le réseau et identification des appareils améliorées

L'un des effets immédiats de l'implémentation de Forescout a été la visibilité globale qu'elle a apportée. En un jour seulement, Forescout a identifié près de 35 000 appareils sur le réseau, soit 10 000 de plus que prévu. La solution a également mis en lumière les vulnérabilités potentielles, qui ont pu être traitées et corrigées rapidement.
À l'issue de cette phase d'identification des actifs, le Groupe ADP s'est appuyé sur la taxonomie de classification multidimensionnelle de Forescout pour les appareils classiques, IoT et OT afin d'identifier la fonction et le type d'appareil, le système d'exploitation et sa version, le fabricant et le modèle, etc. Fort de ces informations détaillées, le Groupe ADP a pu remédier plus rapidement aux problèmes et faire de meilleurs choix en matière de sécurité.

« Forescout nous a procuré une profondeur d'information que nous n'avions jamais eue auparavant et qui a transformé notre approche : de la conjecture, nous sommes passés à la précision », fait observer M. Vautier. Cette compréhension approfondie n'aurait pas été possible avec l'ancienne solution basée sur des certificats.

Meilleure collaboration

Éric Vautier s'est servi de Forescout de manière stratégique pour améliorer la communication entre les départements réseau et informatique. Grâce aux nouvelles capacités, l'équipe réseau est devenue un acteur central, capable de configurer, de surveiller et de superviser les fonctions quotidiennes. Elle peut à présent identifier aisément les appareils sur le réseau et mesurer leur activité.

De son côté, l'équipe informatique de l'aéroport s'est appuyée sur Forescout pour surveiller la sécurité des appareils et détecter les appareils sauvages. Cette approche collaborative a permis d'assurer une implémentation homogène et efficace, favorisant un environnement cohésif où les deux équipes pouvaient travailler de manière synchronisée.

Surveillance améliorée de la sécurité

Grâce à Forescout, le Groupe ADP classe et contrôle rapidement les appareils, ce qui améliore considérablement sa posture de sécurité. La catégorisation affinée et la surveillance vigilante des appareils ont sensiblement réduit les éventuels temps d'arrêt et autres perturbations.

Efficacité accrue

Une gestion habile des menaces de sécurité potentielles a permis au Groupe ADP d'améliorer l'efficacité de ses performances. En prévenant les perturbations de manière proactive, le Groupe ADP a optimisé ses heures d'exploitation, tout en assurant la satisfaction constante des passagers. Cette approche, qui permet de gagner du temps, renforce aussi la réputation du Groupe ADP.

Une solution évolutive

Alors que le Groupe ADP poursuit sa transformation numérique, la solution Forescout lui offre l'évolutivité nécessaire à sa croissance.
« Plus notre réseau évolue, plus l'adaptabilité de Forescout est cruciale », affirme M. Vautier. Elle permet à l'entreprise de maintenir une posture de sécurité robuste alors que son réseau s'agrandit et se diversifie.

La vision d'Éric Vautier dans un futur proche ? Déployer Forescout sur le réseau OT/IoT et approfondir la démarche de classification et de catégorisation de Forescout afin d'améliorer la qualité des données sur les appareils, pour une détection et une correction plus rapides des problèmes potentiels.

La relation entre le Groupe ADP et Forescout illustre un partenariat réussi dans le domaine en constante évolution de la cybersécurité. Elle souligne l'importance de la visibilité, de la collaboration et de l'adaptabilité dans la création d'un environnement réseau sécurisé et efficace.

FORESCOUT

Forescout Technologies, Inc.

Numéro gratuit (US) 1-866-377-8771
Tél. (intl) +1-408-213-3191
Support +1-708-237-6591

Plus d'infos sur Forescout.com