proofpoint

TÉMOIGNAGE CLIENT

Une entreprise de financement automobile étend son programme de gestion des vulnérabilités aux risques liés aux identités avec Proofpoint

Le défi

- Intégration des risques liés aux identités au programme de gestion des vulnérabilités
- Prise en charge difficile des applications d'ancienne génération par la solution de gestion des accès à privilèges (PAM)
- Manque de visibilité continue sur les risques liés aux identités à privilèges

La solution

Proofpoint Identity Threat Defense

- Proofpoint Spotlight

Les résultats

- Sensibilisation renforcée aux risques majeurs liés aux identités
- Amélioration immédiate du niveau de sécurité
- Prise en compte du principal vecteur d'attaque, l'identité, par le programme de gestion des vulnérabilités

L'entreprise

Cette entreprise est un fournisseur mondial de solutions de financement automobile, qui compte plus de 9 000 collaborateurs et est actif en Amérique du Nord, en Amérique du Sud et en Asie. Elle propose des programmes de financement de détail et de crédit-bail aux consommateurs et aux concessionnaires automobiles, ainsi que des produits de prêt commercial afin d'aider les concessionnaires à financer et à développer leurs activités. Elle possède environ 60 milliards de dollars d'actifs.

Le défi

Cette entreprise dispose d'une infrastructure informatique étendue et diversifiée et rencontre des difficultés avec ses applications d'ancienne génération. Bien qu'elle ait mis en place une solution de gestion des accès à privilèges (PAM), celle-ci ne protégeait pas de nombreuses applications d'ancienne génération, en particulier celles qui étaient trop coûteuses à mettre à niveau ou dont la mise hors service était prévue. En outre, certains comptes administratifs et de service ne pouvaient pas être sécurisés. En conséquence, l'entreprise ne disposait pas d'un contrôle total sur les identités et les identifiants de connexion à privilèges et ne bénéficiait pas d'une bonne visibilité sur les risques potentiels liés aux identités. Cela concernait autant les administrateurs informatiques que les utilisateurs lambda.

Comme l'explique le SVP of Global Cybersecurity Strategy and Operations de l'entreprise : « Si vous disposez d'une vaste infrastructure sur site et utilisez Active Directory depuis des années, des vulnérabilités sont fréquentes en raison de décisions prises il y a longtemps. Le déficit technique est immense. De plus, la migration vers le cloud et les activités de fusion-acquisition accroissent la complexité ».

La solution

L'entreprise considérait Proofpoint Identity Threat Defense comme une expansion majeure de sa stratégie complète de gestion des vulnérabilités. Auparavant, l'approche de l'entreprise en la matière consistait à se concentrer sur les CVE et les CWE. L'entreprise avait toutefois conscience que les erreurs de configuration des identités engendraient également de nombreux risques potentiels. Elle avait donc commencé à surveiller tous les éléments de son environnement qui présentaient un risque de cybersécurité, qu'ils soient ou non associés à une CVE. En utilisant le modèle OSI en sept couches comme guide, elle a examiné son approche de l'évaluation automatisée des risques pour s'assurer qu'elle couvrait l'ensemble de son environnement informatique et s'est aperçue qu'il lui manquait des capacités de gestion des risques liés aux identités.

> « L'outil Proofpoint nous a offert de nouvelles perspectives. Nous savions que nous devions accorder davantage d'attention aux risques liés aux identités, mais nous n'avions aucun moyen de le faire. »
>
> AVP IT Vulnerabilities

Face à ce constat, l'entreprise a mis en œuvre la solution Proofpoint de gestion des risques liés aux identités au début de l'année 2021. Proofpoint Identity Threat Defense s'intègre à l'infrastructure Active Directory (AD) de l'entreprise et analyse régulièrement chaque endpoint pour produire un référentiel des risques liés aux identités, que l'entreprise récupère à l'aide de l'API. L'équipe de sécurité informatique passe en revue ces risques et s'entretient régulièrement avec l'équipe de correction des vulnérabilités informatiques afin d'appliquer des modifications visant à réduire les risques à leur environnement et d'en effectuer le suivi. Il s'agit d'un effort collectif, comme l'explique l'AVP IT Vulnerabilities de l'entreprise : « Nous faisons de notre mieux pour travailler en partenariat avec l'équipe informatique ».

Associés aux efforts de correction des vulnérabilités consentis par l'entreprise, des accords de niveau de service (SLA) qui varient selon le niveau de criticité permettent de prioriser les éléments plus critiques.

Les résultats

Immédiatement après la mise en œuvre de la solution, l'entreprise a constaté une amélioration de son niveau de sécurité. Après plus d'un an d'utilisation, l'entreprise observe généralement plusieurs nouveaux problèmes critiques par semaine, qu'elle résout rapidement. « Ces problèmes sont généralement dus à la négligence des utilisateurs. Ceux-ci n'ont pas d'intentions malveillantes, mais ils commettent parfois des erreurs ou agissent dans la précipitation. »

Lorsque nous lui avons demandé ce qu'elle ferait sans la solution Proofpoint, l'équipe n'a pas su quoi répondre, car elle ne connaît aucun autre moyen d'obtenir le type d'informations sur les identités (en particulier sur les endpoints) que fournit la solution. L'AVP IT Vulnerabilities de l'entreprise explique : « Nous n'avons aucun moyen de voir un mot de passe enregistré dans PuTTY, par exemple ».

« Les fusions-acquisitions constituent un cas d'utilisation intéressant, car on procède à une analyse avant et après l'intégration. Avec Proofpoint Identity Threat Defense, je peux évaluer l'intégrité de l'environnement et le niveau de déficit technique. »

SVP of Global Cybersecurity Strategy and Operations

Le SVP of Global Cybersecurity Strategy and Operations ajoute : « Les fusions-acquisitions constituent un cas d'utilisation intéressant, car on procède à une analyse avant et après l'intégration. Avec la solution, je peux évaluer l'intégrité de l'environnement et le niveau de déficit technique ».

À la question de savoir s'il recommanderait Proofpoint Identity Threat Defense à d'autres professionnels, il répond : « Compte tenu des résultats que j'ai obtenus, et de la direction que nous prenons, je recommanderais cette solution à tout professionnel cherchant à améliorer sa gestion des vulnérabilités. Cet outil permet de tout visualiser : vulnérabilités traditionnelles, vulnérabilités liées aux identités et erreurs de configuration ».

Il ajoute : « Il suffit d'une vulnérabilité liée aux identités, une seule, pour mettre à mal tout votre environnement. N'importe quel outil permettant d'améliorer la gestion des vulnérabilités offre une valeur ajoutée, en particulier lorsque vous pouvez visualiser les risques et les réduire au fil du temps. La solution Proofpoint nous a permis de verrouiller des centaines de milliers de portes : c'est énorme ».

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

proofpoint.

0613-003-03-01 06/24