proofpoint.

TÉMOIGNAGE CLIENT

Proofpoint met sa DLP de pointe au service d'un grand groupe de services financiers d'Afrique

Le défi

- Protéger contre les fuites de données accidentelles et intentionnelles par email
- Détecter et prévenir l'envoi d'emails à la mauvaise personne et les pièces jointes erronées
- Assurer la visibilité avec une approche proactive
- Réduire le délai nécessaire pour investiguer, signaler et résoudre les incidents

La solution

- Proofpoint Adaptive Email DLP

Les résultats

- La solution utilise l'IA comportementale, seul moyen de prévenir les fuites de données accidentelles et intentionnelles par email, ce qui permet de réduire les risques et le coût de l'application de mesures correctives.
- Elle permet de prévenir un nombre significatif de fuites de données (plus de 6 500 en deux ans).
- Elle assure un déploiement sans accroc, une maintenance simplifiée et un impact minimal pour les collaborateurs.

L'entreprise

Fondée il y a plus de 175 ans, cette grande banque africaine d'affaires et d'investissement fait partie de l'un des plus grands groupes de services financiers du continent. Cotée en bourse, l'entreprise enregistre près de 2 milliards de dollars de chiffre d'affaires et compte plus de 40 000 collaborateurs.

Le défi

Malgré les contrôles basés sur des règles et le logiciel de prévention des fuites de données (DLP) traditionnel en place, les compromissions de données causées par les fuites de données par email restaient une source de préoccupation. La pile de sécurité de la banque était essentiellement réactive, de sorte qu'au lieu de prévenir les fuites de données ou d'offrir une visibilité sur l'ampleur du problème, l'équipe de sécurité était uniquement en mesure d'analyser les incidents après coup.

Lorsque des incidents de ce type se produisaient, ils se transformaient en événements opérationnels qui prenaient des jours, voire des semaines, en investigations, rapports et mesures correctives. Au vu de la taille de l'entreprise, le processus devenait rapidement chronophage et monopolisait des ressources au détriment d'autres domaines de l'activité.

La banque savait que les fuites de données causées par l'envoi d'emails à la mauvaise personne ou par des pièces jointes erronées pouvaient potentiellement donner lieu à des compromissions de données. Elle était toutefois incapable d'empêcher les collaborateurs d'envoyer des informations sensibles vers des comptes email personnels sans créer des règles restrictives qui constitueraient un frein à la productivité.

« Avant Proofpoint Adaptive Email DLP, nous n'avions pas assez de visibilité sur les fuites de données par email ou sur l'ampleur réelle du problème », explique le responsable de la sécurité des informations de la banque. « Nous savions que ce problème existait, mais n'avions pas de solution ou de stratégie en place pour y remédier de façon proactive. »

Pour couronner le tout, la loi POPIA (l'équivalent sud-africain du RGPD) a créé un sentiment d'urgence et a contraint la banque à évaluer sa stratégie DLP et à identifier des mesures plus efficaces pour empêcher les fuites de données par email.

La solution

Lorsque la banque s'est mise en quête d'une solution, l'équipe chargée de la sécurité des informations a identifié plusieurs fonctionnalités indispensables.

La solution choisie devait pouvoir détecter et prévenir de manière proactive l'envoi d'emails à la mauvaise personne et les pièces jointes erronées, de même que permettre la formation des utilisateurs. Elle devait également limiter les opérations de maintenance et les perturbations, tout en offrant un taux d'efficacité élevé.

La réponse au problème ? Proofpoint Adaptive Email DLP
Si la DLP basée sur des règles joue un rôle essentiel dans la protection des données sensibles connues telles que les données personnelles, les numéros de sécurité sociale et les données de carte de paiement, elle ne détecte pas tous les risques. C'est notamment le cas des données sensibles envoyées à la mauvaise personne et des collaborateurs qui exfiltrent des données en se les envoyant ou en les transmettant à d'autres destinataires non autorisés.

« Proofpoint Adaptive Email DLP ne se contente pas de détecter et de prévenir les fuites de données accidentelles et intentionnelles. Nous l'utilisons également comme outil de sensibilisation des utilisateurs. Les collaborateurs interagissent avec les messages d'avertissement et, de mois en mois, nous observons une évolution de leur comportement. Ainsi, les activités non conformes sont en diminution constante. »

Responsable de la prévention des fuites de données

Proofpoint Adaptive Email DLP tire parti de l'IA comportementale pour prévenir automatiquement les fuites de données accidentelles et intentionnelles par email. Cette approche unique en son genre permet de réduire les risques et les coûts de correction. Proofpoint Adaptive Email DLP analyse plus de 12 mois de données email et étudie les comportements normaux de vos collaborateurs en matière d'envoi d'emails, leurs relations de confiance et la façon dont ils communiquent des données sensibles. Elle est ainsi en mesure d'identifier les comportements anormaux en matière d'emails. Lorsqu'une anomalie semble indiquer l'envoi d'un email à la mauvaise personne, une pièce jointe erronée ou une exfiltration de données, elle informe les administrateurs d'un risque de fuite et avertit l'utilisateur en temps réel, empêchant ainsi la fuite de données sensibles par email.

Proofpoint Adaptive Email DLP a été déployé sans heurts en quelques minutes et a pu commencer à protéger la banque en quelques heures. Il n'a pas été nécessaire de mettre en place et de tester des serveurs, pas plus qu'il n'a fallu créer et mettre à jour des règles. Une fois installée, la solution se laisse facilement oublier. Comme elle fonctionne silencieusement en arrière-plan, les collaborateurs ne sont conscients de sa présence que lorsque cela s'avère nécessaire. Elle est efficace, n'a pas d'impact sur les activités et aide la banque à instaurer une culture robuste de la sécurité informatique, axée sur la confiance et la responsabilisation.

« Proofpoint Adaptive Email DLP a été très facile à déployer et n'exige qu'une maintenance minimale », explique le responsable de la prévention des fuites de données de la banque. « Ce n'est pas un outil dont le fonctionnement exige une attention particulière du point de vue de l'infrastructure. Au contraire, il constitue un aspect dont l'équipe de sécurité n'a désormais plus à se préoccuper. C'était et c'est toujours un point très positif à nos yeux. »

Les résultats

« Avant même d'avoir la preuve de sa valeur, nous avons pu démontrer que Proofpoint Adaptive Email DLP nous aiderait à améliorer les processus internes, à simplifier la gestion des risques et la conformité et, potentiellement, à accroître notre chiffre d'affaires », s'enthousiasme le responsable de la sécurité des informations. « L'équipe de sécurité a reçu une distinction interne saluant son esprit d'innovation, en récompense des effets positifs potentiels que pourrait avoir Proofpoint Adaptive Email DLP. »

Avec Proofpoint Adaptive Email DLP, la banque peut désormais détecter et prévenir automatiquement les incidents susceptibles d'avoir des répercussions majeures sur ses activités.

Proofpoint Adaptive Email DLP analyse les données email historiques pour déterminer le contenu normal, le contexte associé et les schémas habituels de communication. Cette approche permet de dresser un inventaire complet des contacts email, privés et professionnels, de chaque collaborateur de la banque. Des graphiques des relations sont élaborés et mis à jour en continu, étant donné que les comportements en matière d'email changent au fil du temps après le déploiement initial de Proofpoint Adaptive Email DLP.

L'outil apprend constamment et évolue automatiquement en même temps que les relations, sans aucune intervention de la part des équipes de sécurité. Voilà comment Proofpoint Adaptive Email DLP a pu détecter et prévenir 4 027 fuites de données accidentelles et 2 427 emails non autorisés au cours des deux premières années de ce partenariat.

« Proofpoint Adaptive Email DLP ne se contente pas de détecter et de prévenir les fuites de données », commente le responsable de la prévention des fuites de données. « Nous l'utilisons également comme outil de sensibilisation des utilisateurs. Les collaborateurs interagissent avec les messages d'avertissement et, de mois en mois, nous observons une évolution de leur comportement. Ainsi, les activités non conformes sont en diminution constante. »

EN SAVOIR PLUS

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