Proofpoint Adaptive Email Security

Renforcez l'offre de base de protection de la messagerie de Proofpoint avec une couche totalement intégrée d'IA comportementale

Principaux avantages

- Réduction des risques grâce à l'IA comportementale, à la protection de la messagerie interne et à une formation en temps réel
- Accélération du retour sur investissement grâce à la consolidation des éditeurs de solutions de protection de la messagerie
- Économies de main-d'œuvre grâce à une visibilité et à des workflows intégrés
- Déploiement rapide d'API et configuration minimale

Le piratage de la messagerie en entreprise (BEC, Business Email Compromise) constitue une menace omniprésente. Et le problème ne cesse de s'aggraver. Ces cinq dernières années, les entreprises ont constaté une hausse spectaculaire de 560 % des pertes dues aux attaques BEC. Les analystes en sécurité étant déjà incapables de gérer 67 % des alertes qu'ils reçoivent, ils ont besoin de workflows de protection de la messagerie étroitement intégrés. Une approche plus robuste et plus intégrée est nécessaire pour se défendre contre les menaces email en plein essor.

Bloquez le phishing et les attaques BEC grâce à Proofpoint Adaptive Email Security

Proofpoint Adaptive Email Security renforce l'offre de base de protection de la messagerie de Proofpoint grâce à une analyse des comportements et des contenus basée sur l'IA. La solution s'appuie sur une threat intelligence intégrée issue de plus de 2,8 billions d'emails analysés chaque année. Elle a recours à l'apprentissage profond, aux grands modèles de langage, au traitement du langage naturel et plus encore pour vérifier plus de 250 points de données pour chaque email. Pour identifier le phishing interne, elle détecte les pics du volume d'emails et les communications anormales en les comparant aux tendances historiques en matière d'emails.

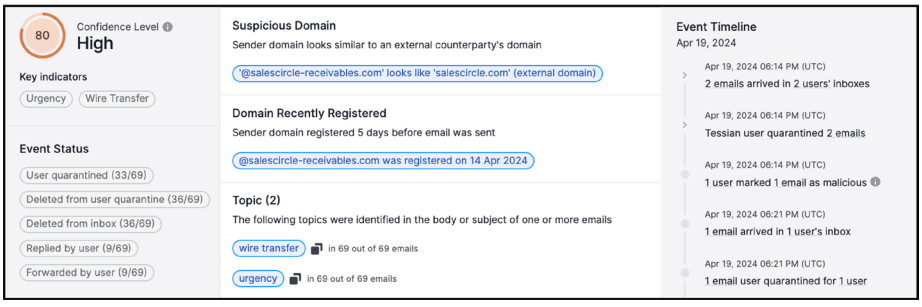

Figure 1. Proofpoint Adaptive Email Security bloque automatiquement les menaces à haut risque avec l'IA comportementale.

Cette suite de solutions fait partie de la plate-forme Human-Centric Security intégrée de Proofpoint et vise à réduire les quatre catégories clés de risques liés aux utilisateurs.

Formation des utilisateurs en temps réel

Les bannières d'avertissement Proofpoint Adaptive Email Security affichent les raisons spécifiques pour lesquelles un email pourrait être malveillant, ce qui aide les utilisateurs à prendre des décisions de sécurité avisées en temps réel.

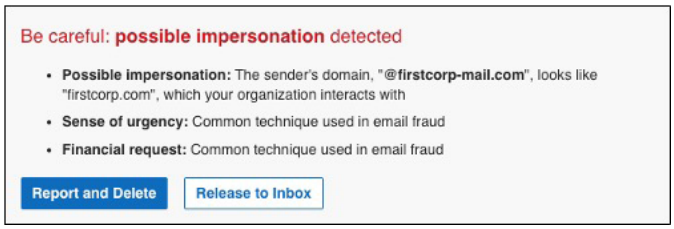

Figure 2. Proofpoint Adaptive Email Security forme les utilisateurs en temps réel et les avertit des risques spécifiques dans leurs emails.

Protection de la messagerie interne

Proofpoint Adaptive Email Security a recours à l'IA comportementale pour bloquer le phishing latéral. La solution détecte les pics de volume des emails et les communications anormales. Elle prévient le phishing interne en identifiant les emails qui contiennent des URL et des pièces jointes malveillantes.

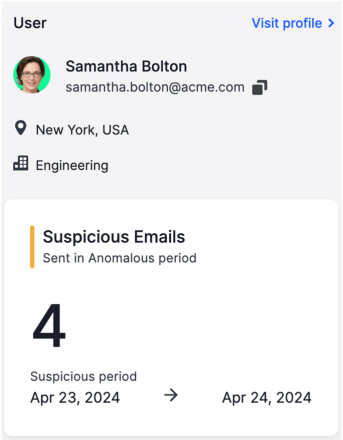

Figure 3. Proofpoint Adaptive Email Security identifie le phishing interne provenant de comptes compromis.

Protection complète de la messagerie

Défense de la messagerie en profondeur, avant la remise jusqu'à la distribution en boîte de réception

Proofpoint Adaptive Email Security est la seule solution intégrée de sécurité des emails dans le cloud (ICES) qui utilise l'ensemble de données le plus vaste et le plus avancé du monde sur les menaces email connues. Elle offre une vue unique et universelle des détections comportementales avant et après la remise, ainsi qu'une explicabilité basée sur l'apprentissage automatique.

La feuille de route d'intégration inclut une boucle de rétroaction basée sur l'IA pour améliorer la détection en amont et unifier la traque, l'investigation et la correction des menaces email.

Déploiement en quelques secondes, protection en quelques heures

Proofpoint Adaptive Email Security s'intègre à l'API Microsoft Graph pour bloquer les emails entrants malveillants. La solution s'intègre parfaitement à Microsoft 365. De plus, elle ne requiert aucun reroutage des emails ni aucune modification des enregistrements MX. L'apprentissage historique ne prend que 48 heures au maximum, ce qui permet à la solution basée sur l'IA comportementale de bloquer les menaces en quelques jours seulement. La protection optimisée par l'IA comportementale bloque les menaces email à haut risque dans votre environnement.

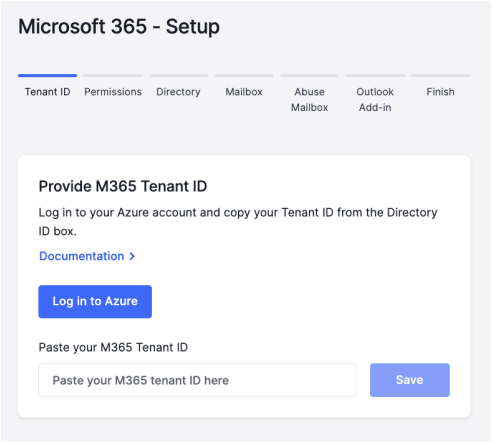

Figure 4. Proofpoint Adaptive Email Security s'intègre à Microsoft 365 en quelques clics seulement.

EN SAVOIR PLUS

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