proofpoint.

Proofpoint Threat Protection

Protégez vos collaborateurs des menaces modernes

Principaux avantages

- Détection et blocage plus rapides des menaces modernes propagées par email
- Neutralisation plus précise des menaces émergentes grâce à une IA continue
- Obtention de renseignements sur les risques liés aux utilisateurs et aux menaces
- Amélioration de l'efficacité opérationnelle
- Sensibilisation du personnel afin d'induire un changement des comportements

La messagerie électronique constitue le premier vecteur de cybermenaces. Aujourd'hui, de nombreuses attaques de malwares, de phishing et d'ingénierie sociale ciblent vos collaborateurs. Selon le rapport d'enquête 2023 sur les compromissions de données (Data Breach Investigations Report) de Verizon, 74 % des compromissions de données impliquent une intervention humaine[1]. Avec Proofpoint Threat Protection, votre entreprise peut protéger ses collaborateurs des menaces modernes.

La cybercriminalité est en pleine croissance

La cybercriminalité est en pleine croissance, car les bénéfices sont importants et les risques faibles. D'après Cybersecurity Ventures, le coût de la cybercriminalité devrait atteindre 10,5 billions de dollars annuels d'ici 2025[2]. Les organisations cybercriminelles fonctionnent comme des entreprises normales dont la motivation est financière. Les cyberpirates cherchent à voler des informations personnelles et d'entreprise précieuses, à usurper des identités et à lancer des attaques visant à commettre des fraudes financières par email. La messagerie électronique étant un outil de communication indispensable pour les entreprises modernes, il s'agit du premier vecteur de menaces ciblant vos collaborateurs. Qui plus est, ces menaces évoluent constamment et sont difficiles à bloquer. C'est pourquoi la protection de vos collaborateurs contre ces menaces modernes est une tâche ardue, même pour les entreprises les plus sophistiquées et complexes. Heureusement, Proofpoint peut vous aider.

1 Verizon, *2023 Data Breach Investigations Report* (Rapport d'enquête 2023 sur les compromissions de données), 2023.
2 Steve Morgan *(Cybercrime Magazine)*, « Cybercrime To Cost The World 10.5 Trillion Annually By 2025 » (La cybercriminalité devrait coûter au monde 10,5 billions de dollars annuels d'ici 2025), novembre 2020.

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.

84 %

des entreprises du classement Fortune 100 font confiance à Proofpoint pour protéger leurs collaborateurs contre les menaces.

Source : Proofpoint, 2023

Détectez et bloquez les menaces email plus rapidement grâce à la détection avant la remise

Grâce à notre fonction de détection avant la remise, vous pouvez détecter et bloquer les menaces connues et inconnues dans toute votre entreprise. Les menaces sophistiquées sont ainsi neutralisées non pas après leur distribution, mais avant. Il s'agit notamment des menaces suivantes :

- Phishing d'identifiants de connexion avancé
- Malwares
- Ransomwares
- Piratage de la messagerie en entreprise (BEC, Business Email Compromise)
- URL malveillantes
- Codes QR
- Pièces jointes
- Etc.

En combinant détection avant la remise et détection et correction automatisées après la remise, votre entreprise peut protéger ses collaborateurs grâce à une solution complète.

Identifiez les menaces grâce à une détection multicouche basée sur l'IA

Nous utilisons une pile de détection multicouche alliant threat intelligence, apprentissage automatique, IA comportementale, détection en environnement sandbox et analyse contextuelle et sémantique (grands modèles de langage, ou LLM). Ces technologies fonctionnent de concert pour détecter plusieurs types de menaces modernes. La pile enregistre ainsi un taux de détection extrêmement fiable de 99,99 % avec une meilleure explicabilité des menaces. Contrairement aux solutions de protection de la messagerie électronique dont la détection ne repose que sur une seule couche, elle génère moins de faux négatifs et de faux positifs, car elle peut neutraliser les messages malveillants avec plus de précision sans bloquer les messages légitimes ni perturber vos activités.

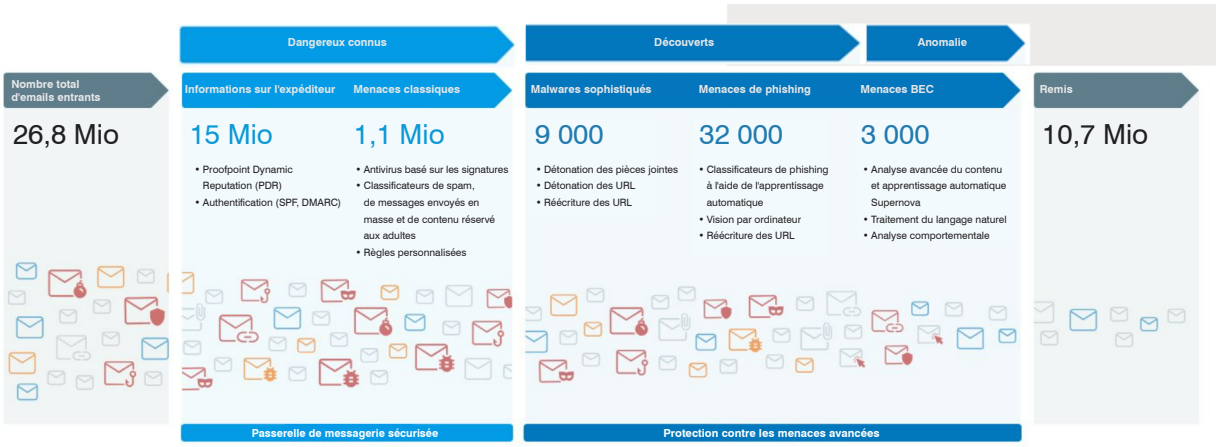

Figure 1. Détection avant la remise multicouche et basée sur l'IA de Proofpoint en action

Obtenez une visibilité complète sur les menaces et les risques liés aux utilisateurs

Avec Proofpoint, vous bénéficiez d'informations précieuses sur vos VAP (Very Attacked People™, ou personnes très attaquées) et les menaces qui les ciblent. Vous pouvez ainsi implémenter des contrôles adaptatifs ciblés : isolation du navigateur, formations de sensibilisation à la sécurité informatique, authentification renforcée, etc. En plus d'une visibilité sur les risques liés aux utilisateurs, vous bénéficiez de renseignements précieux sur vos collaborateurs : les techniques d'attaque qui les visent, leurs vulnérabilités et les privilèges dont ils disposent. Par ailleurs, Proofpoint analyse plus de 3 billions d'emails par an pour ses quelque 230 000 clients, partenaires et fournisseurs. Notre threat intelligence et nos recherches vous offrent à un stade précoce des données télémétriques sur les menaces émergentes jusque-là inconnues.

Améliorez l'efficacité opérationnelle

Avec Proofpoint, vous pouvez détecter et corriger automatiquement les emails malveillants après leur remise. Cette automatisation du processus de tri et de la suppression des menaces contenant des charges virales de leurre vous aide à identifier et à neutraliser les menaces plus rapidement et plus efficacement. Que ces emails indésirables proviennent de comptes internes compromis ou qu'ils aient été transférés ou reçus par d'autres utilisateurs, Proofpoint vous fournit des alertes automatisées, des analyses comparatives et des vues exploitables des menaces, ce qui vous permet de réduire le temps consacré à la correction. Cela allège également la charge de travail de votre équipe, ce qui la rend plus efficace. En outre, les utilisateurs peuvent facilement signaler les messages suspects en un clic à partir d'un avertissement ou grâce au bouton PhishAlarm. S'il s'avère que le message signalé est malveillant, ce dernier et toutes ses copies sont automatiquement mis en quarantaine. Les utilisateurs reçoivent alors une notification par email les informant que le message était malveillant et qu'il a été automatiquement supprimé. Cette notification en boucle fermée a pour effet de les encourager à signaler des messages similaires à l'avenir.

Sensibilisez votre personnel et induisez un changement des comportements

Proofpoint vous aide à réduire davantage les risques liés aux utilisateurs en modifiant les comportements dangereux et en instaurant des habitudes de sécurité durables. Nous utilisons notre threat intelligence étoffée pour orienter votre programme de différentes manières : création de simulations d'attaques de phishing réelles, mise en place de formations guidées par les menaces vous permettant de sensibiliser vos collaborateurs qui se laissent le plus piéger et les personnes les plus attaquées, automatisation de l'analyse des emails signalés par les utilisateurs, etc. Nous vous aidons à stimuler l'engagement de vos utilisateurs grâce à des expériences d'apprentissage personnalisées.

Figure 2. Proofpoint offre une visibilité sur vos VAP (Very Attacked People™, ou personnes très attaquées).

Notre approche adaptative aide vos collaborateurs à retenir ce qu'ils apprennent et à adopter des habitudes de sécurité positives et durables. Enfin, nous vous permettons de mieux communiquer les risques liés aux utilisateurs et l'impact de votre programme à votre direction en effectuant le suivi des changements réels de comportements et en les comparant à ceux d'autres entreprises du secteur.

Offres de services managés Proofpoint

Proofpoint propose les services managés suivants pour Proofpoint Threat Protection :

- **Managed Email Threat Protection —** Bénéficiez d'une expertise proactive, d'une disponibilité ininterrompue du personnel et d'informations à l'intention des dirigeants via une gestion pratique de votre solution de protection de la messagerie électronique. Nous assurons également des vérifications opérationnelles quotidiennes et une application proactive de la threat intelligence.
- **Managed Abuse Mailbox —** Réduisez la charge de travail associée à la vérification manuelle des emails signalés par les utilisateurs. Notre équipe procède à une analyse et attribue des verdicts définitifs à tous les messages signalés non classés.
- **Managed Security Awareness —** Faites évoluer votre approche de la formation à la sécurité informatique des utilisateurs. Nous orientons la stratégie de votre programme en mettant l'accent sur les changements de comportements et en instaurant une culture de la sécurité informatique plus résiliente.

Pour plus d'informations, consultez la page : **www.proofpoint.com/fr/products/aegis**.

EN SAVOIR PLUS

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

0203-007-03-01 3/24

proofpoint.