

# Proofpoint Email Protection

## Détection et neutralisation des menaces malveillantes et sans malware par email

### PRINCIPAUX AVANTAGES

- Blocage des attaques BEC et de phishing ainsi que des malwares avancés à l'entrée
- Sensibilisation des utilisateurs à la sécurité grâce à l'affichage d'avertissements concernant les emails
- Productivité accrue grâce à des fonctions rapides de suivi des emails et à l'application de bonnes pratiques
- Flexibilité totale garantissant l'évolutivité nécessaire aux grandes entreprises
- Efficacité opérationnelle accrue grâce à l'automatisation des opérations de sécurité et de la réponse aux menaces
- Protection étendue grâce à l'authentification intégrée et au chiffrement des emails, à la prévention des fuites de données par email, à la solution Targeted Attack Protection et plus encore
- Accords de niveau de service de premier ordre en cas de déploiement dans le cloud :
  - Taux de disponibilité du service : 99,999 %
  - Efficacité de la protection antivirus : 100 %
  - Temps de latence des emails : moins d'1 minute
  - Taux de neutralisation ou de redirection du spam : 99 %

Proofpoint Email Protection permet de sécuriser et de contrôler vos emails entrants et sortants. La solution tire parti de l'apprentissage automatique et de techniques de détection multicouches pour identifier et neutraliser les emails malveillants. En outre, elle propose une classification dynamique des menaces et autres nuisances actuelles, et vous offre un contrôle granulaire sur de nombreux types d'emails, notamment les emails d'imposteurs, le phishing, les malwares, le spam et les emails à diffusion massive. Proofpoint Email Protection offre également une flexibilité totale grâce à des politiques de sécurité et des règles de routage des emails personnalisées. Il s'agit de la solution de protection de la messagerie électronique la plus déployée par les sociétés du palmarès Fortune 1000. Elle est capable de s'adapter à toutes les entreprises, même les plus grandes. Qui plus est, elle est compatible avec les environnements cloud, sur site et hybrides.

La messagerie électronique est le principal vecteur de menaces. En effet, plus de 96 % des menaces exploitant l'ingénierie sociale (avérées ou présumées) sont véhiculées par la messagerie<sup>1</sup>. Outre les menaces courantes propagées par email telles que les attaques de phishing et les malwares, le piratage de la messagerie en entreprise (BEC, Business Email Compromise) représente une nouvelle menace pour les entreprises. Proofpoint Email Protection détecte les menaces connues et inconnues qui échappent aux autres solutions. En analysant des milliards de messages chaque jour, Proofpoint identifie davantage de menaces, les détecte plus vite et vous protège plus efficacement contre les menaces sans malwares difficiles à détecter, comme les emails d'imposteurs. Grâce à Proofpoint Email Protection, vous neutralisez la grande majorité des menaces en amont de la boîte de réception de vos utilisateurs.

### Interception des menaces émergentes qui échappent aux autres solutions

#### Détection des emails frauduleux, d'imposteurs et de phishing

Proofpoint Email Protection détecte les menaces émergentes en amont de la boîte de réception de vos utilisateurs. Optimisé par NexusAI, Proofpoint Advanced BEC Defense est conçu pour bloquer efficacement un large éventail de fraudes par email, dont le détournement de paiements et la fraude à la facturation fournisseurs depuis des comptes compromis. Comme ces menaces sont souvent dépourvues de charge virale malveillante, elles nécessitent une technique de détection plus sophistiquée.

Proofpoint Advanced BEC Defense est notre moteur de détection piloté par l'apprentissage automatique et l'intelligence artificielle. Il est spécialement conçu pour détecter et bloquer les attaques BEC. Il identifie ces attaques BEC de façon dynamique en analysant plusieurs attributs des messages. Par exemple :

- Données d'en-tête du message
- Adresse IP de l'expéditeur (adresse IP d'origine, réputation)
- Corps du message (mots ou phrases spécifiques, urgence)

Il détermine si le message constitue une menace BEC. En outre, il détecte diverses tactiques utilisées par les auteurs d'attaques BEC, dont les suivantes :

- Usurpation de l'adresse de réponse
- Utilisation d'adresses IP malveillantes
- Utilisation de domaines de fournisseurs usurpés

Proofpoint Advanced BEC Defense offre par ailleurs une visibilité granulaire sur les détails d'une attaque BEC (thème, escroquerie aux cartes cadeaux, détournement de salaires, facturation, leurre, tâche, etc.). Il explique pourquoi le message est suspect, avec des exemples pour l'illustrer. Votre équipe de sécurité peut ainsi mieux comprendre l'attaque et communiquer à son sujet. Les données collectées par NexusAI viennent ensuite alimenter le graphique des menaces Nexus de Proofpoint. Ce dernier analyse et met en corrélation des informations sur les menaces au niveau de la messagerie, du cloud, du réseau et des réseaux sociaux de l'ensemble de nos clients. Vous bénéficiez ainsi d'une protection qui vous permet de garder une longueur d'avance sur les menaces.

## Neutralisation des emails malveillants et indésirables

Nous avons intégré des techniques de détection multicouches à Proofpoint Email Protection afin de vous protéger contre les menaces en constante évolution. La détection basée sur les signatures déjoue les menaces connues telles que les virus, les chevaux de Troie et les ransomwares, tandis que l'analyse dynamique de la réputation évalue en continu les adresses IP locales et mondiales afin de déterminer si les connexions email doivent être autorisées ou refusées. Notre système de classification procède également à la classification dynamique de plusieurs types d'emails : les emails d'imposteurs, le phishing, les malwares, le spam, les emails à diffusion massive, les contenus pour adultes et les emails provenant de personnes de confiance. De plus, il met en quarantaine les emails entrants par type. Ensemble, ces fonctionnalités vous protègent dès les premiers signes d'activité malveillante.

## Suivi de n'importe quel email en quelques secondes

Proofpoint Email Protection est doté d'une fonction de recherche extrêmement performante. Grâce à des dizaines de critères, cette fonction de recherche intelligente localise rapidement des données journalisées, généralement difficiles à trouver. Vous pouvez également effectuer un suivi des emails, notamment de leur origine et de leur destination. Proofpoint Email Protection vous fournit des détails précis

sur les résultats de la recherche, y compris des métadonnées avec plus d'une centaine d'attributs. La recherche s'effectue en quelques secondes seulement. Vous pouvez télécharger et exporter les résultats de votre recherche (jusqu'à un million d'enregistrements). En outre, plusieurs rapports en temps réel sont intégrés au produit et vous offrent une visibilité détaillée sur le flux et les tendances des emails. Grâce à ces données, vous faites face aux problèmes dès leur apparition.

## Flexibilité et évolutivité adaptées aux grandes entreprises

Proofpoint Email Protection répond aux besoins des plus grandes entreprises au monde. La solution vous permet de définir des règles de pare-feu personnalisées pour la messagerie à l'échelle globale, d'un groupe ou d'un utilisateur. Vous pouvez créer des politiques de sécurité et des règles de routage des emails qui répondent à vos besoins et les appliquer facilement. Proofpoint Email Protection offre les mêmes avantages et une plus grande flexibilité grâce à plusieurs options de déploiement (matériel sur site, machine virtuelle, SaaS, etc.).

## Sensibilisation des utilisateurs à la sécurité

L'affichage d'avertissements sur les emails permet à vos utilisateurs de prendre des décisions plus avisées concernant les messages suspects dont ils ignorent s'ils sont légitimes ou malveillants. Une brève description des risques associés à un email spécifique est affichée, tandis que le niveau de risque est restitué de manière claire par un code couleur. Les utilisateurs peuvent signaler des emails suspects directement à partir de l'avertissement, même s'ils consultent leurs messages via des terminaux mobiles. Cette fonctionnalité permet de mieux maîtriser les risques de compromission en incitant vos utilisateurs à se méfier davantage des emails suspects.

Grâce à Proofpoint Email Protection, les administrateurs de la messagerie peuvent également permettre aux utilisateurs de gérer les messages chiffrés et non prioritaires comme les emails diffusés massivement, d'examiner les messages mis en quarantaine et de prendre des mesures appropriées directement dans le volet des tâches d'Outlook. Le feedback des utilisateurs est ensuite transmis à Proofpoint, contribuant ainsi à améliorer la précision générale de la classification des emails à diffusion massive.

## Gestion centralisée pour Proofpoint Email Encryption et Proofpoint Email DLP

Vous pouvez facilement renforcer votre protection en ajoutant Proofpoint Targeted Attack Protection, Proofpoint Email Fraud Defense, Proofpoint Email Encryption ou Proofpoint Email Data Loss Prevention (DLP) à votre arsenal. Bien que Proofpoint Email Protection offre des fonctions de base de chiffrement des emails et de prévention des fuites de données (DLP), vous bénéficiez de solutions DLP plus avancées via la même console de gestion. Cette intégration étroite vous aide à gérer les données sensibles envoyées par email. Elle empêche également les fuites et les pertes de données via la messagerie. Pour finir, elle satisfait plusieurs exigences de conformité.

## EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : [proofpoint.com/fr](https://proofpoint.com/fr).

### À PROPOS DE PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risque des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur [www.proofpoint.com/fr](https://www.proofpoint.com/fr).

©Proofpoint, Inc. Proofpoint est une marque commerciale de Proofpoint, Inc. aux États-Unis et dans d'autres pays. Toutes les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs.