Proofpoint Advanced Email Security

Contrez les menaces avancées véhiculées par la messagerie, rationalisez les opérations et bénéficiez d'une visibilité décisionnelle sur les risques liés aux utilisateurs et votre paysage des menaces

Produits

- Proofpoint Email Protection
- Proofpoint TAP
- Proofpoint TRAP
- Proofpoint Email Isolation
- Proofpoint Browser Isolation
- Proofpoint Security Awareness Training
- Proofpoint Email Fraud Defense
- Proofpoint Internal Mail Defense
- Proofpoint Email Encryption
- Proofpoint Email DLP

Principaux avantages

- Blocage des tentatives de fraude par email et des messages contenant des URL dangereuses, des pièces jointes malveillantes et des ransomwares
- Neutralisation automatique des messages signalés par les utilisateurs ou activés après leur remise grâce à des workflows intégrés
- Visibilité inégalée sur vos collaborateurs, les menaces et les risques liés aux fournisseurs et au cloud, entre autres
- Déploiement aisé de règles DMARC et application rapide et sûre de l'authentification pour bloquer les emails frauduleux imitant des domaines de confiance
- Formation et responsabilisation de vos utilisateurs afin de les transformer en ligne de défense robuste contre les cybermenaces

La messagerie électronique est au cœur des activités des entreprises modernes, mais également leur principal vecteur de menaces. Qui plus est, les attaques par email — du phishing au piratage de la messagerie en entreprise (BEC, Business Email Compromise), en passant par les attaques de la chaîne logistique, les ransomwares et la compromission de comptes cloud — ne cessent d'évoluer. Protéger efficacement ce vecteur contre les menaces représente donc un défi de taille, même pour les entreprises les plus importantes et les plus complexes. Heureusement, Proofpoint peut vous aider.

Notre solution de protection avancée de la messagerie est déployée dans un nombre d'entreprises figurant aux classements Fortune 100, Fortune 1000 et Global 2000 supérieur à celui de tout autre fournisseur. Pour relever le défi, elle adopte une approche en ligne et axée sur les API. Elle garantit ainsi une protection complète de l'ensemble des messages entrants et sortants. Elle ne se concentre pas uniquement sur les emails qui échappent à la détection des solutions de sécurité traditionnelles. Notre approche multicouche intégrée réduit le risque d'attaques fructueuses en détectant les menaces plus rapidement et avec précision. Nos fonctionnalités de détection de pointe et notre plate-forme évolutive vous permettent d'accroître votre efficacité opérationnelle. Grâce aux informations exploitables fournies par Proofpoint, vous pouvez mieux appréhender les risques, prendre des mesures proactives et réagir plus rapidement et efficacement.

Détection et blocage des menaces avancées

Une efficacité fiable

La threat intelligence et les fonctionnalités de détection de Proofpoint vous offrent une défense solide contre les menaces sophistiquées, tout en réduisant les faux positifs.

Nous nous appuyons sur des outils d'analyse de la réputation, de réécriture des URL et de sandboxing prédictif et au moment du clic pour détecter les menaces avec charge virale, comme celles distribuées par le biais de pièces jointes et d'URL. La détection des techniques de contournement et d'obfuscation telles que les CAPTCHA et les liens protégés par mot de passe, des sites au rendu lourd, des redirecteurs et des sites de partage de fichiers est intégrée.

Nous utilisons également les modèles d'intelligence artificielle (IA) et d'apprentissage automatique du graphique des menaces Nexus pour détecter les attaques sans charge virale, telles que les attaques BEC. Ces modèles évaluent des signaux

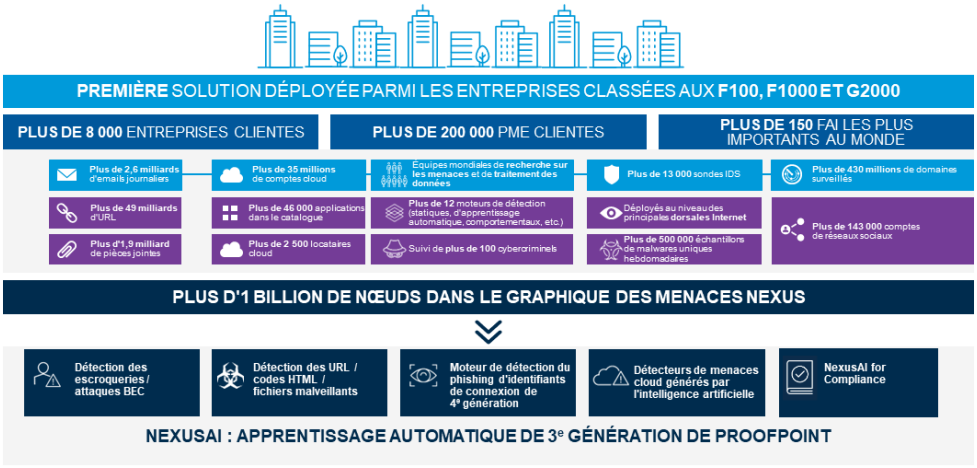

Figure 1. Graphique des menaces Nexus

Dans le paysage des menaces centré sur les personnes tel que nous le connaissons aujourd'hui, vos collaborateurs constituent votre actif le plus précieux, mais également votre principal risque.

tels que les risques liés aux fournisseurs, des signaux utilisateur provenant de suites de collaboration, le traitement du langage naturel du contenu, les relations expéditeur/destinataire et les intentions. Les données contextuelles et de référence nous permettent d'identifier rapidement les emails potentiellement malveillants. Elles complètent à merveille notre threat intelligence et nos autres moteurs de détection ciblés, ce qui permet de réduire les faux positifs.

Nous analysons les emails avec des outils d'analyse du contenu, d'analyse de la réputation et de sandboxing. Nous pouvons ainsi bloquer efficacement les menaces avancées transmises par la messagerie, y compris les malwares polymorphes et les ransomwares, avant qu'elles n'atteignent vos utilisateurs. Par ailleurs, nous vous proposons un sandboxing prédictif des URL au moment du clic afin de détecter et de bloquer les URL malveillantes. La réécriture des URL protège vos utilisateurs sur n'importe quel réseau et terminal. Elle permet également de détecter si un message a été « piégé » après sa remise.

Des clics en toute sécurité grâce à l'isolation de la messagerie et du navigateur

Proofpoint Browser Isolation et Proofpoint Email Isolation offrent un environnement sûr, dans lequel vos utilisateurs peuvent consulter des sites Web, leur webmail personnel et leur messagerie professionnelle en toute sécurité. Les cybercriminels recourent à divers vecteurs de menaces et tactiques pour tenter d'accéder à vos systèmes, comme la compromission de comptes de fournisseurs. Par exemple, ils peuvent cibler vos utilisateurs par le biais de leur messagerie personnelle ou de canaux non protégés. L'isolation vous permet de désactiver les chargements et les téléchargements. Vous pouvez également limiter la saisie de données pendant l'analyse en temps réel d'un site Web. Cela ne prend que quelques secondes. La technologie ajoute une couche de protection supplémentaire pour prévenir le vol d'identifiants de connexion, les malwares et les ransomwares. Elle est particulièrement utile contre les emails de phishing qui contiennent des URL dont l'activité nocive est déclenchée après la remise.

Prévention de la fraude par email grâce à l'authentification des emails

L'authentification des emails ajoute une couche de protection supplémentaire. Son efficacité pour bloquer les menaces d'imposteurs sans malwares, comme les attaques BEC, n'est plus à prouver. Cependant, les entreprises hésitent à adopter et à appliquer les normes DMARC par crainte de bloquer des emails légitimes.

Proofpoint vous aide à déployer et à appliquer l'authentification DMARC en toute confiance, sans bloquer le flux d'emails légitimes. L'authentification DMARC vous protège contre l'usurpation de domaines et les emails frauduleux qui utilisent vos domaines de confiance. Elle bloque les messages frauduleux au niveau de la passerelle Proofpoint, tout en protégeant l'identité des emails de votre entreprise.

Par ailleurs, vous pouvez visualiser de manière centralisée toutes les menaces d'imposteurs, y compris les domaines malveillants similaires au vôtre. Vous bénéficiez de cette visibilité quelle que soit la tactique employée ou la personne ciblée. Grâce à notre service Virtual Takedown, vous pouvez prévenir de façon proactive les attaques par email utilisant des domaines similaires avant leur lancement. Nous simplifions votre implémentation DMARC en mettant à votre disposition un consultant chevronné qui vous assiste tout au long des étapes de votre déploiement. En collaboration avec votre équipe, nous identifions tous les expéditeurs de confiance (y compris les tiers) pour garantir une authentification correcte. Proofpoint a accompagné plus d'un tiers des entreprises figurant au classement Fortune 1000 tout au long de ce processus. Nous pouvons travailler avec les configurations les plus sophistiquées.

Protection des emails internes et neutralisation rapide des menaces

Il est tout aussi crucial de protéger les emails internes que le courrier entrant. Les cybercriminels utilisent des comptes compromis pour envoyer des emails de phishing, lancer des attaques BEC ou propager des malwares. Nous analysons les emails internes pour détecter le contenu malveillant, qu'il s'agisse d'URL ou de pièces jointes. Lorsque nous détectons un email interne malveillant, vous pouvez l'extraire et le mettre en quarantaine automatiquement, même si d'autres utilisateurs l'ont déjà reçu et transféré. Nous fournissons également des rapports répertoriant tous les comptes susceptibles d'avoir été compromis, ce qui vous permet de prendre rapidement des mesures les concernant.

Visibilité sur les attaques et la surface d'attaque constituée par vos collaborateurs

Pour mieux limiter les risques et attirer l'attention de votre direction et de votre conseil d'administration sur ceux-ci, vous devez être en mesure d'identifier :

- Les utilisateurs les plus à risque et les techniques d'attaque employées
- Le paysage des menaces, les objectifs, les cybercriminels et les tendances
- D'autres signaux tels que les risques liés aux fournisseurs et au cloud

Proofpoint vous fournit toutes ces informations, et bien d'autres encore. Grâce à notre approche basée sur une plate-forme, vous bénéficiez d'une compréhension approfondie des risques centrés sur les personnes, sans morcellement des données. Nous vous aidons à être plus proactif contre les menaces sophistiquées.

Réduction des risques grâce à des informations centrées sur les personnes

Dans le paysage des menaces centré sur les personnes tel que nous le connaissons aujourd'hui, vos collaborateurs constituent votre actif le plus précieux, mais également votre principal risque. Nous vous offrons une visibilité inégalée sur les attaques ciblées et la surface d'attaque constituée par vos collaborateurs.

Nous identifions également les utilisateurs qui présentent le plus grand risque pour votre entreprise et vous expliquons pourquoi. Notre rapport sur les VAP (Very Attacked People™, ou personnes très attaquées) répertorie vos utilisateurs les plus ciblés. Notre rapport sur les collaborateurs qui se laissent le plus piéger identifie quant à lui les utilisateurs qui ont cliqué sur des messages malveillants. Vous pouvez effectuer le suivi des VIP via le tableau de bord. Une fois ces informations en main, vous pouvez implémenter des contrôles adaptatifs pour vos utilisateurs vulnérables, ce qui vous permettra de hiérarchiser et de réduire les risques. Ces contrôles peuvent inclure une formation ciblée de sensibilisation à la sécurité informatique, l'isolation du navigateur et l'authentification multifacteur.

Réception d'informations centrées sur les menaces à des fins de contextualisation

Nous fournissons en temps réel des informations d'investigation numérique détaillées concernant les menaces et les campagnes. Notre analyse approfondie des menaces vous fournit toutes les informations requises, notamment la ou les personnes ciblées par l'attaque, son origine, et même les modalités et le déroulement de celle-ci. Nous déterminons également l'objectif de l'attaque. (Par exemple, nous pouvons établir si elle a pour but d'exfiltrer des données, d'installer un ransomware ou de commettre une fraude.) Nous mettons en corrélation les attaques par email et les connexions suspectes afin de vous aider à détecter et à neutraliser plus efficacement les compromissions de comptes. Notre plate-forme vous permet de comparer les types de menaces et les objectifs des cybercriminels dont vous êtes victime à ceux qui ciblent vos homologues.

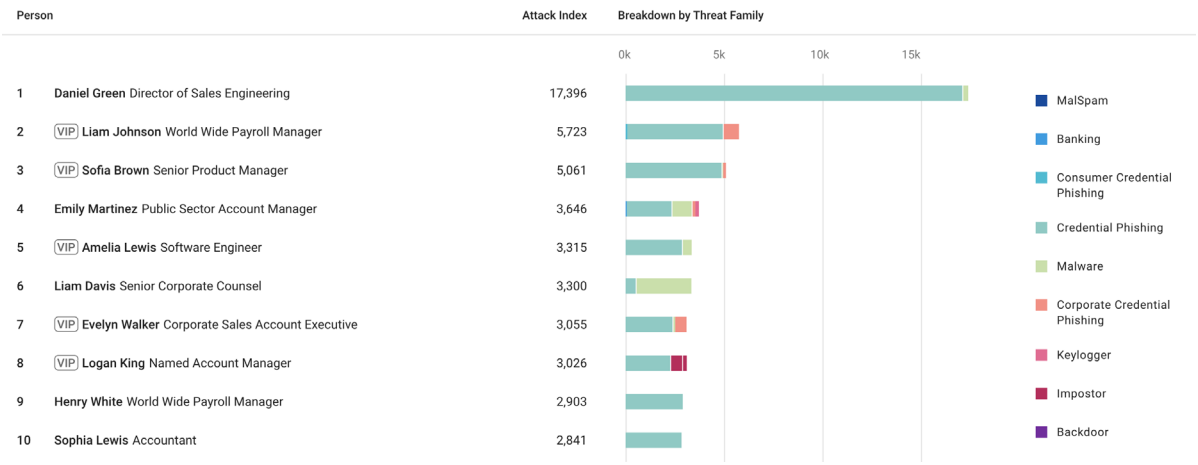

Figure 2. Rapport sur les VAP de Proofpoint montrant les utilisateurs les plus à risque et les types de menaces

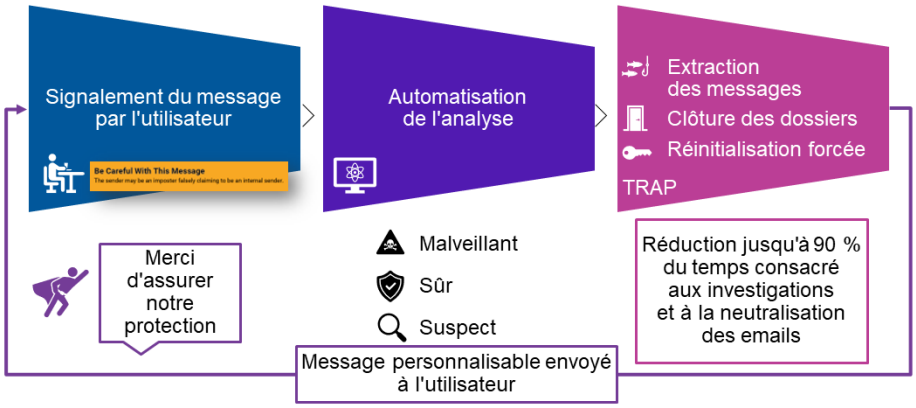

Figure 3. Solution Proofpoint Closed-Loop Email Analysis and Response (CLEAR) avec boîte email de signalement d'abus automatisée

Intégration d'informations sur les risques de compromission de comptes cloud et sur ceux liés aux fournisseurs

Nous vous offrons une visibilité sur les risques de compromission et sur ceux liés aux fournisseurs. Cette visibilité vous permet d'éradiquer complètement les attaques complexes. Nexus Supplier Risk Explorer nous permet d'identifier automatiquement les fournisseurs potentiellement victimes d'une compromission, ainsi que les domaines qu'ils utilisent pour envoyer des emails à vos utilisateurs. Grâce à notre fonctionnalité SaaS Defense intégrée, vous pouvez obtenir des informations sur les utilisateurs potentiellement compromis, les fichiers malveillants ou exposés, ainsi que les applications tierces à risque.

Amélioration de l'efficacité opérationnelle

De nombreuses équipes de sécurité sont en sous-effectif ou débordées. Elles ont souvent bien des difficultés à gérer les multiples fournisseurs et produits de sécurité de l'entreprise, de surcroît rarement compatibles. Nous vous proposons une solution intégrée qui se concentre sur les menaces les plus importantes et automatise leur détection et leur neutralisation. Vous réalisez ainsi des économies et gagnez un temps précieux, car vos équipes de sécurité peuvent consacrer moins de ressources internes à la neutralisation des emails que si elles utilisaient des solutions concurrentes.

Extraction automatique des emails malveillants

Notre solution permet d'éliminer les tâches manuelles et les estimations empiriques associées à la réponse aux incidents. Vous pouvez ainsi neutraliser les menaces plus rapidement et avec une efficacité accrue. Nous supprimons les emails de phishing contenant des URL dont l'activité nocive est déclenchée après la remise. En outre, nous pouvons supprimer — en un clic ou automatiquement — les emails indésirables des comptes internes compromis, même s'ils ont été transférés ou reçus par d'autres utilisateurs. Par ailleurs, notre graphique des menaces Nexus génère des alertes, et collecte et compare automatiquement les données d'investigation numérique, de sorte que vous bénéficiez d'une vue exploitable des menaces. Grâce à cette approche, vous pouvez réduire jusqu'à 90 % le temps consacré à la neutralisation des emails.

Rationalisation du processus de signalement des abus via la boîte email dédiée

Nous vous aidons à rationaliser le processus de signalement des abus via la boîte email dédiée, ainsi qu'à réduire la charge de travail de votre équipe informatique. Les utilisateurs peuvent signaler les messages suspects en un clic, soit directement à partir d'un avertissement, soit via le module d'extension PhishAlarm®. S'il s'avère que le message signalé est malveillant, ce dernier et toutes ses copies peuvent être mis automatiquement en quarantaine. Les utilisateurs reçoivent, quant à eux, un email personnalisé les informant qu'il s'agissait d'un message malveillant. Une telle approche les encourage à signaler des messages similaires à l'avenir. Les administrateurs peuvent obtenir des rapports détaillés sur le comportement des utilisateurs et comparer la précision du signalement des messages malveillants à celle d'autres entreprises du secteur.

Modification des comportements grâce à des formations centrées sur les menaces

Les menaces actuelles véhiculées par email nécessitent généralement une activation quelconque de la part des utilisateurs. Mais vos collaborateurs n'ont pas à être le maillon faible de votre stratégie de cybersécurité. Un personnel sensibilisé à la sécurité informatique peut constituer une ligne de défense robuste contre les cyberattaques.

Proofpoint vous permet de prendre des mesures à l'égard des VAP ou des collaborateurs qui se laissent le plus piéger. Les données collectées à leur sujet sont automatiquement intégrées à notre plate-forme de sensibilisation à la sécurité informatique. La plate-forme utilise ces données pour élaborer un programme de formation plus ciblé et plus efficace. Elle vous permet d'utiliser des simulations réalistes d'attaques de phishing fondées sur la threat intelligence de Proofpoint pour créer des expériences de formation pertinentes. Les utilisateurs qui tombent dans le piège reçoivent immédiatement des explications et des conseils. Ils peuvent ensuite être automatiquement inscrits à une formation spécifique. Nous affichons également à l'intention des utilisateurs des avertissements en cas d'emails suspects, comprenant un bouton « Report Suspicious » (Signaler comme suspect). Ces avertissements comportent de courtes descriptions personnalisables et des visuels des risques liés à un email donné. Ils permettent aux utilisateurs de signaler un message directement à partir de l'avertissement en question. Les utilisateurs peuvent ainsi prendre des décisions plus éclairées. Ces fonctionnalités sont compatibles avec l'ensemble des terminaux et applications.

Protection contre les fuites de données par email

La messagerie électronique est le vecteur de risque par excellence en ce qui concerne les menaces entrantes et les fuites de données en sortie. Vous devez donc protéger vos données sensibles et prévenir les fuites de données via la messagerie. Nous vous offrons la visibilité et les règles préconfigurées dont vous avez besoin pour prévenir les fuites accidentelles ou intentionnelles de données lors des échanges par email.

La prévention des fuites de données (DLP) et le chiffrement sont étroitement intégrés. Ils peuvent être gérés de manière centralisée sur la plate-forme Proofpoint Information and Cloud Security. Grâce au nouveau gestionnaire d'alertes unifié, vous pouvez personnaliser les explorations de données prêtes à l'emploi afin de détecter et de signaler toute infraction aux règles DLP de votre choix. Vous pouvez également simplifier vos opérations grâce à des workflows optimisés et à des fonctionnalités de neutralisation des emails. Nous analysons les informations confidentielles au sein des données structurées et non structurées. En outre, nous mettons à votre disposition des stratégies élaborées avec soin et des dictionnaires prédéfinis. Ceux-ci identifient automatiquement les données soumises à la conformité réglementaire et aux législations en matière de confidentialité des données. Ils vous aident également à respecter les réglementations de protection des données d'un large éventail de secteurs — par exemple, la norme PCI DSS, la loi SOX, la loi HIPAA, le RGPD et d'autres — tout en réduisant les tâches manuelles. Lorsqu'ils sont combinés au chiffrement, vous pouvez définir et personnaliser des stratégies uniques pour chiffrer automatiquement les données des emails. Une telle approche simplifie la gestion et la sécurisation des échanges de données sensibles.

Résumé

La solution Proofpoint Advanced Email Security assure une protection inégalée contre les menaces qui ciblent la messagerie. Elle vous offre une visibilité décisionnelle sur les attaques et les collaborateurs les plus attaqués. Ses avantages sont nombreux :

- Blocage des menaces avancées avant leur distribution
- Visibilité inégalée sur les risques liés au personnel et les menaces, et autres informations
- Amélioration de l'efficacité opérationnelle grâce à l'automatisation de la réponse aux menaces
- Formation et responsabilisation des utilisateurs afin de les transformer en ligne de défense robuste
- Protection contre les fuites de données via la messagerie

EN SAVOIR PLUS

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

À PROPOS DE PROOFPOINT

Proofpoint, Inc. 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 risques 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 75 % des entreprises de l'index Fortune 100, 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**.

proofpoint.

0201-016-01-03 4/22