

Proofpoint Impersonation Protection

Protégez vos communications avec vos partenaires, clients et fournisseurs de confiance



Principaux atouts

- **Protection de vos communications d'entreprise de confiance contre les menaces d'usurpation d'identité**
- **Prévention de l'usurpation de votre identité ou de celle de votre marque**
- **Identification et mise hors service des domaines similaires malveillants**
- **Détection et défense contre les fournisseurs à risque, y compris les comptes fournisseurs compromis**
- **Sécurisation des emails envoyés en votre nom par des applications, des terminaux, des plates-formes SaaS et des agents d'IA**
- **Optimisé par Nexus[®] AI, l'apprentissage automatique, les LLM et l'analyse comportementale**

La plupart des entreprises ont recours à la messagerie électronique comme vecteur de communication principal. Mais les cybercriminels ont trouvé comment détourner les communications professionnelles de confiance, et l'IA générative a rendu ces attaques plus rapides, plus convaincantes et plus faciles à déployer à grande échelle. Ils peuvent usurper l'identité de votre entreprise, de votre marque ou de vos partenaires commerciaux et créer des messages et des sites Web crédibles en quelques minutes au lieu de plusieurs heures.

Selon l'Internet Crime Complaint Center du FBI, le piratage de la messagerie en entreprise (BEC, Business Email Compromise) engendre systématiquement des milliards de dollars de pertes chaque année, et ces pertes continuent d'augmenter d'année en année. Le FBI a également commencé à suivre l'IA en tant que facteur de menace distinct, ce qui lui a permis d'attribuer spécifiquement des dizaines de millions de dollars de pertes liées au BEC à des attaques comportant une composante d'IA confirmée, et avertit que ce chiffre sous-estime probablement l'ampleur réelle du problème.

Ces attaques combinent souvent plusieurs tactiques d'usurpation, notamment des domaines usurpés, des domaines similaires et des comptes de fournisseurs compromis. Ensemble, elles mettent en péril les communications avec les partenaires, clients et fournisseurs de confiance, et compliquent la tâche des destinataires à l'heure de distinguer les messages légitimes des messages frauduleux.

Proofpoint adopte une approche globale et multicouche pour protéger votre entreprise et votre marque contre l'usurpation d'identité. Nous fournissons les outils, la technologie et les ressources nécessaires pour authentifier les emails générés par les utilisateurs et les applications, sécuriser les messages envoyés en votre nom, identifier les comptes de fournisseurs à risque ou potentiellement compromis, et surveiller les domaines similaires malveillants afin de pouvoir les supprimer.

Protégez votre marque contre l'usurpation d'identité

L'une des tactiques d'usurpation d'identité les plus courantes est l'usurpation de domaines, et l'IA générative a rendu les messages frauduleux plus rapides à produire et plus difficiles à distinguer des vrais. Sans des contrôles de sécurité appropriés en place, les cybercriminels peuvent facilement usurper vos domaines de confiance et utiliser l'IA pour élaborer des messages très convaincants à grande échelle. Cela leur permet de cibler vos clients, vos partenaires et même vos collaborateurs avec une rapidité et un degré de raffinement qui n'existaient pas il y a encore un an d'ici. L'authentification des emails est le moyen le plus efficace de les stopper.

Proofpoint Impersonation Protection simplifie la mise en œuvre du protocole DMARC en vous guidant à chaque étape du déploiement et permet d'authentifier à la fois les emails générés par les utilisateurs et ceux produits par les applications. Nos experts collaborent avec vous pour identifier vos expéditeurs légitimes. Ainsi, tous vos emails, y compris ceux provenant d'expéditeurs tiers autorisés, seront correctement authentifiés.

L'intégration à Proofpoint Threat Protection vous permet de mettre en œuvre l'authentification DMARC pour les messages entrants en toute confiance. Elle ajoute une couche de défense contre les tentatives d'usurpation générées par l'IA qui usurpent vos domaines de confiance. Elle vous permet également de déroger aux règles DMARC sans bloquer les emails légitimes ni compromettre la sécurité avec des listes d'autorisation. Cette intégration vous offre une visibilité sur le trafic de messagerie entrant et sortant. Vous pouvez ainsi voir tous les emails sortants qui utilisent vos domaines de confiance, y compris ceux envoyés par des tiers et, de plus en plus, par des agents d'IA agissant en votre nom.

Défendez-vous contre les comptes fournisseurs compromis

Les cybercriminels exploitent de plus en plus la chaîne logistique pour compromettre les communications d'entreprise de confiance. Ils utilisent souvent des comptes fournisseurs compromis pour pirater les fils de discussion entre vous et vos partenaires commerciaux. L'IA générative peut les aider à étudier les conversations antérieures et à imiter le style rédactionnel d'un fournisseur, ce qui rend les messages frauduleux plus difficiles à détecter. Et comme ces emails peuvent provenir de comptes de fournisseurs légitimes et ne contenir aucune charge virale, ils peuvent contourner les contrôles d'authentification et de détection traditionnels. Cela peut entraîner des pertes financières considérables, le vol de données, des extorsions ou des ransomwares.

Proofpoint Impersonation Protection vous aide à détecter et à vous défendre contre les fournisseurs à risque, y compris les comptes potentiellement compromis. Il utilise l'IA comportementale, l'apprentissage automatique et la threat intelligence provenant de l'importante base de clients de Proofpoint pour découvrir les signes de compromission de fournisseurs, y compris les attaques recourant à l'IA générative pour créer des leurres plus convaincants. Les contrôles adaptatifs, tels que l'isolation automatique des URL, aident à réduire l'exposition aux menaces provenant d'expéditeurs compromis. De plus, l'intégration de Proofpoint Impersonation Protection à Proofpoint Threat Protection et le contexte fourni sur les relations entre l'expéditeur et le destinataire simplifient la réponse aux incidents et les investigations tierces.

Détectez et supprimez les sites Web malveillants, y compris les sites similaires

Les cybercriminels créent des sites Web spécialement conçus pour mener des attaques. Certains usurpent l'identité d'autres entreprises, marques ou institutions pour inciter vos collaborateurs, clients ou partenaires à leur faire confiance. D'autres imitent votre propre entreprise, en utilisant des domaines et des pages qui imitent votre logo, votre mise en page et votre marque. L'IA générative a rendu ces deux types d'attaques plus faciles à créer, plus difficiles à repérer et plus rapides à déployer à grande échelle. Les cybercriminels utilisent ces sites dans le cadre du phishing d'identifiants de connexion, du piratage de la messagerie en entreprise, des attaques TOAD et d'autres stratagèmes qui dépendent d'une présence numérique convaincante.

Grâce à Proofpoint Impersonation Protection, nous surveillons en permanence les nouveaux domaines enregistrés susceptibles d'usurper l'identité de votre entreprise et vous fournissons le contexte nécessaire pour évaluer le risque potentiel.

La détection n'est que la première étape. Lorsque vous soumettez un site suspect à notre équipe chargée de la mise hors service, nous l'examinons, recueillons les preuves disponibles et faisons en sorte d'atténuer l'activité malveillante et de supprimer le site. Nous entretenons des relations avec un vaste réseau de fournisseurs d'infrastructures Internet et de partenaires de confiance, notamment des bureaux d'enregistrement, des hébergeurs, des fournisseurs de services de messagerie, des partenaires de liste de blocage, et plus encore.

Notre équipe gère le processus de mise hors service en votre nom, de sorte que vous n'avez pas à déterminer qui contacter ou quelle documentation est requise. Nos services de mise hors service ne se limitent pas aux domaines similaires et s'occupent également de l'atténuation des sous-domaines et URL malveillants, ainsi que des domaines non similaires.

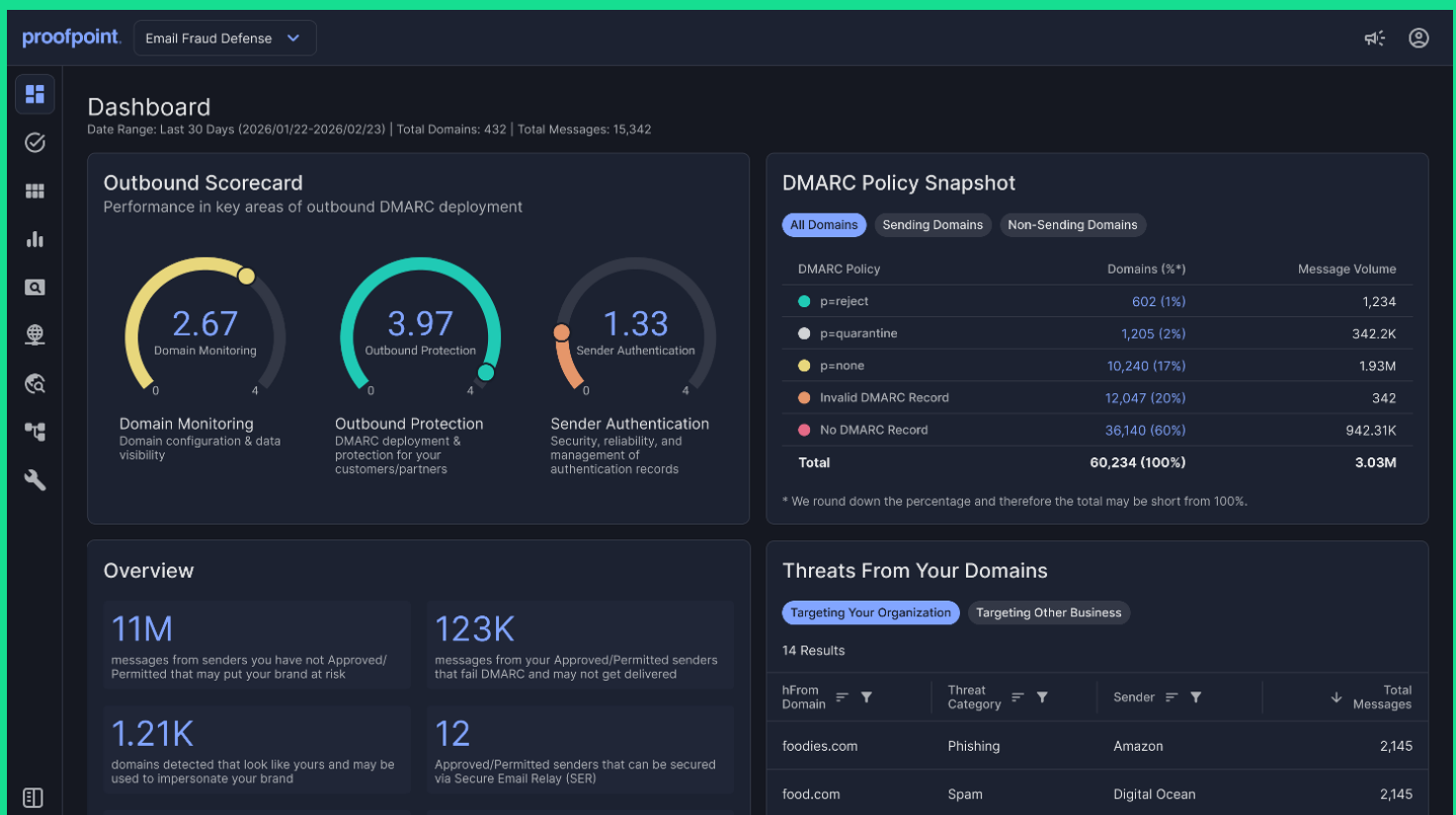


Figure 1. Proofpoint vous offre une visibilité sur les menaces d'usurpation de domaines, les domaines similaires malveillants imitant les vôtres et les emails envoyés à l'aide de vos domaines de confiance.

Sécurisez les emails envoyés en votre nom

Tous les emails qui quittent votre domaine n'émanent pas d'une personne rédigeant un message. Les plates-formes RH envoient des avis de paie, les outils CRM envoient des reçus clients, les terminaux de bureau envoient des notifications de numérisation vers la messagerie électronique et de fax, et les agents d'IA commencent à générer des messages en votre nom. Chaque source peut devenir une porte ouverte aux abus. Dès lors qu'une application, un terminal ou un service d'envoi est compromis, les cybercriminels peuvent utiliser ce canal de confiance pour envoyer des emails malveillants qui semblent provenir de vous, passent les contrôles d'authentification et, lorsqu'ils sont améliorés par l'IA générative, paraissent plus convaincants que jamais.

Proofpoint Impersonation Protection comble cette faille grâce à un relais sécurisé et dédié pour les expéditeurs automatisés qui utilisent vos domaines — des applications internes et des terminaux de bureau aux plates-formes SaaS et aux agents d'IA. Il accepte uniquement les emails provenant de sources vérifiées et authentifiées, applique une analyse anti-spam et antivirus avancée à chaque message et signe les emails approuvés avec DKIM. Vos sources sortantes peuvent ainsi assurer l'alignement avec la norme DMARC et la conformité SPF sans perturber le flux d'emails légitimes. Proofpoint SER isole par ailleurs ce trafic derrière des adresses IP dédiées et réputées, ce qui contribue à protéger votre infrastructure d'envoi ainsi que la réputation de votre marque contre les cybercriminels qui pourraient tenter de profiter de la confiance accordée à votre domaine.

Obtenez le soutien nécessaire pour garantir la visibilité, le contrôle et la conformité

Proofpoint Impersonation Protection vous offre une visibilité et un contrôle centralisés sur les services d'envoi à haut volume, tels qu'Amazon SES. Vous pouvez voir les messages qui quittent votre domaine en masse et les retracer jusqu'à l'application, le terminal ou l'agent d'IA qui les a envoyés. Le chiffrement optionnel et la prévention des fuites de données aident à protéger les données sensibles, y compris les données personnelles et les données médicales, contenues dans les messages transactionnels. Ces contrôles peuvent favoriser la conformité avec des cadres et des réglementations tels que la loi HIPAA et les exigences de la SEC et de la FINRA.

Proofpoint Impersonation Protection vous aide également à vous conformer aux exigences des principaux fournisseurs de boîtes de réception en ce qui concerne l'identité de l'expéditeur et l'intégrité des messages pour les expéditeurs en masse. Grâce à la prise en charge des en-têtes de désabonnement et à la gestion centralisée des listes, il permet aux emails légitimes de continuer à être remis en boîte de réception.

En savoir plus

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

À propos de Proofpoint, Inc. Proofpoint, Inc. est un leader mondial de la cybersécurité centrée sur les personnes et les agents, qui sécurise la manière dont les personnes, les données et les agents d'IA se connectent via la messagerie électronique, le cloud et les outils de collaboration. Proofpoint est un partenaire de confiance pour plus de 80 entreprises du classement Fortune 100, plus de 14 000 grandes entreprises et des millions de petites entreprises. Il les aide à bloquer les menaces, à prévenir les fuites de données et à renforcer la résilience des personnes et des workflows d'IA. La plate-forme de collaboration et de sécurité des données de Proofpoint aide les entreprises de toutes tailles à protéger et à responsabiliser leurs collaborateurs tout en adoptant l'IA en toute sécurité et en toute confiance.

Pour en savoir plus, consultez le site proofpoint.com/fr.

Suivez-nous : [LinkedIn](#)

Proofpoint est une marque déposée ou un nom commercial de Proofpoint, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs.

