Proofpoint Impersonation Protection

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

Principaux avantages

- 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
- Détection et défense contre les fournisseurs à risque, y compris les comptes fournisseurs compromis
- Sécurisation des emails de vos utilisateurs et applications afin qu'ils puissent être considérés comme fiables

La plupart des entreprises ont recours à la messagerie électronique comme vecteur de communication principal. Malheureusement, les cybercriminels ont trouvé comment pirater vos communications d'entreprise de confiance. Ils peuvent ainsi usurper votre identité, celle de votre marque ou celle de vos partenaires commerciaux. D'après le FBI, les usurpations d'identité telles que le piratage de la messagerie en entreprise (BEC, Business Email Compromise) ont coûté plus de 2,7 milliards de dollars aux entreprises. Et le coût d'une compromission de données impliquant un fournisseur compromis avoisinait les 5 millions de dollars[1].

Des tactiques telles que les domaines usurpés, les domaines similaires et les comptes fournisseurs compromis sont souvent employées conjointement lors d'usurpations d'identité. Vous devez protéger vos communications avec vos partenaires, clients et fournisseurs de confiance contre ces menaces. Proofpoint peut vous aider à limiter les risques. Nous authentifions les emails de vos utilisateurs et applications et vous défendons contre les comptes fournisseurs compromis.

Proofpoint adopte une approche globale et multicouche pour vous protéger vous et votre marque contre l'usurpation d'identité. Nous identifions vos fournisseurs à risque. Nous détectons les comptes fournisseurs potentiellement compromis ainsi que les domaines imitant ceux de vos fournisseurs. Nous sécurisons également les emails de vos utilisateurs et applications afin qu'ils puissent être considérés comme fiables.

Protégez-vous, ainsi que votre marque, contre l'usurpation d'identité

L'usurpation de domaines est l'une des tactiques d'usurpation les plus courantes. Sans des contrôles de sécurité adéquats, les cybercriminels peuvent facilement voler vos domaines de confiance. Cela leur permet de cibler vos clients, vos partenaires et même vos collaborateurs. L'authentification des emails est le moyen le plus efficace de les stopper.

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.

1 IBM, *Cost of a Data Breach Report* (Rapport sur le coût des compromissions de données), 2023.

Proofpoint Impersonation Protection implémente la norme DMARC pour vous aider à authentifier les emails de vos utilisateurs et applications. Nous simplifions l'implémentation de l'authentification DMARC grâce à une assistance à chaque étape du déploiement. 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 sécurité pour prévenir les menaces entrantes 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.

Défendez-vous contre les comptes fournisseurs compromis

Les cybercriminels ont transformé la chaîne logistique en un nouveau vecteur de menaces. Ils utilisent souvent des comptes fournisseurs compromis pour pirater des communications par email entre vous et vos partenaires commerciaux. Les emails provenant de fournisseurs compromis ne comportent pas toujours de charge virale malveillante et sont validés par le processus d'authentification. Leur détection est donc difficile. Or ils sont souvent à l'origine d'importantes pertes financières, d'extorsions de données ou d'attaques de ransomwares.

Proofpoint Impersonation Protection vous aide à détecter et à vous défendre contre les fournisseurs à risque, y compris les comptes fournisseurs compromis. Il s'appuie sur l'IA comportementale, l'apprentissage automatique et la threat intelligence issue de notre vaste base de clients pour identifier de façon proactive les comptes fournisseurs potentiellement compromis. Il inclut des contrôles adaptatifs, tels que l'isolation automatique des URL provenant de comptes fournisseurs compromis, pour limiter votre exposition. Son intégration 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.

Identifiez les domaines similaires malveillants

Une autre tactique courante consiste à piéger les destinataires avec des domaines similaires.

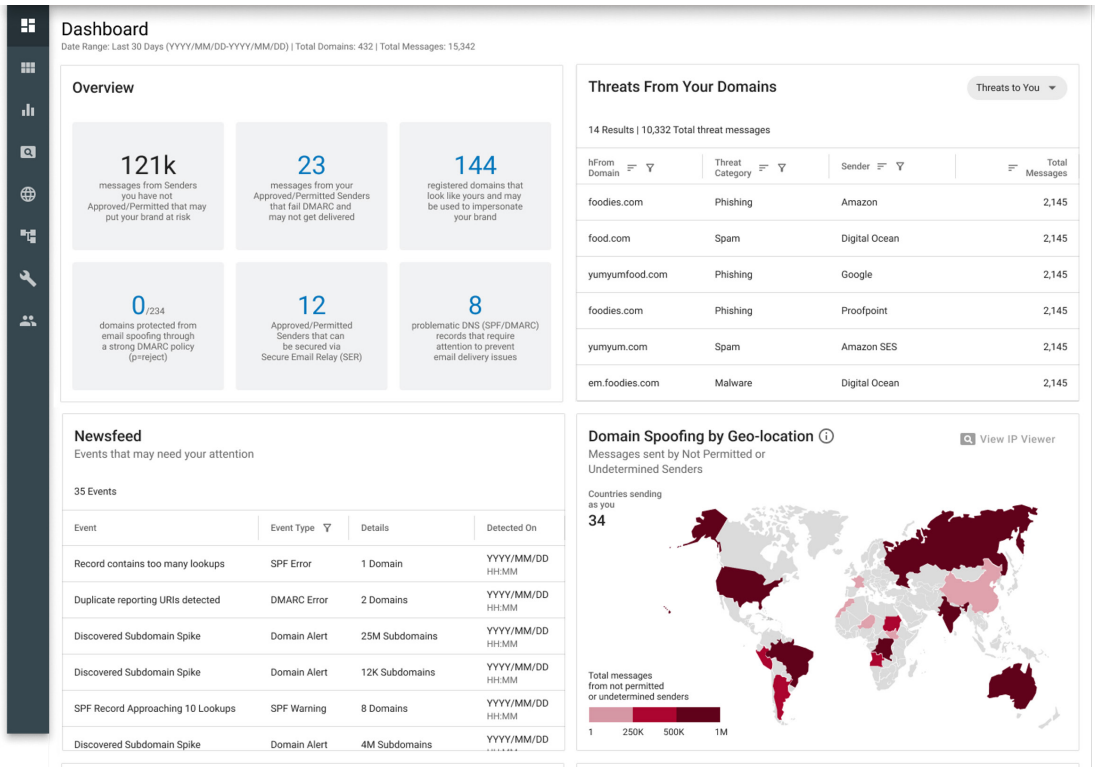

Figure 1. Proofpoint vous offre une visibilité sur les menaces d'usurpation de domaines, les domaines malveillants imitant les vôtres et les emails envoyés à l'aide de vos domaines de confiance.

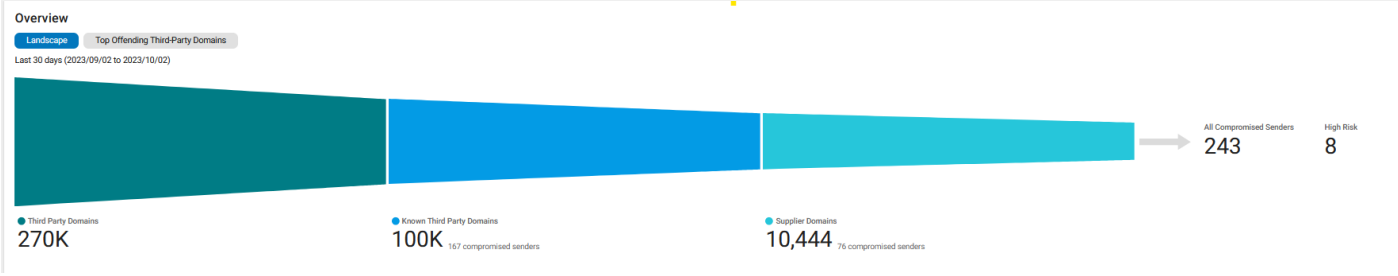

Figure 2. Proofpoint détecte les comptes tiers potentiellement compromis avec lesquels vous traitez et vous offre une visibilité sur les fournisseurs à haut risque.

Les cybercriminels enregistrent des noms de domaine qui ressemblent à s'y méprendre à ceux d'une marque ou d'une entité légitime. L'usurpation de domaines similaires est utilisée lors d'attaques telles que le phishing d'identifiants de connexion, les attaques BEC et même les attaques par téléphone (TOAD, Telephone-Oriented Attack Delivery).

Proofpoint vous aide à identifier les domaines malveillants imitant vos domaines de confiance. Nous détectons de façon dynamique les domaines récemment enregistrés qui usurpent l'identité de votre marque, qu'il s'agisse d'attaques par email ou de sites Web de phishing. Nous vous offrons une visibilité complète sur les domaines suspects. Nous vous aidons également à détecter les domaines malveillants qui imitent ceux de vos fournisseurs. En révélant le volume de messages et les messages distribués par les domaines imitant ceux de vos fournisseurs, nous vous permettons de gérer de façon proactive les fournisseurs à haut risque dont l'identité est susceptible d'être usurpée.

Sécurisez les emails d'applications envoyés en votre nom

Les emails envoyés en votre nom peuvent provenir d'applications tierces sur lesquelles vous n'avez aucun contrôle. Par exemple, certaines entreprises utilisent Workday pour envoyer des emails à leurs collaborateurs au sujet des salaires. D'autres ont recours à Salesforce pour envoyer des newsletters à leurs clients. En l'absence de contrôle, de telles utilisations pourraient rendre vulnérables les emails d'applications qui utilisent vos domaines de confiance. Une fois qu'une application tierce ou un partenaire SaaS est compromis, les cybercriminels peuvent injecter des malwares dans des emails transactionnels dont vous êtes le prétendu expéditeur. Le pire, c'est que ces emails transactionnels contaminés pourraient être validés par le processus d'authentification.

Proofpoint Impersonation Protection sécurise les emails de vos applications ainsi que ceux envoyés en votre nom. Nous appliquons nos contrôles de sécurité et de conformité aux emails transactionnels qui utilisent vos domaines de confiance. Nous authentifions ces emails et appliquons notre détection des menaces de pointe pour identifier les malwares ou les menaces. Vos clients, partenaires commerciaux et collaborateurs sont ainsi assurés de ne recevoir que des emails propres et authentiques de votre part. Cela vous offre également un contrôle centralisé sur les emails transactionnels provenant d'applications tierces et de partenaires SaaS. Vous pouvez mettre fin au trafic de messagerie issu des applications malveillantes de partenaires tiers compromis qui utilisent vos domaines à tout moment.

EN SAVOIR PLUS

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