Proofpoint Email Fraud Defense

Principaux avantages

- Simplification de l'implémentation de DMARC grâce à une assistance à chaque étape du déploiement
- Protection de votre marque contre la fraude par email, sans bloquer les messages légitimes
- Identification automatique des fournisseurs et du risque qu'ils posent
- Visibilité sur tous les emails sortants qui utilisent vos domaines de confiance et des domaines similaires
- Hébergement fiable des enregistrements SPF, DKIM et DMARC grâce aux services d'authentification hébergés de Proofpoint
- Intégration avec la passerelle de messagerie de pointe de Proofpoint, pour favoriser une mise en œuvre flexible et sécurisée de DMARC
- Affichage des taux de réussite DMARC pour les domaines de l'entreprise gérés dans l'environnement Microsoft 365

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.

Proofpoint Email Fraud Defense rationalise l'implémentation de l'authentification DMARC grâce à des workflows guidés et à l'assistance de consultants expérimentés. La solution protège la réputation de votre entreprise contre la fraude par email. Elle permet de visualiser les sources des emails envoyés au moyen de vos domaines de confiance et de domaines similaires. Elle permet par ailleurs de limiter les risques posés par les fournisseurs en identifiant automatiquement vos fournisseurs et les domaines similaires enregistrés par des tiers.

Proofpoint Email Fraud Defense vous guide tout au long du processus de déploiement de DMARC. La solution vous aide à protéger vos clients, partenaires commerciaux et collaborateurs contre le piratage de la messagerie en entreprise (BEC, Business Email Compromise). Avec Email Fraud Defense, Proofpoint protège votre marque en empêchant son exploitation dans des fraudes par email et atténue les risques d'impostures dans le trafic entrant. Nous authentifions également tous les messages envoyés par ou à votre entreprise, sans bloquer les emails légitimes.

Facilité d'utilisation

Des consultants dédiés et des conseils experts

Pour vous aider à configurer l'authentification des emails, Proofpoint crée un plan de projet à votre intention. Ce plan comprend des workflows guidés qui simplifient le processus de configuration. Nos consultants vous assistent tout au long des étapes de mise en œuvre du plan. En collaboration avec vos équipes, nous identifions tous les expéditeurs légitimes (y compris les tiers et les applications non approuvées) pour garantir une authentification correcte. De plus, nous analysons les spécificités de votre environnement de messagerie pour vous aider à hiérarchiser les tâches en fonction des besoins propres à votre entreprise, tels que le volume d'emails et les principaux expéditeurs.

Services d'authentification hébergés

Proofpoint Email Fraud Defense inclut les services SPF hébergé, DKIM hébergé et DMARC hébergé. Ces services hébergés vous aident à configurer et à gérer les règles pour les normes SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) et DMARC (Domain-based Message Authentication, Reporting and Conformance). Géographiquement distribués et tolérants aux pannes, ces services assurent la fiabilité.

SPF hébergé

- Contournement des limites de la recherche DNS (10) imposées par SPF
- Allègement de la charge de travail associée à la modification des enregistrements SPF
- Mise à jour des enregistrements en temps réel, avec validation de la syntaxe
- Renforcement de la sécurité SPF par l'obfuscation de l'infrastructure d'envoi
- Simplification de la gestion des envois massifs à partir de plusieurs domaines utilisant la même infrastructure d'envoi

DKIM hébergé

- Configuration et gestion simplifiées des sélecteurs et des clés DKIM
- Options d'hébergement flexibles pour les sélecteurs DKIM (délégués ou non)
- Prise en charge du protocole DNSSEC (DNS Security Extensions)
- Importation simple de sélecteurs et de clés publiques DKIM

DMARC hébergé

- Configuration et gestion simplifiées des enregistrements DMARC pour vos domaines
- Prise en charge du protocole DNSSEC
- Importation simple des enregistrements DMARC existants

Protection totale de la marque

Pour protéger votre marque, Proofpoint Email Fraud Defense bloque l'envoi d'emails frauduleux via vos domaines de confiance.

Identification des domaines similaires aux vôtres

Proofpoint Email Fraud Defense tire parti des informations d'enregistrement de Proofpoint Domain Discover. La solution détecte les domaines usurpant l'identité de votre marque, qu'il s'agisse d'attaques email ou de sites Web de phishing. Proofpoint analyse des millions de domaines et compare les données d'enregistrement avec ses propres données sur l'activité de la messagerie et les attaques. La solution montre les domaines suspects et comment les cybercriminels usurpent votre marque. Elle envoie également des alertes lorsque des domaines suspects deviennent actifs.

Le module complémentaire Proofpoint Takedown réduit l'exposition des particuliers, de vos partenaires commerciaux et de vos collaborateurs aux domaines similaires. Vous pouvez réclamer la suppression d'un domaine malveillant auprès du bureau d'enregistrement du domaine, du réseau de distribution de contenu ou du fournisseur de services de messagerie. Vous pouvez également exporter les domaines à bloquer au niveau de la passerelle de messagerie Proofpoint.

Visibilité à 360º sur votre écosystème de messagerie

Proofpoint Email Fraud Defense affiche tous les emails envoyés via vos domaines de confiance, y compris ceux destinés aux boîtes email des particuliers, aux passerelles d'entreprise et à votre passerelle.

Notre tableau de bord met en évidence les domaines de votre entreprise que les cybercriminels ont tenté de pirater, ainsi que le taux d'exploitation abusive de chacun d'eux. Il montre les expéditeurs autorisés et leurs enregistrements DMARC, de même que vos règles et taux de réussite pour SPF, DKIM et DMARC.

Proofpoint Email Fraud Defense met à votre disposition des informations exploitables et des recommandations. Ainsi, vous n'avez plus à vous inquiéter d'échouer à l'authentification DMARC ni de bloquer du trafic légitime, tout en neutralisant les cybercriminels.

Visibilité sur les risques associés aux fournisseurs

Proofpoint Email Fraud Defense va au-delà de DMARC pour vous offrir une visibilité sur les risques posés par vos fournisseurs. Le module Nexus Supplier Risk Explorer identifie vos fournisseurs, vérifie leurs enregistrements DMARC et indique les risques qu'ils posent. La solution affiche les messages remis par des domaines similaires. En hiérarchisant les alertes en fonction du niveau de risque, nous vous aidons à vous concentrer sur les incidents les plus graves.

Intégration avec la passerelle de messagerie de Proofpoint

Proofpoint Email Fraud Defense fonctionne de façon coordonnée avec la passerelle de messagerie Proofpoint afin d'appliquer l'authentification DMARC aux messages entrants. La solution vous aide à vérifier la réputation DMARC d'un domaine pour que votre passerelle ne bloque pas les messages légitimes échouant à l'authentification DMARC. Elle vous aide aussi à créer des dérogations aux règles pour les emails légitimes sans affaiblir votre sécurité.

Visibilité DMARC pour Microsoft 365

Si vous employez Microsoft 365 avec vos enregistrements MX (Mail eXchange) qui pointent vers les serveurs sortants de Microsoft, Proofpoint Email Fraud Defense peut tout de même afficher la conformité de vos domaines à DMARC. Cette visibilité vous aide à mettre en œuvre DMARC sur le trafic entrant de vos domaines en toute confiance.

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 85 % 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, 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.