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 les domaines similaires et les emails envoyés via vos domaines de confiance
- Intégration avec la passerelle de pointe de Proofpoint pour une mise en œuvre flexible et sécurisée de DMARC

Proofpoint Email Fraud Defense rationalise l'implémentation de l'authentification DMARC grâce à des workflows guidés et à l'assistance de consultants dédiés. La solution protège la réputation de votre entreprise contre la fraude par email. En outre, elle vous offre une visibilité totale sur les domaines similaires et les emails envoyés via votre domaine. Elle vous 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 d'implémentation de DMARC. La solution vous permet de mieux protéger vos clients, partenaires commerciaux et collaborateurs contre le piratage de la messagerie en entreprise (BEC, Business Email Compromise). Nous protégeons votre marque contre la fraude par email et limitons les risques posés par les menaces d'imposteurs en entrée. Nous authentifions également tous les messages envoyés par ou à votre entreprise, sans bloquer les emails légitimes.

Convivialité

Des consultants dédiés et un workflow guidé

Nous créons pour vous un projet avec un workflow « guidé ». Notre plan vous aide à déployer efficacement l'authentification des emails à grande échelle. Nos consultants vous assistent tout au long des étapes de votre déploiement. En collaboration avec votre équipe, nous identifions tous les expéditeurs légitimes (y compris les tiers) pour garantir une authentification correcte. Nous analysons les spécificités de votre environnement de messagerie pour vous aider à hiérarchiser les tâches en fonction des besoins et critères 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 et DKIM hébergé. Ceux-ci simplifient la configuration et la gestion, tout en renforçant la sécurité.

SPF hébergé

- Contournement des limites traditionnelles de la recherche DNS (10)
- Allègement de la charge de travail associée à la modification des enregistrements SPF
- Mise à jour des enregistrements en temps réel
- Renforcement de la sécurité SPF grâce à la prévention des enregistrements trop permissifs

DKIM hébergé

- Configuration et gestion simplifiées des sélecteurs et des clés DKIM
- Options d'hébergement flexibles des sélecteurs DKIM (délégués ou non)
- Prise en charge du protocole DNSSEC
- Création de services géographiquement distribués et à tolérance de panne
- Importation simple de sélecteurs et de clés publiques DKIM

Protection totale de la marque

Proofpoint Email Fraud Defense prévient l'envoi d'emails frauduleux via vos domaines de confiance. Nous protégeons votre marque et votre réputation contre la fraude par email.

Identification des domaines similaires aux vôtres

Proofpoint Email Fraud Defense tire parti des informations de Proofpoint Domain Discover. La solution identifie automatiquement les domaines similaires aux vôtres. Nous détectons de façon dynamique les domaines récemment enregistrés usurpant l'identité de votre marque, qu'il s'agisse d'attaques email ou de sites Web de phishing. Nous analysons des millions de domaines et corrélons les données d'enregistrement et nos propres données sur l'activité de la messagerie et les attaques actives. Vous bénéficiez d'une visibilité complète sur les domaines suspects. Nous vous montrons comment les cybercriminels usurpent votre marque. Vous recevez instantanément des alertes lorsque des domaines suspects, jusque-là en sommeil, passent à l'état actif.

Avec le module complémentaire Virtual Takedown, vous pouvez réduire l'exposition des consommateurs, de vos partenaires commerciaux et de vos collaborateurs aux domaines similaires malveillants. Qui plus est, vous pouvez réclamer la suppression du domaine auprès du bureau d'enregistrement ou de l'hébergeur. 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 vous offre une visibilité sur tous les emails envoyés via vos domaines de confiance, en ce compris ceux destinés aux boîtes email des consommateurs, aux passerelles d'entreprise et à la vôtre.

Notre tableau de bord détaillé vous fournit les informations suivantes :

- Domaines de votre entreprise que les cybercriminels ont tenté de pirater
- Taux d'exploitation abusive de chaque domaine
- Vos règles et taux de réussite pour l'authentification DMARC, SPF et DKIM
- Expéditeurs autorisés et leurs enregistrements DMARC

Proofpoint Email Fraud Defense vous offre des informations exploitables et des recommandations. Vous bénéficiez d'un suivi et d'une gestion plus performants, et pouvez appliquer des mesures aux tâches ouvertes. Avec Proofpoint Email Fraud Defense, vous n'avez plus à vous inquiéter d'échouer à l'authentification DMARC ni de bloquer du trafic légitime, tout en ayant l'assurance qu'aucun cybercriminel ne pourra usurper vos domaines.

Visibilité sur les risques associés aux fournisseurs

Proofpoint Email Fraud Defense va au-delà de l'implémentation DMARC pour vous offrir une visibilité sur les risques posés par vos fournisseurs. La fonction Nexus Supplier Risk Explorer identifie automatiquement vos fournisseurs, valide leurs enregistrements DMARC et détermine les risques qu'ils posent, notamment en termes de menaces d'imposteurs, de phishing, de malwares et de spam. Nous vous indiquons le volume de messages ainsi que les emails remis par des domaines similaires à ceux de vos fournisseurs. Par ailleurs, vous avez la possibilité de mener des investigations plus approfondies sur toute menace potentielle. En hiérarchisant le niveau de risque du domaine de chaque fournisseur, nous vous aidons à vous concentrer sur les incidents les plus graves.

Intégration avec la passerelle de messagerie de Proofpoint

Proofpoint propose une véritable intégration entre l'authentification des emails et sa passerelle de messagerie sécurisée. Lorsque Proofpoint Email Fraud Defense est associé à la passerelle de messagerie de pointe de Proofpoint, vous pouvez limiter les risques d'imposture en mettant en œuvre DMARC pour votre trafic entrant. Nous vous aidons à vérifier la réputation DMARC d'un domaine spécifique afin que votre passerelle ne bloque pas les messages légitimes échouant à l'authentification DMARC pour une raison quelconque. Nous vous aidons aussi à créer des dérogations aux règles pour les emails légitimes sans mettre en péril votre sécurité.

EN SAVOIR PLUS

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