HORNETSECURITY BY proofpoint.

FACTSHEET

DMARC MANAGER

PROTÉGEZ VOS DOMAINES ET RENFORCEZ LA CONFIANCE DANS CHAQUE EMAIL

Simplifiez la gestion de DMARC, DKIM et SPF, identifiez les expéditeurs non autorisés et corrigez les erreurs de configuration grâce à des actions claires et guidées.

DKIM

DomainKeys Identified Mail

Ajoute une signature numérique qui permet aux systèmes de réception de vérifier le domaine expéditeur et de confirmer que le message n'a pas été modifié pendant son acheminement.

SPF

Sender Policy Framework

Définit les serveurs et services de messagerie autorisés à envoyer des messages au nom de votre

DMARC

Domain-based Message Authentication, Reporting and Conformance

Vérifie que les messages sont alignés avec SPF ou DKIM, indique aux systèmes de réception comment traiter les messages en échec et fournit des rapports sur l'utilisation de vos domaines.

La gestion de l'authentification des emails sur plusieurs domaines est complexe. Des enregistrements DMARC, DKIM ou SPF mal configurés peuvent nuire à la délivrabilité des emails, dégrader la réputation de l'expéditeur et exposer les marques à l'usurpation d'identité et au spoofing.

Les entreprises peuvent aussi manquer de visibilité sur les services qui envoient des emails via leurs domaines, notamment les sources non autorisées, suspectes ou oubliées. DMARC Manager réunit la configuration, la surveillance et la correction guidée dans une seule interface. Il aide les équipes IT à sécuriser leurs domaines, à identifier les sources d'envoi et à maintenir une authentification efficace des emails, sans devoir interpréter manuellement des enregistrements DNS complexes.

GÉREZ FACILEMENT L'AUTHENTIFICATION DES EMAILS ET PROTÉGEZ VOTRE MARQUE

Configurez en toute confiance – Configurez et gérez DMARC, DKIM, SPF et TLS pour plusieurs domaines depuis une interface intuitive unique.

Résolvez les problèmes plus vite– Recevez des recommandations classées par priorité, accédez directement au paramètre ou à la zone d'analyse concernée et suivez la résolution du problème.

Identifiez chaque source d'envoi – Identifiez les services autorisés, non autorisés et suspects qui envoient des emails via vos domaines.

Améliorez la délivrabilité et la confiance envers votre marque – Aidez les emails légitimes à atteindre leurs destinataires tout en limitant l'usurpation de domaine et le spoofing.

FONCTIONNALITÉS

ACTIONS GUIDÉES

Identifiez les erreurs de configuration, hiérarchisez les mesures à prendre et accédez directement au paramètre ou à la zone d'analyse concernée. Les actions sont automatiquement marquées comme terminées dès que le problème est résolu, ce qui facilite le suivi de l'avancement.

CONFIGURATION CENTRALISÉE

Configurez et gérez DMARC, DKIM, SPF et TLS pour plusieurs domaines depuis une interface intuitive. Analysez en un coup d'œil les enregistrements SPF complexes, repérez les directives incorrectes et corrigez les problèmes de configuration sans devoir interpréter manuellement de longues entrées DNS. Des explications claires permettent aux équipes IT de gérer les paramètres d'authentification les plus complexes avec davantage d'assurance.

ANALYSE DES SOURCES D'EMAILS

Obtenez une vue d'ensemble des services et systèmes qui envoient des messages depuis vos domaines. Analysez les volumes d'envoi, les résultats d'authentification, la délivrabilité, la réputation des expéditeurs et les niveaux de menac. Classez ensuite les sources comme autorisées, non autorisées ou suspectes.

VUE PERSONNALISABLE DES DOMAINES

Consultez, depuis une vue unique, les scores des domaines, le volume d'envoi et l'état de DMARC, SPF, DKIM, BIMI, TLS-RPT et MTA-STS. Repérez rapidement les domaines qui nécessitent votre attention, affichez les informations les plus pertinentes pour votre entreprise et exportez les données au format CSV afin de les analyser plus en détail.

ANALYSE DES ÉCHECS ET ALERTES

Comprenez pourquoi certains messages échouent aux contrôles DMARC et identifiez les sources concernées. Configurez des alertes pour les événements importants afin que les équipes IT puissent examiner plus vite les problèmes de configuration ou les activités suspectes. Suivez l'évolution des configurations et des scores des domaines pour faciliter le dépannage et le suivi des modifications. Des rapports TLS détaillés permettent également de détecter les problèmes d'acheminement et les domaines qui ne respectent pas les paramètres de chiffrement attendus.

IDENTITÉ VISUELLE DES EMAILS AVEC BIMI

Les domaines éligibles auxquels une politique DMARC stricte est appliquée peuvent afficher un logo de marque vérifié dans les boîtes de réception compatibles. Cette fonctionnalité renforce la reconnaissance de la marque et la confiance des destinataires. Les alertes relatives à l'expiration des certificats permettent d'éviter toute interruption de l'affichage du logo BIMI.

PROTECT EVERY SENDING DOMAIN. GET YOUR FREE TRIAL: