

Sécurisez vos domaines de messageries avec Red Sift OnDMARC

DMARC ?

DMARC ou littéralement Domain-based Message Authentication, Reporting & Conformance, Il s'agit d'un protocole d'authentification des e-mails sortants qui empêche l'utilisation de votre domaine pour émettre des e-mails frauduleux. Il est construit sur les protocoles SPF et DKIM à qui sont ajoutés des fonctions de rapports et de renforcement qui permet aux émetteurs de bloquer les e-mails qui usurpent leurs domaines d'envoi légitimes et améliore la délivrabilité.

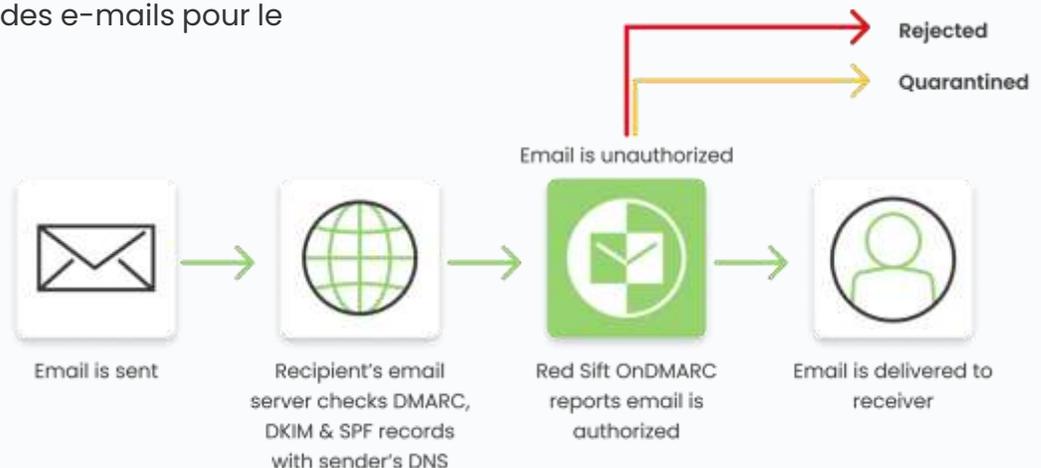
DMARC utilise les résultats des validations SPF et DKIM pour comprendre si l'e-mail est autorisé par le propriétaire du domaine. En utilisant la validation DMARC, il indique aux serveurs des destinataires s'ils doivent rejeter ou mettre en quarantaine les e-mails non conformes.

SPF ?

Sender Policy Framework est un protocole qui valide si un serveur de messagerie est autorisé à envoyer des e-mails pour le domaine.

Comment

**Red Sift
OnDMARC
travaille ?**



96%

En Moyenne , 96% des cyberattacks commence avec un e-mail d'hameçonnage

\$4.6M

Le coût moyen d'une attaque (violation) par hameçonnage est de \$4.65 millions

-5%

Les entreprises voient une baisse de 5% du cours de leur cotation dans les 6 premiers mois de leur violation.

DKIM ?

DomainKeys Identified Mail est une signature digitale qui certifie que le contenu de l'e-mail n'a pas été altéré ou modifié.

Prenez le contrôle de la réputation de vos emails avec **Red Sift OnDMARC**

Avec OnDMARC, vous pouvez stopper les usurpations de domaine d'envoi (exact) qui tentent d'arriver dans les boîtes de réception en appliquant une politique DMARC stricte (p=reject) rapidement et efficacement. Vous améliorerez significativement la délivrabilité de vos messages et serez éligible au BIMi (Brand Indicators for Message Identification).

18.5K

Sources d'envoi non autorisées et bloquées avec succès



99%

Taux moyen de délivrabilité des emails



6 weeks

Temps pour atteindre une conformité DMARC stricte

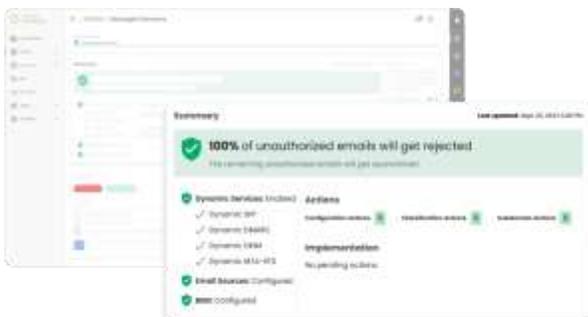


Le meilleur chemin pour aller vers une politique DMARC Stricte

Nos clients observent un temps moyen de 6-8 semaines pour appliquer une politique DMARC complète et stricte (p=reject ou p=quarantine) quelque soit leur taille et leur nombre de domaines d'envoi.

Simplifiez la gestion des SPF, DKIM, DMARC & MTA-STX

Faites, en une seule fois, les changements DNS et gérez toutes les authentifications d'emails à partir de l'interface de OnDMARC. Objectif : gagnez du temps opérationnel, évitez les erreurs de configurations manuelles, ajoutez ou supprimez facilement des services d'authentification.



Garantissez la délivrabilité au-delà des 10 SPF lookup

Rationaliser la gestion des SPF, oubliez les changements manuels dans le DNS. Garantissez une meilleure délivrabilité sans macros.



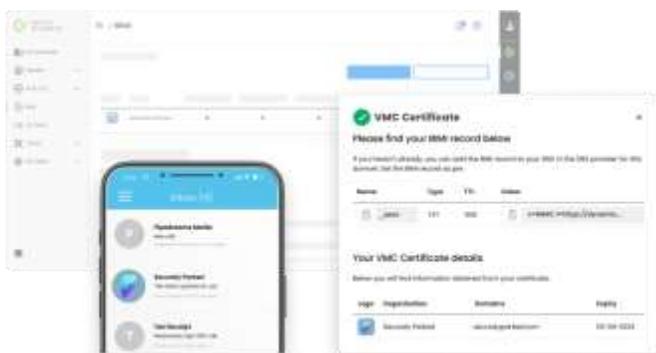
Identifiez rapidement les sources qui ne s'authentifient pas

Les rapports Forensic et le Machine Learning fournissent des informations granulaires sur les emails non authentifiés tout garantissant la confidentialité (RGPD).



Améliorez votre image de marque – reconnaissance et conversion avec BIMi

Red Sift OnDMARC est la seule solution BIMi sur le marché qui intègre le provisionnement de VMC. Améliorez les taux d'ouverture de 39 % et augmentez la mémorisation de la marque de 44 %.



Protégez vous des attaques de phishing qui contournent la protection DMARC

Avec DNS Guardian, vous pouvez rapidement identifier et arrêter le courrier malveillant qui contourne DMARC, y compris les prises de contrôle de domaines ou sous-domaines et de SubdoMailing (subdomain takeover).



Fonctionnalités primées de OnDMARC

Dynamic Services

Gérez les enregistrements SPF, DKIM, DMARC, et MTA-STS depuis l'interface de OnDMARC sans avoir besoin d'accéder à votre console DNS.

Dynamic SPF

Authentifiez vos mécanismes SPF sur l'ensemble de vos services d'envois légitimes et assurez une délivrabilité, sans faille, de vos emails.

Intégration BIMl

Rationaliser et automatiser le processus d'approvisionnement du VMC pour que le passage au BIMl se fasse le plus facilement possible.

Intelligence Expéditeurs

Transformez les rapports Forensics complexes en informations claires et utilisables à propos de vos sources d'envoi dans l'objectifs d'identifier et solutionner les fragilités rapidement.

Investigate

Vérifiez si vos services d'envois légitimes sont correctement configurés et vérifiez leurs conformités aux réglementations et vis-à-vis des recommandations Google – Yahoo.

DNS Guardian

Assurez une meilleure hygiène en surveillant en permanence votre configuration DNS afin d'éviter le SubdoMailing, les Dangling DNS et les prises de contrôle de CNAME.

Red Sift accompagne **+1,000 clients à travers le monde**



ATHLETIC GREENS



TalkTalk



Venez discuter avec nous...

Et découvrir pourquoi tant d'entreprises font confiance à Red Sift pour les protéger. redsift.com

