HORNETSECURITY

FACT SHEET

DMARC MANAGER

SAFEGUARD YOUR BRAND'S REPUTATION BY PROTECTING YOUR DOMAINS AGAINST EMAIL IMPERSONATION, PHISHING, AND SPOOFING WITH INTUITIVE DMARC, DKIM, AND SPF MANAGEMENT.

DKIM

DomainKeys Identified Mail

Digitally signs your email so that recipients know that the email is really from you and has not been altered.

SPF

Sender Policy Framework

Legitimates your domain to be the only one authorized to send emails in your name.

DMARC

Domain-based Message Authentication, Reporting and Conformance

Keeps your email inbox clean and determines what happens to emails that do not pass DKIM or SPF.

Managing email authentication is a headache for many organizations. Setting up and maintaining secure DMARC, DKIM, and SPF policies is a considerable challenge, especially for those managing multiple domains. Without proper DMARC settings, businesses risk their sender reputation and leave themselves vulnerable to email impersonation attacks. At the same time, complying with stringent email provider requirements adds another layer of complexity. The lack of visibility into the performance of email campaigns and the existence of hidden email activity within organizations is another unpleasant difficulty organizations must face. Further the desire for organizations to reach their customers' intended mailboxes rather than their spam folders is unlikely to achieve without proper email security.

EASILY MASTER DMARC, DKIM, AND SPF AND PROTECT YOUR BRAND'S REPUTATION

What is affected?

Email Communication

How does DMARC Manager help you?

Ensure Compliance

Effortlessly set up and maintain DMARC, DKIM and SPF best practice-policies

Easily Manage DNS

Seamlessly add DNS entries and change them within seconds

Prevent Impersonation

Get a comprehensive overview of the sources sending emails via your domains

What improves?

Ensure email delivery by complying with authentication standards and protect your brand reputation at the same time.

HORNETSECURITY

FACT SHEET

FEATURES

Domain Configurator: The service provides you with an intuitive interface to set up and maintain DMARC, DKIM and SPF best practice-policies as well as TLS settings for multiple domains. With DMARC manager, you can administer the SPF/DMARC records and can implement DNS changes within seconds.

Status Dashboard: The dashboard provides you with a comprehensive overview featuring various statistics, including managed domains, number of authorized and unauthorized senders, the volume of authorized and unauthorized emails sent, and the number of emails that have passed or failed DMARC.

Email Sources Analysis: This feature offers you a comprehensive overview of the sources sending emails via your domains. It details email volumes, authentication statuses (DMARC pass/fail), categorization of sources (authorized or unauthorized), deliverability, sender reputation and threat level.

BIMI Email Branding: Once your domain is DMARC compliant, you can use the BIMI feature that allows you to display your logo beside emails in supported inboxes, maximizing email impact, brand recognition and trust.

SMTP-TLS Encryption: Make sure that outbound emails are transmitted securely with SMTP-TLS encryption. Receive detailed reports on emails that were not encrypted and failed to deliver, providing another security layer for your email communications.

Failure Reports and Alerts: Failure reports offer detailed, real-time data on email messages that fail DMARC checks. This helps you to understand who is sending emails on behalf of your domains and why certain emails fail. Set up your chosen alerts and receive an email to the specified email address when an event takes place, enabling faster threat response.