



DMARC MANAGER

DMARC is an email authentication, policy, and reporting protocol that prevents the misuse of someone's own email identity. Almost any domain can be spoofed by cybercriminals who then send fraudulent emails that appear to come from your organization. The consequences can be severe for your brand image. It is therefore critical to be alert and ensure proper DMARC setup and transparent DMARC status.

In addition to that, major email providers often require DMARC to ensure email delivery. It is therefore vital for businesses to be DMARC compliant to reach their customers' inboxes and ensure an email campaign's success. Besides, managing and monitoring hundreds of domains can be time-consuming and complex, DMARC Manager supports admins in this challenge.

CUSTOMER AND PARTNER PAIN POINTS:

- » **Configuration Headaches:** Setting up and maintaining secure DMARC, DKIM, and SPF policies is complex, especially for MSPs and enterprise administrators managing many domains and configurations.
- » **Sender Reputation at Risk:** Without robust email authentication, a customer's legitimacy as an email sender can be compromised.
- » **Vulnerability to Fraud:** The rising threat of email impersonation attacks underscores the need for robust DMARC setups and transparent DMARC status.
- » **Compliance Challenges:** Major email providers like Yahoo and Gmail are increasingly demanding compliance with SPF, DKIM, and DMARC for bulk email senders.
- » **Delivery in the Dark:** Organizations often lack insight into the success of large email campaigns, unsure if failures stem from inadequate SPF, DKIM, or DMARC configurations.
- » **Hidden Email Activity:** „Shadow IT“ creates a lack of transparency, as organizations might be unaware of all entities sending emails under their domain.



OVERCOME THE CHALLENGES WITH DMARC MANAGER, YOUR ALL-IN-ONE DMARC MANAGEMENT PLATFORM:

DMARC Manager empowers organizations to actively control and monitor all emails sent under their domain, preventing unauthorized use of their brand in phishing attempts and spam campaigns. It provides visibility into who else is sending emails under a domain and returns control to the domain owner, strengthening and securing brand reputation. The tool provides an admin with an easy way to set up and maintain DMARC, DKIM and SPF best practice-policies for multiple domains.

By analyzing incoming DMARC reports, DMARC Manager offers insights into email delivery and authentication status, helping identify legitimate campaigns and potential spoofing attempts. Additionally, it enables businesses to enhance their email marketing strategies by ensuring that their emails are perceived by customers as authentic and trustworthy. This comprehensive tool centralizes management of various domains and configurations, facilitating DMARC compliance while protecting your brand's email reputation.



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.

THE BENEFITS OF DMARC MANAGER:

- » **Simplified Configuration:** Easily set up and manage DMARC, DKIM, and SPF best practice-policies for multiple domains through a single, centralized platform with intuitive UI.
- » **Enhanced Email Marketing Impact:** Ensure bulk emails are delivered by complying with authentication standards required by major email providers like Yahoo and Gmail.
- » **Email Traffic Identification & Control:** Define legitimate email sources and detect suspicious and unauthorized email senders.
- » **Brand Reputation Protection:** Boost the trustworthiness and reputation of your brands by safeguarding their domains against fraud, impersonation, and phishing attacks.
- » **Ensured Email Delivery:** Gain actionable insights on how to ensure legitimated emails from your domains reach the intended inboxes, not spam folders.
- » **Elevated Email Compliance:** Achieving DMARC compliance can also strengthen your compliance with industry/global regulations such as PCI DSS, NIST, GDPR, HIPPA and more.

TOP-LEVEL FEATURES:



Domain Configurator: The service provides you with an intuitive interface to setup 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.



BIMl Email Branding: Once your domain is DMARC compliant, you can use the BIMl feature that allows 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.

