DATASHEET

PCI-DSS Compliance with DMARC Analyzer

Gain control of your email domains, boost deliverability, and stop spoofing with easy-to-use tools and expert support—preserving trust while conserving resources.

The Problem

The PCI Security Standards Council sets global standards for secure payment processes. Their Data Security Standards apply to companies handling cardholder data, covering various security measures. PCI DSS v4, effective March 31, 2024, addresses emerging threats with some provisions due by March 2025. DMARC, a future-dated requirement, must be implemented with SPF and DKIM for comprehensive email authentication. While an effective DMARC deployment enhances control over organizational domains and email governance, implementation can be challenging and time-consuming without appropriate tools. Time is running out to achieve compliance.

The Solution

Mimecast's DMARC Analyzer solution protects your brand by providing the tools needed to stop spoofing and misuse of your owned domains, designed to help you reduce the time and resources required to become successfully DMARC compliant while providing the reporting and analytics needed to gain complete visibility of all your email channels.

Use DMARC Analyzer to stop direct domain spoofing protects against brand abuse and scams that tarnish your reputation and cause direct losses for your organization, customers, and partners. For added assurance, Mimecast's DMARC Analyzer Managed Services team stands ready to complement your efforts, leading to low-risk enforcement with limited resources while preserving trust in email.

ONLY 34%

of the world's largest 5000 companies use DMARC[1]

41%

of the domains in the banking sector had no DMARC policy[2]

Mimecast Value

- **Protect customers, preserve trust in email.** Prevent spam and phishing attacks that spoof your brand.
- **Get full visibility and governance of email.** See and control who's sending email on your behalf.
- **Enforcement confidence and assurance.** Accelerate implementation of your DMARC policy.

1&2 https://sendlayer.com/blog/dmarc-coverage-trends/

Feature	Details
DMARC Management	• DMARC enforcement status • Domain management, grouping, and status tracking • Customizable Domain Grouping based organization requirements • Automatic discovery of sub-domains and usage tracking • SPF and DKIM record checker • DMARC record generator • Overview of domain traffic volume, compliance status and verification • DMARC Aggregate data available per result, sending source, organization and host • Forensic reports include subject line, header information and any URLs • Real-time threat reporting with PGP encryption. • Unlimited users*, domains, domain groups and domain volume • Data retention up to 365 days • Optional easy SPF record management to expand authorized sending servers beyond 10
Administration	• Organized, consolidated view of critical information • DNS record monitoring highlighting changes over time. • Self-service email intelligence tools to implement DMARC policy on the gateway • Automated DMARC compliance alerts via email • Create tasks and assign them to team members via a built-in workflow
Services	• Professional services to implement DMARC projects • Optional Managed Services team helps with DMARC deployment and offers unparalleled knowledge and guidance on how to get the most out of DMARC Analyzer*

*DMARC Enterprise Only

DMARC Analyzer Use Cases

Prevent Email Spoofing

Implement a DMARC policy with a “reject” setting instructing receiving mail servers to reject any emails that fail DMARC checks. Continued Regular monitoring of DMARC reports to addresses any legitimate senders that may be misconfigured.

Improving Email Deliverability

To enhance deliverability, implement DMARC with a “quarantine” policy, instructing receiving servers to place suspicious emails in the spam folder instead of outright rejecting them. Additionally, this ensures compliance with Gmail and Yahoo’s recent requirement of setting SPF and DKIM records..

Enhancing Brand Trust

Establish a DMARC policy with a “p=reject” to protect the brand from being misused and signal to customers that the you take email security seriously. By actively monitoring DMARC reports, you can quickly respond to any unauthorized use of your domain.

Secure human risk with a unified platform.

Mimecast’s connected human risk management platform prevents sophisticated threats that target human error. By gaining visibility into human risk across your collaboration landscapes you can protect your organization, safeguard critical data, and actively engage employees to reduce risk and enhance productivity.