Data Sheet

mimecast

PCI-DSS Compliance with DMARC

Conform to PCI Data Security Standards version 4.0 with DMARC Analyzer

The Payment Card Industry Security Standards Council is a global organization responsible for secure payment processes and data. Data Security Standards by PCI SSC applies to companies with access to cardholder data. This set of regulations covers anti-spam, anti-phishing, encryption, and other security measures.

PCI Data Security Standard v3 focused on protecting primary account numbers and sensitive authentication data. Like other regulatory bodies, the PCI Security Standards Council regularly updates its security parameters to meet rising cyber threats. V4 is the latest version and is designed to help organizations more effectively address emerging threats and leverage new protection technologies to address the current threat landscape. The new standard goes into effect on March 31, 2024; however, some technical and harder-to-achieve provisions are "future dated" for implementation by March 31, 2025. DMARC (Domain-based Message Authentication, Reporting, and Conformance) is one of the future dated items and must be implemented alongside complementary measures like SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) to establish a comprehensive approach to email authentication.

An effective DMARC deployment provides control of organizational domains and better governance for sending email sources. However, it can be difficult and time consuming to implement without the right tools. Most organizations take an average 6 to 9 months to achieve full compliance, which doesn't leave much time for DMARC implementation and compliance alongside PCI-DSS V4.0 auditing. Details on updates can be found in the PCI DSS v4.0 Change Summary document on the PCI SSC website.

Mimecast's DMARC Analyzer solution is designed to simplify and accelerate implementation of the DMARC standard, while also giving you full visibility and control of who is sending emails on your behalf.

Why DMARC Analyzer from Mimecast?

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, the self-service solution provides the reporting and analytics needed to gain full visibility of all your email channels. Using DMARC 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.

Get full visibility and governance of email

An effective DMARC deployment allows you to gain control of your owned domains and better govern who is or is not allowed to send emails on your organization's behalf. But without the right tools, it can be difficult and time-consuming to implement. Before enforcing a DMARC reject policy, it is essential to gain full insight into both your inbound and outbound email channels to make sure legitimate email does not get rejected. Mimecast's DMARC Analyzer solution provides the reporting and analytics needed to gain full visibility and governance across all email channels with aggregated reporting, encrypted forensic reports, real-time reports, and monitoring alerts. You can then specify what to do when emails fail DMARC authentication checks. The solution provides total visibility and governance across all email channels and is designed to make enforcement as easy as possible.

Block targeted inbound attacks

Without authenticated sending sources for email, your organization is more likely to be exploited by phishing and spoofing attacks and more likely to experience deliverability issues for legitimate mail. If your organization has many active and dormant domains or third parties that you allow to send emails on your behalf, achieving an effective DMARC configuration can be particularly challenging. Mimecast's user-friendly service is designed to guide you towards a DMARC reject policy as quickly as possible.

DMARC builds on existing SPF and DKIM email authentication techniques by adding a critical element, reporting. Using this information, you can decide who should be authorized to use your domain and who is sending without authorization to block delivery of all unauthenticated mail. You can specify what to do when emails fail DMARC authentication checks, thus changing your policy to P=Reject to protect your organization from inbound attacks.

Key Benefits
DMARC Analyzer

- Blocks impersonation, phishing, and malware attacks by combining email channel visibility and reporting with Mimecast's DMARC enforcement and email security.
- Achieves DMARC enforcement more quickly through self-service tools and user-friendly charts and reporting.
- Enhances protection of your own organization and brand, as well as customers, partners, and suppliers.
- Reduces cost and complexity with a rapidly deployed SaaS-based solution

Enforcement confidence

DMARC reporting can generate overwhelming amounts of data that require significant review time to validate which domains are valid and which are spoofed. This process can take months, requiring continued resource allocation. Get the help and assistance needed with built-in guidance, an extensive knowledge base, and flexible services including our fully managed service. Customer success managers and consultants help manage your DMARC deployment, mitigate risk, and allow you to safely block malicious emails without impacting transactional email channels. On-going management and reporting processes will ensure successful deployment and risk management. Mimecast's DMARC Analyzer solution helps IT and security teams deploy DMARC in a user-friendly and frictionless way, providing a path to both ease and speed the process of moving into policy enforcement (p=reject), even in the most complex environments.

Rapid deployment and cost effectiveness

DMARC Analyzer's approach is unlike any other, providing a fast and simple DMARC deployment with intuitive self-service tools and integrated project management. Mimecast's DMARC Analyzer solution is delivered as a 100% SaaS-based offering for rapid deployment and cost effectiveness.

In addition to the self-service capability within DMARC Analyzer, Mimecast offers Managed Services to proactively guide you through each stage of the DMARC deployment and maintenance, ensuring you benefit from the full range of DMARC capabilities.

How it Works

1. **Publishing your DMARC record.**
   The DMARC txt-record must be published on each domain owned by the organization.
2. **Collecting data.**
   After the DMARC record is published, DMARC source information will be received.
3. **Analyzing the data.**
   Authorized and illegitimate sources per domain can then be identified.
4. **Authenticating the authorized sources.**
   After the authorized sources are detected, authentication for SPF and DKIM per domain is set.
5. **Start enforcing the policy.**
   Once authentication is aligned, you can safely move to a reject policy for each domain.