Datasheet

mimecast

DMARC Management

Gain control of your domain and put an end to spoofing attacks with DMARC Analyzer

Impersonation and spoofing attacks are a significant issue for most organizations, growing at a much faster rate than malware attacks as cybercriminals increase their efforts to exploit people. Attackers risk damaging your brand by targeting your employees, customers, and suppliers alike. Ignoring this problem can significantly impact your reputation, business relationships, and the successful delivery of your own outbound business email. In order to effectively stop these complicated attacks, organizations should combine multiple layers of protection.

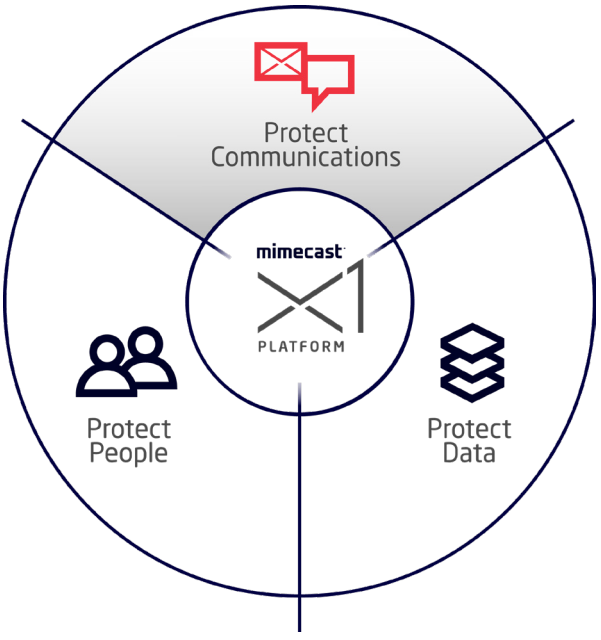
Why DMARC?

Mimecast DMARC Analyzer 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 (Domain based Message Authentication, Reporting, and Conformance) 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.

Key Benefits

DMARC Analyzer

- Blocks impersonation, phishing, and malware attacks by combining email channel visibility and reporting with Mimecast's DMARC enforcement and Targeted Threat Protection.
- 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.



How it Works

- **Publishing your DMARC record.** The DMARC txt-record must be published on each domain owned by the organization.
- **Collecting data.** After the DMARC record is published the customer starts receiving DMARC source information.
- **Analyzing the data.** The customer must identify the authorized sources per domain.
- **Authenticating the authorized sources.** After the authorized sources are detected, the customer must authenticate SPF and DKIM for each source per domain.
- **Start enforcing the policy.** Authentication is done, the customer can now safely move to a reject policy for each domain.

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.

The self-service 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 – 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.

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.

If you're an organization with many active and dormant domains or third parties that you allow to send emails on your behalf, ensuring 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.

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 DMARC Analyzer is delivered as a 100% SaaS-based solution for rapid deployment and cost effectiveness.

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.

Two Distinct Offerings

Every organization is unique, and your DMARC journey is no exception. DMARC Analyzer offers the choice between a Standard package and Fundamentals package to best meet your organization's needs.

Features & capabilities	Standard package	Fundamentals package
Active domains	5/25/50/100/250+	5
Inactive domains	unlimited	unlimited
Active users	unlimited	3
Data retention (in days)	365	90
Monthly DMARC email volume	unlimited	2,000,000
SPF delegation	add-on	add-on
Implementation Services*	Available for add-on purchase	Not available for add-on purchase
Managed Services*		

*DMARC Analyzer Implementation Services and Managed Services simplify your DMARC experience with the support and guidance of Mimecast experts. Available for purchase only with the DMARC Analyzer Standard package.