Datasheet

mimecast

# Mimecast DMARC Analyzer

Gain control of your domain and put an end to spoofing attacks with email channel analysis and DMARC reporting.

**Impersonation and spoofing attacks are a significant issue for most organizations, growing at a much faster rate than standard malware attacks as cybercriminals exploit human weaknesses.**

Attackers will target your own organization and employees, customers and suppliers, cultivating risk of damage to your brand. Stopping these often malware-less attacks is not straightforward and, to be most effective, should combine multiple layers of protection.

Mimecast DMARC Analyzer helps you protect your brand by providing the tools needed to stop spoofing and misuse of your owned domains. Designed to help you reduce the time and resource 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.

## Key Benefits

- More effectively block impersonation, phishing and malware attacks by combining email channel visibility and reporting with Mimecast DMARC enforcement and Targeted Threat Protection.
- Move to DMARC enforcement more quickly through self-service tools and user friendly charts and reporting.
- Better protect your own organization and brand, customers, partners and suppliers.
- 100% SaaS solution for rapid deployment and cost effectiveness.

# Why DMARC

Using DMARC (Domain-based Message Authentication, Reporting and Conformance) to stop direct domain spoofing protects against brand abuse and scams that can tarnish your reputation and lead to direct losses for your organization, your customers and partners.
An effective DMARC deployment allows you to gain control of your owned domains and better govern who is or isn't allowed to send emails on your organization's behalf.

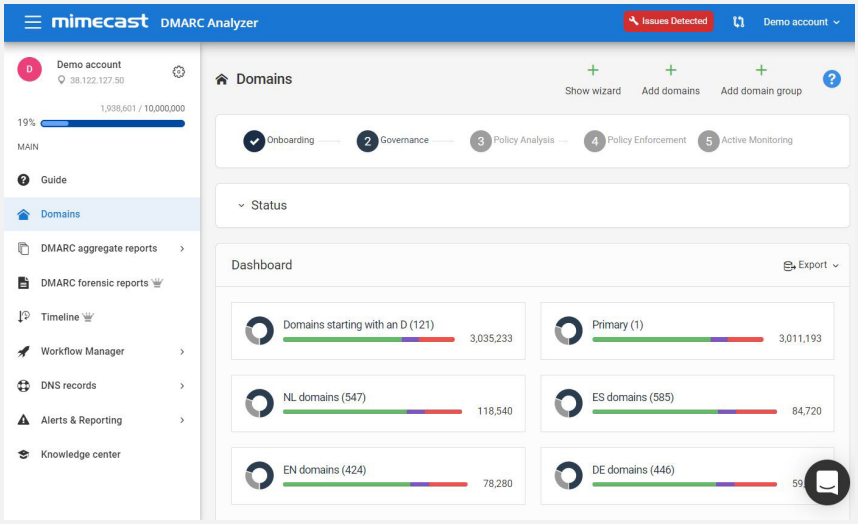


*Fig 1: Domain dashboard*

However, it can be difficult and time consuming to implement without the right tools. 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. If you're an organization with many active and dormant domains or third-parties that you allow to send email on your behalf, ensuring an effective DMARC configuration can be particularly challenging.

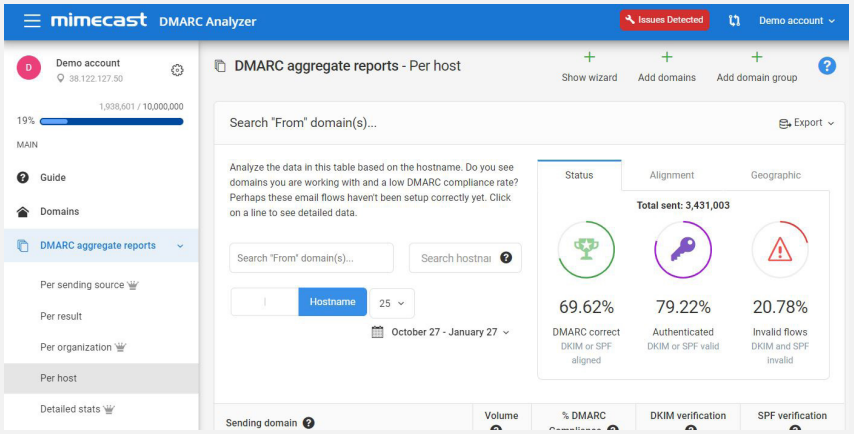


*Fig 2: Aggregate report grouped by hostname of sending IP addresses*

**This is where DMARC Analyzer helps through:**

- An easy to use SaaS solution to manage complex DMARC deployment.
- 360° visibility and governance across all email channels.
- Self-service email intelligence tools to implement DMARC policy on the gateway.
- Alerts, reports and charts to help achieve enforcement and monitor ongoing performance.
- An SPF Compression service made available to resolve lookup limit issues.

Unlike other DMARC solutions that often need ongoing professional services to be successful, Mimecast DMARC Analyzer is designed for simple and effective self-service to reduce the time, effort and cost of stopping domain spoofing attacks. Additional services and support are available if needed.

## Combination is Key

**Impersonation Protect works with Mimecast URL Protect, Attachment Protect and Internal Email Protect for comprehensive protection against advanced email-borne threats. Data Leak Prevention (DLP) helps prevent exfiltration of sensitive and personal data.**

Protection against direct domain spoofing alone cannot prevent all impersonation attacks. Combining the Mimecast DMARC Analyzer reporting and email validation solution with our Targeted Threat Protection provides defense both at your perimeter and beyond it, to protect your organization, relationships, and reputation.

As part of Targeted Threat Protection, Impersonation Protect delivers effective protection against impersonation attacks by identifying combinations of key indicators in an email to determine if the content or sender are suspicious, even in the absence of a malicious URL or attachment. These indicators include:

- Newly observed and newly registered domains
- Display name spoofing & reply-to mismatch
- Lookalike domains including the use of non-western character sets
- Key words matching those in our threat dictionary

Together, Mimecast email security and DMARC Analyzer provide comprehensive protection against impersonation attacks and direct domain spoofing. Protecting your employees, customers, supply chain and overall organization, Mimecast helps safeguard your organization from targeted attacks and brand abuse.

## Find out more:

**To find out more about Mimecast DMARC Analyzer, visit mimecast.com/products/dmarc-analyzer**