sure.business mimecast

Cybersecurity Solutions
Mimecast 3.0 DMARC Analyser

Introduction

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 organisations, growing at a much faster rate than standard malware attacks as cybercriminals exploit human weaknesses. Attackers will target your own organisation 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.

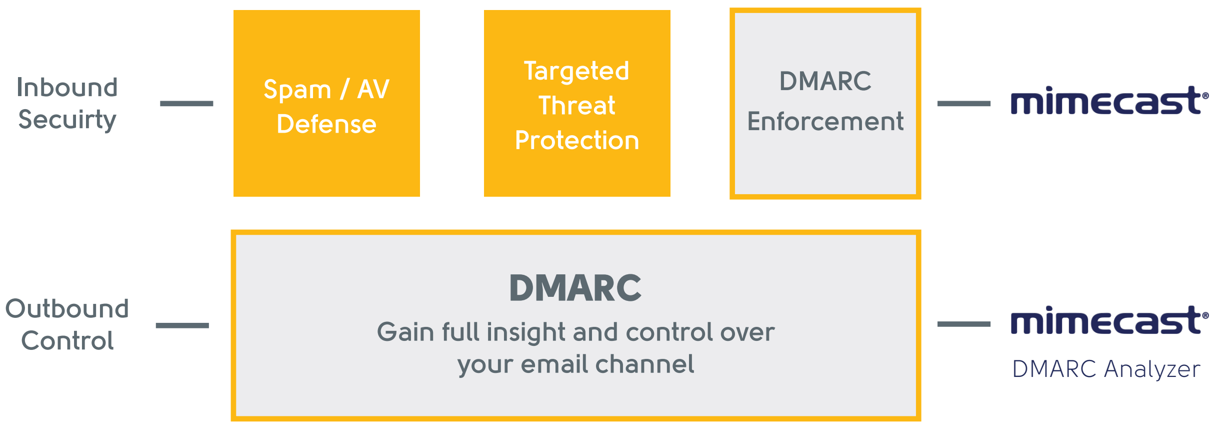
Mimecast DMARC Analyser helps you protect your brand by providing the tools needed to stop spoofing and misuse of your owned domains. Designed to help you reduce the time and resource required to become successfully DMARC compliant, the self-service solution provides the reporting and analytics needed to gain full visibility of all your email channels.

Mimecast's cloud architecture has been developed to offer a comprehensive service with a single platform.

Sure and Mimecast have partnered to offer a unique 'offshore' variant of the Mimecast suite, with all data contained in the Sure owned and operated data centres located in Jersey and Guernsey (Channel Islands).

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 organisation 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 organisation, 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 organisation's behalf. 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 organisation 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.

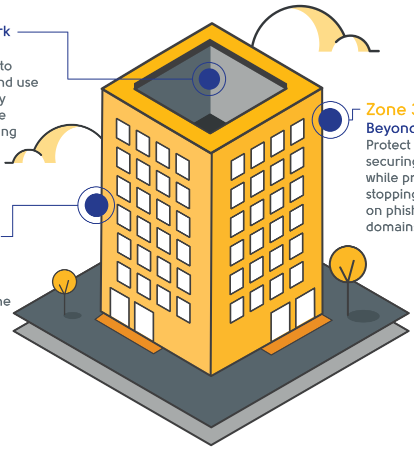
DMARC Analyser Features

- 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 DNS Delegation service made available to resolve lookup limit issues.

Unlike other DMARC solutions that often need ongoing professional services to be successful, Mimecast DMARC Analyser 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.

Cyber Resilience Platform

Mimecast 3.0 email security provides a comprehensive cyber security, resilience and compliance platform to protect your organisation's email, data, users and web.



Zone 2
Inside Your Network & Organisation
Educate employees to recognise threats and use best practice security policies with effective online security training programs.

Zone 1
At Your perimeter
Protection from inbound phishing, malware and spam attacks whether in the office, at home or mobile.

Zone 3
Beyond Your Perimeter
Protect your brand by securing your domains, while proactively stopping attacks that rely on phishing and lookalike domains.