Service Sheet

Mimecast DMARC - Managed Service

Overview

DMARC is Domain-based Message Authentication, Reporting and Conformance, a technical standard that helps protect email senders and recipients from advanced threats that can be the source of an email data breach.

What does Mimecast DMARC - Managed Service do?

DMARC can benefit your customers by providing another layer of protection that guards against attacks like impersonation fraud, where an attacker uses a legitimate domain to send a fraudulent message.

If you and your customer require expert guidance and support opt into managed services to get additional guidance and tips from Infinigate Cloud experts.

Features

Reviews email message headers to ensure the accuracy of the information provided. DMARC works with DKIM and SPF authentication to verify legitimate emails before delivery and reject malicious emails before they are delivered.

Checks whether emails have been sent from an authorised IP or domain, specifying how domains can be contacted if there are authentication issues and provides the forensic information needed to monitor and quarantine suspect emails.

Prevent direct domain spoofing, where attackers use an organisation's exact domain in the "from" address in an email.

Provides AI-enhanced detections, advanced phishing protection, URL analysis and rewriting.

Who is the Mimecast DMARC - Managed Service for?

This managed service for any customer who has up to five domains and does not have the internal capacity to monitor inbound and outbound mail to ensure all mails are received and sent correctly. Once enabled, the service will save time and cost by ensuring all domains are running efficiently.

About this service

Prerequisites

To engage this managed service, you will need to be an existing Mimecast customer with the appropriate licences and purchased the corresponding bolt on.

Commitment length:

One year

Contact Us

portal.infinigate.cloud

infinigate cloud