

MIMECAST SECURITY MANAGEMENT SERVICE

Manage, control and safeguard vital data across your organisation.
Beyond Cloud.



Our Mimecast Security Management Service, powered by Mimecast, protects you from the number one cyber security threat in your organisation: human error.

For threats including clicking on a malicious link sent by someone impersonating a member of senior management, accidentally (or maliciously) deleting emails or Microsoft Teams chat messages, or browsing unsafe websites on a company device, we've got you covered.

Attacks don't stop at your network's edge. The protection provided by these services works at the three critical layers of your organisation:

- **At the email perimeter.** Prevent an attack reaching your end user's inbox
- **Inside your network and organisation.** Prevent the spread of an attack once activated

- **Beyond your perimeter.** Prevent attacks to your reputation and brand from spoofed emails and weaponised copies of your website

All features of this service are 100% cloud hosted and managed by our Mimecast certified experts. This means you don't need to worry about lead times, large capex costs or forgetting to configure something correctly.

Mimecast Security Management Service Benefits

Best-in-class protection against the most advanced email-borne threats



Simplified data governance and compliance with best-in-class archiving capabilities



Security awareness training content that users actually enjoy and look forward to watching



Brand and reputation protection against spoofed emails and weaponised copies of your website



Contextual warning banners display in any mail client, with clear explanations of why an email has been flagged as a potential threat



100% cloud hosted software means you're always protected against the latest known threats



Best-in-class SLAs on email delivery and archiving features



All features managed and supported by Six Degrees' Mimecast certified experts



Mimecast Security Management Service Features

We provide these features in a modular fashion, so you only pay for the features you need.

| Feature | Overview |
|--------------------------------------|--|
| Email Security | Cloud-based Secure Email Gateway protects organisations and employees using any cloud or on-premises email platform. It defends against inbound spear-phishing, malware, spam and zero-day attacks by combining innovative applications and policies with multiple detection engines and intelligence feeds. |
| Email Archiving | Cloud Archive helps you meet today's regulatory, legal, and corporate requirements quickly and accurately. Whether for European Union General Data Protection Regulation (GDPR) compliance, internal audits, compliance reviews, or legal challenges, your organisation can reduce the burden of responding to queries and investigations with Cloud Archive. |
| Web Security | Protect your employees and guest Wi-Fi users against malicious and inappropriate websites with a 100% cloud-based service that integrates with the Email Security solution for consistent cyber protection. |
| Security Awareness Training | A security awareness training program designed to engage employees and reduce the risk of human error. The Security Awareness Training includes many topics that are relevant to Microsoft 365 security and compliance. These include instructions in compliance for GDPR, PCI and HIPAA, as well as training in how to deal with impersonation fraud, ransomware and phishing attacks. |
| DMARC Analyser | DMARC Analyser provides a software solution which empowers organisations to manage complex Domain-based Message Authentication, Reporting, and Conformance (DMARC) deployments easily via their user friendly DMARC analysing software, acting as your expert guide to move you towards a reject policy as fast as possible. The solution provides 360° visibility and governance across all email channels. |
| CyberGraph | By understanding relationships and connections between senders and recipients, including the strength or proximity of the relationships, CyberGraph can detect and alert users to anomalous behaviours. Email tracker prevention disarms trackers embedded in emails, while identity graph technology powered by machine learning detects anomalous behaviours that could be indicative of a malicious email. Meanwhile, contextual warning banners use crowdsourced intelligence to engage and empower users at the point of risk. |
| Brand Exploit Protect (BEP) | Even unsophisticated attackers can register domains that look like yours and use your brand as bait to target the people who trust it. They'll even clone your website to steal credentials, personal information, and money. BEP uses a combination of machine learning and quadrillions of targeted scans to identify even unknown attack patterns at an early stage, blocking compromised assets before they become live. When active attacks are discovered, they can be remediated quickly to minimise damage to your brand and your customers. |
| Archiving for Microsoft Teams | Archive for Microsoft Teams enables organisations to protect, discover, investigate, and recover data from internal and external threats that challenge cloud messaging and collaboration platforms today. |

Mimecast's
Credentials



For more information about the Mimecast Security Management Service, please contact sales@6dg.co.uk or call 0800 012 8060.