G-Cloud 15
Service Definition
for
Mimecast Protection Cloud Gateway

Delivering IT for future-thinking organisations

enquiries@quadris.com | 0161 537 4980 |www.quadris.com

1 Service Overview

Mimecast Protection Cloud Gateway is a cloud-delivered secure email gateway (SEG) service that provides advanced, AI-driven protection against email-borne threats, business email compromise (BEC), impersonation attacks, malware, ransomware, and phishing.

The service operates as a supplemental or replacement email security layer for Microsoft 365, Exchange, Google Workspace, and hybrid environments, protecting inbound, outbound, and internal email traffic. Mimecast Protection Cloud Gateway supports UK public sector security, resilience, and compliance requirements by reducing the risk of email-based attacks while maintaining continuity of service.

Mimecast Protection Cloud Gateway is delivered as a SaaS solution hosted within Mimecast's globally distributed cloud infrastructure and is managed through a single administrative console.

2 Service Scope

Mimecast Protection Cloud Gateway provides:

- Secure Email Gateway (SEG) with advanced threat protection
- AI-driven detection of phishing, impersonation, and BEC attacks
- Internal email protection to reduce lateral threat movement
- Optional continuity and resilience features (plan dependent)
- Optional browser isolation, collaboration protection, and data recovery (plan dependent)
- Integration with Microsoft 365, Exchange, and Google Workspace

3 Service Editions

Mimecast Protection Cloud Gateway is available in three editions:

- **Critical Protection Cloud Gateway**
- **Advanced Protection Cloud Gateway**
- **Premium Protection Cloud Gateway**

Each edition builds on the previous tier, enabling buyers to select the level of protection appropriate to their risk profile and operational requirements.

4 Core Functional Capabilities

4.1 Email Security (SEG + Targeted Threat Protection)

All editions provide core secure email gateway functionality to detect and block malicious emails before delivery, using signature-based, heuristic, and AI-driven threat detection. This protects against phishing, ransomware, malware, and known and emerging email threats.

4.2 Internal Email Protect

Internal Email Protect extends threat detection to internal and outbound email traffic, reducing the risk of compromised accounts being used to attack internal users or supply chain partners. Automated remediation enables rapid response without complex manual intervention.

4.3 Advanced Business Email Compromise (BEC)

Advanced BEC protection uses behavioural analysis and machine learning to identify sophisticated impersonation attacks, including CEO fraud, invoice fraud, and domain spoofing that may bypass traditional controls.

5 Advanced and Premium Capabilities (Edition Dependent)

5.1 Browser Isolation (Advanced & Premium)

Integrated, browser-agnostic isolation technology provides 100% protection against advanced web threats delivered via email links, ensuring malicious content cannot execute on user devices.

5.2 Sync & Recover (Advanced & Premium)

Provides rapid recovery of email data from a secure, independent source, supporting resilience against data loss, corruption, or accidental deletion.

5.3 Email Continuity (Advanced & Premium)

Maintains access to email services during Microsoft 365 or Exchange outages, ensuring operational continuity for critical communications.

5.4 Collaboration Threat Protection (Premium)

Protects Microsoft OneDrive, SharePoint, and Teams against malicious file sharing and collaboration-based threats. This capability requires appropriate Microsoft 365 licensing.

5.5 Content Security (Advanced & Premium)

Includes secure messaging, large file send, and privacy controls to protect sensitive data and support compliance with data protection obligations.

6 Feature Comparison by Edition

Capability	Critical	Advanced	Premium
Secure Email Gateway (SEG + TTP)	✓	✓	✓
Internal Email Protect	✓	✓	✓
Advanced BEC Protection	✓	✓	✓
Browser Isolation	–	✓	✓
Sync & Recover	–	✓	✓
Email Continuity	–	✓	✓
Collaboration Threat Protection	–	–	✓
Content Security	–	✓	✓

(Recommended add-ons available across all editions include DMARC Analyzer, Incydr, Engage, Archive, and Aware).

7 Service Delivery Model

Mimecast Protection Cloud Gateway is delivered as a fully cloud-hosted service. No on-premises infrastructure is required. The service integrates directly with existing email platforms using standard connectors and DNS configuration.

8 Security and Compliance

- Designed to support UK public sector security requirements
- Protects email as the primary threat vector
- Supports data protection and compliance through encryption, retention, and secure messaging (edition dependent)
- Operates across cloud, on-premises, and hybrid environments

9 Onboarding and Implementation

Quadris supports onboarding through:

- Initial service design and configuration
- Secure integration with the buyer's email platform
- Policy alignment with organisational security requirements
- Administrator training (service model dependent)

10 Quadris Support Model

Quadris offers two support models for Mimecast Protection Cloud Gateway to meet differing buyer requirements.

10.1.1 Option 1: Assisted (Named Administrator) Support

Service Description
Designed for organisations that wish to operate Mimecast Protection Cloud Gateway themselves, with structured assistance from Quadris.

Inclusions

- Initial configuration support
- Administrator training
- Named Quadris security contact
- Best-practice policy guidance
- Escalation support for complex issues

Buyer Responsibilities

- Day-to-day administration
- Policy management and tuning
- Incident response actions
- User management

10.1.2 Option 2: Fully Managed Service

Service Description
Quadris operates Mimecast Protection Cloud Gateway on behalf of the buyer as a fully managed security service.

Inclusions

- Full service configuration and optimisation
- Ongoing monitoring and tuning
- Incident investigation and response
- Threat remediation
- Regular service reporting
- Vendor liaison with Mimecast

Buyer Responsibilities

- Provide business context and risk priorities
- Approve policy changes where required
- Act on business-impact decisions

10.1.3 Quadris Support Responsibility Matrix

Activity	Assisted Support	Fully Managed
Initial Configuration	R (Quadris) / A (Buyer)	A (Quadris)
Policy Management	A (Buyer)	A (Quadris)
Threat Monitoring	A (Buyer)	A (Quadris)
Incident Response	A (Buyer)	A (Quadris)
Platform Optimisation	C (Quadris)	A (Quadris)
Vendor Escalation	C (Quadris)	A (Quadris)
Reporting	C (Quadris)	A (Quadris)

(R = Responsible, A = Accountable, C = Consulted)

11 Service Management

Quadris delivers service management aligned with CCS guidance, including:

- Defined escalation routes
- Named contacts (where applicable)
- Regular service reviews (managed service)
- Clear exit and transition support

12 Exit Management

Quadris supports structured exit management, including:

- Configuration handover
- Documentation transfer
- Support for migration to alternative solutions
- Secure removal of administrative access

13 Pricing and Commercials

Pricing is subscription-based and dependent on:

- Selected Mimecast edition
- Number of users
- Selected Quadris support model

Pricing is published separately on the Digital Marketplace.

14 Summary

Mimecast Protection Cloud Gateway provides a scalable, resilient, and highly effective email security service suitable for UK public sector organisations. Combined with Quadris' assisted or fully managed support models, buyers can select an operational approach that aligns with internal capability while maintaining strong protection against the most prevalent cyber threat vector.