G-Cloud 15
Service Definition
for
Mimecast Engage

Delivering IT for future-thinking organisations

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

1 Service Description

1.1.1 What the Service Does

Mimecast Engage provides a human-centric approach to security awareness by continuously analysing user behaviour and risk signals across the Mimecast ecosystem. It identifies high-risk individuals and behaviours, then delivers targeted interventions at the point of risk.

Key capabilities include:

- Centralised human risk scoring across the organisation
- Individual employee risk profiles based on real and simulated phishing data and training outcomes
- Automated behavioural nudges and micro-learning interventions
- A comprehensive, compliance-aligned security awareness training library
- Phishing simulation to test and improve organisational resilience
- Automation to simplify programme administration and reporting

This approach enables security teams to focus on genuine risk reduction rather than generic training completion metrics.

1.1.2 Intended Outcomes

- Reduced likelihood of successful phishing and social engineering attacks
- Improved visibility of human risk across the organisation
- Measurable behaviour change aligned to real-world threats
- Increased efficiency in managing security awareness programmes
- Ongoing compliance with recognised security and data protection standards

2 Service Features and Capabilities

2.1.1 Human Risk Dashboard

- Organisation-wide human risk scoring
- Identification of the highest-risk employees
- Visibility of inbound phishing attack frequency (Attack Factor)

2.1.2 Individual Risk Profiles

- Per-user risk scoring based on real phishing events, simulations and training activity
- Visibility of individual attack exposure relative to the wider organisation
- Record of actions taken in response to risky behaviours

2.1.3 Behavioural Nudges

- Automated, just-in-time feedback triggered by real security events
- Short, engaging micro-learning modules (20–40 seconds)
- Reinforcement of positive behaviours and correction of risky actions

2.1.4 Security Awareness Training

- Library of 140+ TV-style, humour-led micro-learning modules
- Coverage of key topics including phishing, social engineering, impersonation, data protection and privacy
- Content designed to maximise engagement while remaining informative

2.1.5 Phishing Simulation

- Extensive library of realistic phishing templates
- Measurement of organisational susceptibility to email-based threats
- Insight into trends and improvement over time

2.1.6 Rapid Deployment and Automation

- Interactive first-time setup enabling deployment in minutes
- Highly automated 12-month programme administration
- Ability to scale administration effort up or down as required

3 Compliance and Standards

Mimecast Engage supports alignment with recognised industry and regulatory standards, including:

- ISO 27001
- NIST Cybersecurity Framework
- PCI DSS
- GDPR
- HIPAA (where applicable)

The service enables organisations to evidence ongoing security awareness activity and continuous improvement, supporting audit and assurance requirements.

4 Service Scope

4.1.1 Included

- Cloud-hosted Mimecast Engage platform
- Access to human risk dashboards and reporting
- Security awareness training and phishing simulation libraries
- Behavioural nudges and micro-learning content
- Platform updates and feature enhancements

4.1.2 Not Included

- End-user devices or connectivity
- Incident response services beyond awareness and training
- Non-Mimecast third-party system integration (unless agreed separately)

5 Onboarding and Implementation

Mimecast Engage is delivered as a SaaS service and requires no on-premise infrastructure. Initial onboarding includes:

- Tenant provisioning
- Initial configuration and policy setup
- Integration with the Mimecast ecosystem
- Optional administrator training and knowledge transfer

Typical deployment can be completed within days, subject to organisational readiness and data availability.

6 Service Management

The service is managed via a secure web-based administration portal. Customers can:

- Monitor organisational and individual risk levels
- Configure training campaigns and phishing simulations
- Review reports and compliance metrics
- Adjust automation and intervention thresholds

7 Security and Data Protection

Mimecast Engage is hosted in secure, resilient cloud environments and operates in accordance with Mimecast's security and data protection controls. Data is processed solely for the purpose of delivering the service and supporting human risk reduction.

8 Quadris Support Model

Quadris offers two support options to complement Mimecast Engage, enabling organisations to choose between self-management with expert assistance or a fully managed service.

8.1.1 Option 1: Quadris Assisted (Named Administrator Support)

This option is designed for organisations that wish to operate Mimecast Engage themselves, with access to expert support from Quadris.

Service Description

- Initial administrator training and onboarding support
- Named Quadris security consultant
- Guidance on configuration, risk interpretation and programme optimisation
- Best-practice advice aligned to public sector requirements

Buyer Responsibilities

- Day-to-day platform administration
- Campaign and policy configuration
- Review and action of reports and insights

8.1.2 Option 2: Quadris Fully Managed Mimecast Engage

This option is suited to organisations that want Quadris to operate Mimecast Engage on their behalf.

Service Description

- Full platform configuration and ongoing administration
- Continuous monitoring of human risk metrics
- Management of training campaigns and phishing simulations
- Regular reporting and service reviews
- Recommendations to improve security posture and reduce risk

Buyer Responsibilities

- Provide organisational context and objectives
- Review reports and recommendations
- Act on wider organisational change as required

8.1.3 Quadris Support Model Comparison

Activity	Quadris Assisted (Named Admin Support)	Quadris Fully Managed
Service onboarding and initial setup	**Buyer (R)** / Quadris (R)	**Quadris (R)** / Buyer (C)
Platform configuration and tuning	**Buyer (A)** / Quadris (C)	**Quadris (R/A)**
Policy and rule configuration	**Buyer (R)** / Quadris (C)	**Quadris (A)** / Buyer (C)
Day-to-day service administration	**Buyer (R)** / Quadris (C)	**Quadris (A)**
Monitoring dashboards and alerts	**Buyer (R)** / Quadris (C)	**Quadris (A)**
Investigation of risk events	**Buyer (R)** / Quadris (C)	**Quadris (A)**
User risk scoring and prioritisation	**Buyer (R)** / Quadris (C)	**Quadris (A)**
Training and awareness campaign management	**Buyer (R)** / Quadris (C)	**Quadris (A)**
Phishing simulation management	**Buyer (R)** / Quadris (C)	**Quadris (A)**
Behavioural nudge configuration	**Buyer (R)** / Quadris (C)	**Quadris (A)**
Reporting and compliance evidence	**Buyer (R)** / Quadris (R)	**Quadris (R)** / Buyer (C)
Service optimisation and recommendations	Buyer (C) / **Quadris (R)**	**Quadris (R)**
Incident escalation and coordination	Buyer (C) / **Quadris (R)**	**Quadris (R)**
Service review and roadmap planning	Buyer (C) / **Quadris (R)**	**Quadris (R)**

Key: R = Responsible, A = Accountable, C = Consulted

9 Exit Management

Quadris will support an orderly exit at the end of the contract term. This includes:

- Knowledge transfer to the buyer or a replacement supplier
- Export of relevant configuration and reporting data (subject to Mimecast capabilities)
- Support during transition to minimise service disruption

10 Pricing

Pricing is provided on a per-user subscription basis and varies depending on the selected support model (Assisted or Fully Managed). All pricing will be published transparently on the Digital Marketplace.

11 Service Constraints

- Requires integration with the Mimecast platform
- Effectiveness depends on availability of behavioural and phishing data
- Internet connectivity required to access the service