G-Cloud 15
Service Definition
for
Mimecast Incydr

Delivering IT for future-thinking organisations

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

1 Service Description

Mimecast Incydr is a cloud-native insider risk and data exfiltration protection service designed to help organisations identify, investigate and respond to data loss caused by employees, whether accidental or malicious. The service provides deep visibility of how sensitive data is accessed, moved and shared across endpoints, cloud services, browsers and email, without relying on complex policy management or disruptive controls.

Incydr enables security teams to prioritise high-risk behaviour, automate proportionate responses and reduce investigation time, while maintaining user productivity and minimising operational overhead.

This service is suitable for public sector organisations seeking to protect sensitive data such as personal data, intellectual property and confidential information from insider-led data exposure.

2 Service Scope

This service provides software-as-a-service (SaaS) access to the Mimecast Incydr platform, including deployment, configuration and operational use of insider risk monitoring and response capabilities.

3 Key Benefits

- Improved visibility of insider-led data exposure across endpoints, cloud services and collaboration tools
- Faster detection and investigation of high-risk data exfiltration events
- Reduced administrative burden through automated risk prioritisation and response
- Protection of sensitive data without disrupting legitimate user productivity
- Support for compliance, governance and internal policy enforcement

4 Core Features

4.1.1 Cloud-native SaaS platform

- Fully cloud-hosted, SaaS delivery model
- Cross-platform support for Windows, macOS and Linux
- Compatible with Microsoft 365 and Google Workspace environments
- Lightweight endpoint agent with minimal performance impact
- Pre-built integrations with SIEM, SOAR, XDR, IAM, HR and ticketing systems

4.1.2 Data exfiltration detection

- Monitoring of file movement across endpoints, cloud storage, browsers and email
- Detection of data transfers to unsanctioned or untrusted destinations

- Visibility of activity involving source code repositories, cloud sync tools, GenAI services and messaging platforms
- Ability to review and validate the contents of exfiltrated files

4.1.3 Risk prioritisation

- Behaviour-based risk scoring using a multi-dimensional risk model
- Prioritisation based on users, data sensitivity and destination risk
- Identification of regulated and custom data types without complex policy configuration

4.1.4 Automated response and controls

- Real-time prevention controls for high-risk activity, including uploads, copy/paste and removable media use
- Integrated micro-training to correct risky behaviour at the point of action
- Built-in case management for investigation, evidence capture and reporting
- No-code workflow automation to integrate response actions with security and identity tools

4.1.5 Reporting and insight

- Actionable dashboards highlighting data exposure trends and insider risk
- Reporting suitable for security, HR, legal and senior stakeholders
- Historical activity analysis to support investigations involving leavers or policy breaches

5 Service Constraints and Assumptions

- Internet connectivity is required for service operation
- Endpoint agent deployment is required for full visibility
- Buyer is responsible for defining internal data handling policies and acceptable use standards

6 Security and Compliance

- SaaS platform hosted within Mimecast's secure cloud infrastructure
- Role-based access control for administrative functions
- Audit logging and evidential reporting to support investigations and compliance

7 Onboarding and Implementation

Typical onboarding includes:

- Initial service setup and tenant configuration
- Endpoint agent deployment guidance
- Integration with identity, HR and security tooling
- Baseline risk configuration and dashboard setup

8 Service levels

Service availability is provided in line with Mimecast's standard SaaS service levels.

9 Pricing Model

Pricing is typically based on the number of protected users and the selected support model. Licensing and support costs are provided separately on the Digital Marketplace.

10 Quadris Support Model

Quadris offers two support options to complement the Mimecast Incydr service.

10.1.1 Option 1: Assisted (Buyer-managed)

Quadris provides onboarding support, training and named administrator assistance, enabling the buyer to operate Incydr independently with expert guidance.

Inclusions:

- Initial service onboarding and configuration support
- Administrator training and knowledge transfer
- Named technical contact for operational queries
- Best-practice guidance for policy tuning and investigations

Buyer responsibilities:

- Day-to-day operation and monitoring
- Incident investigation and response actions
- User communications and internal policy enforcement

10.1.2Option 2: Fully managed service

Quadris operates Mimecast Incydr on behalf of the buyer, providing continuous monitoring, investigation and response management.

Inclusions:

- Full service configuration and optimisation
- Ongoing monitoring of insider risk events
- Investigation and prioritisation of incidents
- Managed response workflows and reporting
- Regular service reviews and optimisation

Buyer responsibilities:

- Strategic oversight and policy approval

- HR and legal engagement where required

10.1.3 Support responsibility (RACI) comparison

Activity	Assisted (Buyer-managed)	Fully managed
Platform configuration	R (Quadris) / A (Buyer)	R/A (Quadris)
Day-to-day monitoring	R/A (Buyer)	R/A (Quadris)
Incident investigation	R/A (Buyer)	R/A (Quadris)
Response actions	R/A (Buyer)	R/A (Quadris)
Reporting	R (Quadris) / A (Buyer)	R/A (Quadris)
Policy definition	R/A (Buyer)	R/A (Buyer)

11 Exit management

On service termination, Quadris will support:

- Secure export of reports and investigation records
- Removal of administrator access
- Guidance on agent decommissioning
- Knowledge transfer to support service transition

12 Service compatibility

This service aligns with G-Cloud Lot 2b requirements for cloud software services.