G-Cloud 15 Lot2a Service Definition for Managed EDR Powered by CrowdStrike Falcon X

Delivering IT for future-thinking organisations

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

1 Introduction

Managed Endpoint Detection and Response (EDR) powered by CrowdStrike Falcon is a cloud-native security service designed to detect, investigate and respond to advanced threats across endpoint environments. The service combines the CrowdStrike Falcon EDR platform with Quadris-delivered management, threat hunting, and operational support.

The service provides continuous endpoint telemetry, behavioural detection, and human-led analysis to identify malicious activity that may bypass traditional security controls. It is suitable for UK public sector organisations requiring enhanced endpoint visibility, rapid threat detection, and expert response guidance.

2 Service Scope

The service delivers endpoint detection, investigation, and response capabilities using the CrowdStrike Falcon cloud platform, augmented by Quadris-managed operational services.

- The scope includes:
- Endpoint threat detection and alerting
- Continuous monitoring of endpoint activity
- Investigation and contextual analysis of security events
- Threat containment and response guidance
- Optional managed threat hunting services

The service operates independently of legacy antivirus and does not rely on signature-based detection.

3 Supported Environments

The service supports endpoints protected by the CrowdStrike Falcon sensor, including:

- Windows
- macOS
- Linux

Coverage extends to on-premises, cloud-hosted, and remote endpoints.

4 Functional Capabilities

4.1 Endpoint Detection and Monitoring

- Continuous monitoring of endpoint activity using behavioural and indicator-of-attack (IOA) techniques

- Detection of malware, ransomware, fileless attacks, credential abuse and lateral movement
- Real-time alerting enriched with contextual telemetry and threat intelligence
- Visibility of attack timelines, impacted assets and indicators

4.2 Threat Investigation

- Centralised investigation console providing detailed detection context
- Attack visualisation and process tree analysis
- Mapping of detections to the MITRE ATT&CK® framework
- Retention of detection and investigation data to support analysis and audit

5 Managed Threat Hunting (Optional)

Quadris provides an optional managed threat hunting capability delivered by experienced security analysts. This service delivers continuous, proactive analysis to identify stealthy or novel attacker behaviour that may not trigger automated detections.

Threat hunting activities use CrowdStrike telemetry and threat intelligence to:

- Identify anomalous activity
- Investigate suspected adversary behaviour
- Provide contextual threat reports and response advice
- This capability is delivered as an extension of the buyer's security team.

6 Reporting and Visibility

- Centralised dashboards providing endpoint security status
- Prioritised alerts with severity classification
- Context-rich threat reports and briefings
- Email notifications for security events
- Audit-friendly reporting to support compliance and assurance activities

7 Service Benefits

- Improved detection of advanced and stealthy endpoint threats
- Reduced time to detect and respond to security incidents
- Centralised visibility across distributed endpoint estates
- Behaviour-based detection that does not rely on signatures
- Expert human analysis to supplement automated detection
- Reduced operational burden on internal IT and security teams
- Support for security assurance and audit activities

8 Service Management

8.1 Management Interface

- Secure, cloud-based management console provided by CrowdStrike Falcon
- Role-based access controls for operational and investigative functions
- Centralised visibility of detections, investigations and response actions

8.2 Monitoring and Oversight

- Continuous monitoring of endpoint alerts
- Analyst review of high-severity detections
- Ongoing tuning and optimisation of detection policies

9 Security

9.1 Data Security

- Endpoint telemetry transmitted securely to the CrowdStrike cloud platform
- Logical separation of customer data within a multi-tenant architecture
- Access to management interfaces protected by authentication and role-based access

9.2 Platform Assurance

- CrowdStrike Falcon is a cloud-native SaaS platform designed for high availability and scale
- Detection logic and threat intelligence updated continuously without customer intervention

10 Onboarding and Implementation

10.1 Onboarding

- Initial service setup and tenant configuration
- Deployment of the CrowdStrike Falcon sensor
- Validation of endpoint connectivity and telemetry
- Configuration of alerting and access controls

Typical onboarding can be completed rapidly due to the lightweight, agent-based architecture.

11 Quadris Support Services

Quadris provides optional support services for Managed Endpoint Detection and Response (EDR) powered by CrowdStrike Falcon to assist organisations in the effective operation, monitoring, and ongoing use of the service. These support services are designed to align with differing public sector operating models, ranging from assisted self-managed operation to a fully managed, Quadris-operated service.

Quadris support services are offered in addition to the CrowdStrike Falcon EDR software subscription.

11.1 Base Support Service – Assisted Self-Managed Operation

The Base Support Service is intended for organisations that wish to retain operational responsibility for endpoint security while receiving structured onboarding, guidance, and access to experienced Quadris security analysts.

Under this model, the buyer performs day-to-day monitoring and response activities within the CrowdStrike Falcon platform, with Quadris providing advisory support, investigation assistance, and escalation guidance where required.

11.2 Inclusions

- Initial service onboarding support, including:
    - Validation of tenant configuration and access
    - Guidance on Falcon sensor deployment
    - Review of detection policies and alerting configuration
- Administrator and analyst guidance covering:
    - Interpretation of EDR alerts and detections
    - Investigation workflows and use of detection context
    - Severity assessment and incident prioritisation
    - Use of dashboards, timelines, and reporting
- Advisory support for:
    - Incident response decision-making
    - Threat containment and remediation planning
    - Security assurance and audit preparation
- Liaison with CrowdStrike technical support where required

11.3 Buyer Responsibilities

- Day-to-day monitoring of EDR alerts and detections
- Investigation and triage of security events

- Authorisation and execution of response actions
- Deployment and maintenance of the Falcon sensor
- Endpoint administration, patching, and configuration
- Compliance with internal security, legal, and governance requirements

11.4 Intended Use

This service is suitable for organisations with in-house IT or security capability that wish to retain control of endpoint security operations while reducing risk through access to expert guidance and escalation support.

11.5 Managed Support Service – Quadris-Operated Service

The Managed Support Service is intended for organisations that require Quadris to operate the EDR service on their behalf. Quadris assumes responsibility for continuous monitoring, investigation, threat hunting, and operational management of the CrowdStrike Falcon EDR platform in accordance with agreed policies and procedures.

The buyer retains overall accountability for risk ownership and remediation decisions but does not perform routine EDR operational tasks.

11.6 Inclusions

- Full service onboarding and configuration
- Ongoing operation of the EDR service, including:
  - Falcon sensor deployment guidance and validation
  - Continuous monitoring of alerts and detections
  - Investigation and contextual analysis of security events
  - Proactive threat hunting using endpoint telemetry
- Incident management support, including:
  - Severity-based incident prioritisation
  - Response and containment recommendations
  - Coordination of escalation for high-severity threats
- Regular reporting, including:
  - Alert and incident summaries
  - Threat activity trends
  - Operational service reporting
- Liaison with CrowdStrike technical support for incident resolution and platform issues
- Support for audits, investigations, and compliance-related requests

11.7 Intended Use

This service is suitable for organisations seeking to reduce operational overhead, where internal security capability or capacity is limited, or where a managed detection and response model is required.

11.8 Buyer Responsibilities

- Quadris support services do not replace the underlying CrowdStrike Falcon EDR subscription
- Quadris does not perform endpoint patching or system administration unless explicitly agreed
- Quadris does not replace the buyer's incident response or business continuity obligations
- All services are delivered remotely unless otherwise agreed

11.9 Service Boundaries and Assumptions

- Quadris support services do not replace the underlying CrowdStrike Falcon EDR subscription
- Quadris does not perform endpoint patching or system administration unless explicitly agreed
- Quadris does not replace the buyer's incident response or business continuity obligations
- All services are delivered remotely unless otherwise agreed

11.10 Support Service Responsibility Matrix (RACI)

Key:
R – Responsible (performs the activity)
A – Accountable (owns the outcome / approval)
C – Consulted (provides guidance or input)
I – Informed (kept informed)

Activity	Base Support Service (Assisted Self-Managed)	Managed Support Service (Quadris-Operated)
Service onboarding and initial configuration	R (Quadris) / A (Buyer)	R (Quadris) / A (Buyer)
Falcon sensor deployment	R (Buyer) / C (Quadris)	R (Buyer) / C (Quadris)
Detection policy configuration	R (Buyer) / C (Quadris)	R (Quadris) / A (Buyer)
Continuous alert monitoring	R (Buyer)	R (Quadris)
Alert triage and investigation	R (Buyer) / C (Quadris)	R (Quadris)

Activity	Base Support Service (Assisted Self-Managed)	Managed Support Service (Quadris-Operated)
Threat hunting activities	I (Buyer)	R (Quadris)
Incident severity classification	R (Buyer) / C (Quadris)	R (Quadris) / A (Buyer)
Response and containment advice	C (Quadris)	R (Quadris)
Execution of response actions	R (Buyer)	R (Buyer)
Reporting and dashboards	R (Buyer)	R (Quadris) / I (Buyer)
Audit and compliance support	C (Quadris)	R (Quadris) / A (Buyer)
Liaison with CrowdStrike support	C (Quadris)	R (Quadris)
Endpoint ownership and administration	A (Buyer)	A (Buyer)

12 Service Constraints and Dependencies

- Requires deployment of the CrowdStrike Falcon endpoint sensor
- Internet connectivity required for telemetry and management access
- The service provides detection and response guidance but does not automatically remediate systems unless explicitly configured
- Endpoint availability and visibility are dependent on sensor health and network connectivity

13 Pricing and Licensing Model

Pricing is subscription-based, typically per endpoint, and includes access to the CrowdStrike Falcon platform. Managed service components are priced according to the level of operational support required.

14 Exit Management

- Endpoint sensors can be removed on service termination
- Access to management consoles is withdrawn
- Historical reports can be exported prior to exit
- Support for planned service exit in line with G-Cloud requirements

15 Intended Users

- Central government departments
- Local authorities
- NHS and healthcare organisations
- Education and research institutions
- Other UK public sector bodies

16 Summary

Managed Endpoint Detection and Response powered by CrowdStrike Falcon provides advanced endpoint threat detection, investigation, and response capabilities supported by expert operational services from Quadris. The service supports improved cyber resilience, faster incident response, and enhanced visibility across endpoint estates, aligning with the expectations of a **G-Cloud 15 Lot 2 Cloud Software service**