G-Cloud 15
Service Definition
for
Cisco Secure Endpoint

Delivering IT for future-thinking organisations

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

1 Service Description

Cisco Secure Endpoint is a cloud-delivered endpoint protection, detection, and response (EDR) service that provides comprehensive security for endpoints across Windows, macOS, Linux, iOS, and Android platforms. The service integrates prevention, detection, threat hunting, and response capabilities into a single lightweight agent, using continuous monitoring and cloud-based analytics to protect against known, unknown, and emerging cyber threats.

The service is designed to help public sector organisations prevent breaches, rapidly detect advanced threats that evade traditional controls, and respond effectively to security incidents. Cisco Secure Endpoint is underpinned by Cisco Talos threat intelligence and integrates with the wider Cisco Security ecosystem to support a defence-in-depth approach aligned to UK Government security principles.

2 Service Scope

This service provides endpoint security capabilities delivered as Software as a Service (SaaS). It includes agent deployment, centralised policy management, continuous monitoring, threat detection, and response tooling. The service can be consumed as a buyer-managed solution with Quadris support, or as a fully managed service operated by Quadris on behalf of the buyer.

3 Service Benefits

- Reduces the risk of malware infection and ransomware outbreaks through layered prevention controls.
- Detects advanced and low-prevalence threats using behavioural analysis and cloud analytics.
- Provides rapid investigation and response capabilities to minimise impact and recovery time.
- Supports remote and hybrid working by protecting endpoints on and off the network.
- Integrates with Cisco Talos threat intelligence for up-to-date protection against emerging threats.

4 Service Features

4.1.1 Prevention

Cisco Secure Endpoint uses multiple preventative technologies to block threats at the earliest possible stage, including:

- Machine learning–based malware detection trained on Cisco Talos telemetry.
- File reputation and antivirus engines for known malware.
- Exploit prevention for memory-based and fileless attacks, including zero-day exploits.

- Behavioural protection to detect malicious use of legitimate tools (living-off-the-land techniques).
- Script protection to reduce the risk of script-based attacks.
- Device control to manage and restrict USB mass storage devices.
- Host-based firewall management for Windows and macOS endpoints.

4.1.2 Detection

Continuous monitoring and analytics are used to identify suspicious activity, including:

- Cloud-based Indicators of Compromise (IoCs) from Cisco Talos.
- Custom host-based IoCs using open standards to support incident response.
- Low-prevalence file detection to surface targeted or advanced threats.
- Vulnerability visibility and risk scoring (available in higher licence tiers) to prioritise remediation.

4.1.3 Threat Hunting

Cisco Secure Endpoint supports proactive threat hunting through:

- Advanced Search capabilities with pre-built and custom queries for investigation and compliance.
- Cisco Talos Threat Hunting (Premier tier), providing analyst-led hunts and detailed attack-chain reporting.

4.1.4 Response and Remediation

The service provides integrated response tools to contain and remediate threats, including:

- Endpoint isolation to prevent lateral movement while maintaining access for remediation.
- File and device trajectory analysis to understand the full scope of an incident.
- Dynamic malware analysis using Cisco Secure Malware Analytics sandboxing.
- Retrospective security to automatically block threats identified after initial compromise.
- Remote scripts (Advantage and Premier tiers) to support containment, eradication, and recovery.

5 Onboarding and Implementation

Quadris supports buyers through a structured onboarding approach that can include:

- Initial service setup and tenant configuration.
- Policy design aligned to organisational risk and user profiles.
- Agent deployment guidance and validation.

- Knowledge transfer to buyer administrators where applicable.

6 Service Management

The service is managed through a centralised web-based console providing dashboards, alerts, and workflow support for investigation and response. APIs are available for integration with third-party systems and security operations tooling.

7 Security and Compliance

Cisco Secure Endpoint is designed to support UK public sector security requirements. Endpoint telemetry is analysed in Cisco's secure cloud environment, with access controls and audit logging available through the management console. The service aligns to common security frameworks, including MITRE ATT&CK for threat mapping and investigation.

8 Service Levels and Editions

Cisco Secure Endpoint is available in multiple licence tiers. Feature availability varies by edition.

Capability	Essentials	Advantage	Premier
Antivirus and file reputation	✓	✓	✓
Machine learning malware detection	✓	✓	✓
Exploit and behavioural protection	✓	✓	✓
Device control and host firewall	✓	✓	✓
Cloud-based IoCs	✓	✓	✓
Low-prevalence threat detection	✓	✓	✓
Advanced Search	✗	✓	✓
Vulnerability visibility and risk scoring	✗	✓	✓
Remote response scripts	✗	✓	✓
Talos Threat Hunting	✗	✗	✓

9 Pricing Model

Pricing is provided on a per-endpoint subscription basis and varies by licence tier and support model. Pricing details are published on the Digital Marketplace.

10 Platform Support

The service supports the following operating systems:

- Microsoft Windows
- Apple macOS
- Linux
- Apple iOS
- Google Android

11 Exit Management

On service termination, Quadris will support the orderly export of configuration and reporting data where applicable and assist with agent removal in line with agreed exit plans.

12 Quadris Support Model

Quadris provides optional support services for Cisco Secure Endpoint to assist organisations in the effective operation, administration, and ongoing use of the service. These support services are designed to meet differing operational models within the public sector, from self-managed environments requiring limited assistance to fully managed services delivered on behalf of the buyer.

Quadris support services are offered in addition to the Cisco Secure Endpoint software subscription.

12.1 Base Support Service – Assisted Self-Managed Operation

12.1.1 Service Description

Under this model, the buyer retains responsibility for operating Cisco Secure Endpoint, with Quadris providing enablement, guidance, and escalation support. This option is suitable for organisations with in-house security or infrastructure teams who wish to manage their own policies and operations, while accessing specialist expertise when required.

12.1.2 Inclusions

- Initial onboarding and configuration support.
- Administrator training and knowledge transfer.
- Named Quadris security consultant.
- Advisory support for policy tuning and best practice.
- Support for incident investigation queries during business hours.

12.1.3 Buyer Responsibilities

- Day-to-day monitoring and alert triage.
- Incident response actions and remediation.
- Ongoing policy management and agent deployment.

12.2 Managed Support Service – Quadris-Operated Service

12.2.1 Service Description

Under this model, Quadris operates Cisco Secure Endpoint as a Service on behalf of the buyer. Quadris assumes responsibility for configuration, monitoring, policy management, and incident response activities, providing a managed security service aligned to public sector operational requirements. This option is suitable for organisations seeking to reduce operational overhead or lacking in-house expertise.

12.2.2 Inclusions

- Full service onboarding and configuration.
- Continuous monitoring of endpoint alerts.
- Threat investigation and prioritisation.
- Incident response and containment actions.
- Regular service reporting and review meetings.
- Liaison with Cisco where vendor escalation is required.

12.2.3 Buyer Responsibilities

- Provide business context and escalation contacts.
- Approve agreed response actions where required.
- Maintain endpoint estate readiness (supported OS, connectivity).

12.3 Service Boundaries and Assumptions

- Quadris support services do not replace the underlying Cisco Secure Endpoint subscription.
- All services are delivered remotely unless otherwise agreed.

12.4 Support Service Responsibility Matrix (RACI)

Activity	Base Support Service (Assisted Self-Managed)	Managed Support Service (Quadris-Operated)
Initial setup	Quadris (R) / Buyer (A)	Quadris (R) / Buyer (A)
Policy configuration	Buyer (R) / Quadris (C)	Quadris (R) / Buyer (A)
Agent deployment	Buyer (R)	Quadris (R)
Alert monitoring	Buyer (R)	Quadris (R)
Incident investigation	Buyer (R) / Quadris (C)	Quadris (R) / Buyer (I)
Containment and response	Buyer (R) / Quadris (C)	Quadris (R) / Buyer (I)
Service reporting	On request	Included

R = Responsible, A = Accountable, C = Consulted, I = Informed