G-Cloud 15
Service Definition
for
Cisco Secure Access

Delivering IT for future-thinking organisations

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

1 Service Description

Cisco Secure Access delivers the core capabilities of Security Service Edge, combining secure internet access and secure private access into a single cloud-native service. It protects users working from offices, homes, or mobile locations as they access SaaS applications, internet resources, and private applications hosted on-premises or in the cloud.

The service is grounded in zero trust principles, enforcing least-privilege access based on identity, device posture, location, and contextual risk signals. All policies are managed centrally through a unified console, providing consistent enforcement and visibility regardless of user location or device type.

Key outcomes include:

- Secure, seamless access for hybrid and remote users
- Reduced attack surface through identity-aware controls
- Simplified operations through platform consolidation
- Improved user productivity with minimal friction

2 Key Capabilities

2.1.1 Zero Trust Network Access (ZTNA)

Provides granular, application-level access to private applications without exposing network infrastructure. Access decisions are enforced per session following authentication and device posture checks, preventing lateral movement and reducing risk.

2.1.2 VPN-as-a-Service (VPNaaS)

Supports legacy and non-web applications that cannot be protected by ZTNA, delivering cloud-based VPN functionality with identity-driven policies and simplified user experience.

2.1.3 Secure Web Gateway (SWG)

Inspects and controls web traffic using full proxy technology, enabling URL filtering, malware protection, sandboxing, TLS inspection, and detailed activity reporting.

2.1.4 Cloud Access Security Broker (CASB)

Provides visibility and control over SaaS application usage, including generative AI services. Enables discovery, risk assessment, and enforcement of acceptable use policies.

2.1.5 Firewall-as-a-Service (FWaaS)

Enforces Layer 3–7 security controls for internet and private application traffic, including intrusion prevention powered by Cisco Talos threat intelligence.

2.1.6 Data Loss Prevention (DLP)

Identifies and protects sensitive information in motion and at rest using predefined and custom data identifiers aligned to regulatory requirements such as GDPR and PCI DSS.

2.1.7 DNS-Layer Security

Blocks access to malicious and inappropriate domains before connections are established, reducing exposure to threats across all devices and locations.

2.1.8 Digital Experience Monitoring (DEM)

Monitors endpoint, network, and application performance to improve user experience and accelerate troubleshooting.

2.1.9 AI Access Controls

Enables safe adoption of generative AI by enforcing usage guardrails, controlling data ingress and egress, and reducing shadow AI risk.

3 Service Features

- Unified Secure Client supporting managed and unmanaged devices
- Client-based and clientless access options
- Centralised policy management and reporting
- Integration with leading identity providers
- Built-in threat intelligence from Cisco Talos
- Optional remote browser isolation
- Multi-organisation support for large or federated environments

4 Service Levels and Resilience

Cisco Secure Access is delivered as a fully cloud-hosted service from Cisco's global security infrastructure. The platform is designed for high availability and scalability, with automated updates applied by Cisco to maintain service performance, security, and feature currency.

5 Security and Compliance

The service supports public sector security and compliance requirements through:

- Zero trust access controls
- Centralised audit logging and reporting
- Data protection and loss prevention capabilities
- Integration with existing security operations tooling

Specific compliance certifications and accreditations depend on the selected Cisco Secure Access package and deployment model.

6 Onboarding and Migration

Cisco Secure Access includes tooling to support migration from legacy VPN solutions and Cisco Umbrella deployments, reducing deployment effort and disruption. Quadris supports onboarding through structured implementation planning and knowledge transfer aligned to buyer requirements.

7 Service Management

The service is managed through a single cloud console, enabling administrators to define and enforce security policies, monitor activity, and investigate incidents. Role-based access controls support secure administration across teams.

8 Support Model – Quadris Services

Quadris offers two support options to complement Cisco Secure Access, enabling buyers to select the level of operational assistance that best fits their internal capability and risk appetite.

8.1.1 Option 1: Assisted (Named Administrator Support)

Designed for organisations that wish to operate Cisco Secure Access internally while receiving expert guidance from Quadris.

Inclusions:

- Initial onboarding and configuration guidance
- Named Quadris security consultant
- Administrator training and enablement

- Best-practice advice for policy design
- Support during change and optimisation activities

Buyer Responsibilities:

- Day-to-day administration and monitoring
- Policy configuration and enforcement
- Incident response and remediation

8.1.2 Option 2: Fully Managed Service

Designed for organisations seeking to outsource day-to-day operation of Cisco Secure Access to Quadris.

Inclusions:

- Full platform configuration and management
- Ongoing policy administration and optimisation
- Monitoring and operational oversight
- Incident investigation and response support
- Regular service reviews and reporting

Buyer Responsibilities:

- Strategic oversight and governance
- Approval of policy changes
- User and access requirements definition

8.1.3 RACI Comparison – Quadris Support Options

The table below summarises responsibility allocation for key service activities across the two Quadris support models.

Service Activity	Assisted (Named Administrator Support)	Fully Managed Service
Service onboarding and initial configuration	R (Quadris) / A (Buyer)	R (Quadris)
Security architecture and policy design	R (Quadris) / A (Buyer)	R (Quadris)
Day-to-day platform administration	R (Buyer)	R (Quadris)
User and device onboarding	R (Buyer)	R (Quadris) / A (Buyer)

Policy changes and optimisation	R (Buyer) / C (Quadris)	R (Quadris)
Monitoring and operational oversight	R (Buyer)	R (Quadris)
Incident investigation and response	R (Buyer) / C (Quadris)	R (Quadris)
Vendor liaison with Cisco	R (Buyer) / C (Quadris)	R (Quadris)
Reporting and service reviews	R (Buyer) / C (Quadris)	R (Quadris)
Knowledge transfer and documentation	R (Quadris) / A (Buyer)	R (Quadris)

R = Responsible, A = Accountable, C = Consulted

9 Exit Management

Quadris supports structured exit management to ensure continuity of service and data protection at contract end. This includes knowledge transfer, configuration handover, and support during transition to an alternative supplier or in-house operation.

10 Pricing Model

Pricing is subscription-based and varies depending on the selected Cisco Secure Access package, user volumes, and Quadris support option. Detailed pricing is provided via the G-Cloud Digital Marketplace.

11 Service Constraints

- Internet connectivity is required to access the service
- Some features depend on endpoint and identity provider compatibility
- Feature availability may vary by Cisco Secure Access package

12 Summary

Cisco Secure Access provides a modern, cloud-delivered approach to secure access for hybrid workforces, consolidating multiple security capabilities into a single platform. Quadris enhances this capability with flexible support options, enabling public sector organisations to adopt zero trust securely and confidently.