G-Cloud 15 Lot2a Service Definition for Fortinet Fortiweb WAF as a Service

Delivering IT for future-thinking organisations

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

1 Introduction

Fortinet Web Application Firewall (WAF) as a Service is a cloud-delivered application security service designed to protect web applications and APIs from common and advanced threats. The service uses Fortinet web application firewall technology combined with Quadris-delivered configuration, management, and operational support.

The service provides protection against application-layer attacks such as SQL injection, cross-site scripting (XSS), bot abuse, and automated exploitation. It is suitable for UK public sector organisations operating internet-facing or cloud-hosted web applications requiring consistent security controls, visibility, and managed operation.

2 Service Scope

The service delivers managed web application firewall capabilities, including:

- Application-layer traffic inspection
- Protection against OWASP Top 10 threats
- Bot mitigation and abuse prevention
- Virtual patching for application vulnerabilities
- Centralised policy management and reporting
- Ongoing monitoring, tuning, and operational support

The service can be delivered for cloud-hosted, on-premises, or hybrid web applications.

3 Supported Environments

- Internet-facing web applications
- Cloud-hosted applications
- Hybrid application environments
- APIs and web services
- Public sector digital services and portals

4 Functional Capabilities

4.1 Web Application Protection

- Inspection of HTTP and HTTPS traffic
- Protection against OWASP Top 10 vulnerabilities
- SQL injection and cross-site scripting (XSS) prevention
- Application-layer intrusion detection and blocking

- Bot detection and mitigation
- Rate limiting and abuse prevention

4.2 Virtual Patching and Threat Mitigation

- Virtual patching to mitigate known application vulnerabilities
- Rapid deployment of updated security rules
- Reduction of exposure while application fixes are developed

4.3 Centralised Management

- Centralised WAF policy management
- Securely hosted management and analytics platforms
- Configuration versioning and backup
- Role-based policy administration

5 Service Features

- Fully managed Fortinet WAF service
- Bespoke WAF policy design and configuration
- Centralised rule and policy management
- Continuous monitoring of application traffic
- Customisable security rules and protections
- Regular review and tuning of WAF policies
- Security event logging and reporting
- Integration with existing network and firewall services

6 Service Benefits

- Improved protection of web applications and APIs
- Reduced risk of application-layer attacks and data breaches
- Centralised visibility across application security controls
- Reduced operational burden through managed service delivery
- Faster response to emerging application threats
- Support for regulatory and security assurance requirements

7 Service Management

7.1 Management Interface

- Secure access to WAF management and reporting platforms
- Centralised service request and change management via the Quadris EyeQ portal
- Role-based access to reports, dashboards, and configuration views

7.2 Monitoring and Oversight

- Continuous monitoring of WAF health and application traffic
- Review of security events and blocked attack attempts
- Proactive identification of false positives and tuning opportunities

8 Security

8.1 Application and Data Security

- Encrypted inspection of HTTPS traffic
- Secure handling of logs and configuration data
- Logical separation of customer environments
- Support for secure application architectures

8.2 Platform Assurance

- Service built on Fortinet WAF technology
- Regular updates to security rules and threat intelligence
- Integration with Fortinet Security Fabric where applicable

9 Onboarding and Implementation

9.1 Onboarding

- Initial assessment of application architecture
- Identification of protected applications and endpoints
- WAF policy design aligned to application behaviour
- Deployment and validation of protections

9.2 Transition

- Testing of security rules and traffic flows

- Controlled move into live enforcement mode
- Handover into managed service operation

10 Quadris Support Services

Quadris provides optional support services for Fortinet Web Application Firewall (WAF) as a Service to assist organisations in the effective operation, management, and ongoing assurance of application-layer security controls. 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 WAF service.

Quadris support services are provided in addition to the underlying Fortinet WAF technology and associated licences.

10.1 Base Support Service – Assisted Self-Managed Operation

The Base Support Service is intended for organisations that wish to retain day-to-day operational responsibility for their Fortinet WAF deployment while receiving structured onboarding, guidance, and access to experienced Quadris security engineers.

Under this model, the buyer performs routine WAF administration and monitoring activities, with Quadris providing advisory support, best-practice guidance, and escalation assistance where required.

10.2 Inclusions

- Initial service onboarding support, including:
  - Validation of WAF deployment and connectivity
  - Review of protected applications, URLs, and APIs
  - Baseline WAF policy and rule-set review
- Administrator guidance covering:
  - WAF rule and policy management
  - OWASP Top 10 protection and tuning
  - Bot mitigation and rate-limiting configuration
  - Log review, alert interpretation, and reporting
- Advisory support for:
  - Reducing false positives and tuning application profiles
  - Virtual patching strategies for application vulnerabilities
  - Audit preparation and security assurance activities
- Liaison with Fortinet technical support where required

10.3 Buyer Responsibilities

- Day-to-day WAF monitoring and administration
- Review and approval of WAF policy changes
- Execution of approved configuration updates
- Ownership and maintenance of protected applications
- Management of TLS certificates where HTTPS inspection is required
- Compliance with internal security, governance, and change management processes

10.4 Intended Use

This service is suitable for organisations with in-house application, security, or DevOps capability that wish to retain operational control while reducing risk through access to expert guidance and structured support.

10.5 Managed Support Service – Quadris-Operated Service

The Managed Support Service is intended for organisations that require Quadris to operate and manage the Fortinet WAF service on their behalf. Quadris assumes responsibility for configuration management, monitoring, tuning, and operational oversight of the WAF environment in accordance with agreed policies and procedures.

The buyer retains accountability for business risk, application ownership, and approval of material security policy changes.

10.6 Inclusions

- Full service onboarding and configuration
- Ongoing management of the WAF service, including:
    - WAF rule and policy management
    - OWASP Top 10 and application-layer threat protection
    - Bot mitigation and abuse prevention tuning
    - Centralised management and reporting
- Operational activities, including:
    - Continuous monitoring of application traffic and security events
    - Proactive identification of false positives and rule optimisation
    - Virtual patching in response to emerging vulnerabilities
- Change and incident support, including:
    - Implementation of approved WAF changes
    - Investigation of suspected application-layer attacks
    - Escalation and coordination with Fortinet technical support

- Regular service reporting and operational summaries
- Support for audits, compliance reviews, and assurance activities

10.7 Intended Use

This service is suitable for organisations seeking to reduce internal operational overhead, where application security expertise is limited, or where a fully managed WAF service is required.

10.8 Buyer Responsibilities

- Defining application security policies and risk appetite
- Approving WAF rule changes and enforcement modes
- Maintaining ownership of web applications and APIs
- Remediation of application vulnerabilities
- Ensuring compliance with data protection and regulatory obligations

10.9 Service Boundaries and Assumptions

- Quadris support services do not replace the underlying Fortinet WAF licences or platform
- Quadris does not develop, patch, or modify application code
- Quadris does not replace secure application development practices
- All services are delivered remotely unless otherwise agreed

10.10 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)
Application scope definition	R (Buyer) / C (Quadris)	R (Quadris) / A (Buyer)
WAF policy and rule definition	A (Buyer) / C (Quadris)	A (Buyer) / C (Quadris)
WAF rule implementation	R (Buyer)	R (Quadris)

Activity	Base Support Service (Assisted Self-Managed)	Managed Support Service (Quadris-Operated)
Enforcement mode management (monitor/block)	R (Buyer)	R (Quadris) / A (Buyer)
Continuous WAF monitoring	R (Buyer)	R (Quadris)
Security event investigation	R (Buyer) / C (Quadris)	R (Quadris)
False-positive tuning and optimisation	R (Buyer) / C (Quadris)	R (Quadris)
Virtual patching	C (Quadris)	R (Quadris)
Reporting and dashboards	R (Buyer)	R (Quadris) / I (Buyer)
Audit and compliance support	C (Quadris)	R (Quadris) / A (Buyer)
Liaison with Fortinet support	C (Quadris)	R (Quadris)
Application ownership and remediation	A (Buyer)	A (Buyer)
TLS certificate management	A (Buyer)	A (Buyer)

11 Service Constraints and Dependencies

- Requires supported Fortinet WAF deployment model
- HTTPS inspection requires certificate management
- Effectiveness depends on accurate application profiling
- The service does not replace secure application development practices

12 Pricing and Licensing Model

Pricing is subscription-based and typically includes:

- Managed WAF service fees
- Fortinet WAF licensing
- Optional support tiers

Pricing is determined by the number of protected applications and traffic volumes.

13 Exit Management

- WAF configurations and rules can be exported on service termination
- Managed services are withdrawn in a controlled manner
- Support for planned service exit in line with G-Cloud requirements

14 Intended Users

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

15 Summary

Fortinet Web Application Firewall as a Service provides managed, application-layer protection for public-facing and cloud-hosted applications. Delivered using Fortinet technology and Quadris operational expertise, the service reduces application risk while supporting secure, resilient digital services aligned with G-Cloud 15 expectations.