G-Cloud 15
Service Definition
for
Barracuda WAF As a Service

Delivering IT for future-thinking organisations

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

1 Service Description

Barracuda Web Application Firewall (WAF) as a Service provides comprehensive protection for web applications and APIs against common, advanced, and emerging threats. The service uses machine-learning-backed threat detection, behavioural analysis, and automated policy enforcement to protect against OWASP Top 10 web and API risks, DDoS attacks, bot abuse, and zero-day exploits.

The service is delivered from Barracuda's globally distributed cloud platform, operating across multiple points of presence to provide resilience, scalability, and low-latency protection for internet-accessible services.

2 Service Scope

The service provides north-south and, where required, east-west application traffic protection for HTTP and HTTPS-based services. It supports applications hosted in public cloud, private cloud, hybrid, and on-premises environments.

3 Service Features

- Protection against OWASP Top 10 web and API security risks
- Zero-day threat protection using machine learning-backed active threat intelligence
- Full-spectrum DDoS protection for volumetric and application-layer attacks
- Advanced bot protection, including credential stuffing and automated abuse prevention
- API security for JSON and GraphQL APIs, including schema-based and ML-driven discovery
- TLS/SSL inspection and secure application delivery controls
- Centralised management, logging, and reporting
- API-first configuration supporting DevSecOps and automation
- High availability through a globally distributed cloud architecture

4 Service Benefits

- Reduces the likelihood and impact of cyber attacks on public-facing services
- Removes the requirement for on-premises security appliances
- Enables rapid onboarding and protection of new applications
- Automatically scales to meet demand and attack conditions
- Supports compliance with public sector security and assurance requirements

5 Service Delivery Model

The service is delivered as a subscription-based, cloud-hosted solution. Application traffic is routed through the Barracuda WAF cloud platform using DNS-based redirection or reverse proxy configuration. Security inspection and enforcement are applied before traffic reaches the protected application.

6 Onboarding and Implementation

Quadris provides structured onboarding support, including:

- Initial service provisioning
- Application discovery and traffic profiling
- Policy configuration and tuning
- Validation and transition to live service

7 Service Management

The service includes access to a secure management portal providing near real-time visibility of traffic, security events, and policy enforcement. Logging and reporting can be integrated with third-party SIEM, SOAR, or XDR platforms.

8 Security and Compliance

The service supports alignment with public sector security requirements, including the NCSC Cloud Security Principles. Security updates, threat intelligence, and signature updates are applied automatically by the platform.

9 Service Levels

Service availability, support response times, and service credits (where applicable) are defined contractually and aligned to Digital Marketplace requirements.

10 Pricing Model

Pricing is subscription-based and is determined by the number of protected applications, traffic volumes, and selected service options. Pricing is published via the Digital Marketplace.

11 Dependencies

- Internet connectivity between end users and protected applications
- DNS or network configuration to route traffic via the service

12 Exit Management

On service termination, traffic routing can be reverted to the buyer's original configuration. Configuration data can be exported where supported, supporting orderly service exit and transition.

On service termination, traffic routing can be reverted to the buyer's original configuration. Configuration data can be exported where supported by the platform.

13 Quadris Support Model

Quadris provides optional support services for Barracuda WAF 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 Barracuda WAF software subscription.

13.1 Base Support Service – Assisted Self-Managed Operation

13.1.1 Service Description

Under this model, the buyer retains responsibility for operating Barracuda WAF as a Service, 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 WAF policies and operations, while accessing specialist expertise when required.

13.1.2 Inclusions

- Initial onboarding support and service provisioning
- Administrator training covering core WAF functionality and best practice
- Named Quadris technical contact
- Configuration guidance and design advice
- Support with initial policy setup and tuning
- Escalation support for complex configuration or security issues
- Best-practice advice aligned to public sector security requirements

13.1.3 Buyer Responsibilities

- Day-to-day operation of the WAF service
- Ongoing policy management and tuning
- Monitoring alerts and security events
- Responding to incidents affecting buyer applications
- Managing application changes and notifying Quadris where guidance is required
- Ensuring appropriate internal processes for security monitoring and response

13.2 Managed Support Service – Quadris-Operated Service

13.2.1 Service Description

Under this model, Quadris operates Barracuda WAF 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 WAF expertise.

13.2.2 Inclusions

- Full service onboarding and configuration
- Continuous policy management and optimisation
- Monitoring of security alerts and events
- Incident response coordination related to WAF events
- Change management for protected applications
- Regular service reporting
- Liaison with Barracuda support as required

13.2.3 Buyer Responsibilities

- Ownership and operation of the protected applications
- Providing timely information on application changes
- Making risk and business decisions relating to application availability
- Maintaining internal incident management and escalation processes

13.3 Service Boundaries and Assumptions

- Quadris support services do not replace the underlying Barracuda WAF subscription.
- All services are delivered remotely unless otherwise agreed.

13.4 Support Service Responsibility Matrix (RACI)

Activity	Base Support Service (Assisted Self-Managed)	Managed Support Service (Quadris-Operated)
Service provisioning	Quadris (R) / Buyer (A)	Quadris (R) / Buyer (A)
Initial configuration	Quadris (R) / Buyer (A)	Quadris (R) / Buyer (A)
Administrator training	Included	Not required
Day-to-day WAF management	Buyer (R)	Quadris (R)
Policy tuning and optimisation	Buyer (R) / Quadris (C)	Quadris (R)
Monitoring and alerting	Buyer (R)	Quadris (R)
Incident response	Buyer (R) / Quadris (C)	Quadris (R)
Change management	Buyer (R)	Quadris (R)
Service reporting	On request	Included

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