G-Cloud 15
Service Definition
for
Imperva Application Security

Delivering IT for future-thinking organisations

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

1 Service Description

Imperva Application Security is a comprehensive, integrated Web Application and API Protection (WAAP) platform designed to protect critical applications, APIs, and data from cyber threats while maintaining high availability and performance. Delivered by Quadris under G-Cloud 15 Lot 2a, the service enables public sector organisations to secure modern web, mobile, and API-driven applications deployed in cloud, on-premises, or hybrid environments.

Imperva uses a defence-in-depth architecture combining cloud-based and runtime protections, advanced analytics, and global threat intelligence to reduce cyber risk without disrupting end-user experience. Quadris provides implementation, support, and optional managed services aligned to Crown Commercial Service (CCS) exemplar language and Digital Marketplace requirements.

2 Service Scope

Imperva Application Security protects:

- Web applications (public-facing and internal)
- APIs, including undocumented and shadow APIs
- Mobile application back-ends
- Application infrastructure deployed in cloud, on-premises, or hybrid models

The service inspects and enforces traffic at the edge and within runtime environments, ensuring protection from the user through to the application and data layers.

3 Service Features

- Cloud-based Web Application Firewall (WAF) protecting against OWASP Top 10 threats
- API Security with continuous discovery of public, private, and shadow APIs
- Distributed Denial of Service (DDoS) protection using a global scrubbing network
- Advanced Bot Protection to prevent account takeover, fraud, and scraping
- Runtime Application Self-Protection (RASP) for in-application threat detection
- Client-side protection against skimming and data exfiltration attacks
- Machine-learning driven Attack Analytics to reduce alert fatigue
- Global content delivery and application delivery optimisation (CDN)
- Integrated security policies and signatures maintained by Imperva Research Labs

4 Service Benefits

- Protects critical public-facing applications and APIs from cyber attack
- Maintains service availability and performance during malicious activity
- Reduces operational burden through integrated, vendor-consolidated security

- Improves visibility of application and API risk across hybrid environments
- Supports faster and safer application release cycles
- Helps meet regulatory and compliance obligations (including PCI DSS)

5 Architecture and deployment

Imperva uses a layered security model:

- **Edge protection:** Cloud WAF, DDoS mitigation, bot management, CDN and analytics delivered via Imperva's global Points of Presence (PoPs)
- **Application layer:** On-premises or virtual WAF gateways and RASP agents embedded during development
- **API layer:** Continuous API discovery, classification, and positive security enforcement
- **Analytics layer:** Centralised security analytics and attack prioritisation

Quadris supports cloud-only, on-premises, and hybrid deployments depending on buyer requirements.

6 Onboarding and Implementation

Quadris follows a structured onboarding approach:

- Discovery and requirements validation
- Architecture and deployment design
- Configuration and policy setup
- Testing and go-live support

7 Service Management

Quadris provides onboarding, configuration, and operational support aligned to buyer requirements. Service management activities include:

- Initial service setup and onboarding
- Policy configuration and tuning
- Incident support and escalation
- Change management and service reviews

8 Security and compliance

- Protection against OWASP Top 10 and OWASP API Top 10 threats
- Client-side attack mitigation to protect personal and payment data
- Always-on DDoS protection with near-zero latency
- Continuous signature and policy updates from Imperva threat intelligence
- Supports compliance with PCI DSS and related security standards

9 Service Levels and Support

Support is provided during UK business hours with options for enhanced and managed support depending on the chosen Quadris support model. Incident response and escalation procedures are agreed during onboarding.

10 Pricing Model

Pricing is subscription-based and dependent on deployment model, protected assets, and chosen support option. Pricing is published on the Digital Marketplace.

11 Dependencies

- Internet connectivity is required for cloud-based components
- Some features depend on Imperva licensing tiers

12 Exit Management

Quadris supports service exit in line with CCS guidance. Exit assistance includes:

- Knowledge transfer and documentation
- Configuration export where supported by Imperva
- Support during transition to a replacement service

13 Quadris Support Model

Quadris provides optional support services for Imperva Application Security 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 Imperva Application Security 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 Imperva Application Security, 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 security policies and operations, while accessing specialist expertise when required.

13.1.2 Includes

- Initial onboarding and configuration support
- Named administrator support
- Knowledge transfer and operational training
- Best-practice guidance and policy review

13.1.3 Buyer responsibilities

- Day-to-day operation and monitoring
- Policy management and tuning
- Incident response and remediation

13.2 Managed Support Service – Quadris-Operated Service

13.2.1 Service Description

Under this model, Quadris operates Imperva Application Security 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 security expertise.

13.2.2 Includes

- Full platform operation and monitoring
- Policy management and continuous tuning
- Incident investigation and response
- Regular service reporting and optimisation

13.2.3 Buyer responsibilities

- Defining security requirements and risk appetite
- Approving major policy or architectural changes
- Ownership and operation of the protected applications

13.3 Service Boundaries and Assumptions

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

13.4 Support Service Responsibility Matrix

Activity	Base Support Service (Assisted Self-Managed)	Managed Support Service (Quadris-Operated)
Platform operation	Buyer	Quadris
Policy configuration	Buyer (with guidance)	Quadris
Monitoring & alerting	Buyer	Quadris
Incident response	Buyer	Quadris
Training & knowledge transfer	Quadris	Included
Service reporting	Optional	Included