G-Cloud 15
Service Definition
for
Imperva Cloud Data Security

Delivering IT for future-thinking organisations

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

1 Service Description

Imperva Cloud Data Security is a cloud-delivered data security service designed to provide visibility, monitoring, and protection for sensitive data stored in public cloud Database-as-a-Service (DBaaS) environments. The service enables organisations to securely adopt cloud databases by identifying where sensitive data resides, monitoring access and activity, and supporting compliance with data protection regulations.

The service is delivered as a SaaS solution and integrates with leading public cloud platforms to provide near real-time insight into cloud-hosted data assets, reducing the risk of accidental or malicious data exposure.

2 Service Scope

Imperva Cloud Data Security supports organisations migrating data workloads to the cloud or operating hybrid environments by delivering:

- Automated discovery and inventory of cloud database assets
- Classification of sensitive data across DBaaS platforms
- Continuous monitoring of database activity and access
- Detection of anomalous or risky user behaviour
- Centralised dashboards and reporting
- Pre-configured security alerts and audit reporting

The service is suitable for production, development, and test environments and supports secure DevOps and digital transformation initiatives.

3 Service Features

- **Automated Database Discovery**
  Rapid onboarding with automated identification of cloud database assets.
- **Sensitive Data Classification**
  Identification and classification of regulated and business-critical data.
- **Activity Monitoring and Analytics**
  Continuous monitoring of database access and activity with anomaly detection.
- **Centralised Visibility**
  Unified dashboard providing discovery results, classification insights, and alerts.
- **Compliance Enablement**
  Built-in reporting and alerting to support regulatory requirements such as GDPR, PCI DSS, and HIPAA.
- **Cloud-Native Delivery**
  Delivered as a SaaS service with minimal infrastructure overhead.

4 Service Benefits

- Improves visibility and control over cloud-hosted data
- Reduces the risk of data breaches and unauthorised access
- Supports secure cloud migration and DBaaS adoption
- Enables compliance with data protection regulations
- Provides actionable insights for security and risk teams

5 Supported Environments

Imperva Cloud Data Security is designed for public cloud environments and Database-as-a-Service platforms, supporting organisations operating cloud-first or hybrid data architectures.

6 Onboarding and Implementation

Initial onboarding includes:

- Tenant configuration and access setup
- Integration with supported cloud platforms
- Initial database discovery and data classification
- Baseline policy and alert configuration

Onboarding complexity depends on the number of cloud environments and data sources.

7 Security and Compliance

Imperva Cloud Data Security supports organisations in meeting regulatory and governance obligations by maintaining a consistent inventory and audit trail of cloud data assets and access activity. The service supports compliance initiatives including GDPR, PCI DSS, and HIPAA through monitoring, reporting, and visibility capabilities.

8 Service Levels and Availability

The Imperva Cloud Data Security platform is delivered as a highly available SaaS service. Platform availability, resilience, and maintenance are provided by Imperva as the software vendor.

Quadris support services (described below) operate during UK business hours unless otherwise agreed.

9 Pricing Model

Pricing is based on the Imperva Cloud Data Security subscription and the selected Quadris support option. Detailed pricing is published in the Digital Marketplace pricing document.

10 Dependencies

- The service relies on supported cloud providers and DBaaS platforms
- Internet connectivity is required
- Buyer must maintain appropriate cloud access permissions

11 Exit Management

Quadris supports structured exit management, including:

- Knowledge transfer and documentation
- Configuration handover
- Support for transition to buyer-managed or alternative suppliers

Data remains under the buyer's ownership at all times.

12 Quadris Support Model

Quadris provides optional support services for Imperva Cloud Data 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 Cloud Data Security 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 Imperva Cloud Data 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.

12.1.2 Inclusions

- Initial enablement and configuration support
- Administrator training and knowledge transfer
- Named Quadris technical contact
- Configuration guidance and best-practice advice
- Support for policy tuning and reporting setup

12.1.3 Buyer Responsibilities

- Day-to-day operation of the Imperva platform
- Alert review and response
- Policy management and change control
- Compliance reporting and internal governance

12.2 Managed Support Service – Quadris-Operated Service

12.2.1 Service Description

Under this model, Quadris operates Imperva Cloud Data Security 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.

12.2.2Inclusions

- Full platform configuration and management
- Continuous monitoring of alerts and activity
- Policy tuning and optimisation
- Incident investigation support
- Regular reporting and service reviews

12.2.3 Buyer Responsibilities

- Provisioning of cloud access and approvals
- Defining business and compliance requirements
- Acting on escalated incidents and risk decisions

12.3 Service Boundaries and Assumptions

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

12.4 Support Service Responsibility Matrix

Activity	Base Support Service (Assisted Self-Managed)	Managed Support Service (Quadris-Operated)
Platform Configuration	Buyer	Quadris
Data Discovery & Classification	Buyer	Quadris
Alert Monitoring	Buyer	Quadris
Policy Tuning	Buyer (with guidance)	Quadris
Incident Investigation	Buyer	Quadris
Compliance Reporting	Buyer	Quadris
Platform Access Management	Buyer	Buyer