Quorum Cyber

Service Description Purview Data Security Deployment Services G Cloud 15

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Table of Contents

Service Overview

Background

Organisations face increasing risk from insider threats, accidental data leakage, and misuse of sensitive information across on premises, cloud, endpoint, and collaboration platforms. Traditional perimeter-based controls lack the context required to understand user behaviour, intent, and risk, leading to blind spots, alert fatigue, and delayed response. At the same time, regulatory pressures (GDPR, PII, financial data protection) demand stronger visibility, evidence, and governance over how data is accessed, shared, and communicated internally. The biggest challenge is that the tools available to organisations to assist with these problems require skills that are difficult to obtain, and require many years of experience to deploy quickly and effectively.

Quorum Cyber's Solution

Quorum Cyber delivers Microsoft Purview Data Security Deployment Services to help organisations design, build, and deploy data security configurations that enable effective response to data security challenges. Through the deployment of Purview, we enable organisations to understand, protect, and govern their data across cloud and on-premises environments.

The service combines strategic design, technical implementation, and operational readiness to embed sustainable, contextual data protection capabilities aligned to business, regulatory, and security objectives.

Discovery

We work with stakeholders across security, legal, HR, and data protection to understand your organisation's data landscape, regulatory obligations, and insider risk exposure. This phase identifies sensitive data types, key risk scenarios, and critical business processes to ensure the solution is aligned to operational and compliance requirements.

Where required, we also assess existing operating models and maturity across data protection, investigations, and governance functions to inform the overall service design.

Design

Using the outputs from discovery, we design tailored Microsoft Purview configuration aligned to your organisational context. This can include defining escalation paths, investigation workflows, evidence requirements, and role-based perspectives to ensure risk is assessed and managed appropriately across the business.

We help define Sensitivity Labels, classification schemes, and governance structures, providing the frameworks and guidance required to deploy, operate, and maintain these controls within your unique environment. This phase may also include the design of Target Operating Models for capabilities such as Insider Risk Management, DLP, and eDiscovery.

Build

We configure and tune Microsoft Purview data security technologies to support the designed use cases. This can include policy creation, data classification, labelling configuration, monitoring and reporting setup, and the establishment of Standard Operating Procedures (SOPs) to support ongoing operation and maintenance.

Our services cover the full breadth of the Microsoft Purview suite, including:

- Information Protection (classification, labelling, on-demand scanning across cloud and on-premises)
- Data Loss Prevention
- Insider Risk Management

- Communication Compliance
- Information Barriers
- Data Lifecycle Protection and Records Management
- eDiscovery
- Unified Data Governance (Data Catalog)
- Data Security Posture Management
- Compliance Management

Where required, we also design and build supporting capabilities outside of Purview that influence data security outcomes, such as Microsoft 365 Multi-Geo and SharePoint Advanced Management.

Deploy

The solution is deployed into your environment with active monitoring to validate effectiveness and reduce false positives. We work closely with you to establish and tune policy impact before controls become user visible.

Policies are refined using both Quorum Cyber's experience and real-world organisational behaviour, ensuring controls are proportionate, actionable, and aligned to productivity while maximising data security outcomes.

Handover

We deliver a structured handover that includes documented operating models, SOPs, and triage workflows. Customers receive clear reporting and investigation guidance, enabling internal teams to operate the solution confidently.

Where required, the service can transition into Quorum Cyber's managed service, providing ongoing monitoring, optimisation, and expert-led response across DLP and Insider Risk capabilities.

Differentiators

- Complete Purview solution – Design & deployment specialists across all Purview workloads
- Multi-stakeholder lens – configuration guided by legal, HR, DPO, IT and security teams
- Operationalised outcomes – clear workflows, SOPs, and triage models, not just technology deployment
- Contextual risk over raw alerts – combines user behaviour, data sensitivity, and environmental signals into actionable insight
- Microsoft-native expertise – deep integration across Insider Risk, DLP, Defender, Sentinel, and M365
- Managed service extension – seamless integration into Quorum Cyber's Managed Data Security service for ongoing management, monitoring and response

Service Features

- Design, configuration and deployment of Microsoft Purview unstructured data security components
- Tailored DLP policy design (GDPR, PII, financial, custom data types)
- Insider Risk Management policy development and implementation
- Policy tuning and false-positive reduction period
- Unified data risk visibility across on premises, cloud, endpoint, and external signals
- Migration support from third-party DLP platforms (e.g. Symantec)
- Custom dashboards aligned to data security, compliance, and security operations

Service Benefits

- Reduced risk of insider threats, data leakage, and regulatory breaches
- Improved visibility into how sensitive data is accessed and used
- Faster, clearer decision-making on data security issues through contextual evidence
- Lower operational overhead via automation and managed workflows
- Stronger regulatory and compliance posture
- Confidence that data protection controls are effective, tuned, and sustainable
- A clear path from implementation to fully managed protection