

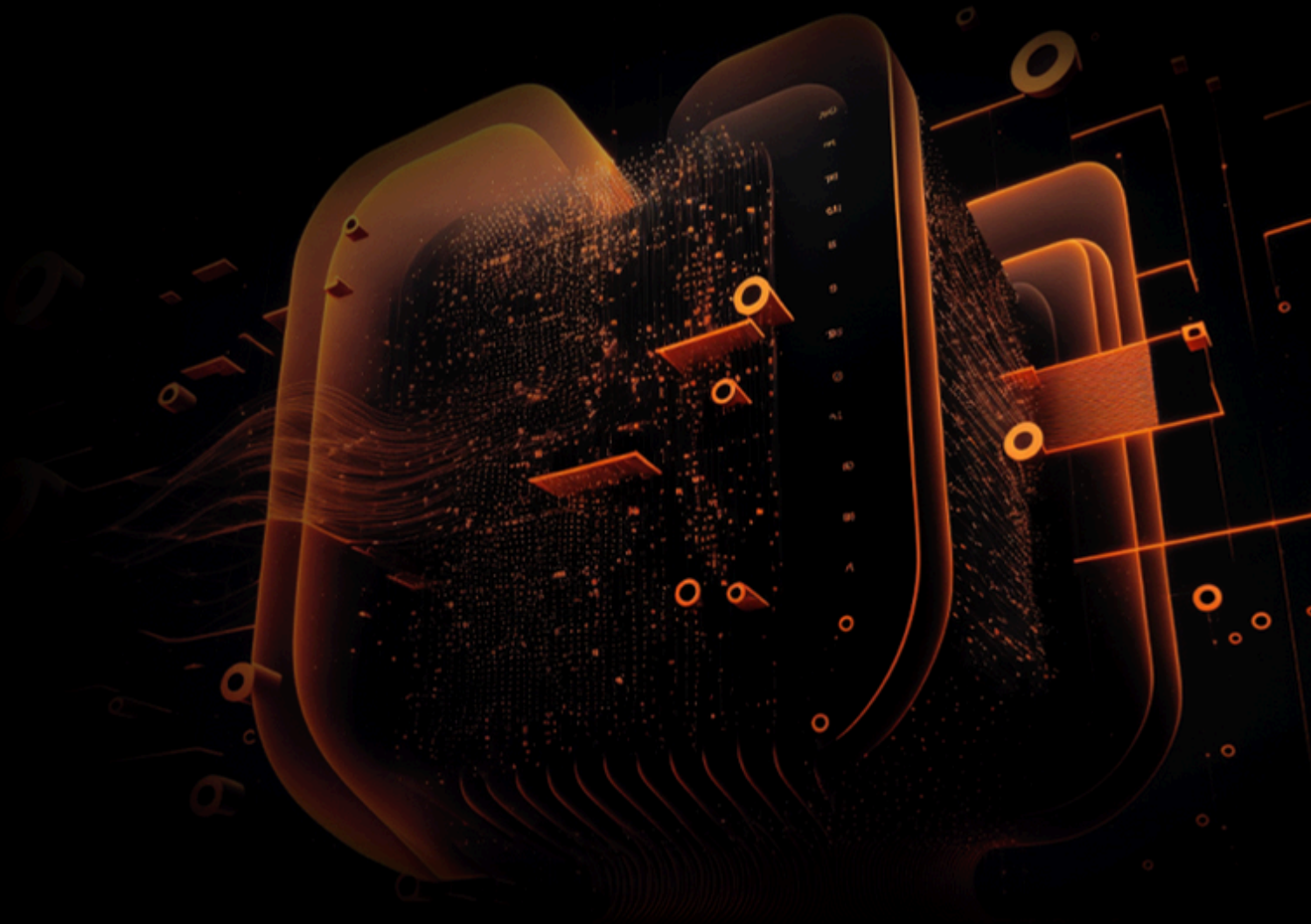


Data Security as a Service

Microsoft Purview

G-Cloud 15

Service Description



Service Description

Data Security as a Service | Assure 365

This Schedule forms part of Schedule 3 to the Agreement between Customer and Provider and sets out a description of the Services, Service Levels and Service Credits in relation to the Data Security as a Service module from Assure 365 as given on a Service Order.

1. Additional Definitions

The following definitions apply in this Schedule:

Assure 365: Assure 365, or A365, is a collection of modular managed services designed to enable Customers to outsource their cybersecurity and IT operations. Each module should be taken as a standalone service or packaged within in a bundle of services. Some examples of modules include SOC as a Service, Identity as a Service, Endpoint as a Service.

Microsoft Purview: a suite of data related technologies which can be broadly categorised into the following areas: data security, data governance, risk and compliance.

The Service is provided through the implementation and ongoing management of the Customer's Microsoft Purview environment. Specifically included within this service is Information Protection and Data Loss Prevention

BAU: Business as usual is the normal operation of typical and routine tasks or functions within an organisation, for example in relation to data security, a BAU task may be the routine auditing of sensitivity label usage by the Customers end-users.

2. Additional Commercial Terms Relating to Data Security as a Service

N/A

3. Additional Commercial Obligations Relating to Data Security as a Service

3.1 The customer will retain an active Microsoft Purview tenant alongside Entra ID for the duration of the Service.

3.2 The customer will retain valid Purview licenses such as M365 Business Premium, Purview P1, or Purview P2. It is important to note that this Service is scoped to include the configuration and management of Purview Information Protection and Purview Data Loss Prevention. As such, some Purview features are gated behind your organisations license, such as automatic sensitivity labelling which is only possible with the Purview P2 license.

3.3 The customer will be responsible for any costs relating to the acquisition and ongoing subscription of M365, or other Microsoft licenses required to enable the Provider to provide the Service.

3.4 The customer will provide the Provider with the appropriate level of access to enable the provision of the full breadth and depth of the Service, including onboarding and ongoing management, the expected level of access required is the 'Global Administrator' Entra ID role.

4. Data Security as a Service

4.1 The Data Security as a Service module from Assure 365 leverages the Microsoft Purview suite of solutions to provide a fully outsourced data-led security and operations managed service to configure and maintain the Customers Purview environment in a secure manner. For the avoidance of doubt, the Data Security as a Service module is intended to discover, classify, and protect data-at-rest across the M365 ecosystem only. As an example, this Service does not address data-at-rest or data-in-transit in Microsoft Azure or non-Microsoft technologies.

4.2 Onboarding – Data Security as a Service:

4.2.1 The Provider will issue a project plan outlining the high-level technical steps necessary to complete the onboarding of the Service

The Customer will grant appropriate access to the Provider

4.2.2 The Provider will deliver a bespoke onboarding in which the Customers' data security requirements will be obtained and documented.

4.2.3 The appropriate data security controls will be implemented.

4.2.4 The Provider will perform a robust data discovery exercise to identify the existing data-at-rest across the Customers on-premises and cloud environments.

4.2.5 The Provider will recommend a data classification strategy to best classify the identified data types from step 4.2.5. The Customer may choose to accept this recommendation or make alterations.

4.2.6 The Provider will configure the necessary technical controls available within Microsoft Purview to implement the agreed upon data classification strategy via Purview Sensitivity Labels. Where the Customer has the appropriate licensing, automated data classification controls can be implemented at the discretion of the Customer.

4.2.7 The Provider will configure the necessary data loss prevention controls available within Microsoft Purview to implement the agreed upon data classification strategy via Purview Data Loss Prevention.

4.2.8 The Provider will configure the necessary data retention controls available within Microsoft Purview to implement an agreed upon data retention strategy.

4.3 Ongoing - Data Security as a Service:

4.3.1 Maintenance of data security policies and configuration, and continued alignment to established best practice.

4.3.2 Management of minor changes such as bringing additional user groups in or out of scope of the deployed data security policies.

4.3.3 24 x 7 x 365 auditing of Microsoft Purview through the unified audit log.

4.3.4 Creation, ongoing maintenance, and deployment of new Microsoft Purview Sensitivity Labels as required to adhere to the Customer's define data classification strategy.

4.3.5 Creation, ongoing maintenance, and deployment of Microsoft Purview Data Loss Prevention policies as required to adhere to the Customers' define data classification strategy.

4.3.6 Creation, ongoing maintenance, and deployment of Microsoft Purview Data Retention policies as required to adhere to the Customer's define data classification strategy.

4.3.7 Routine review of data security policy configuration to ensure alignment to your organisation's data classification strategy. These reviews will be scheduled and conducted by the Provider on a quarterly basis.

4.3.8 Advice provided to Customer to harden their systems to prevent security Incidents where potential data security vulnerabilities or lack of best practice by Customer have been identified by the Provider during operation of Microsoft Purview.

4.3.9 Where applicable, the Provider will implement appropriate security policies, within agreed technology stacks, where the Provider deems it beneficial to the ongoing success of the Data Security as a Service module.

4.3.10 Business Hours support for general Customer enquiries relevant to Microsoft Purview.

4.4 Unless otherwise expressly agreed, the following are not included in Data Security as a Service:

4.4.1 Configuration and management of any technologies adjacent to, but not a part of, the Microsoft Purview technology suite.

4.4.2 Configuration and management of any data-at-rest or data-in-transit within Microsoft Azure.

4.4.3 Configuration and management of non-Microsoft data security technologies.

4.4.4 Incident response actions in case of a suspected or confirmed data breach or data loss event.

4.4.5 Remedial/recovery work following a data breach or data loss event.

5. Exclusions

5.1 Unless otherwise expressly agreed, the following are not included in the Service and but chargeable to the Customer as professional services:

5.1.1 Once the Service is being managed a re-architecture of data security from the ground up.

5.1.2 Significant or fundamental changes to how the security policies functions.

5.2 Only the activities, deliverables, and responsibilities expressly detailed within this Service Description are included. Any service elements not specifically stated are excluded from the scope unless agreed in writing by both parties.

6. Service Levels

The Provider will respond according to the following Service Levels on Ticket Open and the priority levels assigned by the Provider.

Response Time (contractual)

	Priority Level	Target SLA	Expected Performance
Enhanced Hours 24x7x365	P1 – High	15 Mins	95%
	P2 – Medium	30 Mins	95%
Standard Business Hours	P3 – Moderate	1 Hour	95%
	P4 – Minor	2 Hours	95%

Triage time (non-contractual)

	Priority Level	Target SLA	Expected Performance
Enhanced Hours 24x7x365	P1 – High	1 Hour	90%
	P2 – Medium	2 Hours	90%
Standard Business Hours	P3 – Moderate	8 Hours	90%
	P4 – Minor	24 Hours	90%

Monthly Response Time performance is calculated as follows:

For each Priority Level the performance for Response Time (“Actual Performance”) is calculated as:

Actual Performance = Number of incidents recorded for each Priority Level within SLA Target in any month / number of Incidents recorded for the Priority Level in total in any month * 100

This is then compared to the Expected Performance for each Priority Level given in the Response Time table above.

7. Service Credits

If the Actual Performance is less than the Expected Performance in any month for either of the P1 or P2 Priority Levels, Service Credits equivalent to (1) week's Charges for the Service shall be due to Customer such that maximum Service Credits of two weeks Charges for the Service may be payable in any month.

Service Credits cannot be obtained in relation to:

- Triage Time;
- In connection with P3 or P4 Priority Levels; and,
- During the first 3 months of the Service being live.

Data Security as a Service

**Prevent Data Breaches. Enforce Compliance.
Safeguard Sensitive Information.**

Powered by Microsoft Purview. Realised by CyberOne.

CyberOne's Data Security as a Service offers full visibility, control and protection for your data, optimising security and governance for Microsoft 365 Copilot readiness. Powered by Microsoft Purview, this managed service ensures governance, risk management and compliance across the data lifecycle with minimal management effort.

Part of CyberOne's Assure 365 suite, our fully outsourced Managed Microsoft Security solution offers modular cyber security services tailored to your needs. It delivers comprehensive, scalable protection to strengthen resilience and empower you to focus on your core business objectives.

What is Microsoft Purview?

Microsoft Purview is a comprehensive data security solution that empowers organisations to gain visibility and control over their data estate. It enables discovery, classification and protection of sensitive information across on-premises, multi-cloud and SaaS environments.

Seamlessly integrated with Microsoft's Security suite, Purview provides unified data management, supporting compliance, risk management and robust data protection.

CyberOne's Data Security as a Service, powered by Microsoft Purview, delivers end-to-end data governance, helping organisations secure sensitive data, streamline compliance and maximise readiness for Microsoft 365 Copilot with minimal overhead.



Key Features of CyberOne's Data Security as a Service

CyberOne's Managed Data Security Service provides visibility, control and protection for your data, minimising risks and ensuring compliance. Powered by Microsoft Purview, our service strengthens data governance, safeguards sensitive information, supports regulatory needs and prepares your organisation for AI and Microsoft 365 Copilot.



Data Discovery

Continuous discovery to identify and map at-rest data across on-prem and cloud.



Data Protection & Encryption

Prevent unauthorised access, ensuring privacy and security across your organisation.



Automated Data Classification

Setup and maintenance of policies to protect sensitive information



Data Loss Prevention (DLP)

Controls to prevent data exfiltration across email, web, removable media and cloud repositories.



Insider Threat Management

Auditing and alerting for unusual user data access, reducing risks of internal threats.



eDiscovery & Data Preservation

Efficient management of data for legal investigations, SARs and case management.



Data Lifecycle & Retention

Implementation of retention and archiving policies to ensure regulatory compliance.



Data Governance & Compliance

Regulatory adherence with regular audits and data alignment to policies.



Microsoft 365 Copilot Readiness

Creation of a secure, compliant environment for Microsoft 365 Copilot AI, with robust data governance, protection, and lifecycle management.

Unlock Business Value with CyberOne

24x7 Data Protection

Continuous monitoring and rapid response to secure sensitive data and prevent unauthorised access.

Scalable Data Governance

Enforces data policies across environments seamlessly, ensuring compliance and data security at scale.

Unified Data Visibility

Centralised insights across your data for enhanced detection, response and decision-making.

Controlled Data Access

Securely manage data access to minimise unauthorised use and protect sensitive information.

Insight-Driven Data Compliance

Real-time analytics and reporting to meet regulatory needs and proactively manage risks.

Optimised Data Operations

Automate data management, freeing up resources and simplifying compliance.

Seamless Experience

Secure sensitive data without disrupting workflows, enabling uninterrupted access to critical information.

Proactive Risk Management

Identifies and mitigates vulnerabilities early to prevent data exposure.

Copilot & AI Readiness

Modernise your business with a secure, compliant data environment optimised for AI and Microsoft 365 Copilot.

Cost-Effective Compliance

Maximise your investment in Microsoft by reducing tool costs and enhancing compliance.

Why Choose CyberOne's Data Security as a Service?

CyberOne's Managed Data Security Service delivers the expertise, resilience and efficiency needed to protect data, ensure compliance and unlock insights.

1. Microsoft Purview Expertise

CyberOne's certified specialists bring deep knowledge of Microsoft Purview, ensuring best-practice implementation and maximum data security.

2. Proven Data Protection Standards

Backed by ISO 27001 certification, CyberOne implements rigorous security protocols to consistently safeguard sensitive data across your ecosystem.

3. 24x7 Data Monitoring

CyberOne's CREST-accredited SOC offers around-the-clock monitoring and rapid response to protect against data breaches and misuse.

4. Simplified Compliance Management

CyberOne automates and manages compliance tasks, reducing the burden on your internal teams while maintaining regulatory alignment.

5. Maximised Microsoft ROI

Optimise your Microsoft investment with CyberOne's certified expertise across Purview, Microsoft 365 and the wider Security suite.

6. Insightful Reporting & Analytics

CyberOne's real-time insights empower your organisation with detailed reporting to inform strategy and meet audit requirements.

7. Future-Ready Data Environment

CyberOne prepares your organisation for modern technology with secure, compliant support for AI and Microsoft 365 Copilot.

8. Tailored Risk Mitigation

CyberOne proactively identifies and addresses data vulnerabilities specific to your business, reducing exposure before threats materialise.

About CyberOne

CyberOne is a Microsoft Security Solution Partner and member of the Microsoft Intelligent Security Association (MISA). We deliver one of the UK's most advanced AI-augmented Managed eXtended Detection & Response (MXDR) services, recognised with Microsoft-verified Managed XDR solution status, enabling organisations to move with confidence from risk to resilience. Powered by Microsoft's market-leading security technologies and realised by CyberOne's accredited experts, we help businesses anticipate and contain modern threats so they can thrive.

With 24x7x365 Global SOC coverage, NCSC accredited Cyber Incident Response, CREST SOC and Penetration Testing accreditations and guaranteed SLAs, CyberOne combines Microsoft Security with expert consulting, professional and managed services to protect operations, achieve compliance and build lasting resilience.

Accreditations & Certifications

CyberOne's services are backed by the world's leading standards bodies including NCSC, CREST and ISO as well as our key technology partners, whilst our experts are backed by industry-leading certifications, cementing our role as leaders in cyber security.



✉ hello@cyberone.security

☎ +44 (0) 3452 757575

🌐 cyberone.security