wanstor

Microsoft Purview

Service Description

Confidentiality and copyright

The information contained in this document, is confidential and is issued by Wanstor Ltd on the understanding that it will be used only by the staff of, or consultants to, the client and where consultants are employed, the use of this information is restricted to use in relation to the business. In particular, the contents of this document may not be disclosed in whole or in part to any other party without the prior written consent of Wanstor Ltd. © Copyright Wanstor. All rights reserved.

wanstor

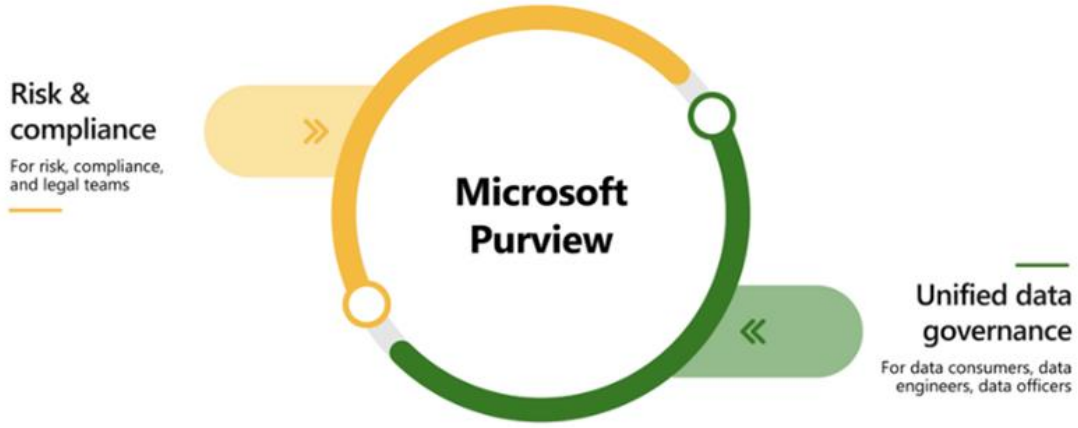
EXECUTIVE SUMMARY

In the modern business landscape, effective data management is a significant challenge, especially as organisations grow, diversify, and adopt advanced technologies such as Artificial Intelligence. Challenges such as data fragmentation, compliance risks, security breaches, and poor data quality often hinder data-driven decision-making and innovation.

Microsoft Purview, a unified data governance service, offers a solution to these challenges. It enables companies to discover, catalogue, classify, and map their data across various environments, including on-premises, cloud, and other hybrid setups. Purview provides a holistic view of your data landscape, facilitating an understanding of data lineage and easy visibility of dependencies.

Wanstor can help you protect sensitive data across clouds, apps, and devices with information protection, data loss prevention, and insider risk management. We also help you identify data risks and manage regulatory compliance requirements with audit, communication compliance, compliance manager, and eDiscovery.

We do this by assisting you in applying data sensitivity labels, terms, and glossary to standardise data definitions and classifications. Wanstor aid in creating, agreeing upon, and enforcing data governance policies and rules to ensure compliance and security.



wanstor

Service Overview

The Wanstor service covers both Establishment of the rules governing your data and the configuration of Microsoft Purview to reflect the rules defined. The service consists of two phases – Establishment and Configuration.

Establishment

- Assist in evaluating your current data governance maturity, identifying gaps and opportunities for improvement.
- Design and implement a solution tailored to your business goals and other data requirements.
- Assist with the integration of Microsoft Purview with your existing data sources, platforms, and other supported tools.
- Configure initial scans, catalogues, and classifications for your data assets, ensuring automatic and continuous updates.
- Create an up-to-date map of your entire data estate, including data classification and end-to-end lineage.
- Work with you to agree and apply data sensitivity labels, terms, and glossary to standardise your data definitions and classifications.
- Set up basic monitoring for Microsoft Purview such as access metrics, alerting rules and diagnostic settings. (If the customer opts not to take the associated managed service, these alerts will be directed to the customers nominated contacts).

Workshop Outcomes

Outcomes of our initial design workshop for implementing Microsoft Purview include:

- **Data Cataloguing**: Establish clear criteria for cataloguing data, including critical metadata attributes, data sources, and classification criteria that align with your business objectives.
- **Access and Permissions**: Ensure Microsoft Purview has the necessary permissions and access credentials to connect to various data sources and conduct scans across your organisation's data repositories.
- **Roles and Responsibilities**: Define the roles and responsibilities for data stewards and owners within Microsoft Purview. This includes managing

and maintaining metadata quality and accuracy, assigning ownership to specific data sets, and ensuring accountability for data-related decisions.

- **Data Classification Policies**: Help establish data classification policies to categorise data based on sensitivity, regulatory requirements, and other factors. Wanstor will provide additional guidance for data classification based on departments and teams.
- **Technical Infrastructure Readiness**: Prepare your technical infrastructure for Microsoft Purview. This includes verifying network configurations, implementing security protocols, and addressing any technical dependencies or requirements specified by Wanstor through the discovery process for a successful Purview deployment.
- **Software Compatibility**: Ensure that all software, applications, and systems that will interact with Microsoft Purview are compatible. This includes any third-party software or legacy systems.
- **Resource Availability:** Help understand the availability of necessary resources, including skilled personnel, hardware, and software, for the successful implementation and operation of Microsoft Purview.

Once the workshop(s) have been successfully completed, Wanstor will implement the agreed configurations.

Configuration

- Create, agree, and enforce data governance policies and rules to ensure compliance and security.
- Assist in protecting sensitive data across clouds, apps, and devices with information protection, data loss prevention, and insider risk management.
- Help identify data risks and manage regulatory compliance requirements with audit, communication compliance, compliance manager, and eDiscovery.
- Aid in empowering your data consumers to find valuable data and generate insights with data map, data catalogue, and data lifecycle management.

wanstor

Customer Responsibilities

While Wanstor are responsible for the setup and management of the tool, providing a valuable service is dependent on ongoing context of the data and its business relevance. To that end, the following remain the responsibility of the customer

- **Data governance**: The customer is responsible for the standards set for the classification, labelling, and protection of their data. This includes determining which data should be classified as sensitive or confidential. Wanstor will advise, but the customer remains responsible for the decisions made on what to classify and how that data is subsequently protected.
- **User management**: The customer is responsible for assigning appropriate licenses and managing user roles and permissions.
- **Compliance**: The customer is responsible for ensuring their use of Microsoft Purview complies with all applicable laws and regulations, including data protection and privacy laws.
- **Security**: While Microsoft provides tools to help secure data, the customer is responsible for configuring these tools to meet their specific security needs after the initial configuration of the product by Wanstor.
- **Data Breach Response**: In the event of a Data breach, the customer is responsible for incident response, including notifying affected users and reporting the incident to any relevant authorities.

Dependencies, Assumptions and Exclusions

- **Non-Compliant Data Sources**: Any data sources that do not comply with the organization's data governance policies or fail to meet the technical requirements for integration with Microsoft Purview are excluded from the scope of the service which includes anything that Microsoft MSGraph cannot connect to.
- **Currently Unsupported Systems**: Microsoft Purview is designed to support a wide range of data sources and file types. However, there are some systems and file types that are not currently supported1. Here are some examples:
    - **Azure Data Factory**: While it's an Azure service, it doesn't support classification, live view, lineage, labelling, access policy, and data sharing1.

- **Azure Databricks Unity Catalogue**: This service doesn't support any of the capabilities mentioned above1.
- **Amazon Redshift, MongoDB, Salesforce, Tableau**: These services are not currently supported by Microsoft Purview1.
- **File Types**: For AVRO, ORC, and PARQUET file types, the scanner does not support schema extraction for files that contain complex data types (for example, MAP, LIST, STRUCT)1.