KPMG Microsoft

KPMG data protection with Microsoft Purview

Transforming the way you protect your data assets

One of the single most important assets for an organization is its data, and many struggle to have a consolidated and complete view. They often find themselves with many siloed legacy systems, without accountable owners or an understanding of the type of data stored or processed on these systems. This results in a lack of visibility, traceability, and clarity regarding sensitive data.

KPMG can assist organizations in evolving their data protection capabilities leveraging Microsoft Purview™ capabilities that exist within their E3 and E5 licenses. Leveraging our methodology alongside the Purview suite helps organizations automate key components of their data protection program and maximize the value of existing investments.

Data Protection—What does "good" look like ?

- Define a clear strategy for data protection based on your organization's business and technology
- Insight into an organization's data and what an organization considers sensitive data
- Ability to effectively manage data risk across an organization's enterprise ecosystems
- Efficient discovery, cataloging, and classification of sensitive data assets
- Prevent and mitigate the impact of data breaches, particularly for sensitive and mission critical data assets
- Adapt to new and evolving global regulations for data protection
- Evolve with changing business requirements

Industry insights on data loss

$4.35M
Global Average cost of data breach in 2022 reported to be $4.35M, an all-time high[1]

1,802
1,802 data breaches in 2022[2]

$164
The average cost per lost or stolen record in a data breach is $164[1]

83%
83% of breaches involved external actors.[3]

$3.05M
Breaches at organizations with fully deployed security AI and automation cost $3.05M less than breaches at organizations with no security AI and automation deployed.[1]

$5.87M
Organizations lose an average of $5.87 million in revenue due to a single non-compliance event.[5]

86%
U.S. General Population believes that data privacy is a human right.[4]

[1] IBM Security, "Cost of Data Breach Report 2022"
[2] Identity Theft Resource Center, "2022 Data Breach Report"
[3] Verizon, "Data Breach Investigation Report 2022"
[4] KPMG, "Corporate data responsibility survey 2022: The path to transparency —and trust"
[5] Saviynt, "The True Cost of Non-Compliance"

The path to transformation

Better understanding of data protection needs

Understanding the appropriate risk-based need for data protection tailored to your industry and organization.

Alignment with business goals

An effective data protection program and goals should be made in partnership with business vision & goals.

Effective data control framework

A customizable data control framework, with enhanced data protection and privacy policies, compliant with industry best practices, frameworks, and standards such as NIST, ISO, GDPR, Zero Trust, PCI, etc.

Enhanced visibility with technology enablement

Enhanced visibility of your critical data assets with a technology-enabled automated approach for active discovery, cataloging, classification & protection.

KPMG methodology aligned with Microsoft Purview features

KPMG offers a holistic data protection methodology that focuses on safeguarding sensitive or confidential data that is created, gathered, and utilized by the organization. In our experience, data protection programs should encompass all domains within the methodology in varying capacities. Below we have aligned the features within Microsoft Purview to our Data Protection Methodology. The features are available to Microsoft customers, across both E3 and E5 licenses, can empower organizations

Data protection methodology

Strategy	Establish a data protection strategy to protect data from any internal or external risks or threats.	
Governance	Formally define policies, roles, and responsibiities for Data Protection	Compliance manager Privacy risk management Information barriers
Discovery and classification	Discover, categorize, and tag data based on importance, sensitivity, or other organization specific factors.	Content explorer Sensitive info types Trainable classifiers Exact data match (EDM) classifiers Recommended data classification labels Automatic data classification labelings AIP labeling client for file share Microsoft information protection SDK
Protection	Implement data protection measures throughout the entire data lifecycle.	Protected labels Data loss prevention Office 365 Message Encryption (OME)
Monitoring and remediation	Monitor for exfiltration of certain data types. Audit and log user activities, analyze alerts.	Activity explorer Communication compliance Insider Risk Management (IRM)
Archival and deletion	Establish and enforce retention and deletion policies for data assets	Retention labels eDiscovery and legal hold Records management
Response and recovery	Response to data related incidents and reporting to established key metrics	Sentinel logging DLP incident response within defender
Training and awareness	Educate stakeholders on data handling principles and the company’ s policies	Policy tips Email notification

Not for the first time

Global beverage manufacturer

Client Issue: Client requested help transitioning from one DLP solution to another. They wanted to assess existing implementation of DLP in old solution, identify areas of improvement, and utilize all the capabilities available in their new solution.

KPMG's assistance: KPMG performed a series of interviews and workshops to understand current DLP implementation, current DLP and Insider Risk Program, and existing plans for utilizing the new solution. KPMG prepared a holistic DLP program Gap Analysis with suggested recommendations to remediate gaps and improve overall program. Gaps span areas of DLP capabilities, architecture, process, and governance. KPMG made suggestion on policy improvements and created a roadmap to help guide the client on implementing priority features Purview based on their program goals and organization maturity. One of the key recommendations was implementing Microsoft Insider Risk Management™.

Benefits to client: KPMG assisted with a POC of Microsoft Insider Risk Management (IRM). All existing insider risk use cases were built into IRM helping to save multiple hours a day of Analyst Triage time. KPMG developed a Sentinel Workbook with 15 different Key Performance Indicators to help monitor DLP activity at a high level. This workbook, leveraged by both leadership and analysts, enabled the client to see real time metrics regarding data loss activity, a capability which did not previously exist. Additionally, leveraging Microsoft Purview suite helped the client save costs and consolidate capabilities into a single solution.

Why KPMG

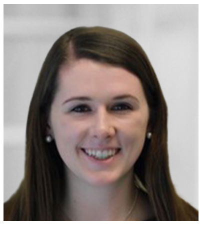
KPMG brings a combination of technological and compliance-based experiences as well as deep business and industry knowledge. Our onshore and offshore data protection professionals have hands-on experience with the Microsoft Purview product suite and bring additional general and domain subject matter experience to help organizations apply risk-based security controls for their most sensitive assets. Our direct experience using Microsoft Purview in our own internal test environment has prepared us to quickly adapt and configure Microsoft's product to fit an organization's specific needs and a variety of use cases.

Contact us

Michael Gomez
Principal
Cyber Security Services
E: michaelgomez@kpmg.com

Jim Wilhelm
Principal
Cyber Microsoft Alliances Leader
E: jameswilhelm@kpmg.com

Venoth Lal
Director
Cyber Security Services
E: venothlal@kpmg.com



Elizabeth McConnell
Senior Associate
Cyber Security Services
E: elizabethmcconnell@kpmg.com

Ryan McGurgan
Senior Associate
Cyber Security Services
E: rmcgurgan@kpmg.com

Microsoft Intelligent
Security Association

Microsoft Security

Microsoft Verified
Managed XDR Solution

Some or all of the services described herein may not be permissible
for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.