FORTRA™

Optimizing Microsoft Purview with Fortra's Data Classification

Extend Data Classification Coverage Across Your Ecosystem

Why Data Protection Matters

To maintain public trust, comply with privacy regulations, safeguard against reputational and legal risks, and prevent costly data breaches, organizations must make data protection a top priority. In an increasingly interconnected, digital world, securing sensitive information is crucial for preventing intellectual property theft, corporate espionage, and financial fraud. Investing in robust data protection measures is not only a compliance necessity but a strategic imperative for building resilience and trust in an increasingly risky security landscape. But to maintain relationships with external suppliers, partners, and vendors, it's just as critical that these organizations' data protection efforts avoid unnecessary business friction.

The challenge for organizations today is to successfully strike the balance between complexity and efficacy in their data protection strategies, including finding tools that are flexible and configurable, yet still easy to use. Microsoft Purview Information Protection, often referred to as MIP or simply Purview, serves as an example of a common data classification tool that is simple to use but that has limitations as a standalone solution. A best-of-breed solution, however, should enhance Purview without sacrificing ease of use and should fit seamlessly into how end users work on a day-to-day basis. Whether it is roadmap flexibility, technology integration and interoperability, or support for applications and file types, your classification vendor choice must support the data protection needs of your organization not just now, but well into the future.
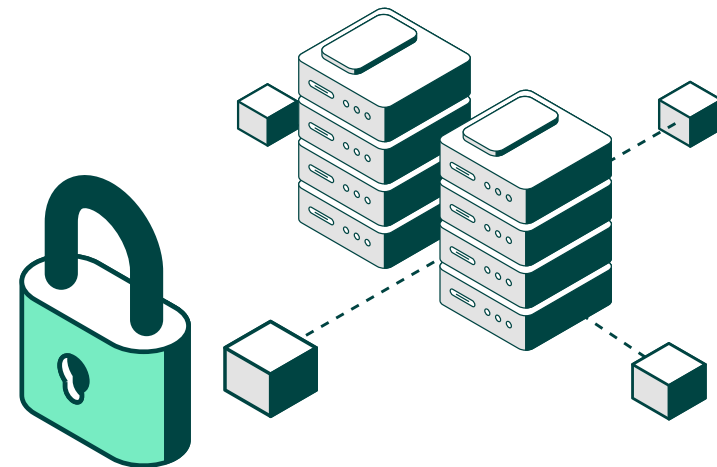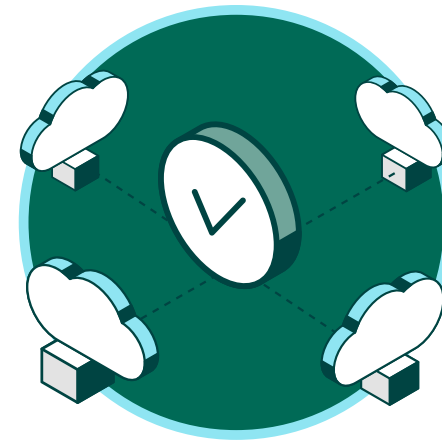
Purview's Limitations

Microsoft Purview's limited labeling and classification interface for information protection, known as Sensitivity Labels, forms one of the building blocks of the larger Purview package. Within the Purview governance portal, customers can categorize data assets by assigning unique tags or classes (sensitivity labels) to that data, providing a basic level of data classification. However, there are often occasions where an organization finds it needs additional enhancement. As a standalone solution, these are just some of the ways in which Purview falls short:

METADATA LIMITATIONS

Metadata is often the main driver of best-in-class data classification solutions, but Purview on its own has limited capabilities. Purview only has two user-defined fields, one being for sensitivity with only two levels. Additionally, it is only able to read other metadata as part of a migration and only from certain places. Complying with niche regulations with specific requirements, like the CUI program, ITAR, and others remains impossible with Purview alone.


LABELING LIMITATIONS

Along with a breadth of metadata capabilities, useful data classification products have extensive data labeling capabilities. Again, however, Purview falls short on its own in this way. It has limited flexibility around classification schema, as only a single value can be selected from a drop-down list. Visual markings are often crude, there is little user control over when they're applied, and formatting is very limited.

Policy Limitations

If your organization already has intricate data protection policies in place, you may find that Purview on its own has limitations in following those policies, as the conditions to control labeling are limited. Purview's policy engine itself often relies on other tools and products to function at a high level, resulting in a less favorable user experience.
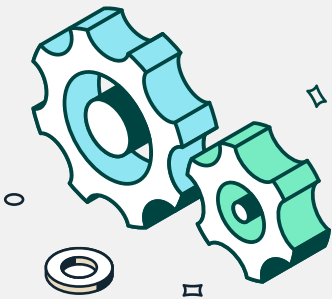
Functionality Limitations

More generally speaking, Purview has functionality issues that can make it a pain to utilize on its own. The user experience is quite limited, with little ability to tailor the UI or messaging, and there is little user assistance to be had in what it does provide. MIP is entirely unable to check meeting invites, for example, which may have sensitive information included that Purview will miss.

Platform Limitations

While robust data classification solutions will generally run anything that can be run on a Windows machine and often even work cross-platform, this is not the case with Purview. MIP is limited to a fixed framework and is unable to classify all file types on Windows.
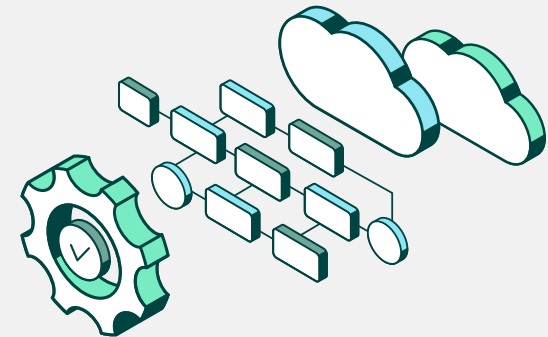
# How Fortra's Data Classification Enhances Purview

Adding Fortra's Data Classification Suite (DCS) into your security portfolio brings enhanced labeling and metadata capabilities to the simple labeling capabilities of Purview, enabling smooth, enhanced functionality.

DCS allows you to map Microsoft sensitivity labels to more refined DCS label values, meaning DCS users can process documents and emails from MIP users. This means that you can allow some of your users with less data protection duties to use MIP, while allowing those who need a more sophisticated data protection experience, such as users in the legal and compliance, privacy, and financial spheres, to use the nuanced approach delivered by DCS. Our Purview Classification Adapter provides the interface between Microsoft labels and DCS, allowing more comprehensive data protection coverage. Furthermore, it facilitates streamlined compliance with ever-evolving regulatory requirements and protects intellectual property.

Metadata

While applying a DCS label can be used to set MIP labels, it can also set sophisticated metadata values to drive downstream security technologies such as DLP, archive and retention, and secure email gateways. This helps improve the ROI of your other security tools.
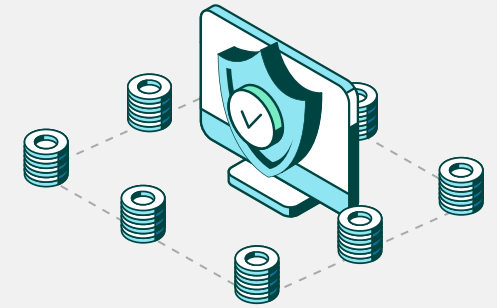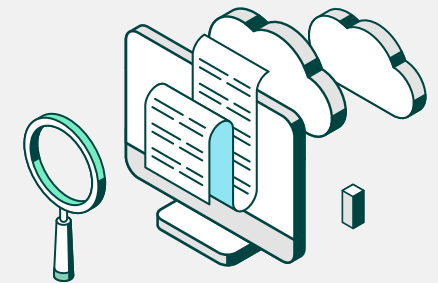
Labeling

MIP allows the configuration of a limited number of labels. While this may work for some users in your business, it is likely unsuitable for those dealing with PII, PCI, and/or PHI, among other regulations. Moreover, any user who needs to protect intellectual property will require a more nuanced data labeling scheme that cannot be provided by MIP's set list of choices.

Enhanced Policy Capabilities

Any data classification product must allow flexibility when dealing with the user or else it is doomed to fail. DCS supports allowing the user to choose whether to provide visual markings. For example, it may not be appropriate to visually mark a third-party document that should be classified. Likewise, DCS can present different warnings or blocks to users when they downgrade from one label value to another.

Functionality

DCS can present the labeling values in a clean interface that can be configured to help the user make the right choice. The values presented will change depending on previous choices or through the AI-assisted discovery. Furthermore, the UI can be customized to use organizations' branding and logos, giving a sense of ownership of the labeling experience to the organization.
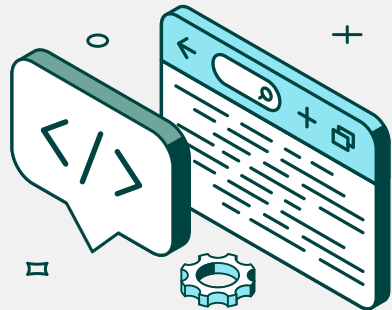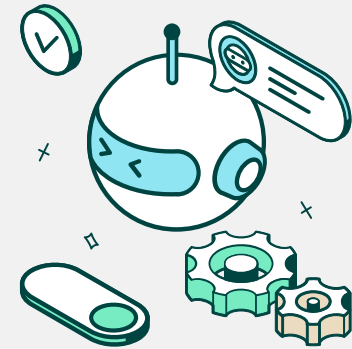
Cross-platform Capabilities

DCS has rich, cross-platform support. DCS runs on Microsoft operating systems but is also able to classify any file type on the Mac filestore. Likewise, the data-at-rest scanning tool, DCS for Data at Rest, can scan Windows fileshares, SharePoint, OneDrive, Google Drives, and other repository types.

Why You Need More Than Just Purview

1

Combining Purview with Fortra's Data Classification gives organizations the ability to offer the level of granularity required for compliance with emerging regulations such as GDPR, CCPA, CMMC, CUI, and ITAR as well as many more regional-based regulations globally.

2

The basic levels of classification that Purview provides might be a good starting point, but your long-term solution needs to be powerful, flexible, and future-proofed. Pairing it with Fortra's Data Classification can make that happen.

3

The superior functionality of a best-of-breed data classification solution like Fortra's Data Classification allows for greater coverage and integration across different security and data management solutions, productivity tools, and platforms, providing better value and return on investment.

4

Data protection tools should always adhere to the specific requirements of the organization —— never the other way around. Folding Fortra's Data Classification into Purview can provide the necessary granularity to fulfill all business needs, whether they align with compliance or are solely for internal/departmental use.

5

Organizations create and handle a significant amount of data, but not all data is equal. Combining Purview with Fortra's Data Classification can allow organizations to simultaneously keep up with the changing security landscape and facilitate smooth workflows.

6

Fortra's Data Classification, beyond identifying and classifying sensitive data, will help organizations better understand how and where those classifications are being applied. This allows for the identification of trends and usage, more accurate reporting, and better insight into how rules could be appended or automated.

Fortra's Data Classification Can Be the Answer for Your Organization

Taking a combined approach to enterprise information protection with enhanced data classification at the core enables policy issues and integration requirements to be tackled together to deliver maximum value for your business. Organizations can address regulatory compliance challenges now, attend to their current classification challenges, and solve those that will be introduced around the corner.

Learn how Fortra's Data Classification can give your data protection strategy the boost it needs by chatting with one of our experts today.

Member of
Microsoft Intelligent
Security Association

▣ Microsoft

MISA Member

We're proud to be a MISA member. Both Microsoft and Fortra share a customer-first focus, meaning our partnership is to ensure our solutions work together to satisfy our customer needs in a global environment that is ever-increasing in complexity. By complementing each other's solutions and leveraging the strengths of both Microsoft and DCS, our partnership will ensure our customers can meet their global obligations as the laws and regulations that govern us continue to evolve in the future.

LEARN MORE

FORTRA™