USE CASE

Microsoft Purview Optimization

Purview Is a Powerful Start

Microsoft Purview provides organizations with a strong foundation for discovering, classifying, and protecting data across the Microsoft ecosystem. But the effectiveness of everything that follows depends on getting those classifications right in the first place.

That can be a significant undertaking. Purview's classification models can require teams to train them using representative examples of the data they want to identify—including both good examples that belong in a category and bad examples that do not. For some data types, that can mean creating and maintaining dozens or even hundreds of examples before a model can reliably tell them apart.

The challenge doesn't end when training is complete. Organizations constantly create, copy, modify, and move data across Microsoft 365 and beyond. As the environment evolves, maintaining classifications can become harder, and inaccurate labels can undermine the policies and controls that depend on them.

The result is a powerful governance platform that can still spend a lot of time determining what your data means before it can effectively govern it.

Every Policy Starts With a Label

Training takes time. Building representative sets of good and bad examples for each data type can make classification a substantial manual effort.

Data is more nuanced than patterns. Keywords and patterns can help identify information, but they don't always capture the meaning, context, or business relevance that distinguishes one record type from another.

Classification drives everything downstream. The accuracy of a classification affects the sensitivity label applied to the data—and the policies and protections that depend on it.

The data keeps changing. New information is constantly created, and existing information changes, making it harder to keep classifications accurate over time.

You Need Better Data Intelligence

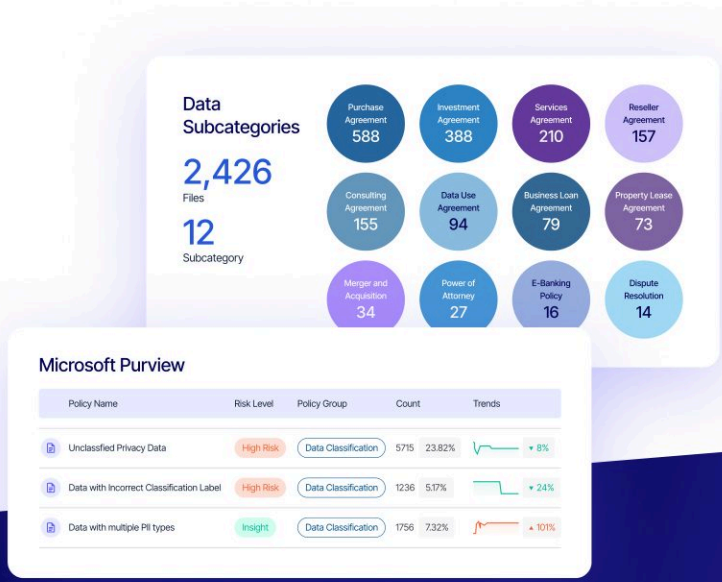
Give Purview a deeper understanding of your data so it can apply the right classifications and labels without requiring your team to build and maintain an extensive library of training examples.

Give Purview a Better Read on Your Data

Concentric AI enhances Microsoft Purview with semantic data intelligence that understands what information is, what it means, and why it matters. Rather than asking security teams to teach a model what every data type looks like through extensive positive and negative examples, Concentric AI uses patented language models to understand data based on its content, context, and business relevance.

That deeper understanding can be used to identify thousands of data categories and subcategories, improve classification accuracy, and apply Microsoft Information Protection (MIP) sensitivity labels more precisely, giving Purview better information to work with.

- **Discover deeper data context.** Identify sensitive and business-critical information across structured and unstructured data, with granular visibility into thousands of categories and subcategories.
- **Classify based on meaning.** Distinguish data by its content, context, and business relevance rather than relying solely on keywords, patterns, or manual training.
- **Put better labels to work.** Apply accurate classifications and MIP sensitivity labels so Purview policies and protections can act on a clearer understanding of the data.



Make More of Your Purview Investment

Better data intelligence helps organizations:

Improve policy accuracy by giving Purview more precise classifications and labels.

Reduce classification effort by minimizing the need to build and maintain large libraries of positive and negative training examples.

Strengthen data protection by applying sensitivity labels that more accurately reflect the information they are meant to protect.

Support safer Copilot use by identifying which information is sensitive and where stronger controls may be needed as AI adoption expands.

About Concentric AI

Concentric AI enables organizations to accelerate safe AI adoption through its unified AI and data security governance platform. Powered by the Semantic Intelligence Engine's patented language models, the platform discovers, governs, and protects business-critical and compliance-sensitive data at rest, in motion, and used by AI through a consistent policy framework.

Get a Demo