

Microsoft Purview and Concentric AI: Working Better Together



For organizations today, achieving robust data governance, compliance, and security across their expansive data landscapes is much easier said than done. But with the right toolsets, addressing these business-critical objectives and securing sensitive data can be managed efficiently and securely.

To address these concerns, companies running Microsoft 365 with an E5 license have access to Microsoft Purview, formerly known as Security and Compliance Center. But Purview alone may not be sufficient.

In this article, we'll discuss the benefits and downsides of Microsoft Purview and explore why deploying Microsoft Purview and Concentric AI together can create a robust data security posture.

When combined, the solutions can specifically accommodate the needs of an organization's hybrid or multi-cloud data landscape. Working together, organizations can meet compliance and effective data governance, enable proactive detection of data risks, and drive multidimensional data discovery and classification.

Microsoft Purview: How it tackles data discovery

Microsoft Purview is a comprehensive data governance and compliance solution aimed at facilitating effective management of an organization's data landscape. One of its core functionalities is the ability to discover, classify, and organize data across different sources in regulated environments — which is hugely beneficial for any organization.

Purview offers three methods for data discovery:

Regex-based: This approach looks for patterns in data, primarily to identify Personally Identifiable Information (PII) such as names, credit card numbers, etc. Purview has almost 400 pattern identifiers.

Pre-trained Machine Learning (ML) classifiers: These are predefined models (Purview has 50) capable of identifying and categorizing specific types of information, including financial statements, agreements, and others.

Trainable ML classifiers: These classifiers allow customers to fine-tune the data categorization according to their requirements. Customers provide sample data to train classifiers, which then recognize and assign documents to corresponding categories.

While Trainable classifiers may sound great in theory, they require customers to send 50 documents of the type they want to train the classifier on. The model then trains for 24 hours, and customers must test it in a sample environment with 200 positive and negative samples. It takes 12 days to train each model.

These mechanisms have their limitations. Regex patterns may result in false positives and negatives, pre-trained classifiers cannot be retrained, and creating new trainable classifiers requires significant time and effort.

Concentric AI: Next-level data discovery

While Purview focuses mainly on data governance and compliance, Concentric AI excels with its deep learning models. Concentric AI's Semantic Intelligence provides a more advanced method for data discovery and categorization that does not rely on predetermined rules, patterns, or policies.

What this means is Concentric AI employs AI-powered semantic intelligence to understand the context of data. With context-sensitive data categorization, organizations gain a comprehensive view of the data, allowing enhanced security, identification of risky data activities, and corrective actions for data misclassification.

Plus, Concentric AI's more flexible approach supports over 1100 thematic categories, offering a granular view of data. The AI models can adapt to customer environments and do not require massive upfront work or continuous supervision.

Security teams can also flexibly train The Concentric AI models using their own data our AI models may not be familiar with, and the solution quickly adapts to their environment.

Concentric AI Semantic Intelligence also supports data discovery and classification across Microsoft and non-Microsoft environments, leveraging native labeling frameworks. It can support autonomous risk identification from inaccurate entitlements, risky sharing, wrong location, and unauthorized access.

The power of working together

Despite their independent offerings, Microsoft Purview and Concentric AI can create an incredibly robust data management and security ecosystem when combined. Purview's strength lies in its cost-effective DLP and compliance capabilities. It provides a robust platform for regulated industries to manage their data landscapes effectively.

Concentric AI, on the other hand, delivers a powerful layer of AI-driven data discovery, risk detection, and enhanced categorization. It complements Purview by addressing many of its limitations in discovery, classification and risk detection, while using Microsoft Information Protection labels.

Organizations can use Concentric AI to understand all of their data at-rest and the risk associated to it. Once organizations know the data they have, they can use Purview's DLP for data in-motion to conduct the enforcement of policies in an effective manner with accurately classified and labeled data. Together, the two solutions enable organizations to have a more extensive understanding of their data, reinforce security, and drive data-based decision making.

While Purview predominantly supports Microsoft environments, Concentric AI extends the scope of data discovery and classification to non-Microsoft environments too, ensuring a broad coverage of an organization's data ecosystem.

By using both these tools alongside each other, organizations can maintain compliance and data governance across their multi-cloud or hybrid data landscape while gaining proactive detection of data risks and multidimensional data discovery and categorization.



The bottom line: 4 key ways Concentric stands out

Most accurate and comprehensive data discovery

- Deep learning for autonomous, accurate data categorization
- Over 1100 categories to identify sensitive customer information, intellectual property, business documents, personally identifiable information, PHI etc. — without rules
- Curated catalog of AI models for high accuracy

Autonomously surfaces risk to business-critical data

- Risk-distance self learns and provides risk-oriented view into sensitive data
- No rules, upfront policy development or end-user involvement

Managed Data Security

- Autonomously discover, categorize, and remediate potential security risks
- Our expert team complements the product, addressing any complex challenges
- You're not just getting a product, you're getting a 24/7 dedicated security partner

Quick and easy time to value

- Minimal effort to derive value and for ongoing administration
- SaaS solution with zero ongoing administrative burden
- Secures data in SaaS services, the cloud and on-premises
- Easy, seamless integration with 3rd party security investments

With Concentric AI, you get:

- Autonomous cloud data discovery, classification and remediation
- Agentless integration with numerous cloud products and services
- The freedom to manage risk without rules or regex
- A solution that's easy to deploy — sign up in 10 minutes, see value in days

Want to see for yourself, with your own data, how Concentric AI stands out and can work together with Purview? Contact us today.

