USE CASE

Better Together: DLP with Semantic Intelligence™ and Microsoft Purview

Between cloud apps, hybrid work, and a growing number of collaboration tools, corporate data is everywhere, and protecting it is more challenging than ever. It's being shared, copied, duplicated, and deleted: it's being leaked through insiders and misconfigurations, and it's being exfiltrated by attackers.

Data loss prevention (DLP) tools such as Microsoft Purview enforce the policies set up to protect data from breaches and compliance violations. But your DLP tool can only be as effective as your data discovery, categorization, and classification. If data hasn't been correctly classified to start with, this undermines the tool's capability to accurately enforce the policies you've set up to prevent unauthorized access or to ensure that the right people have access to the right data.

And while Purview is a powerful tool, it's also complex. It can be challenging for IT staff to formulate the proper queries for enforcement, and they often end up missing issues or generating too many false positives.

Data security governance tools such as Semantic Intelligence™ are designed to help organizations protect their most sensitive data by giving them insight into where the data resides, who has access, and how it's being used.

Missing the Mark

While your DLP tools do a bang-up job of preventing unauthorized users from accessing data labeled as sensitive, they're falling short when it comes to accurately identifying and classifying data in the first place.

They're unnecessarily denying access to data because it's been incorrectly classified as sensitive. Authorized users are increasingly frustrated and having to create workarounds just to do their job.

Productivity is taking a hit, and even with all this blocking, you're not confident you're stopping the actual threats from getting to your data.

Red Herrings and Dashed Security Dreams

You've got Microsoft Purview but implementing it is no walk in the park. You're overwhelmed trying to understand the regex and being blasted with so many false positives that it's making your head spin.

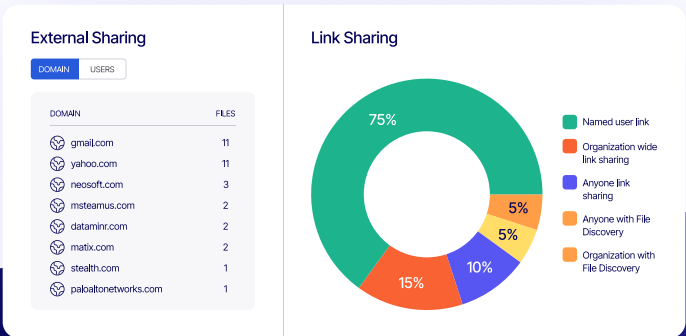
You need a partner that can help you get the most out of your DLP tool.

Elementary, My Dear Watson

Concentric AI's Semantic Intelligence™ platform and Microsoft Purview work together to deliver data security that is both strategic and proactive. Semantic Intelligence is like Sherlock Holmes—leaving no stone unturned as it diligently uncovers your data risks. Purview is more like Scotland Yard, using the findings to bring down the hammer and protect your data.

While it's true that DLP tools such as Purview can also discover and classify sensitive data, they're regex-based and not nearly as effective as our solution. We use context-driven discovery, categorization, and classification to understand exactly where your sensitive data resides and how it's being used. Purview acts on these insights, using classification labels that have been assigned based on a data record's sensitivity level to enforce policies in real time. Without these labels, it cannot effectively protect your data from being shared or accessed by unauthorized parties.

Say an authorized user sends an email containing PII to an unauthorized user. If our solution has previously labeled this data as sensitive, and if proper access policies for this level of classification are set up in Purview, then Purview will read the label and dynamically block the message from being transmitted.



Crocket and Tubbs for your DLP

It's not fast cars and designer duds, but Semantic Intelligence and Microsoft Purview do for your data what Miami Vice's dynamic duo did for South Beach in the 80s.

- **Maximize your ROI:** Get the most out of Purview with a strong foundation of discovery, categorization, and classification.
- **Protect against data loss:** Pair solutions that identify and secure your data in real time, whether it's at rest, in use, or in motion.
- **Apply appropriate controls:** Stay compliant by applying protections based on data sensitivity.
- **Maintain data privacy:** Stop PII and PHI from getting into the wrong hands.
- **No more alert fatigue:** Focus on real threats and not false positives.
- **Stop productivity roadblocks:** Protect your data without slowing down business.
- **Protect sensitive 0365 data:** Get solutions that support Microsoft Information Protection (MIP) sensitivity labels.
- **In-house expertise:** Get guidance navigating Purview's complexity.

About Concentric AI

Concentric AI is intelligent data security made easy. Semantic Intelligence™ discovers, categorizes, monitors, and protects data across cloud and on-premises environments. With AI-driven insights and co-managed services, the company helps businesses mitigate risk and streamline compliance through a single end-to-end platform, wherever their data lives and however it travels.

Contact us today to schedule a live demo and see for yourself how pairing Semantic Intelligence and Microsoft Purview helps you protect your most sensitive data.

Schedule a Demo