USE CASE

Semantic Intelligence for Data Classification

Data is no longer just information; in today's connected world, it's the new gold. Securing it is a top priority because when (not if) an organization suffers a breach, the financial, legal, and reputational consequences can be severe.

But protecting data that is sprawled across a diverse and distributed environment is easier said than done. Your team is tasked with managing and classifying your most sensitive data, but they aren't experts in every area of the business, so how can they be expected to understand every data record, what needs to be protected, and who should have access?

Delegating this task to the business units that do know the content, like sales or finance, is neither scalable nor reliable. Manual classification requires extensive training and is costly, time-consuming, and prone to error.

And there's also the need to ensure that protections align with business goals — too much control and productivity (and budget) takes a hit; not enough and data is unnecessarily exposed to risk.

Traditional rule-based methods don't factor in context, and this hikes up false positives. Some data records are over-classified, while others that contain sensitive data are assigned lower-than-appropriate classifications — or even skipped altogether, which puts the data at risk of falling into the wrong hands.

Garbage In, Garbage Out

The security tools that you're using to enforce data protection and access control, such as data loss prevention (DLP) and zero trust network access (ZTNA), rely on your data being accurately classified.

But you're running into problems because the tools you're using to classify your data are doing it based on key words or phrases without understanding context.

Limiting access to all data records containing payment card information (PCI) to the finance team isn't working because now sales is locked out of their accounts receivable documents, and they're not happy.

You need to be able to assign accurate classification labels that are based on data record type as well as on the sensitive data they contain.

A House Built on Sand Cannot Stand

Accurately classifying your data starts with a rock-solid understanding of what you have. But without the right solution, things could get a bit wobbly.

Concentric AI's patented technology makes classification easy by contextually discovering and categorizing the data in your environment.

The Wind Beneath Your Classification Wings

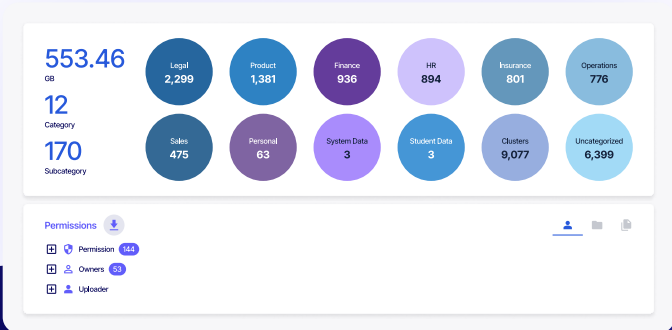
Before you can assign classifications, you need to know, with a high degree of confidence, exactly what type of sensitive data you have.

Concentric AI's Semantic Intelligence platform uses patented deep learning technology to contextually discover and thematically categorize your structured and unstructured data. And it does this without relying on end users, agents, or complex regex-based policies.

While other tools use pattern recognition to tell you that a data record contains PCI, PII, or PHI, they can't tell you what type of document it is. But our platform can do this. It will find your business-critical data — your sales plans, and your go-to-market strategy, your source code and competitive intelligence — because it understands context.

Once you know exactly what type of document you have, you can accurately classify documents and create access policies based on the type of data record they are instead of on a sample of their content.

Our platform also uses built-in Microsoft Purview Information Protection (MIP) sensitivity labels to protect data within the Microsoft 365 ecosystem. It can also read and apply labels from several other classification frameworks, including Google, AWS, and Box.



Precision and Confidence Over Pattern-Matching

You can't have accurate classification without intelligent data discovery and categorization. We help you understand the sensitivity level of every data record you have, so you can confidently assign the correct protections.

- **Minimize classification errors:** Get accurate classifications that neither expose sensitive data nor restrict access for authorized users.
- **Roadmap for accuracy:** New data records that are semantically similar are automatically classified in line with policies.
- **Monitor your risks:** See your unclassified and misclassified data records in one view with custom risk tiles.
- **Ace your audits:** Identify and remediate issues such as incorrect classification before the auditors show up.
- **Support zero–trust:** Reduce the risk of data breach and insider threat with classification that supports your access controls.
- **Seamlessly integrate:** Read and apply labels from other classification frameworks.

About Concentric AI

Concentric AI is intelligent data security made easy. Our platform discovers, classifies, monitors risk, and protects data across cloud and on-premises environments. With AI-driven insights and co-managed services, we help businesses reduce risk, streamline compliance, and eliminate duplicate data records — transforming data from a liability into a well-managed asset.

Contact us today to schedule a live demo and see for yourself how we can help protect your most sensitive data with accurate classifications based on context-driven discovery and categorization.

Schedule a Demo