USE CASE

Data Classification

Not All Data Is Created Equal

Organizations generate millions of data records, but not all deserve the same level of protection. A routine business document, a customer record, and a confidential piece of intellectual property may sit side by side, even though mishandling each can have very different consequences.

And the data doesn't sit still. New information is constantly created, copied, modified, and shared across cloud, SaaS, and on-premises environments. As AI applications consume more enterprise data, knowing which information is sensitive has become even more important.

That makes accurate classification increasingly difficult. Security teams can't manually keep up with millions of records, while traditional approaches based on keywords, regex, and manually assigned labels can miss the nuances that make one piece of information more sensitive than another.

When the labels are wrong, or missing altogether, the security controls that depend on them can be wrong, too.

Labels Are Only Useful If They're Accurate

There is simply too much data. The volume of information being created across the enterprise makes manual classification difficult to scale.

Important details get missed. Keywords and patterns can identify what's in a file without understanding what the information means or why it matters.

Labels can fall behind. Data changes, moves, and gets created every day. Classifications need to keep pace.

Downstream controls depend on accuracy. When sensitive information is mislabeled or not labeled at all, policies, DLP, compliance efforts, and other security controls become less effective.



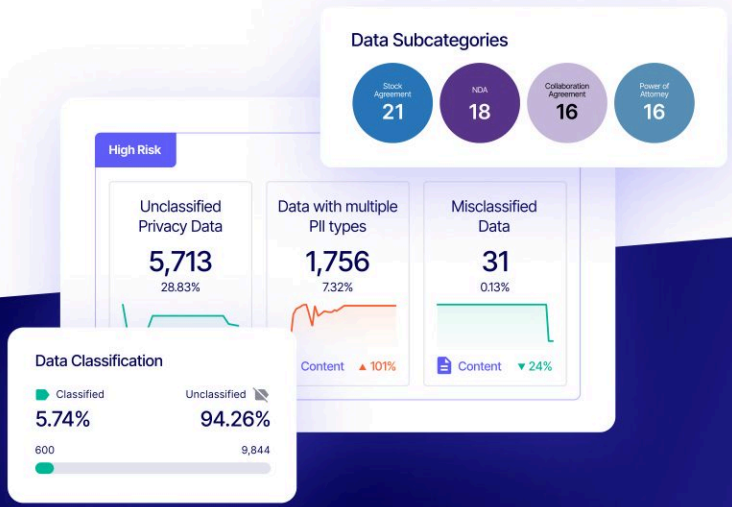
You Need Classification That Keeps Up

Accurately identify and label data based on its meaning, sensitivity, and business value, so the right policies and controls can follow the data wherever it goes.

Classification That Understands Context

Concentric AI automatically classifies and labels enterprise data using patented language models that look beyond keywords and patterns to understand what information a record contains, what type of data it is, why it matters, and how it should be handled. That semantic understanding enables accurate, consistent classification across structured and unstructured data without the manual effort of building and maintaining extensive rules or custom classifiers.

- **Classify data across your environment.** Identify and label sensitive and business-critical information across cloud, SaaS, and on-premises environments, including regulated data, intellectual property, financial information, legal documents, HR information, source code, and more.
- **Keep classifications current.** Continuously update sensitivity labels as data changes, moves, and is created, so classifications don't become stale as the environment evolves.
- **Work with the frameworks you already use.** Use built-in Microsoft Purview Information Protection (MIP) sensitivity labels to protect data across Microsoft 365, while reading and applying labels from other classification frameworks, including Google, AWS, and Box.
- **Enable enterprise-scale classification.** Autonomously classify millions of records without the manual effort required to build and maintain extensive regex libraries, rules, or custom classifiers.



Put Better Labels to Work

Accurate classification gives the rest of your security and governance program better information to work with:

Strengthen security controls with policies informed by meaningful data context, helping protect sensitive information without unnecessarily restricting legitimate access.

Reduce manual effort by eliminating time-consuming classification projects and ongoing maintenance.

Improve compliance by consistently identifying regulated and sensitive information across the enterprise.

Maximize existing investments by giving DLP, Microsoft Purview, and other security technologies richer data intelligence.

Accelerate safe AI adoption by understanding which information is appropriate for AI use and where additional safeguards are needed.

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