USE CASE

# Data Discovery

## Your Data Has a Social Life

The way organizations create, share, and use data has fundamentally changed. Data rarely stays where it was created. It gets copied, modified, shared, moved between systems, and tucked away in places no one remembers to check. And now, copilots, chatbots, and other AI applications are becoming new destinations for enterprise information.

As data spreads across cloud, SaaS, and on-premises environments, tracking it becomes a moving target. Millions of files can contain everything from customer and financial information to intellectual property and business-critical documents. Some are sensitive. Some are duplicates. Some are stale. Others may look similar but serve very different business purposes.

The more data an organization accumulates, the harder it becomes to see the bigger picture. What data do you have? Where does it live? Which of it matters? And what might be hiding in plain sight?

Without that clarity, security teams can spend valuable time sorting through findings, trying to separate meaningful risks from everything else.

### Too Much Data. Too Little Clarity.

**Critical information gets buried.**
Sensitive and business-critical data can disappear into the sheer volume of information organizations accumulate.

**Risk is difficult to prioritize.**
Without understanding the data, it is hard to distinguish meaningful exposure from a finding that poses little real risk.

**Investigations take time.**
Every low-risk finding that demands attention is time taken away from the exposures that truly matter.

**AI raises the stakes.**
As more enterprise data flows into AI applications, understanding what information exists and where it resides becomes increasingly important for safe AI adoption.

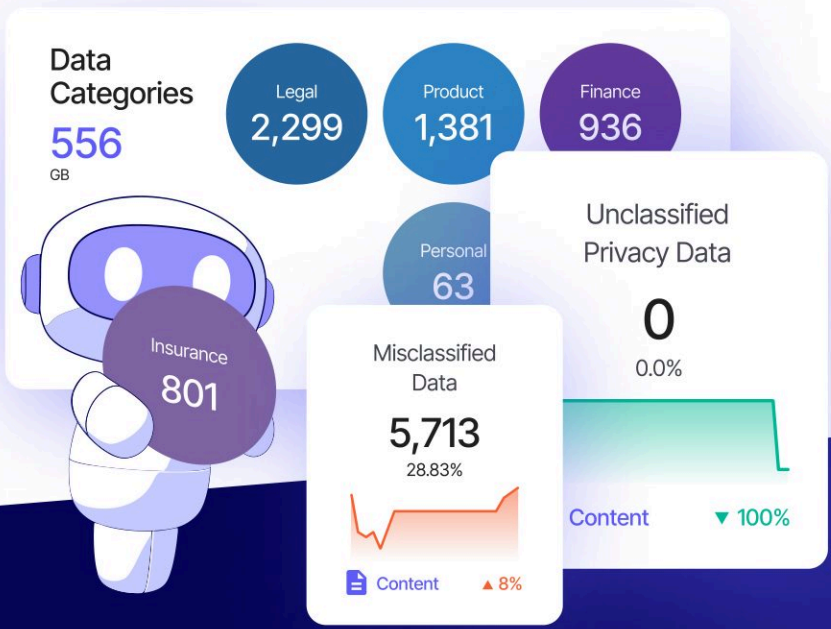
## You Need a Clearer Picture

Discover, understand, and prioritize the data that matters most, giving your team the insight to turn data overload into informed security decisions.

# From Chaos to Clarity

Concentric AI discovers sensitive and business-critical data wherever it resides, using patented language models to understand its meaning, context, and business impact. Rather than relying solely on pattern matching, manual labels, or trainable classifiers, Concentric AI uses semantic understanding to distinguish important information from noise, explain why it matters, and determine where to apply security controls.

- **Discover data across your environment.** Identify sensitive and business-critical information in both structured and unstructured data across cloud, SaaS, and on-premises environments. This includes regulated data, intellectual property, financial information, legal documents, customer records, source code, HR data, and more.
- **Put data in context.** Go beyond where the information resides to understand its sensitivity, meaning, business value, and associated risk.
- **Prioritize what needs attention.** Focus on the exposures that matter most and spend less time investigating findings that pose minimal risk.




## When You Know Your Data, Everything Works Better

A clearer understanding of your data gives your organization a stronger foundation to:

**Reduce risk** by focusing security efforts on the data and exposures that matter most.

**Strengthen compliance** by identifying regulated information and improving data governance.

**Maximize existing security investments** by providing better data intelligence for DLP, Microsoft Purview, and other security controls.

**Accelerate safe AI adoption** by understanding what sensitive information exists and where additional safeguards may be 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