USE CASE

AI Readiness

Your AI Ambition Needs a Strong Data Foundation

AI adoption is moving quickly. Organizations are experimenting with copilots, assistants, and other AI capabilities to work faster, automate tasks, and put more information to work. But before AI can safely make use of enterprise data, organizations need to understand their data themselves.

That can be harder than it sounds. Sensitive, proprietary, and business-critical information is spread across cloud, SaaS, and on-premises environments. Data is constantly created, copied, modified, and shared. But information appropriate for one purpose may not be appropriate for another.

Security and IT teams need a clear picture of what information exists, where it resides, how sensitive it is, and what needs protection before AI initiatives scale. Without that foundation, organizations can find themselves trying to answer fundamental data questions after AI adoption is already underway.

The goal isn't to slow AI down. It's to make sure the data is ready to move with it.

AI Ambition is Outpacing Data Readiness

You don't know what you don't know. Sensitive and business-critical information can be scattered across the enterprise, making it difficult to determine what data exists and where it resides.

Not all data is AI-ready. Information varies in sensitivity, business value, ownership, and regulatory requirements. Not everything should be automatically made available for AI use.

Data doesn't stay put. New information is constantly created, while existing data is copied, modified, and moved across the environment. A point-in-time assessment can quickly become outdated.

The foundation matters. AI initiatives depend on knowing what data exists and how it should be handled. Without that understanding, governance decisions are made without the full picture.

You Need to Know Your Data Before AI Does

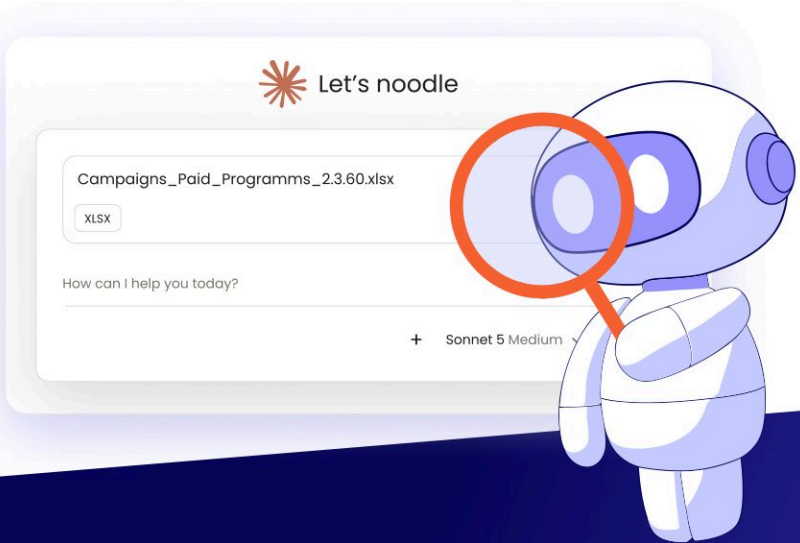
Understand the data behind your AI initiatives so you can determine what is appropriate to use, what needs protection, and where stronger governance may be needed.

Give AI the Context It Needs

Concentric AI helps organizations prepare their data for AI adoption by discovering and understanding sensitive, business-critical, and proprietary information across the enterprise.

The Semantic Intelligence™ Engine looks beyond where data resides to understand its content, sensitivity, business value, and context. That gives security and IT teams the data intelligence they need to make informed decisions about how information should be used and protected as AI adoption expands.

- **Discover what you have.** Identify sensitive, business-critical, and proprietary information across cloud, SaaS, and on-premises environments, giving teams a clearer picture of the data available to support AI initiatives.
- **Understand what matters.** Put data in context by assessing its sensitivity, meaning, business value, and relevance—not simply where it resides.
- **Identify what needs protection.** Determine which data requires stronger controls based on its sensitivity, business importance, and potential impact.
- **Keep your data picture current.** Continuously monitor data as it is created and changes, so AI readiness evolves with the environment rather than relying on a one-time assessment.



Move From AI Curiosity to AI Confidence

A clearer understanding of your data helps organizations:

Accelerate AI adoption by equipping teams with the data intelligence needed to move forward with greater clarity.

Reduce data risk by identifying sensitive and business-critical information before AI initiatives scale.

Make better governance decisions by understanding what data exists, where it resides, and how to manage it.

Prepare for what comes next with a data foundation that can evolve as AI adoption—and the data supporting it—expands.

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