USE CASE

Insider Threat

Your Data Has New Ways Out

The way people access, share, and use information has changed dramatically.

Employees, contractors, partners, and AI applications interact with sensitive data every day. Downloads, shares, uploads, and copies happen faster than traditional controls can keep pace.

And risk doesn't always look risky. A routine action can become a serious exposure, depending on the data involved.

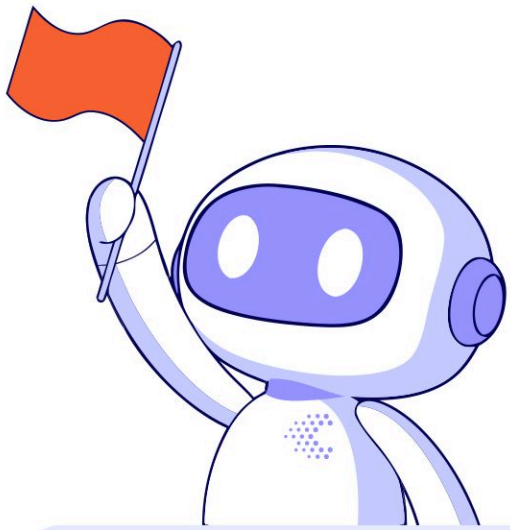
An employee downloads a few files to work from home.

A contractor shares a folder with a partner.

Someone uploads a document to an AI application for a little help with a project.

A user moves a collection of files to a location where they can work with them more easily.

On their own, these actions may seem completely ordinary. But when sensitive data is involved, ordinary behavior can have serious consequences.



Insider Risk Isn't Always Intentional

Everyday actions can create exposure. Employees may share, download, or upload sensitive information simply to get their jobs done—but the same activity can also signal deliberate misuse when someone is leaving the organization or otherwise acting outside their role.

Warning signs hide in the noise. Unusual activity means little if you don't understand the data involved.

Context changes everything. Without knowing which data is at risk, security teams struggle to distinguish normal behavior from real threats.

You Need Context Behind the Behavior

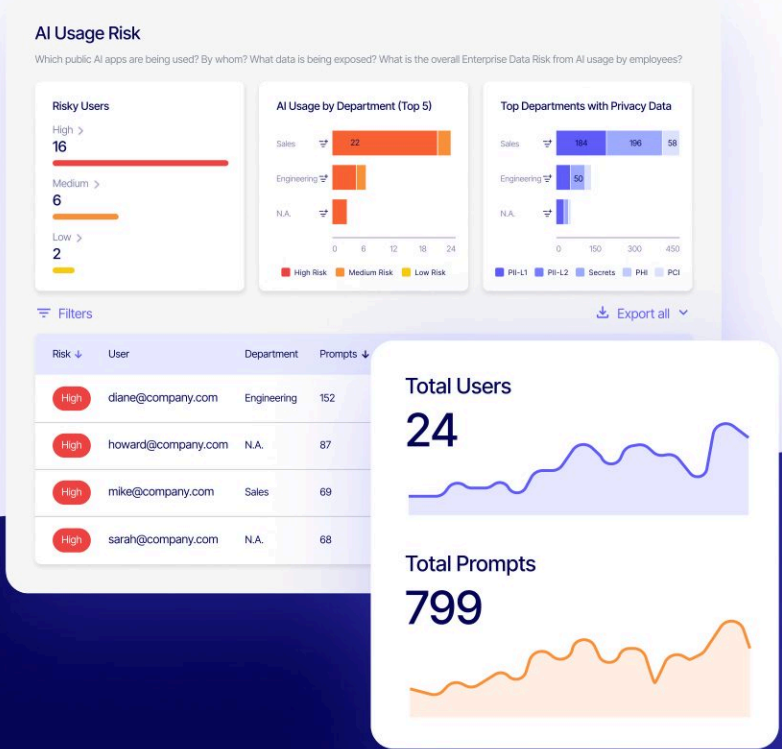
Understand who is interacting with data, what they're doing, and which data is involved, so your team can focus on the activity that poses meaningful risk.

Connect the Dots Between Data and Behavior

Concentric AI combines user activity with an understanding of the data to identify risky interactions and provide security teams with the context they need to focus on what matters.

The Semantic Intelligence™ Engine understands the sensitivity, meaning, and business importance of the data, so unusual behavior can be evaluated alongside the data involved rather than treated as a threat in isolation.

- **Understand user behavior.** Identify anomalous activity such as excessive downloads, unusual sharing, suspicious deletions, and unexpected data movement.
- **Know what data is at risk.** The Semantic Intelligence™ Engine reveals whether activity involves sensitive, regulated, or business-critical information.
- **Prioritize meaningful threats.** Focus investigations on activity that creates real exposure, whether the behavior is accidental, unusual, or intentional.



Reduce Risk Without Slowing the Business

Better context helps your organization:

Catch risky behavior earlier by identifying potential insider incidents before sensitive information moves beyond your control.

Reduce investigation time by quickly understanding who did what, when they did it, and what data was involved.

Protect sensitive information across the ways people work, with visibility into file sharing, email, cloud applications, and AI workflows.

Enable productive collaboration by protecting critical data without treating normal workplace activity as a threat.

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