USE CASE

CONCENTRIC

Concentric AI for Data Detection and Response

Technology is evolving and driving real gains in productivity and efficiency. Today, users can access data from anywhere, collaborate in real time, and use AI insights to inform their decisions. But innovation also introduces risk.

New tools are expanding how information is created, shared, and stored, but as systems become more interconnected and as data multiplies across cloud and on-prem environments, security teams are struggling to keep track of who's doing what to their sensitive data.

Many organizations don't have visibility into their data. They don't know where it is, what's being done with it, or which AI tools it's being shared with. Without insight into how users are interacting with data, security teams can't tell when access, movement, sharing, or download behavior doesn't match normal usage patterns.

This means they can't protect their most sensitive data from external threats, insider threats that hide in plain sight, or legitimate users who unintentionally expose it to risk. They can only react after the data has been compromised.

The Red Flags You Missed

Your data is constantly exposed to risk—whether deliberate or inadvertent. From the attacker who used stolen credentials to exfiltrate company IP to the ex-employee who downloaded customer records before leaving, and the current employee who accidentally pasted sensitive data into ChatGPT.

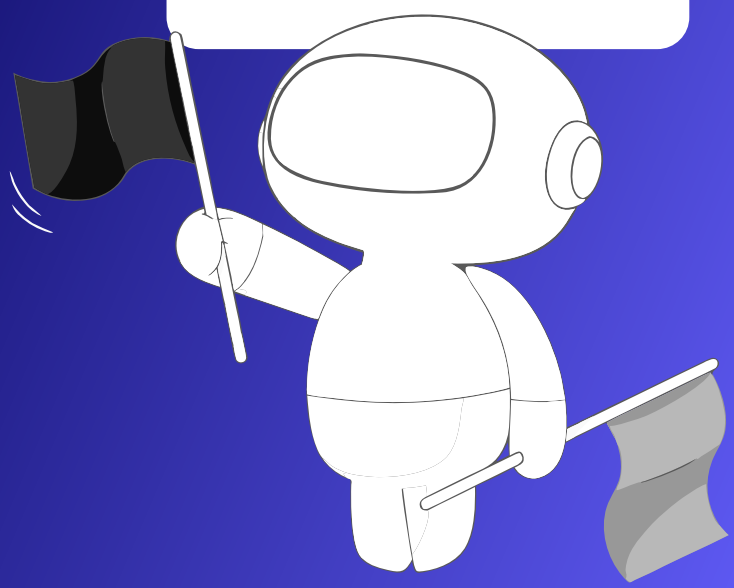
Alarm bells should have sounded for all these actions, but they didn't.

Whether it's intentional or just a big whoops, you need to be able to spot sketchy behavior as it happens, and you need a detailed timeline of every edit, copy, and download, so you don't just have suspicions, you have proof.

Bad Intentions and Epic Blunders

Data is constantly at risk from malicious actors and even from well-intentioned employees who make honest but costly mistakes. But while these risks are inevitable, data loss shouldn't be.

A solution that tracks every interaction and flags anomalous activity in real time will help you ensure your data doesn't slip through the cracks.



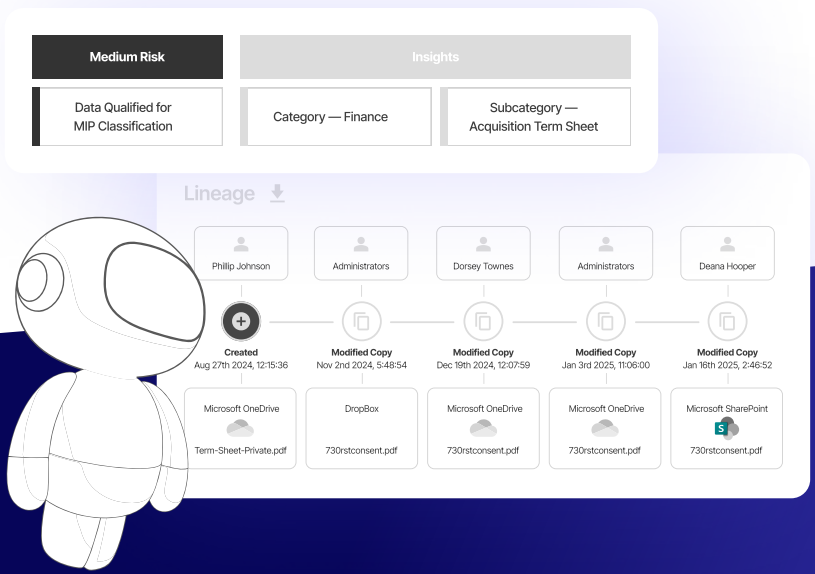
Catch Your Data Curveballs

Concentric AI's AI and data security governance solutions continuously monitor and alert on anomalous data activity so you can zero in on data threats in real time—the risky sharing, the excessive downloads, the unusual access, the data leaked to GenAI tools—all of it.

The user behavior data analytics UBDA feature in the Semantic Intelligence™ platform leverages contextual discovery and categorization to connect abnormal user activity to specific data categories and then create actionable risk alerts based on the activity.

The platform's data lineage feature provides comprehensive insights into how data is moving across your organization, who's accessing it, and what they're doing with it—every view, edit, download, and share. The feature's audit trail of access and usage shows regulators how data is handled, processed, and stored, and radically simplifies reporting.

The Semantic DLP product shows you all the AI tools being used at your organization—sanctioned and unsanctioned. It logs every prompt, response, and policy violation, giving forensic teams the in-depth insights they need when there's an investigation.



Stay Ahead of the Game

Know exactly who accessed your data and what they did with it, so you can act before any damage is done.

Get real-time actionable alerts: See anomalous user activity as it relates to sensitive data.

Proactively secure data: Stop risky sharing, flag unusual access, block large downloads of sensitive data to personal accounts, and prevent sensitive data from being leaked to GenAI applications.

Mitigate insider risk: Ensure offboarded employees don't leave with company IP.

Identify and remediate risks fast: Accelerate investigations with deep, AI-driven data context.

Support compliance goals: Stay audit-ready with continuous monitoring, comprehensive reporting, and full data lineage.

About Concentric AI

Concentric AI is intelligent data security made easy, helping businesses discover, understand, and protect sensitive information across cloud and on-prem environments. Its AI-powered data security governance solutions deliver precise visibility, automated protection, and safe AI adoption—so organizations can reduce risk, strengthen compliance, and confidently innovate without compromising what matters most.

Contact us today to schedule a live demo and see for yourself how we can help you spot and stop risky behavior before your most sensitive data is compromised.

Schedule a Demo