Mapping Concentric AI Capabilities to the Gartner AI TRiSM

Recently, Concentric AI was named a Representative Vendor in the Gartner Market Guide for AI Trust, Risk and Security Management (AI TRiSM). Here's how our AI and data security governance capabilities map to TRiSM's key functional technology layers to provide the visibility and context organizations need to understand their data and establish guardrails for safe AI adoption.

AI Governance

AI Runtime Inspection and Enforcement Systems

(AI applications)

Continuous monitoring of and guardrails for public AI usage

- Dynamic discovery and inline contextual categorization of data
- Identification of all public AI usage, including sanctioned or shadow AI, allowing security teams to either create policies that prevent the sharing of sensitive information or to block the apps altogether using other network-based security tools
- Automatic warning, blocking, or redacting when sensitive data is shared with public AI
- Detection of enterprise policy violations such as sensitive data being shared in prompts or uploads with capability to export conversation histories detailing complete text of every user prompt and corresponding model response
- Mapping of data flows to and from AI tools with high-level dashboards tracking sensitive data movement across departments and showing highest-risk AI applications and users

Tracking and policy enforcement for enterprise Copilots and Cowork

- Dedicated risk tiles identify which data records Microsoft Copilot can access
- Activity monitoring shows what data Copilot shared, with whom, and when
- Reveals what permissions Microsoft Copilot, ChatGPT Enterprise, Claude Enterprise, and other AI tools are inheriting and using to access data
- Capability to set and enforce policies to enforce role-based access and ensure sensitive ensure sensitive data is not being exposed to unauthorized users or AI tools

Information Governance

- Full visibility into and control over data throughout its life cycle to enable establishment of trusted data foundations for AI
- Context-aware discovery, classification, permissioning, and access control ensure sensitive data is not accessed by unauthorized users or shared with AI tools
- Continuous monitoring to identify and autonomously remediate risks such as classification issues, excessive permissions, unauthorized access, risky sharing, sensitive data exposure
- Integration with other security tools and cloud APIs to streamline remediation
- Automated retention policies ensure duplicate and stale data is retained, archived, or deleted
- Comprehensive data lineage capabilities for full record of data access and usage
- Built-in Compliance Dashboard delivers clear insights into adherence to relevant AI regulations such as PCI-DSS, HIPAA, GDPR
- Continuous monitoring of entitlements and autonomous enforcement of zero-trust access policies to ensure users have only permissions required for their roles

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.

Schedule a Demo