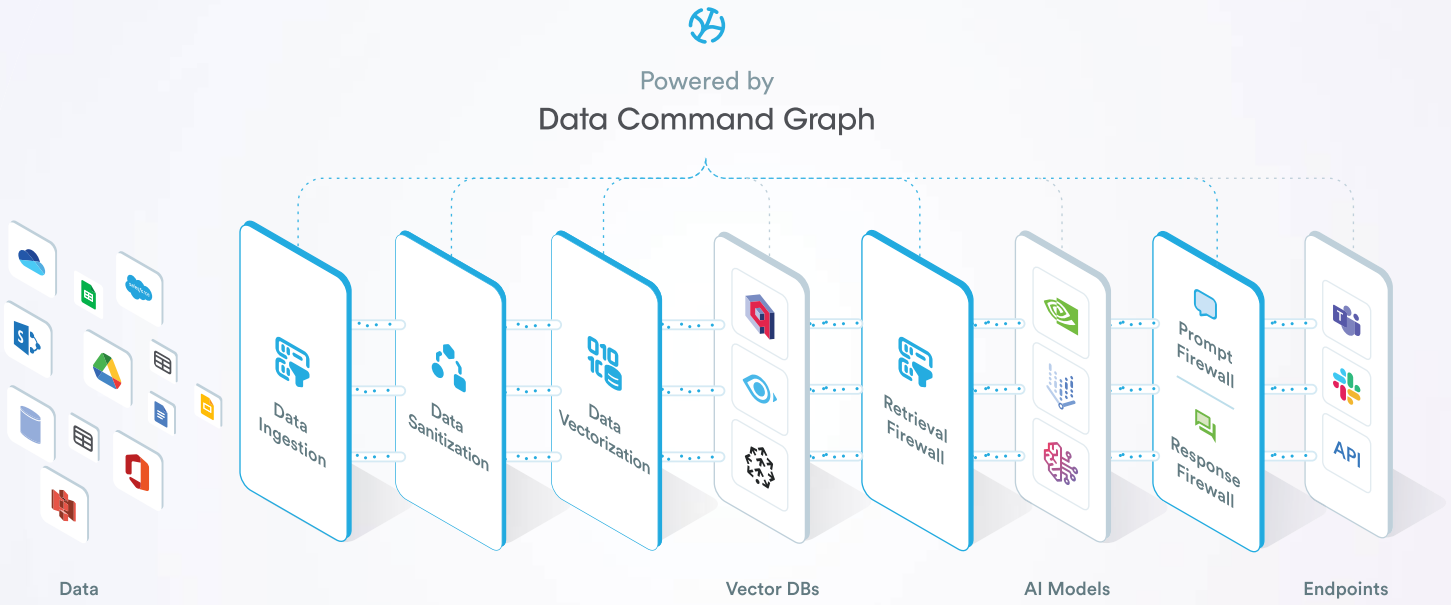
gencore AI

Build Safe Enterprise AI

Build safe, enterprise-grade AI systems, copilots, and agents using your proprietary data—in minutes



As enterprises adopt generative AI, data and AI teams face numerous hurdles: securely ingesting unstructured and structured data, maintaining proper controls and governance, preventing malicious attacks, and ensuring visibility across AI systems.

Gencore AI enables businesses to build safe, enterprise-grade AI systems, copilots, and agents within minutes by leveraging proprietary data across various systems and applications.

sales@gencore.ai

www.gencore.ai

Key Capabilities

Build Safe Enterprise AI Copilots

Create AI copilots and knowledge systems by combining data from multiple systems in minutes. Automatic enterprise controls, AI usage monitoring, and full provenance tracking ensure safety and transparency.

Safely Sync Data to Vector Databases

Securely ingest and sync data at scale from various systems. Create custom embeddings with metadata for vector databases, preparing enterprise data for LLM usage.

Curate & Sanitize Data for Model Training

Easily assemble, cleanse, and sanitize high-quality datasets for AI model training and tuning.

Protect AI Interactions

LLM Firewall moderates AI interactions, aligning with enterprise policies, preventing sensitive data leaks, and guarding against prompt injections and jailbreaking attempts.

Key Features

Data Selection & Ingestion

Safely ingest data using hundreds of native connectors. Define data scope and automatically learn enterprise controls, including access entitlements, for later application at the AI usage layer.

Data Extraction & Normalization

Process diverse file formats, including unstructured data, extracting and parsing information while maintaining context and relationships for enhanced vector DB comprehension.

Data Classification & Sanitization

Classify and redact sensitive data on-the-fly, ensuring privacy and compliance before AI model ingestion.

Data Vectorization

Create custom embeddings with metadata for vector databases using an embedding model of your choice, preparing enterprise data for LLM use.

LLM Selection

Select from a wide range of large language models (LLMs) to build an AI system that aligns with the business goals and operational requirements for a specific use case.

LLM Firewalls

Protect AI interactions with natural language conversation-aware firewalls. Implement policies to block attacks, prevent data leaks, and maintain corporate alignment.

AI System Provenance

Visualize sensitive data flow and generate audit trails. Map interrelations between data, AI models, entitlements, AI agents, and governance controls.

Ready to Build Safe Enterprise AI? Visit

gencore AI

sales@gencore.ai

www.gencore.ai