IronCore Labs Launches VectorLens to Help Security Teams Find Hidden PII in AI Vector Embeddings

New local CLI tool scans vector embeddings directly, helping privacy, security, and GRC teams discover sensitive data in RAG AI pipelines

IronCore Labs: Lock Your-Data. Unlock Your AI.

BOULDER, CO, UNITED STATES, June 30, 2026 /EINPresswire.com/ -- IronCore Labs, a data security company focused on application-layer encryption for sensitive data and AI, today announced the availability of VectorLens, a private command-line tool that scans AI vector embeddings locally to discover and classify personally identifiable information (PII) and other sensitive data hidden inside vector databases.

Vector embeddings power semantic search, Retrieval-Augmented Generation (RAG), AI assistants, recommendation systems, and other modern AI workflows. Although embeddings appear to be meaningless arrays of numbers, they contain approximate copies of the source data used to create them. As organizations adopt AI more broadly, those embeddings can become unsecured copies of customer records, documents, support tickets, HR data, financial information, health information, and other regulated data.

> AI systems are creating new copies of sensitive data faster than security and governance teams can track them, VectorLens gives teams a way to track the PII hiding inside vector embeddings."
>
> *Patrick Walsh, CEO*

VectorLens helps teams answer a question that other data security tools cannot: what sensitive data is already sitting inside the vectors themselves?

"AI systems are creating new copies of sensitive data faster than security and governance teams can track them," said Patrick Walsh, CEO and co-founder of IronCore Labs. "VectorLens gives

teams a way to look directly at their vector embeddings, quantify the PII hiding there, and decide what needs to be monitored, governed, or encrypted."

Unlike text-first data discovery and DSPM tools that require access to the original source text or depend on labels applied before embeddings are created, VectorLens scans exported vectors directly. That means teams can inspect orphaned, imported, unlabeled, or unmanaged embeddings even when the original source data is unavailable.

VectorLens runs locally on macOS and Linux as a self-contained binary. Users export embeddings from their vector database, run a scan, and receive a report showing which vectors contain sensitive data. The tool can generate inline output, machine-readable JSON, or a polished PDF report for security, privacy, compliance, and executive stakeholders. VectorLens works with any vector store that can export vectors to JSONL or Parquet, including Pinecone, Weaviate, Milvus, Qdrant, Elastic, and Postgres/pgvector.

At launch, VectorLens supports common embedding models including all-minilm-l6-v2, bge-m3, gtr-t5-base, text-embedding-ada-002, and text-embedding-3-large, with additional model support planned. It can classify categories such as names, email addresses, phone numbers, physical addresses, dates of birth, credit card numbers, social security numbers, numeric identifiers, and other sensitive content.

Because VectorLens runs in the customer's own environment, IronCore Labs never sees the vectors or private data being scanned. The tool only performs lightweight network calls for license validation and high-level usage metrics.

AI shadow data is a growing problem. VectorLens helps organizations identify exposure, catch regressions, audit unmanaged vector databases, support AI governance, and decide when vector encryption is appropriate.

VectorLens is available now and free to try. Teams can learn more, request a license key, and start scanning vectors at the IronCore Labs website.

About IronCore Labs

IronCore Labs builds application-layer encryption and data control tools for companies that need to protect sensitive data in SaaS, search, and AI systems. Its products help engineering teams build privacy-preserving applications with capabilities such as customer-managed keys, encrypted search, tenant-level data controls, and vector encryption for AI workflows. By preventing data leakage and insider risk, IronCore helps businesses stay ahead of threats, differentiate on security features, meet global privacy regulations and adopt AI with confidence.

PR Liason
IronCore Labs

pr@ironcorelabs.com
Visit us on social media:
LinkedIn
YouTube
X
Other
