

SecuPi Introduces Data Security Platform for Self-Hosted AI

On-premises, private-cloud, VPC and air-gapped options protect sensitive data in AI workflows while meeting privacy, compliance and sovereignty requirements.



SecuPi

Data Security Platform for the AI Era

NEW YORK, NY, UNITED STATES,
September 15, 2026 /

EINPresswire.com/ -- SecuPi today announced its Data Security Platform for self-hosted AI environments, helping organizations protect sensitive data from preparation and retrieval through inference and agent actions. The platform controls what humans and AI agents can access, see, and do while keeping data and security controls within customer-controlled infrastructure.

“

Keeping an AI model inside your environment is only the first step. You also need to control the sensitive data it can access and the actions agents can perform.”

Alon Rosenthal, CEO, SecuPi

SecuPi combines runtime attribute-based access control (ABAC), real-time monitoring of sensitive-data activity, a kill switch to block malicious agent activity, and field-level protection through format-preserving encryption (FPE), tokenization and dynamic masking.

Banks, healthcare organizations, government agencies and other regulated enterprises are adopting self-hosted AI to maintain control over sensitive information, proprietary

knowledge and infrastructure. However, hosting an AI model internally does not, by itself, prevent unauthorized access, rogue agent actions or excessive exposure of sensitive data. Organizations still need to govern which information each user or agent can retrieve, which sensitive details it can see and which actions it can perform.

SecuPi addresses this challenge by enforcing data access policies in real time across databases, data lakes, files, applications and analytics platforms. It applies fine-grained authorization at the object, table, row, column and field levels, as applicable to the data source, helping ensure that AI workloads receive only the information authorized for a legitimate business purpose.

“Keeping an AI model inside your environment is only the first step. You also need to control the

sensitive data it can access and the actions agents can perform,” said Alon Rosenthal, CEO and co-founder of SecuPi. “SecuPi brings runtime access control, encryption, privacy protection and real-time auditability to self-hosted AI, even when models, data and security controls must remain entirely within an air-gapped environment.”

Data protection within customer-controlled environments

SecuPi can be deployed alongside self-hosted AI models in on-premises data centers, customer-controlled private clouds and virtual private clouds (VPCs), or air-gapped and “dark-room” environments. Organizations can apply consistent security policies within approved geographic and operational boundaries.

The platform provides:

Field-level data protection: Apply FPE, tokenization, dynamic masking and redaction to limit sensitive-data exposure while preserving data formats where required.

AI data preparation: Discover and automatically de-identify sensitive information before it is used in training, retrieval, inference or analytics.

Real-time monitoring and blocking: Monitor data activity, analyze behavior and block agent activity that violates policy.

Identity and auditability: Link agent activity to the human on whose behalf it is performed and maintain tamper-resistant records of data access and actions.

Centralized policies: Apply consistent controls across structured and unstructured data in supported enterprise systems.

Together, these capabilities help organizations make sensitive data available for authorized AI use while maintaining control over its exposure and use.

Enforcement across enterprise data sources

SecuPi applies controls where data is accessed and processed. Its enforcement architecture includes transparent instrumentation agents, database and API gateways, and integration interfaces such as APIs, SDKs, user-defined functions (UDFs) and command-line tools.

Supported integration points span agent connectivity through Model Context Protocol (MCP) servers, data pipelines using Spark, Kafka, NiFi and Python, and query and database environments including Hive, PostgreSQL, MongoDB and Trino. Organizations can select the enforcement components appropriate to their infrastructure, including environments that must operate entirely within isolated networks.

This architecture supports protection across AI workflows, including data preparation, retrieval-augmented generation (RAG), inference and agent actions. It enables organizations to enforce access restrictions and protect sensitive fields before retrieved information reaches the model, while governing subsequent access to enterprise systems.

SecuPi complements existing data catalogs, identity providers, security tools and AI governance platforms, translating governance context and access policies into runtime enforcement.

About SecuPi

SecuPi is a Data Security Platform for the AI Era, helping global enterprises control what AI

agents and users can access, see, and do across data platforms, databases, data lakes, files and applications. Recognized as a Gartner Cool Vendor, SecuPi provides fine-grained authorization, real-time monitoring, sensitive-data discovery, de-identification, format-preserving encryption, tokenization and dynamic masking.

SecuPi serves organizations across financial services, healthcare, telecommunications, manufacturing and other data-sensitive industries. The platform supports on-premises, customer-controlled cloud and air-gapped deployments.

For more information, visit www.secupi.com.

Deena Moskovitz

SecuPi

[email us here](#)

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/942399425>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.