Nullafi's New AI Data Firewall: Unleash the Full Power of AI Without Ever Exposing Your Sensitive Data

Overview

The Nullafi AI Data Firewall is a new, groundbreaking cipher/decipher technology designed to allow organizations to leverage the full power of Large Language Models (LLMs) and AI agents without ever exposing sensitive, underlying data to them. By treating these tools as restricted users, Nullafi ensures that sensitive information is never accessed, processed, or stored, effectively eliminating the compliance, privacy, and security risks associated with AI usage.

How It Works

Nullafi uses a patent-pending, stateless, deterministic cipher process that preserves the analytic capabilities of the AI without letting it see or interact with the underlying sensitive data. The mechanism relies on a sophisticated, reversible process that maintains the utility of the data for the AI while keeping it secure.

- **In-Transit Processing:** When a user interacts with an AI agent or model, Nullafi detects and classifies sensitive data as it is uploaded or prompted. Sensitive data is masked and tokenized before it reaches any model.
- **Ciphered Data Analysis:** The AI tools (LLMs, apps, agents, assistants) operate entirely on the ciphered text. They can still perform complex tasks, such as summarizing a document or identifying material elements – such as contract terms or PCI data – despite the sensitive data being ciphered.
- **Deciphering on Consumption:** Once an AI tool generates a response, Nullafi deciphers the data on the way out to the end user. This makes the security layer completely invisible to the person receiving the information, while keeping the AI tools blind to the organization's sensitive data.
- **Stateless, Reversible, and Deterministic:** The cipher is reversible, so the original data can be recovered whenever needed, without Nullafi having to store the underlying data at all. Because it is deterministic, the same input always produces the same cipher value. This allows the AI to perform complex lookups, associate records, and analyze patterns without ever knowing the actual content.

Key Features

To ensure total data security while maintaining the full utility of AI tools, the Nullafi AI Data Firewall is built upon a foundation of versatile data handling, precise security management, and seamless technical integration.

- **Universal Data Support:** The firewall handles both structured data (such as relational databases) and unstructured data (such as non-SQL databases and documents).
- **Granular Access Control:** Security teams can set specific permissions to determine which users are authorized to see deciphered data in the final AI output and which should only see the masked versions.
- **Rapid Integration:** The capability is designed for automated deployment within existing cloud environments like GCP, AWS, and Azure, and easily integrates with major commercial databases and AI tools.

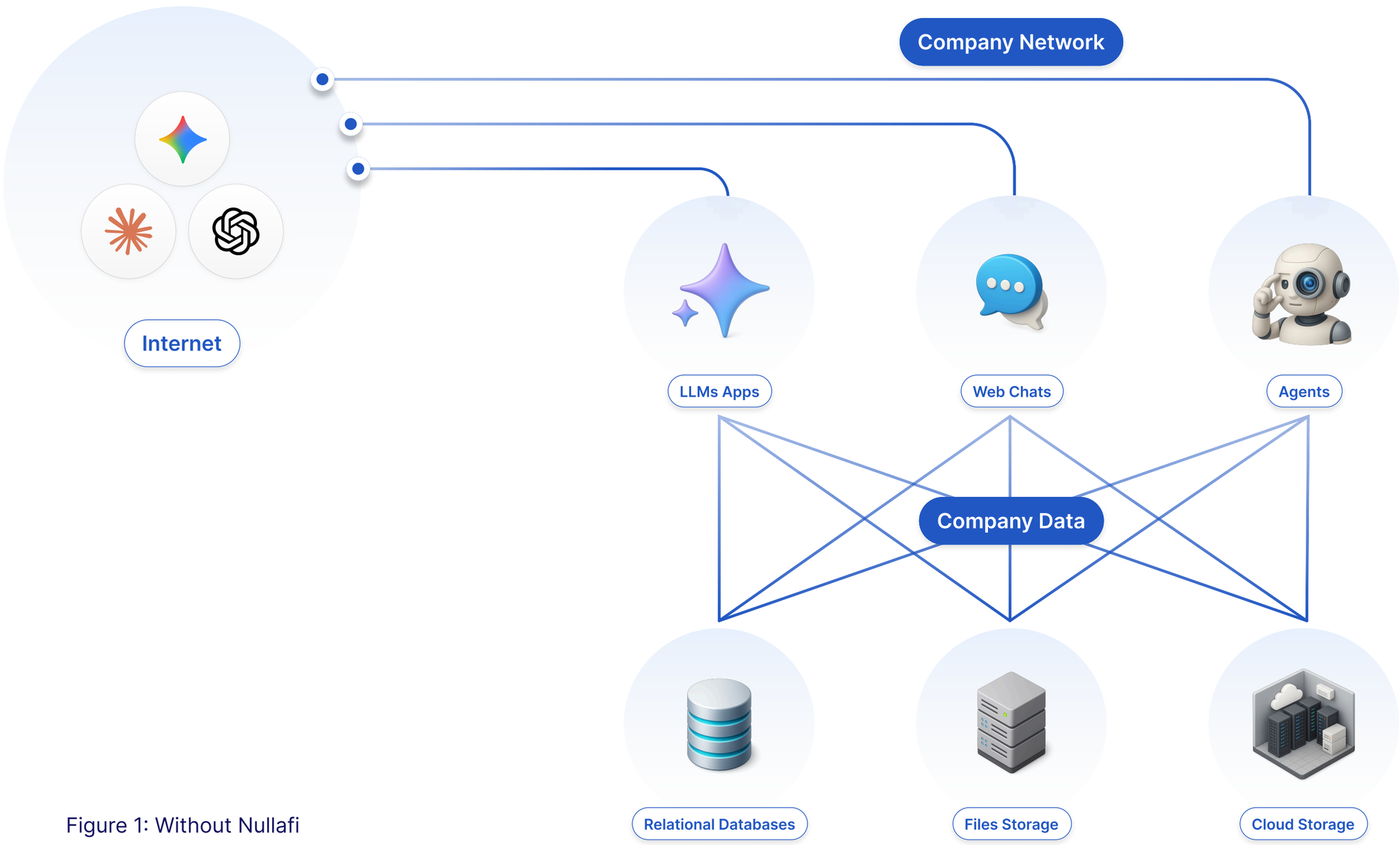

Figure 1: Without Nullafi

Key Benefits

The Nullafi AI Data Firewall provides a revolutionary security layer that allows organizations to harness the full power of Large Language Models and AI agents while maintaining:

- **Complete Data Control** – This technology ensures that data remains within your control. The LLM never sees or stores the actual underlying sensitive data, which mitigates the risk of data leaks or unauthorized model training on private information.
- **Granular User Access Control** – Security teams can set user permissions to determine who is allowed to see deciphered data in the final output and who should only see the masked version.

- **Effective AI Utility** – With Nullafi, your AI tools and models retain the ability to analyze, summarize, and query the data effectively, even though it is ciphered.
- **Seamless User Experience** – Since deciphering happens automatically on consumption, authorized users receive the information they need without any manual steps, friction, or delay.
- **Production-grade Data in Every Environment** – With Nullafi, organizations only have to cipher once, yielding a single source of truth with no upstream cycle coupling as well as faster testing/ engineering cycles and drift-free deployments.
- **Safe AI Enablement** – Organizations can put AI to work on real data without exposing valuable corporate or customer information and without worrying about breaching data protection regulations

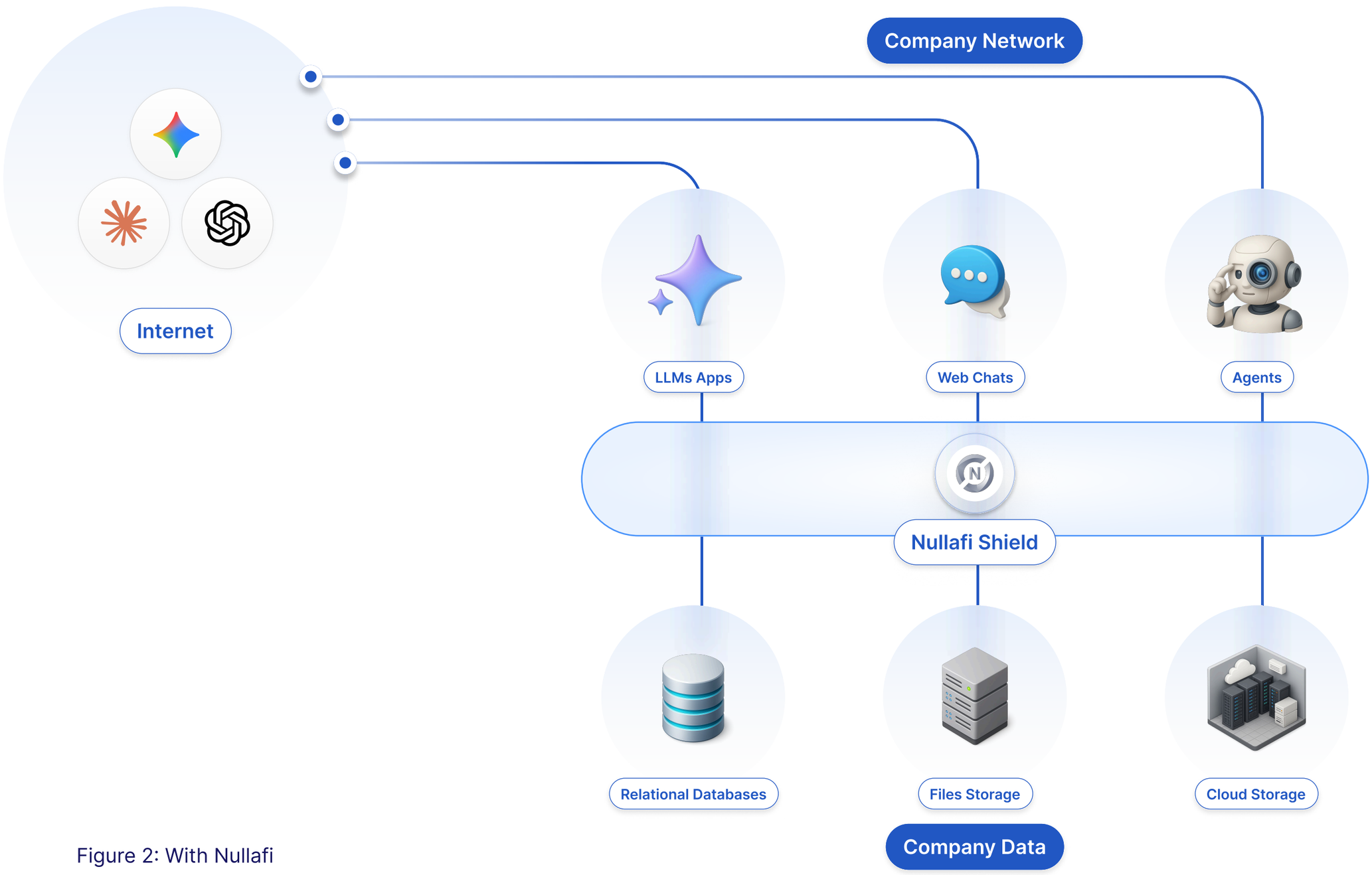

Figure 2: With Nullafi

Use Cases

The Nullafi AI Data Firewall enables organizations to safely operationalize AI by addressing four foundational data protection use cases:

1) Data Security

At the heart of Nullafi's new feature is a reversible and deterministic cipher. This technology is a significant advancement over traditional hashing or one-way tokenization because it ensures that the same sensitive input always results in the same ciphered value. This unique property allows an AI agent to perform critical functions, such as complex data lookups and record associations, without ever knowing the actual content of the data. Essentially, the AI is treated as a restricted user that only interacts with protected, ciphered information.

2) Data Privacy

The technology prioritizes privacy through in-transit processing. As data is uploaded or queried, Nullafi automatically detects and ciphers sensitive identifiers before they reach the LLM. This keeps the model “blind” to private information like PII or financial details while it performs its analysis. Privacy is further extended to the end user through granular access controls, where security teams can specify which authorized personnel are allowed to see the deciphered results in the AI’s response and which users should only see the masked or ciphered versions.

3) Data Sovereignty

For organizations with high-stakes data, the AI Data Firewall ensures complete data sovereignty. Because the LLM never sees, processes, or stores the raw underlying data, there is no risk of unauthorized model training on an organization’s proprietary or private information. This allows companies to maintain absolute control over their data assets, ensuring that their intellectual property and sensitive customer information never leak into the broader training sets of third-party AI providers.

4) Nth-Party Security Risk Management

Nullafi’s technology serves as an essential AI guardrail for managing the risks associated with third- and Nth-party vendors and cloud environments like Snowflake and GCP. It provides a secure layer that ciphers data before it leaves the organization’s controlled environment, allowing for the safe adoption of external AI tools, especially in highly regulated industries and geographies. Ciphered data that is ingested, processed, or trained by third-party software and AI tools is protected from regulatory and IP risks. By making the security layer totally invisible to the standard workflow, organizations can mitigate Nth-party data security risks while still benefiting from the speed and utility of modern AI tools, assistants, LLMs, and agents.

About Nullafi

Nullafi is the first dynamic data protection platform purpose-built to see and control data in motion anywhere it flows, in real time. We can sit between every user, application (including AI), and data source to give you instant visibility and granular control over who sees what, where, and when – without agents, friction, or delay. We primarily serve enterprise and mid-market companies, technology resellers, and application developers. With rave reviews from analysts, multiple patents granted, and key partnerships established, Nullafi is transforming data security as we know it.

Learn how Nullafi helps organizations protect sensitive data in the age of AI without slowing innovation. Schedule a personalized demo to see how Nullafi enables safe, scalable AI usage or contact us at sales@nullafi.com.