# Is Your Data Protected in the Age of AI?


## Enable AI Innovation Without Giving Away the Data You Can't Afford to Lose

AI is rapidly becoming embedded across the enterprise – agents, copilots, summarizers, chatbots, analytics engines, and internal LLMs are now part of everyday workflows. These tools deliver enormous productivity gains, but they also introduce fundamental new data risks. AI sees everything that flows through it. Customer PII, financial records, PHI, payroll data, internal documents, confidential emails; if the data exists, AI systems can ingest and/or output it.

Nullafi enables organizations to safely use AI by protecting sensitive data wherever it flows, before it reaches AI tools, agents, models, analytics systems, or downstream platforms. Our platform provides guardrails for AI data usage, helping organizations control how sensitive information interacts with AI. This includes the ability to enforce policies around whether employees can upload sensitive data to AI tools or retrieve AI-generated data containing protected information, for example. As well, by dynamically anonymizing sensitive information in real time, Nullafi ensures data remains usable for AI and analytics while eliminating the risk of exposure, misuse, or regulatory violation.

> **The result:** AI innovation without sacrificing data security, privacy, or compliance.

## The Challenge: AI Changes the Rules of Data Exposure

Security teams are under pressure to enable AI adoption while ensuring sensitive data is never exposed, stored, or learned. But traditional security tools were not designed for AI-driven data consumption, because AI fundamentally alters how data is accessed, processed, and retained.

For example, they:

- Ingest massive volumes of data automatically
- Persist data in prompts, embeddings, logs, and training pipelines
- Operate across cloud, SaaS, and hybrid environments
- Create new, often invisible, data copies outside traditional controls

As a result, sensitive data can unintentionally:

- Leak into AI prompts and model memory
- Be stored in vector databases and logs
- Expand compliance scope across systems
- Increase the impact of insider misuse or credential compromise

## The Nullafi Solution: Dynamic Data Protection Built for the AI Era

Nullafi protects sensitive data as it is moving, ensuring sensitive data never reaches AI models, logs, or training data. Instead of blocking AI usage or requiring complex application changes, Nullafi:

- Intercepts sensitive data in real time
- Masks, redacts, or anonymizes data before AI access
- Preserves data utility so AI tools remain effective
- Eliminates the risk of AI exposure at the data level

This approach allows organizations to safely operationalize AI without redesigning applications, retraining users, or slowing innovation.

Nullafi operates inline with data flows across applications, AI tools, analytics platforms, and downstream systems, protecting sensitive information wherever it flows. With this solution, customers benefit from:

1) **Sensitive Data Identification**

   Nullafi automatically detects sensitive data such as PII, PHI, PCI, and proprietary information.

2) **Real-Time Data Redaction & Masking**

   PII and governed data, such as SSNs, addresses, credit card numbers, PHI, payroll data, and financial records, are intercepted and masked in flight before being sent to or processed and logged in AI systems.

3) **Preserved Usability**

   Anonymized data maintains format, relationships, and statistical integrity, so AI and analytics continue to work as expected.

4) **No Required Application Changes**

   Existing applications, AI tools, and workflows remain unchanged.

Because sensitive data never enters the AI system, AI can’t leak what it never saw. With Nullafi, there is no accidental training ingestion, no model regurgitation of sensitive information, no prompt injection leaks, and no LLM-exposed customer data incidents.

## Key Benefits

Because every access, redaction, and policy decision is logged, Nullafi delivers complete visibility for security teams, clear evidence for compliance and audits, and reduced audit stress (as well as manual reporting), as well as:

**Safe AI and LLM Adoption:** Enable ChatGPT, copilots, and internal LLMs without exposing sensitive or regulated data. AI systems receive only policy-compliant data – never raw sensitive information.

**Zero Trust Data Usage:** Extend zero trust principles beyond access to ensure sensitive data is protected wherever it flows, including AI pipelines, analytics platforms, and logs.

**Insider Risk Mitigation:** Limit unnecessary exposure of sensitive data (even for authorized users) while preserving productivity and normal workflows.

**Compliance and Audit Readiness:** Nullafi delivers a fully automated, exportable audit log of every data interaction, down to the second and the user. You shrink your compliance scope because the sensitive data never actually enters the AI system, so it can’t be leaked or misused later.

**Breach Impact Reduction:** Ensure compromised or exfiltrated data is unusable and non-actionable, dramatically reducing the blast radius of incidents.

Security teams define exactly what AI can and cannot see, such as names but not SSNs, titles but not salaries, transcripts but not payment data, emails but no PHI. This enables least-exposure data usage without impacting productivity.

## Key Use Cases

**Protecting AI Inputs and Outputs:** Prevent sensitive data from entering AI prompts, embeddings, training datasets, and inference pipelines.

**Secure Copilot and GenAI Enablement:** Allow employees to use AI assistants safely without risking data leakage or IP exposure.

**Analytics and Data Science Protection:** Enable data-driven insights while ensuring analysts and models never access raw sensitive data.

**Insider Risk and Least-Exposure Access:** Ensure users see only policy-appropriate data without changing applications or roles.

**Reducing Regulatory Exposure:** Minimize where sensitive data exists to simplify GDPR, CCPA, HIPAA, PCI, and emerging AI governance compliance.

## Why Nullafi

Nullafi was purpose-built for environments where data must remain usable but not exposed. Unlike traditional masking, tokenization, or access-only controls, Nullafi:

- Protects data dynamically and continuously
- Works across AI, analytics, and operational systems
- Preserves business value while eliminating data risk

It is the data protection layer required for the AI era.

## Get Started Today

AI adoption doesn’t have to come at the cost of data security. 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.**

## 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, 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 in North America. With rave reviews from analysts, multiple patents granted, and key partnerships established, Nullafi is transforming data security as we know it. Learn more at **www.nullafi.com**.