



**INDIGO
VAULT**

Engineered by WTW

Preventing AI models from exposing corporate data

Today's AI landscape

Nearly 99% of Fortune 500 companies are investing in generative artificial intelligence (AI) to drive business growth. AI continues to revolutionize industries, the benefits are undeniable. From improving efficiency to enabling advanced analytics and better decision making, AI has quickly become integral to business operations. However, with the increasing use of AI, especially in generative models like large language models (LLMs), a growing concern has emerged: the risk of exposing sensitive corporate data.

AI systems, such as LLMs, learn by consuming vast amounts of data, including corporate documents, emails and internal reports. These documents can contain personally identifiable information (PII), confidential business strategies and other sensitive information that should remain secure. As AI models learn from these data sets, there's a chance that this sensitive information can be accidentally exposed. This could happen through AI's responses to user prompts or through malicious actors exploiting the AI system with techniques like prompt engineering.

The risks of AI data exposure

AI models are designed to read and process information to build their knowledge base, and once they've ingested data, they can respond to queries or assist with tasks. However, this creates a significant vulnerability. If the AI model has access to sensitive corporate documents, it may inadvertently reveal private information during user interactions or during normal operations. Worse, adversaries may try to exploit the system by manipulating the AI's responses through carefully crafted prompts to access restricted data.

Traditionally, companies have relied on data classification systems and cataloging efforts to control which documents are accessible to AI models. This process involves tagging and labeling all data, restricting sensitive content based on access permissions. While effective, this method is labor-intensive and prone to errors, especially in large organizations where data is constantly changing and growing. The challenge lies in the continuous need to update these classifications, as data access policies and user permissions change over time. Even with strict controls in place, there's no guarantee that AI models won't accidentally access and expose sensitive information.

How Indigo Vault works

Indigo Vault provides seamless, real-time encryption for every document that enters its system. When a file is dragged and dropped into the Vault, it becomes encrypted instantly. This prevents all external AI models from reading or training on the file's contents, making it impossible for models to extract sensitive corporate information, even if they are integrated into workflows or applications.

Unlike other security solutions that rely on complex tagging and access control, Indigo Vault's encryption is built into the system, removing the risk of human error. It's a set-and-forget solution that ensures your data stays protected, without requiring constant updates to classification schemas or permissions.



Conclusion

AI offers incredible potential for transforming business productivity, but it also brings new security challenges, particularly when it comes to protecting sensitive corporate data. Indigo Vault's encryption solution helps companies safeguard their documents from AI exposure, preventing inadvertent or malicious leaks of critical information. By offering always-on protection without requiring complex data classification, Indigo Vault is a powerful tool for responsible AI deployment, ensuring that your data remains secure, and your business stays protected.



Contact us today to discuss
how Indigo Vault can protect
your documents from unwanted
AI exposure.

contact@indigovault.com

About Indigo Vault

Indigo Vault provides quantum-computing resistant protection for companies' critical information security needs. The WTW patented technology uses the strongest possible encryption to protect assets integrated with Microsoft Azure and Office.

Leveraging best-in-class technology with nearly two centuries of risk management expertise, Indigo Vault helps organizations reduce risks to business from insider threat, data breaches and intellectual property loss by securing cyber terrain.

Find out more at [indigovault.com](https://www.indigovault.com)

<https://www.linkedin.com/showcase/indigovault/>

Copyright © 2024 Indigo Vault. All rights reserved.
IV_168650_1224

[indigovault.com](https://www.indigovault.com)



**INDIGO
VAULT**

Engineered by WTW