VOTIRO

Case Study

Insurance Industry Leader

Eliminates threats embedded in shared files by partnering with Votiro

About the
Customer

A leading global firm with roots in a prominent offshore business hub, this Company boasts a rich heritage in offering comprehensive risk transfer products and services. Through its vast subsidiaries and branch networks across multiple continents, it delivers both insurance and reinsurance services in domains like property, professional lines, marine, and energy.

Highly regarded for its claims-paying ability, this firm boasts billions in revenue with tens of billions in assets backing up its operations.

The Challenges

Managing Malicious Macros and More

Before implementing Votiro, the Company leveraged a widely-used cloud platform for its storage needs that didn't provide adequate protection from malicious files. Their business operations regularly dealt with huge files from customers and partners, some of which ran into hundreds of megabytes, making the task of ensuring no malware was hidden inside a considerable challenge.

Though they'd previously implemented sandboxing and an email gateway, their infrastructure remained exposed to malicious macros. These concealed threats, capable of activating malicious code, posed significant risks, from malware and rootkits to ransomware and keyloggers.

A significant challenge stemmed from their multifaceted data ingestion sources, as they received data through API file uploads and via emails. Predominantly, the data came in ZIP files, which often contained Word documents or PDFs — common carriers of harmful macros.

Combatting this threat was no small task, as existing solutions, such as antivirus (AV), cannot detect all hidden threats in files. The Company resorted to outright blocking all macros, leveraging a security vendor that flattened and stripped files.

However, this drastic approach severely hampered operations and proved to be an unsustainable solution, prompting the Company to seek a more refined and effective countermeasure.

Before
Implementing Votiro Cloud

International Ops, International Threats

The Company was exposed to international threats through their business dealings with global organizations, many of which may not prioritize security and leave them vulnerable to threats.

Lack of Consistent Defense

Gathering data from customers is crucial to driving business operations, but current solutions didn't provide a reliable defense against hidden threats, and blocking macros only stops a portion.

After
Implementing Votiro Cloud

Additive to Business Operations

Quick and simple installation and integration help the Company continue to focus on delivering quality insurance products to its customers.

Disarming Threats in Files

Votiro disarms all content, eliminating hidden zero-day malware from incoming files without user intervention.

VOTIRO

votiro.com | sales@votiro.com

Votiro

The Insurance Company seamlessly integrated Votiro into its email communications and API file gateway to prevent potential hidden threats.

With Votiro, the Company can now:

- **Rapidly implement** Votiro's API-based integration, ensuring that the core data ingestion sources were promptly secured.

- **Establish a barrier** against malware or phishing attempts that place sensitive customer information at risk.

- **Create a seamless shield** of security, operating autonomously without requiring employee actions within their current workflow.

- **Continue to utilize macros** throughout their organization, reaping the business benefits of their features without the risk.

- **Feel confident** that no matter which of the 180+ file types customers might provide, the data will be properly sanitized of malicious elements, even within ZIP files.

- **Empower the Company's staff** to concentrate on delivering trustworthy insurance products without being burdened by security concerns.

VOTIRO

Try Votiro Free for 30 Days

See how Votiro stops threats before they ever reach your endpoint with a **free trial!**

🌐 votiro.com   ✉ sales-us@votiro.com