

Revolutionary Data Security



Business Profile

Broadridge is a global financial technology company with almost \$5 Billion in revenue that helps publicly traded companies deliver necessary shareholder information such as proxy statements, annual reports, and investor relations documentation. It oversees important shareholder communications, annual meetings, and proxy voting.

As securities moved into the digital space, the need for physical certificates to show ownership diminished. Along with this, the ownership of securities is constantly in flux, increasing the challenge of ensuring legitimate shareholders have access to information and voting access.

Broadridge is a technology-driven company designed to deliver these valuable services on behalf of public organizations. Doing this requires a massive team of over 10,000 employees worldwide and a complex technology stack to ensure that their information is continually updated and remains completely confidential.

Challenge

Broadridge delivers services such as proxy voting worldwide. Existing architecture pushes the process of voting within the borders of the US. This creates a scenario where handling the votes and data for overseas organizations occurs outside their borders.

Perspective customers based in EMEA (Europe, Middle East, and Africa) were evaluating Broadridge. One of their primary concerns was the ability of staff in the US to have any degree of access to votes and results. In addition to GDPR regulations, the customer was also interested in maintaining a high degree of confidentiality.

Existing Broadridge architecture would not facilitate removing the US from the voting pipeline as the processing servers resided on US soil. To re-architect, the voting to allow their information to remain entirely in EMEA would require the installation of a proprietary mainframe costing upwards of \$10 Million.



Installing a new mainframe would have solved the problem but at a high cost. This approach is also not scalable for future customers with similar privacy needs. Having to bear similar expenses to accommodate all geographic regions would become cost prohibitive and create a maintenance challenge resulting in additional expenses for upkeep throughout the product lifecycle.

Broadridge needed a solution that could integrate with existing architecture and allow similar functionality to be delivered in the future.



Results

Since the integration and implementation of the Sotero Data Security platform, Broadridge has solved multiple challenges, including:

- Ensuring data privacy remains intact across borders
- Scalably limiting access to sensitive data across organizational groups and geographies
- Integrating data privacy controls into new applications and data sets from customers to protect sensitive data throughout its lifecycle
- Meeting compliance objectives in providing continual evidence that unauthorized users have not accessed data
- Delivering additional threat monitoring across protected data sources to identify attempts at inappropriate access from both internal and external users

Solution

Sotero transformed the process of how Broadridge protected data. The Sotero Encryption API encrypts information directly in the existing application to ensure that all data remains confidential.

Implementing the encryption API eliminated the need for adding a proprietary mainframe. All data that customers sent overseas was guaranteed to remain confidential and inaccessible to US-based staff. With the dynamic nature of the Encryption API, individuals overseas that required access to the data could do so on the fly.

By implementing the Sotero solution, Broadridge was able to realize immediate ROI. The additional privacy controls allowed them to take on 25 customers who would otherwise not have been interested in the original infrastructure.

The Sotero solution came with the added benefit that it is dynamically scalable for other organizations and regions in the future without having to install additional hardware. Sotero's cloud-based deployment is easily integrated into new and existing applications without the need for custom coding.

Utilizing this functionality came into play shortly after Broadridge met the original use case. An existing customer had a unique data set with highly sensitive information to share. Existing processes would not have lent sufficient protection to this information or made sharing it labor intensive. With Sotero, the new data set was easily integrated, allowing dynamic data protection throughout the entire lifecycle, ensuring that it was secure en route and while stored.

About Sotero

The Sotero Data Security Platform provides a centralized way to encrypt and protect data through its entire lifecycle – at rest, in transit, and in use. With real-time detection and automated quarantine of malicious access, Sotero also prevents active threats, giving you 360-degree data security without disrupting the user experience. With our lightning-fast encryption and our point and click set-up, Sotero's solution is easy to deploy and manage, ensuring you are protected in a matter of days, not weeks or months.

Secure third-party data management that means business

Data stays encrypted at all times, enabling you to share data with downstream systems and third parties without ever putting security or privacy at risk.

