High Tech Company Secures Millions of Business Sensitive Documents

Summary

Organization
A Fortune 1000 company that is a leading provider of infrastructure appliances and software defined storage

Industry:
High-Tech, over 4500 employees

Use Case
Prevent improper sharing of documents with external parties

Customer Environment
Primarily cloud-based

Business Problem
Securing business critical data in a highly collaborative environment

Results
Analyzed over 12 million files and secured over 2600 business critical files that were erroneously shared.

Enabled better security and controls after new search and indexing tool was implemented.

The Business Problem

As a leading provider of infrastructure appliances and software defined storage, in a very competitive environment, this organization needs to be nimble and encourages a culture of collaboration among its employees.

As a cloud-first organization, they use everything from OneDrive, Google Drive & Dropbox as well as productivity tools such as O365 and Google Suite. This **open collaboration** has allowed the employees to work anywhere while still being productive, significantly increasing employee engagement and innovation. However, one of the key challenges has been securing business critical data. Specifically, the organization wanted to **prevent improper sharing of business sensitive documents** such as source code, product roadmap and M&A documents **with external parties**.

While this sharing was rarely done knowingly, the organization was concerned that careless users might have shared sensitive documents enabling their competition and negatively affecting their brand.

The organization could easily find a list of documents that had been shared externally. However, combing through them to **determine which of these documents were business-critical and that were shared inappropriately was a key requirement**. The security team wanted to focus their efforts on issues that could impact the business operations the most. If their security team had attempted to find these improperly shared

documents manually, it would have taken them months and with the business sensitive data changing regularly, the results would not have been accurate or comprehensive.

This was new challenge and the CISO needed a novel solution to increase data security and reduce risk from careless users.

Choosing Concentric

Concentric's Semantic Intelligence technology **understands the meaning or context behind documents**. The CISO found this approach not only innovative but also highly applicable in their cloud-first environment. **Not having to rely on end-users** or their security team **to identify business-critical content** was extremely valuable because of their phenomenal data growth and collaboration inside and outside their organization. The CISO believed that with technology that uses deep learning techniques to **automate decisions made by end-users and security teams,** for the first time he could stay ahead of the curve when it came to minimizing data risk.

How It Works

Concentric Semantic intelligence technology **groups documents into thematic clusters by deep learning the meaning** behind of documents. Leverage thematic understanding to auto-classify documents without relying on end users. Concentric **surfaces High-Risk documents** by dynamically understanding content sensitivity and appropriate classification, entitlement, sharing properties etc. This **data risk is remediated** and the data protected by changing sharing permissions either through native capability or through integration with third party tools.

Implementation and Results

The organization implemented Concentric for proof of concept (POC) **analysis of over 12 million documents housed in OneDrive**. Concentric was set up easily in a few hours. It combed through all the documents on OneDrive to **develop a thorough semantic understanding of the content** in each document. It then categorized these documents based on thematically similar clusters (NDAs, patents, product roadmaps etc.). **Meta data for these documents** such as ownership, entitlements, sharing and classification were also extracted.

> "Finding sensitive documents that have been shared inappropriately is exactly the kind of information we were looking for. This helps us significantly reduce the risk around our sensitive data and a critical part of our data security portfolio."
>
> CISO
> High Tech Company

Each document within a cluster was then assessed to understand if it had been shared erroneously compared to the other documents within the cluster. They found ~2600 business critical files that had been erroneously shared, including finance plans, product design docs, sales and partner documents . These documents were flagged for review.

Within 3 weeks after set up, the organization had

CONCENTRIC

4340 Stevens Creek Blvd., Suite 112
San Jose, CA 95129
Tel: +1 (408) 816 7068
Email: contact_us@concentric.ai

a comprehensive list of documents **that had been improperly shared with external parties**. They also found another 2200 sensitive files that were shared inappropriately within the organization. The organization took the next steps to revoke access and correct permissions to all business-critical documents such as M&A files, product roadmaps and source code.

Next Steps

The organization saw phenomenal results with their POC; in order to prevent improper sharing of documents across the organization, they are rolling out Concentric for data across all cloud stores and apps.

Furthermore, evaluating their security gaps, the organization realized that they could **use Concentric to resolve a couple of other security issues**.

> "We also like that Concentric can help us discover all our sensitive data to ensure that biz critical data is not easily accessible by all users as part of our a new enterprise indexing and search initiative that we have underway"
>
> CISO
> High Tech Company

The organization had **adopted a new search and indexing software** across their various clouds and apps **allowing employees to easily find the documents they were looking for**. This was done with the idea of enabling easy access to documents across various cloud stores and applications. The **inadvertent result** of this was that employees would more easily find business-critical data that they otherwise might not have had access to. The CISO wanted to ensure that security was not compromised in the process of driving easy access.

They have adopted Concentric to identify business critical data such as product roadmaps and M&A documents that should be restricted from search and indexing. This has allowed for **easy search and indexing of documents across the organization while not compromising sensitive files**.

Benefits and Results

- With Concentric's novel solution, this organization was able to identify business critical data that has been shared externally. What would have taken hours, if at all possible, was solved in a few weeks.
- An additional benefit was the ability to know which employees have shared business-sensitive documents with their personal email, causing a security loophole.
- As the organization allows employees to easily access documents across all cloud and apps, the security team can curtail searches on sensitive documents.

CONCENTRIC

4340 Stevens Creek Blvd., Suite 112
San Jose, CA 95129
Tel: +1 (408) 816 7068
Email: contact_us@concentric.ai