How a Global Financial Firm Reduced Exposed Sensitive Data by 86% with Varonis

CASE STUDY

"Before Varonis, we didn't have a clear picture of our permissions landscape. With Varonis, we were able to pinpoint those issues and remediate global group access within the span of two weeks."

ABOUT THIS CASE STUDY:

Our client is a global financial firm. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Identifying and locating sensitive information (PII, PCI, etc.) in on-premises servers
- Ensuring compliance with data privacy regulations, including GDPR and CCPA
- Remediating global group access to decrease the risk of data breaches

SOLUTION

The most robust data security platform:

- **DatAdvantage** shows where users have too much access and helps remediate access control
- **Data Classification Engine** scans and classifies personal info and other sensitive data
- **Data Classification Policy** Pack automatically identifies and classifies GDPR and CCPA data
- **DatAlert Suite** monitors and alerts on all critical data and systems

RESULTS

- Protection for approximately 3,000 employees
- 86% decrease in sensitive folders with open access
- Over 38,400 work hours saved annually
- Ongoing support as they move data into the cloud

Challenges

Securing PII, PCI, GDPR, CCPA, and other sensitive information

As a financial services firm, one Varonis client (anonymous by request) is responsible for protecting a host of sensitive data, including non-public research, financial transaction records, client information, and employee information (PII, PCI, etc.).

According to the company's Senior Data Analyst, the firm needed an efficient way to locate and identify sensitive data in their on-premises servers. That led them to Varonis.

> "When individuals leave, the burden of identifying what data they had falls on managers. But most managers can't even identify all of the data living on their personal devices. Trying to ask them for a specific employee's file server data was a hopeless pursuit."

As a global company, the firm is also responsible for ensuring compliance with all current and future data privacy regulations, including the California Consumer Privacy Act (CCPA) and the EU General Data Protection Regulation (GDPR).

> “With 3,000 employees, manually reviewing the information stored on our file servers was a daunting task. To maintain compliance with GDPR and CCPA, we needed a way to automatically find, classify, and validate confidential information.”

The Senior Data Analyst was also concerned with risk remediation. Insider and outsider breaches had cost other companies untold brand damage and resulted in significant intellectual property loss. To avoid the same fate, this firm needed more visibility into where it was exposed and the ability to lock down global group access.

> “We didn’t have the ability to quantify what global access looked like in our environment. For the sake of risk reduction, we needed an easier way to review and remediate access management.”

But the Data Analyst had no idea how widespread the issue actually was until a Data Risk Assessment revealed that **86% of the firm’s sensitive folders—including almost 50,000 files were open to everyone.**

> “Most managers can’t even identify all of the information living on their personal devices. Trying to ask them for a specific employee’s file server data was a hopeless pursuit.”

Solution

Increased visibility and control into their on-prem environment

With widespread overexposure, the global financial firm needed swift and demonstrable remediation. Four Varonis products helped them lock down their servers and fortify their cybersecurity.

1. **DatAdvantage for Windows, Exchange, and Directory Services** supports the firm's on-prem data stores and email. It automatically maps who is able to access sensitive data, who is actually accessing sensitive data, and areas where overexposure has left them vulnerable to a data breach.

> "DatAdvantage was eye-opening in terms of what we needed to fix to address user privacy. We didn't realize we had so much overexposed information, so being able to capture it and immediately work toward remediation was a big win."

2. **Data Classification Engine** enables them to work toward their primary goals: data inventorying and privacy remediation. With Data Classification Engine automatically scanning and classifying data, the burden of remembering where data lives no longer rests with individual users and group managers.

> "Varonis does a couple of different things: data discovery, sensitive data classification, and it helps us identify data that we otherwise might not have known about. We can then use Varonis to restrict permissions and remediate the risk associated with administrative access."

3. **Data Classification Policy Pack** enhances data classification via a vast library of pre-built rules and patterns. By automatically enforcing data privacy standards laid out by regulations such as GDPR and CCPA, Policy Pack streamlines compliance efforts.

> “You need to cater to different regulations depending on location. So regulations are different in the EU versus California versus New York. Varonis helps you meet those various regulations by constantly seeking out and pinpointing data that might put you at risk of non-compliance; it’s doing this 24/7 in our environment.”

4. **DatAlert Suite** provides real-time monitoring and alerting of all critical systems. The firm is now exploring Splunk integration, which will allow them to query and correlate Varonis alerts using Splunk Enterprise.

> “DatAlert helps us keep an eye on things we otherwise couldn’t keep an eye on. For example, one of the great features is the behavior- based security alerts.
>
> So if a user based in the U.S. is usually active between 3 a.m. and 11 a.m., and their credentials suddenly log in from Mexico at midnight, Varonis alerts us to the abnormal behavior. Or if a user with insufficient account credentials attempts to access a folder containing sensitive data, we get an alert on that.”

"We didn't realize we had so much overexposed information, so being able to capture it and immediately work toward remediation was a big win."

Results

86% Decrease in sensitive folders with open access within the first four months

With full visibility into where sensitive information was exposed and more insight into the steps necessary for risk reduction, the Senior Data Analyst was able to take decisive remedial action.

"Before Varonis, we didn't have a clear picture of our permissions landscape. With Varonis, we were able to pinpoint those issues and remediate global group access within the span of two weeks."

In just four months, the firm's data analysis team used Varonis to restrict access to over 35,000 files containing sensitive information. All-in-all, they **decreased the number of sensitive folders with open access by 86%.**

According to the Senior Data Analyst, Varonis has helped the firm substantially decrease its attack surface and improve its approach to compliance—all while saving an astronomical amount of time.

> “When we consider how long manual remediation takes, the extra people we would need to hire, their hourly wages or salaries, and the desk space we’d have to provide, I’d say Varonis saves us a minimum of 38,400 hours in a given year.
>
> And that’s a conservative estimate. It assumes that we could accomplish the same tasks with only 20 extra people—and, honestly, I don’t think we could.”

Looking ahead, the firm is planning to move some of their data into the Microsoft 365 environment. In preparation for that move, they’re already evaluating other Varonis products, such as DataPrivilege and Automation Engine, which will support their move to the cloud.

“I’d say Varonis saves us a minimum of 38,400 hours in a given year. And that’s a conservative estimate.”

Suss out the overexposed data that's leaving your business at risk of a data breach.

Varonis gives you more visibility and control into your on-prem and cloud environments.

REQUEST A DEMO