# How Varonis Helped a Global Manufacturing Company Avoid a Data Loss Disaster & Tackle GDPR Compliance

CASE STUDY

"Varonis gives us the insight and immediate alerting we need to protect our customers and meet data privacy requirements. I don't know how we would have achieved GDPR compliance without Varonis."

## ABOUT THIS CASE STUDY:

Our client is a large manufacturing company with locations around the world. We have happily accommodated their request to anonymize all names & places.

## HIGHLIGHTS

### CHALLENGES

- Remediating over-exposed data
- Ensuring personal data meets regulatory requirements
- Protecting revenue and brand image from insider and outsider threats

### SOLUTION

The most robust data security platform, fully integrated with their SIEM:

- **DatAdvantage** for Windows supports their on-premises data stores
- **Data Classification Engine** for Windows and SharePoint scans and classifies sensitive data
- **Data Classification Policy** Pack helps identify data protected under the EU GDPR and CCPA
- **Automation Engine** finds and automatically fixes folders with global group access
- **DatAlert Suite** for continuous monitoring and alerting on data and systems

### RESULTS

- 79% decrease in folders with open access
- Multiple terabytes of stale data classified and automatically deleted or archived
- Data protection for servers in 6 locations, with 4 locations pending

# Challenges

## Folders at risk of insider and outsider data breaches

At 4 a.m. on a Sunday morning, a major manufacturing company (anonymous by request) that generates over $1.5B in annual revenue was faced with a serious problem. Someone had deleted an entire shared drive.

The company had taken precautions and backed up their data, but figuring out exactly what was deleted and recovering it manually would take time—and cost the company a lot of money.

As the Information Security Manager explains:

> “We’re talking about a file server that everybody works off of. The entire office would have been without service for a day or two—we would have lost days’ worth of business.”

Fortunately, the company was in the midst of a proof of concept (POC) of Varonis when the incident occurred. Varonis sent the Information Security Manager an alert as soon as it detected the anomaly—and it enabled them to get ahead of a potentially costly situation.

> “I received the alert. I was able to disable the account, which gave me time to follow-up. Varonis’ logs showed me exactly what was deleted, and I was able to quickly recover the files.”

Varonis gave them a forensic trail to follow that showed them exactly what had happened. They learned that a security guard had accidentally deleted the company's S: drive while cleaning out what he thought was his own personal drive.

It hadn't been a data breach; it had been an honest mistake, **caused by overexposed data.**

> "Varonis helped cut down response and remediation times. Its logs showed us which folders had been deleted and who was responsible. A problem that could have cost us days' worth of business took less than an hour to resolve."

The incident highlighted the company's need for more robust data security. Over-permissiveness had left their servers vulnerable to insider and outsider threats—and put them at risk of non-compliance with data protection regulations like GLBA and GDPR.

It was an ongoing problem that the Information Security Manager couldn't seem to get ahead of—the task was a massive undertaking and their small team was stretched thin.

> "We made a couple of attempts to manually clean up our file servers— lock down permissions, eliminate stale data, that sort of thing. But all of those efforts stalled; we didn't have enough visibility into our infrastructure to know what could or couldn't be deleted. That's why we reached out to Varonis."

"A problem that could have cost us days' worth of business took less than an hour to resolve [with Varonis]."

# Solution

## Remediation automation + more data visibility

The first thing the Information Security Manager did with Varonis was plumb the depths of the company's open access and broken permissions problems. What they discovered shocked them.

- 52,448 folders with open access
- 517 folders with broken permissions
- 296,417 folders with stale data (75% of all data was stale)

> "We knew there were issues, but we didn't have the hard numbers to show the higher-ups what we were talking about. Varonis' Data Risk Assessment gave us the ammunition we needed to show our management board the actual risks we had in our environment."

With over 40 locations around the world, all with similar overexposed data issues, the company needed remediation—fast. To facilitate their infrastructure clean-up, they adopted five Varonis products.

**DatAdvantage** gives the data security team crucial visibility into active permissions and a detailed audit trail to follow.

> "We can look at who accessed each folder over the past six months. If it's only a few people, Varonis helps us determine who needs access to that information. If no one needs access, the folder can be safely archived or deleted."

**Data Classification Engine** automatically scans and classifies sensitive data, both on their Windows servers and shared drives.

> “We have sensitive personal data and intellectual property that we don’t want to be made public. Data Classification Engine scans for sensitive data, like PII, and classifies it.”

**Data Classification Policy Pack** (formerly called GDPR Patterns) gives them a vast library of pre-built rules and patterns to help pinpoint EU citizen data in order to comply with GDPR. GDPR compliance is non-negotiable for a major company that operates within the EU.

> “Varonis helps us achieve GDPR compliance by scanning and classifying EU citizen data. Before, if someone asked us to delete all of their personal data, we would have no way of knowing where it was. With Varonis, we can create custom rules to search for that information and effortlessly delete it if we no longer need it.”

**Automation Engine** is a fast, efficient, and safe way to remove global group access across a huge volume of at-risk folders. With it, the small team is able to set and forget remediation, fixing thousands of folders without lifting a finger.

> "With Automation Engine, we were able to automatically modify and remove global access to all of our folders without disrupting anybody's work. There was zero impact on our users."

Finally, the **DatAlert Suite** provides day-to-day monitoring for their servers. The powerful threat detection and response system helps mitigate the risk of insider threats, defend against cyberattacks like ransomware, and trace suspicious activity to its source.

> "Varonis is able to understand usage patterns for user behavior analysis. If a user starts deleting a bunch of files, we get an alert. If there are signs of mass encryption or a ransomware attack, we get an alert. It's a powerful solution that you can customize based on your needs."

"Varonis' Data Risk Assessment gave us the ammunition we needed to show our management board the actual risks we had in our environment."

# Results

## Data security and infrastructure improvements

The company has now installed Varonis data protection in six locations across the United States. In 2020, four of their European locations will also be rolling out Varonis in their environments.

> “Our goal is to eventually have Varonis oversee all of our file servers and core infrastructure throughout the company.”

With Varonis, the Information Security Manager has now **decreased open access by 79%** and **identified terabytes of stale data**—all in a fraction of the time a manual clean-up would require.

> “I used to spend day in, day out fixing permissions. And when it came to eliminating stale data, there was no good way to detect it. We weren’t using our resources efficiently.”
>
> “With Varonis, we’ve been able to automate remediation and eliminate terabytes of stale data. It’s given us room to improve our performance—not just from a security standpoint, but also from an overall infrastructure standpoint.

Varonis proved its value during the POC, by helping the company quickly recover from a potentially costly data loss incident. Now, it helps defend their servers against insider and outsider threats on a daily basis.

> “We always have Varonis running in the background. If there’s anything that needs our attention, DatAlert lets us know.”

Varonis has also given this manufacturing company the visibility and insight needed to remain GDPR compliant.

> “Varonis gives us the insight and immediate alerting we need to protect our customers and meet data privacy requirements. I don’t know how we would have achieved GDPR compliance without Varonis.”

> “With Varonis, we’ve been able to automate remediation and eliminate terabytes of stale data. It’s given us room to improve our performance—not just from a security standpoint, but also from an overall infrastructure standpoint.”


# Is your data infrastructure GDPR ready?

Varonis helps you fix overexposed data, detect threats, and meet data privacy requirements.

REQUEST A DEMO