How Varonis Helped a Life Sciences Company in Scotland Stop an Insider from Selling Trade Secrets

CASE STUDY

"One user tried to email some of our price lists to a competitor through their personal account. Varonis helped us see what data they were accessing and build a case against them."

ABOUT THIS CASE STUDY:

Our client is a Scottish company in the life sciences sector. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Protecting intellectual property and sensitive client data
- Enforcing GDPR and MHRA in a highly-regulated sector
- Preventing insider threats before company data is leaked

SOLUTION

- **DatAdvantage** maps data access activity across file and email systems
- **Data Classification Engine** finds and classifies sensitive data
- **Policy Pack** enhances Data Classification Engine with GDPR patterns
- **DatAlert** monitors and alerts on critical systems

RESULTS

- Stopped an insider from selling sensitive company information before the data breach occurred
- Built a case against the user by identifying anomalous activity and every file they touched
- Discovered and fixed security vulnerabilities to mitigate the risk of future data leaks

Challenges

Thwarting a costly exfiltration attempt

The user knew what they were doing when they logged into their personal email account and attached the confidential price lists.

They worked for a Scottish company in the life sciences sector (anonymous by request). The right buyer—especially competitors—would pay handsomely for insider information.

Fortunately, the IT manager had prepared for this worst-case scenario. They knew how much damage unscrupulous employees could do with trade secrets:

> “We potentially would have lost business. But the real fear is that this person could have done this multiple times—profiting on the side, while a competitor benefits at our expense.”

To mitigate the risk, the IT manager had built up a security stack that included both Varonis and an email gateway.

Varonis had originally been purchased to help eliminate stale data and protect financial information, PII, and intellectual property. **Data Classification Engine** and **Policy Pack** made it easy to enforce and comply with GDPR and MHRA (Medicines and Health products Regulatory Agency) rules.

Now Varonis would help them stop an insider from selling trade secrets and enable them to build a case against that individual.

> “Varonis doesn’t just help us identify stale users or manage file and folder growth. It also provides us with behavior analytics so we get real-time alerts on an unusual activity or behavior, such as a user accessing a high volume of files or files they don’t need.”

Without Varonis, figuring out what had been accessed would be nearly impossible. And, in a hypothetical scenario where that user began maliciously deleting files, discerning what to restore would have been a long and complicated process.

> “It would be very difficult and laborious to go back and access backups. We’d spend hours—days—digging through log files to try and figure out what had been changed. We wouldn’t be able to go back with 100% confidence.”

"Varonis provides us with behavior analytics so we get real-time alerts on unusual activity or behavior, such as a user accessing a high volume of files or files they don't need."

Solution

Detailed user forensics

When the user tried to send the incriminating email, the company's email gateway caught and held the files. Varonis alerted the IT manager to the attempted data breach and contextualized the attack.

> "I trust Varonis because it provides real-time alerts and behavioral analytics on each individual user account. It helps clarify what's normal activity for them—and if anything changes, I know about it."

Varonis gave the IT manager the insight they needed to build a case.

- **DatAlert** flagged the user's behavior as anomalous. That person had never accessed that type of data before, nor did they typically use their personal email account to send company files. DatAlert uncovered...
    - The user responsible
    - The time of the attack
    - The file they were attempting to move
    - The device they were using
    - The IP address of their device
    - Their geolocation

> "I could see the user accessing files that had nothing to do with them; they were from a different department—a different team."

The IT manager then turned to **DatAdvantage**, which mapped everything the user had touched, changed, or deleted and provided a holistic picture of their active permissions.

In conjunction with **Data Classification Engine**, which automatically scans for and classifies sensitive data, the IT manager discovered that the user was deliberately seeking out proprietary information they should have no reason to access.

Having built their case, the IT manager had all the evidence they needed to confront and terminate the guilty party.

> “Varonis gives us a lot more comfort and visibility. It has proved that it will help us catch insider threats in the future—and this incident helped us refine our permissions and alerting.”

The IT manager then used the knowledge that the user was able to access sensitive data to tighten permissions and fix what might otherwise be a huge, unchecked vulnerability.

> “I could see the user accessing files that had nothing to do with them; they were from a different department—a different team.”

Results

Defenses hardened against future attacks

This story has a happy ending: The company stopped the attempted data leak and rooted out the source of the problem.

But if this company hadn't invested in mitigative solutions, their situation could have been far worse...

The user may not have been caught until after they'd traded away proprietary data. They may never have been caught. And, worse, the company would be totally in the dark if the user continued to sell trade secrets.

The IT manager is happy that an early decision to invest in good data governance is now helping the company enforce GDPR and defend sensitive information against bad actors.

> "Varonis gives us a lot more visibility of data that we never had before. Managing data is not something that gets a lot of priority in terms of time and resources, so it's a huge help."

The IT manager says that having Varonis also "acts as a deterrent," dissuading others from attempting to steal or leak data in the future. But just in case, the company continues to harden its defenses against insider and outsider threats.

"Varonis is a powerful solution. Being able to instantly analyze our data security and see where we need to take action saves us time and money. The support is excellent and the software easily saves me a few hours every week."

"Managing data is not something that gets a lot of priority in terms of time and resources, so Varonis is a huge help."

What is your peace of mind worth?

Sleep easier, knowing that Varonis helps you prevent leaks and protect sensitive data.

REQUEST A DEMO