How a Large U.S. Mining Company Accurately Classifies and Cleans Up Millions of Files With Varonis

> Varonis makes every aspect of data governance a lot less time-consuming — from reporting to spotting problems at a glance. They've helped us wrangle an unmanageable amount of data.

About this case study:

Our customer is a large mining company in the United States. We have happily accommodated their request for anonymity.

Highlights

Challenges

- Monitoring their environment for threats like ransomware
- Detecting suspicious activity in Active Directory
- Enhancing the capabilities of a small IT security team

Solution

Varonis Data Security Platform:

- **DatAdvantage** provides complete visibility and control over your critical data and IT infrastructure
- **Data Classification Engine** finds and classifies sensitive data automatically
- **Data Transport Engine** enforces rules for data movement and migration
- **DatAlert** monitors critical systems and detects abnormal behavior

Results

- Millions of files remediated
- Locked down PII and other sensitive data
- Automatically enforced retention policies

Challenges

Gaining complete on-prem data visibility

An American mining company needed to get a handle on its sensitive data. The IT team wanted to proactively lock down PII on their local network and stay ahead of threats like ransomware.

> **An IT admin for the company explains, "The primary goal was identifying our sensitive data so that we could figure out what to do with it afterward."**

The company had been in business a long time — much longer than modern retention requirements — and accumulated a lot of sensitive data. Classifying, deleting, and quarantining so much data was impossible without more visibility and control over the environment.

> **"We didn't know how or where to start. All we knew was that it was too much to do manually."**

The company's team evaluated eight potential solutions, including Varonis. Then they narrowed the list down to three top contenders and performed a proof of concept for each.

Of the three potential solutions, Varonis was the standout choice. One of the other products repeatedly failed to scan their environment and deliver results, but Varonis was able to scan the company's environment in its entirety.

> **"Out of all of the products we tried, the best value and functionality is, without a doubt, Varonis."**

> **"Varonis was the absolute best at setting up a proof of concept quickly, concisely, and professionally. Nobody else matched their product knowledge or response speed."**

Solution

A suite of tools designed to find and fix exposed data

After completing due diligence, the company landed on Varonis. According to the IT admin, the decision made key users very happy because partnering with Varonis was “a night and day difference” from other vendors.

> “
>
> **The IT admin says, “Our system engineer helped set up each proof of concept, and at the end of almost every call, he’d say, ‘Can we please just go back to Varonis?’ So he’s happy now.”**

With Varonis in place, the IT team is finally able to capture a clear snapshot of their data environment.

DatAdvantage for Windows and Directory Services paints a picture of the entire domain hierarchy, recommends best practices on unused group memberships, identifies and flags over permissiveness, and gives the IT team safe change-modeling capabilities for groups and ACLs.

> “
>
> **“The simplicity and information provided in the dashboard are amazing. Varonis takes your hard-to-trace information and puts it all in one snapshot. Its AI-identified trends are extremely helpful. It really does the hardest part for you.”**

Data Classification Engine does the heavy lifting on data classification and optical character recognition (OCR). This enables the IT team to capture 100% of documents, including image files on PDFs. It also finds and identifies sensitive files, including exposed PII.

> “
>
> **“We’re focused on sensitive file discovery. Now we can send reports to site-level contacts and HR managers. It really helped during our cleanup phase. ”**

Data Transport Engine then enables automated retention policies. Custom rules automatically move, archive, quarantine, or delete sensitive data based on content type, age, sensitivity, and access activity.

Finally, **DatAlert** monitors all critical systems, detects abnormal behavior, and helps the IT team mobilize quickly in the event of ransomware or other malicious activity.

Using Varonis, the IT team successfully discovered and fixed a number of potential issues, including privileged accounts with passwords set to never expire, open access on sensitive files, and improperly stored PII (tax return data, active credit card numbers, and more).

> **“Varonis takes your hard-to-trace information and puts it all in one snapshot. Its AI-identified trends are extremely helpful. It really does the hardest part for you.”**

Results

On-prem environment on lockdown

With Varonis, the mining company successfully completed one phase of remediation. The first scan uncovered 17,000 sensitive files that were safe for removal. A second scan with OCR enabled uncovered an additional 23,000 sensitive files.

> **“In the first phase of cleanup, we removed 17,000 sensitive files. But by removing those sensitive files, we actually removed over a million native files. In the next phase of cleanup, we'll remove another 23,000 sensitive files, which will be millions more. We couldn't do it without Varonis.”**

Without Varonis, the IT admin says that purging sensitive data accumulated over decades would be nearly impossible. But with Varonis, the process is fast and effective, and the built-in change-modeling ensures that nothing is broken in the process.

> **“Varonis makes every aspect of data governance a lot less time-consuming — from reporting to spotting problems at a glance. They've helped us wrangle an unmanageable amount of data.”**

Varonis also provides reassurance for senior leaders and legal teams that good retention policies are in place and followed.

> **“Varonis enables us to minimize what's exposed. If it's not needed, we're deleting it. If it is needed, we're restricting access. We feel more confident in the state of our data and who has access to it as a result.”**

Once all of their on-prem data is locked down, the IT admin plans to focus on the company's online environment. When they do, **DatAdvantage for SharePoint Online** will enable them to enforce good data governance in the cloud.

"In the first phase of cleanup, we removed 17,000 sensitive files. But by removing those sensitive files, we actually removed over a million native files. We couldn't do it without Varonis."

VARONIS

Meet complex data retention requirements with ease.

Request a demo