How an International Law Firm is Remediating Nearly 470,000 Stale Sensitive Files With Varonis

CASE STUDY

> “Developing an in-house solution for auditing files and monitoring access would have been a crazy undertaking. Now add the capabilities of DatAlert and Data Transport Engine into the mix, and I don’t think you can replicate it. I can’t even imagine what it would cost.”

ABOUT THIS CASE STUDY:

Our client is an international law firm. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Gaining visibility and access control in critical file systems
- Mitigating the risk of data breaches and cyberattacks
- Moving sensitive files to secure locations en masse
- Eliminating stale data and enforcing retention policies that comply with data regulations

SOLUTION

The most robust data security platform:

- **DatAdvantage** to audit file access and review access permissions for remediation
- **Data Classification Engine** to classify and locate files with PII and other sensitive data
- **Data Transport Engine** to move sensitive data to secure locations and delete stale data
- **DatAlert Suite** to monitor file and email systems for signs of ransomware and other threats

RESULTS

- Tighter control and least-privilege implemented in all file servers
- Automated clean-up rules for over 2.6 million folders containing sensitive data
- Ongoing data migration for new files containing sensitive data
- Advanced threat detection and behavior-based security alerts

Challenges

IMPROVING DATA SECURITY AND INCIDENT RESPONSE

One of the largest international law firms (anonymous by request) approached Varonis with a problem that needed solving—they lacked clarity and visibility surrounding events in their file server.

As their Infrastructure Engineer explains:

> “We couldn’t answer questions like, ‘What happened to this file?’ or ‘What did this user change?’ We needed a solution that would help us audit our file servers.”

The Infrastructure Engineer understood that less visibility means more risk to data security. If they were to fall victim to a data breach or cyberattack, they might not know it until it was too late.

> “It often takes a disaster before companies are willing to spend money on data security. We couldn’t afford to wait for a disaster.”

An inability to sufficiently track and secure sensitive data would also put the firm at risk of non-compliance with international data privacy regulations, such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR).

To protect itself and its clients, the firm needed the ability to find and classify sensitive data, audit events in their server, and limit folder access to just the people who needed it.

The law firm also needed a way to transport sensitive data to more secure locations without complicating the workflow of over 2,000 employees. And, to enforce their 90-day retention policy, they needed an efficient way to quarantine and delete stale data.

These needs led them to Varonis.

> “Varonis’s backend infrastructure, platform, and reports—all of it is turnkey. Achieving something similar in-house would take a lot of work and an entire team of developers. Instead, we chose the most reputable company with the best track record.”

> “It often takes a disaster before companies are willing to spend money on data security. We couldn’t afford to wait for a disaster.”

Solution

MORE VISIBILITY AND CONTROL INTO CRITICAL SYSTEMS

DatAdvantage for Windows solves the law firm's urgent need for visibility by mapping permissions and user access history across file and email systems. If users have too much access, DatAdvantage provides a safe and easy way to test and commit changes to access control lists.

Data Classification Engine automatically scans their files for PII, PCI, HIPAA-related data, and other sensitive information. This solution helped the law firm identify 489,769 files containing sensitive data spread out across their network.

> "We're protecting data on our office file servers by frequently auditing who has access to that information and using Data Classification Engine to identify sensitive files."

After sensitive files have been classified, **Data Transport Engine** automatically migrates data from their office file server to a secure location based on predefined rules, without breaking permissions.

Data Transport Engine makes it easy to create and enforce data migration rules with special consideration for sensitive and regulated content. Even after the first migration is complete, it will continue automatically detecting and moving new sensitive data on an ongoing basis, while ensuring that nothing gets lost in the shuffle.

> "When Data Transport Engine moves a file, it leaves behind a 'stub file'—a small text file that links users to the file destination. This ensures that users who need access can still find the files and we're not making their lives more difficult."

But Data Transport Engine doesn’t just make it easy to move sensitive files to more secure locations—it also **automatically moves, archives, quarantines, or deletes stale data**.

This feature enables the law firm to enforce their 90-day data retention policy and streamline all of their compliance efforts.

> “When we need to run a report on the health of our file systems, we use Varonis. It helps us prepare for pre-assessment audits before applying for data privacy certifications.”

The final piece of the puzzle is the Varonis DatAlert Suite, which provides continuous monitoring on all data and systems and issues alerts whenever it detects suspicious activity.

> “We are using DatAlert to monitor for signs of intrusion or data breaches. DatAlert has built-in threat models that will help us mitigate the effects of ransomware and detect it before it can cause too much damage.”

The Infrastructure Engineer’s favorite thing about DatAlert is its flexibility. They’ve used it to create a number of bespoke alerts, including one custom script that automatically alerts IT whenever someone attempts to access a stub file containing sensitive data.

> “I created a DatAlert rule that sends our information governance team an email when a user clicks on a protected file. This allows us to reach out proactively, tell the user that they tried to access a file containing classified information, and ask why they need access.”

“When we need to report on the health of our file systems, we use Varonis. It helps us prepare for pre-assessment audits before applying for data privacy certifications.”

Results

EASY AND AUTOMATED CLEAN-UP OF OVER 2.6 MILLION FOLDERS

With Varonis systems in place, the law firm’s security team quickly and effortlessly identified over **2.6 million folders—93.36% of total folders—that contain sensitive data**.

They were able to trace sensitive data to 469,769 files within those folders. They also learned that over **95% of those sensitive files were considered stale**, and needed to be quarantined or deleted.

With Data Transport Engine, they’ve now begun the process of migrating sensitive files to a secure location. They’ve also begun automating the data retention process; Varonis has already helped them eliminate thousands of stale files.

“We’re using Data Transport Engine to move sensitive data—PHI, PCI, and other personal information—from our office file servers to a secure location. Then we’re going to focus on data retention.”

Once they complete their first big migration, Data Transport Engine will continue helping the law firm automate clean up of new files.

> “We have Data Transport Engine monitoring our systems on a set schedule. When it detects a file that hasn’t been touched for 90 days, it automatically moves or deletes that file.”

When it comes to return on investment, the law firm’s Infrastructure Engineer says that it’s beyond calculation:

> “Developing an in-house solution for auditing files and monitoring access would have been a crazy undertaking. Now add the capabilities of DatAlert and Data Transport Engine into the mix, and I don’t think you can replicate it. I can’t even imagine what it would cost.”
>
> “I don’t know of any other platform that does exactly what Varonis does. All of their products add up to one extremely valuable solution.”

> “We’re using Data Transport Engine to move sensitive data—PHI, PCI, and other personal information—from our office file servers to a secure location. Then we’re going to focus on data retention.”

VARONIS

Protect sensitive data. Automate compliance.

Varonis takes the complexity out of file auditing, securing sensitive information, and maintaining retention policies.

REQUEST A DEMO