How A Large U.S. Insurance Company Cleaned Up 3 Million At-Risk Folders in Under Two Weeks With Varonis Automation Engine

CASE STUDY

> “At this point, we just set it and forget it. Running Automation Engine at regular intervals ensures that broken permissions never last more than a week. We’ve been doing this for almost two years in our environment and we’ve never had a problem.”

ABOUT THIS CASE STUDY:

Our client is a large U.S. insurance company. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Over 75% of their data was stale and in need of archiving or deletion
- No visibility into customer PII and HIPAA unstructured data
- 3M+ folders with a complicated structure. Manually trying to limit global access would take years.

SOLUTION

The most robust data security platform:

- **DatAdvantage** for Windows, Directory Services and Unix
- **Data Classification Engine** to find and fix sensitive data
- **DatAlert Suite** to detect and eliminate potential threats
- **Automation Engine** to put remediation on autopilot
- **Data Transport Engine** to automatically move, archive, or delete stale data

RESULTS

- Fixed 60 TBs of over-exposed data with Automation Engine in 2 weeks
- Helped ensure HIPAA and SOX compliance
- Achieved HITRUST certification

Challenges

STALE DATA, NO VISIBILITY, AND 3 MILLION AT-RISK FOLDERS

Before Varonis, the Senior Security Engineer for a large U.S. Insurance Company (anonymous by request) was attempting to manually remediate global access to the organization's folders.

An internal audit had found large amounts of inactive data, PII data open to all users, and a huge number of broken ACLs. They had a pressing need for data classification and permission remediation in order to mitigate risk and ensure HIPAA and SOX compliance.

> "We had a problem—a security gap that left us vulnerable to bad actors who might try to gain access to sensitive user data."

But solving the issue wasn't easy. Over 75% of their data was stale—increasing cost and risk, while adding little value. All of it needed to be classified and then archived or deleted.

Their organization's complicated folder structure made manually locating sensitive, regulated data within their unstructured environments difficult. They had no visibility into their unstructured data, and no way to identify data owners.

> “Without Varonis to go through our shared drive and identify where PHI, PII, and other sensitive data was at risk, cleaning up all of our folders would have been impossible.”

The audit also revealed almost 3 million at-risk folders, including 140,000 folders with sensitive data that were open to everyone. Using custom PowerShell scripts to find and fix permissions for all 3 million folders was a nearly impossible (and potentially risky) task.

> “Going through and trying to fix permissions manually is time-consuming, and we’re a small team with other pressing things to do. Maybe if we had more people working on it and more time to dedicate to it, we could get through it in a year.”

“Without Varonis to go through our shared drive and identify where PHI, PII and other sensitive data was at risk, cleaning up all of our folders would have been impossible.”

Solution

REMEDIATION ON AUTOPILOT WITH AUTOMATION ENGINE

The first step in remediation was to implement DatAdvantage, Data Classification Engine, and the DatAlert Suite.

DatAlert is their first line of defense against suspicious behavior. It's an advanced threat detection and response system that provides daily protection with hundreds of built-in threat models.

> "DatAlert gives me peace of mind. I don't have to worry about bad actors in our environment because the alerts trigger any time there's a potential issue."

DatAdvantage and **Data Classification Engine** were instrumental in helping them find sensitive data, audit existing permissions, and begin limiting access to critical, protected folders.

> "We used Varonis to run reports on the locations of broken permissions. It saved a lot of time compared to trying to clean them up manually because we knew exactly where to look."

But with 3 million folders open to everyone, this organization needed a way to put global group access remediation on autopilot. They needed **Varonis Automation Engine**.

> “Setting up Automation Engine took less than half an hour. There was no need for configuration; we just turned it on and let it run. Automation Engine immediately started fixing our broken ACLs and permissions in the background.”

Two weeks later, Automation Engine finished cleaning up their massive access control list. All 3 million folders—60 terabytes of over-exposed data—were fixed.

> “It was so easy. I didn’t think it would be super difficult, but I wasn’t expecting it to be as easy as it was.”

But while the Security Engineers knew that the initial cleanup was important, they also knew how quickly problems can creep back in. By running Automation Engine on a weekly basis, broken ACLs continue to be fixed automatically.

Next, they launched straight into a proof of concept for Data Transport Engine, which automatically moves, archives, quarantines, or deletes data based on predefined parameters.

> “Like the rest of the Varonis interface, Data Transport Engine is simple to use, but it’s powerful in the sense that you can configure it to effortlessly move certain files to different locations and then let it run in the background.”

> “Setting up Automation Engine took less than half an hour. There was no need for configuration; we just turned it on and let it run. Automation Engine immediately started fixing our broken ACLs and permissions in the background.”

Results

60 TBS OF OVER-EXPOSED DATA CLEANED UP IN 2 WEEKS

According to the Senior Security Engineer, Automation Engine decreased the time spent on ACL clean up and remediation by 98.7%. It helped them clean up 60 terabytes of over-exposed data while allowing them to focus on other mission-critical tasks—doing in two weeks what would have taken their small team the better part of a year to accomplish.

Now, they run Automation Engine each weekend and run a report every Monday to catch any errors that might have crept in (e.g., if someone improperly copied a directory into another parent folder).

> “At this point, we just set it and forget it. Running Automation Engine at regular intervals ensures that broken permissions never last more than a week. We’ve been doing this for almost two years in our environment and we’ve never had a problem.”

By giving them more visibility into their unstructured environments, Varonis has helped them rein in their out-of-control data and ensure that PII and HIPAA data is only accessible by those who need it. This goes a long way toward ensuring regulatory compliance.

> “We use Varonis to make sure PII data like social security numbers and date of birth are locked down. Data Transport Engine helps enforce our retention policies by purging sensitive data that hasn’t been touched or accessed within a certain timeframe.”

In recent years, this organization also achieved HITRUST certification. With Varonis, they were able to demonstrate that they have a robust security framework in place, show that they have implemented the necessary controls to protect ePHI, and prove compliance with HITRUST CSF.

> “Achieving certification requires specific safeguards and visibility requirements. Being able to see where our sensitive data is and protect it with Data Classification Engine and DatAlert were huge value-adds that helped us move forward with HITRUST.”

This organization has now been using Varonis for over five years. Together, they’ve built a strong and lasting partnership.

> “Varonis’ support is the best support of any software solution that I have worked with. They’re always there to help at no additional cost. There’s no reason not to reach out for a demo, spin it up in your environment, and see all the value it provides.”

“We use Varonis to make sure PII data like social security numbers and date of birth are locked down. Data Transport Engine helps enforce our retention policies.”

VARONIS

Find and fix all your open shares in no time flat.

Mitigate risk and lock down your sensitive data by automating remediation with Automation Engine.

REQUEST A DEMO