VARONIS

How Varonis Helped a Local Government Automate Data Security Posture Management

> We went from 65,000 open, at-risk files down to zero in a matter of months. With Varonis, we achieved a better security posture than we thought possible.

About this case study:

Our customer is a local government in the U.S. We have happily accommodated their request to anonymize all names and places.

HIGHLIGHTS

Challenges

+ Securing folder permissions to limit external exposure without impacting operations
+ Ensuring compliance with HIPAA, PCI, CJIS, and more
+ Remediating 65,000-plus files spread across 200TB of data

Solution

The Varonis cloud-native Data Security Platform:

+ Continuously discovers and classifies critical data across SaaS apps, email, cloud, and hybrid file systems
+ Locks down permissions and prevents exposures
+ Proactively detects and helps prevent threats

Results

+ Best-in-class data security posture management
+ Effortless compliance management
+ Recouped licensing fees
+ Previously unseen threats detected and defeated

CHALLENGES

Prioritizing data convenience over security

As a large local U.S. government grew, its blast radius expanded, and like many large organizations, data convenience for the sake of business continuity and efficiency took priority over security.

Although users could access the data they needed more easily, the potential damage one compromised account or malicious insider could inflict was far greater.

From a compliance management perspective, the situation was dire. Local agencies must comply with several data regulations, including HIPAA, PCI, CJIS, and more. Violations for noncompliance can result in hefty fines.

Even worse was the fact that lives were on the line. Ransomware can grind routine services and operations to a halt. Dozens of agencies were at risk, including first responder services.

A Storage Admin for the government explains:

> **"We have to comply with HIPAA, PCI, and other criminal-justice compliance regulations. We have police departments. We have health departments. We knew sensitive data was out there, but we didn't know where exactly or how it was being presented to the rest of the network."**

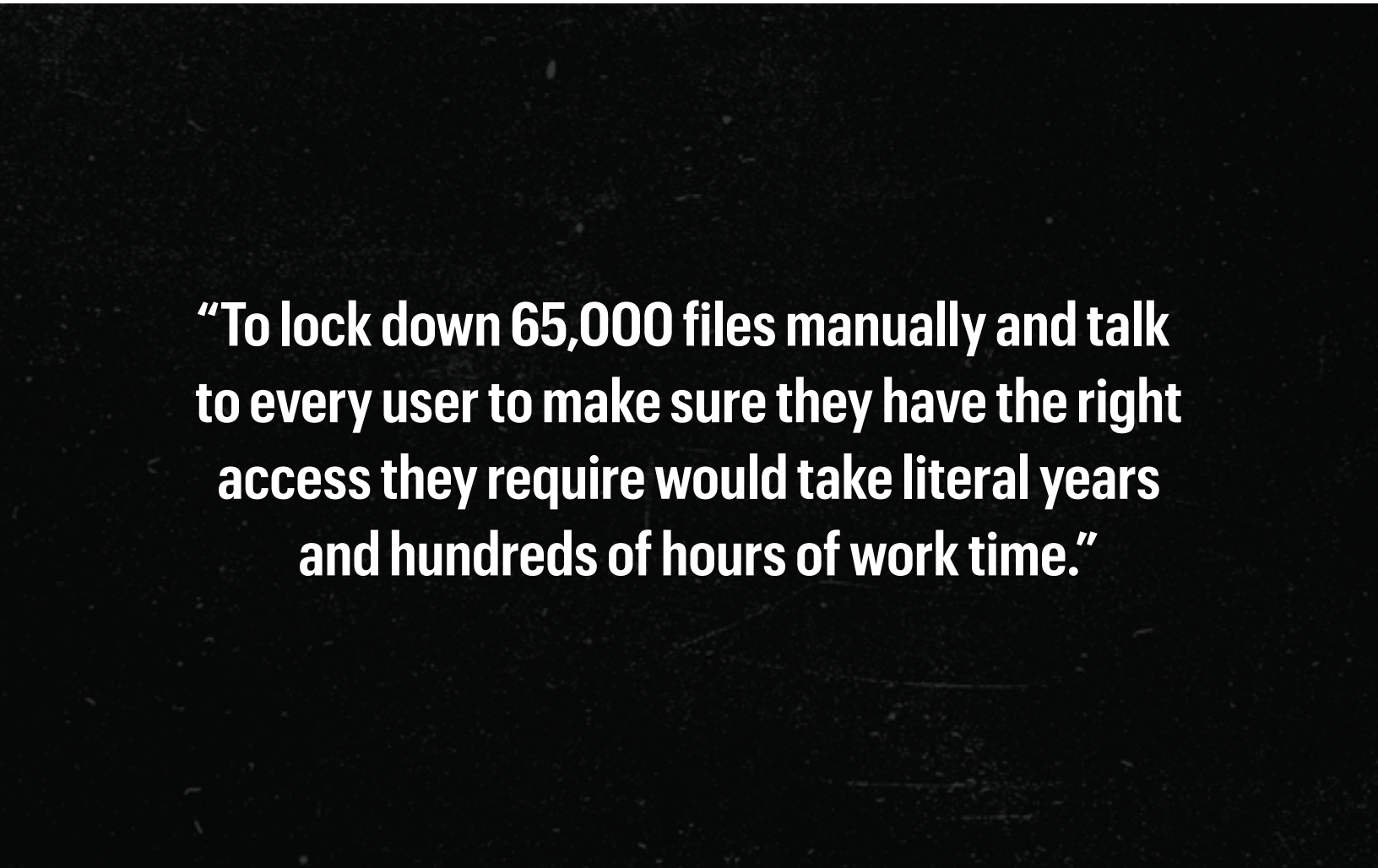
“We knew sensitive data was out there, but we didn’t know where exactly or how it was being presented to the rest of the network.”

Navigating an “impossible” remediation project

While the government searched for a solution, its risk profile continued to escalate.

They had thousands of overexposed files across its 200TB data stores, and any of the government’s 10,000-plus users could inadvertently click on a phishing link, putting sensitive information at risk.

> **“To lock down 65,000 files manually and talk to every user to make sure they have the right access they require would take literal years and hundreds of hours of work time.”**
>
> **“We couldn’t get it done. We tried for years. No one could take time to review it all, and security was not a priority on users’ lists. Their job is to do their jobs. They’re not hiring people to take care of file security.”**



SOLUTION

Locking down environments

After the government started with Varonis' self-hosted Data Security Platform, they finally locked down permissions for more than 10,000 users and 65,000-plus overexposed files.

When Varonis announced the availability of its cloud-native Data Security Platform, the government decided to make the switch and take advantage of even more automation capabilities, in addition to easier deployment.

> **"Varonis' cloud-native platform allowed us to spread our impact of Varonis and its abilities to other areas, including our Active Directory and Microsoft 365 environments, in addition to the original on-prem environment."**
>
> **"We were able to offload a lot of the infrastructure and have very good response time without having to maintain the infrastructure on-site to keep up with the reporting that we were doing, especially as we added the other environments."**

With the Varonis Data Security Platform, the government could accomplish three essential things automatically and at scale:

1. Discover and classify critical data.

2. Ensure only the right people have access.

3. Detect abnormal behavior.

> **"Varonis scans our data and identifies where our sensitive data is. At the same time, Varonis identifies the security risks and combines those into a report that shows, 'Hey, you have sensitive data that has open permissions. You need to take action and use automation to secure it.' It's a trifecta of security."**

To the IT team's delight, Varonis integrated seamlessly with NetApp systems to continuously discover and classify critical data and effortlessly remediate exposure. The local government extended this to all SaaS apps and email, its cloud infrastructure, and its hybrid file system.

> **"We initially purchased Varonis for a very specific use case of securing these environments. Varonis successfully and efficiently scanned our data, provided reports, and then took it a step further by providing automation tools that we could use to resolve the issues we were seeing."**

Reducing their blast radius with automation

The Varonis AI-powered automation now remediates new risks and policy violations as they appear. This includes auto-fixing misconfigurations, applying or fixing sensitivity labels, revoking unnecessary permissions, and remediating public links to sensitive data.

The Varonis Data Security Platform works in the background without impacting day-to-day business operations for the government or its users.

> **"We had to address balancing security and convenience and the Varonis automation helped balance that out and give us the security without requiring any interactions from the users at all."**
>
> **"We secured all files open to our internal environment without any real interaction with the user communities. They didn't have to lift a finger. It was simple for the administrators — point-and-click security."**

Varonis also automatically enforces least privilege to ensure that only the right people can access sensitive data. Now their potential blast radius is significantly reduced if a user accidentally clicks on a phishing email or follows a suspicious link.

> **"When it comes to automating the configuration of permissions — including adding, changing, and removing permissions — we're able to schedule those at night, run them while people are off-hours, fix permissions, update permissions, and service user requests without any kind of interruption. Schedule it, fire, and forget."**
>
> **"We secured all files open to our internal environment without any real interaction with the user communities. They didn't have to lift a finger. It was simple for the administrators — point-and-click security."**

RESULTS

Best-in-class data security posture management

Within a few months of switching to the Varonis cloud-native Data Security Platform, the local government's IT team successfully accomplished what had previously been impossible.

> **"The greatest success was automating the remediation of our global access groups. That process alone reduced our risk of [this type of] exposure 100%. We went from 65,000 open, at-risk files down to zero in a matter of months. With Varonis, we achieved a better security posture than we thought possible."**
>
> **"Varonis has been 100% accurate, with zero false positives that I've seen. Now we have clear visibility into how it's being used and exposed or, in this case, secured."**

Effortless compliance management

The local government can now visualize its data risk, prevent exposures, and detect threats in real time. And when compliance auditors come knocking, the IT team has the reporting to show that their environments are still in good health.

Added cost savings from increased visibility

The final cherry on top of the data security sundae comes in the form of cost savings. For example, the local government used Varonis to identify and delete hundreds of stale accounts, recouping hundreds of thousands of dollars in licensing fees.

> **"We identified stale directory accounts and deleted those accounts, freeing up the associated Microsoft 365 licenses and saving hundreds of thousands of dollars. Varonis gave us the observability to audit user IDs, remove inactive accounts, and recoup those license fees."**

Automate your data security posture management.

Request a demo