How a Publicly Traded Investment Company Fixes Tens of Thousands of Broken Permissions with Varonis

CASE STUDY

"If I cleaned up broken permissions every day for eight hours a day, it would take me three years. With Varonis, it takes under a week."

ABOUT THIS CASE STUDY:

Our client is a publicly traded investment company. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Enforcing CCPA compliance
- Identifying and locking down sensitive customer data
- Fixing broken permissions inherited through M&A activity

SOLUTION

Varonis Data Security Platform:

- **DatAdvantage** maps data access activity
- **Data Classification Engine** finds and classifies sensitive data
- **Policy Pack** enhances Data Classification Engine with CCPA patterns
- **DatAnswers** simplifies CCPA compliance
- **DatAlert** monitors and alerts on critical systems
- **Edge** detects and helps prevent DNS exfiltration attempts
- **Automation Engine** safely and quickly fixes thousands of broken permissions

RESULTS

- Increased visibility to find and fix the most vulnerable areas
- Fixed 30,000 broken permissions in under a week
- Simplified CCPA compliance and introduced time-saving automations

Challenges

Getting up to speed on compliance regulations

One Varonis customer—a full-service, publicly traded investment company (anonymous by request)—is subject to many data regulations, including Sarbanes-Oxley (SOX) and the California Consumer Privacy Act (CCPA).

The company needs to comply with every customer request to delete sensitive personal data. If they can't, because they lack the resources or don't know where the data is stored, they would lose customer trust and could be fined thousands of dollars for each violation.

At first, keeping track of this sensitive data manually was doable... but the company was growing fast. Before long, it became impossible to know where everything was being stored. As the Security Manager explains:

> "When I joined the team, no one could tell me where our data was. No one could tell me where our classified data was. No one could tell me where our regulatory data was. We had to get this company up to speed on its regulation compliance."

The small size of the IT security team was only part of the problem. The larger issues were a lack of automation to help enforce least privilege and no easy way to search through hundreds of thousands of files for CCPA-regulated data.

> “Even if you have a thousand people, no one has the work hours to go through every server and look for classified documents. And all of your best practices go out of the window the moment someone creates an open access document that you don’t know about.”

Mergers and acquisitions (M&A) also threw a wrench into compliance. When “business as usual” involves acquiring other companies and their infrastructure, you risk inheriting their data and permissions problems as well.

In this investment company’s case, one acquisition came with tens of thousands of broken permissions. The Security Manager realized that if they did nothing but focus on broken permissions day-in and day-out, **fixing it would still take them over three years.**

> “When you’re doing an M&A, things move fast. Sometimes, for security reasons, people don’t want you to look under the hood before the papers are signed. We inherited one server alone that had 30,000 broken permissions.”

“Even if you have a thousand people, no one has the work hours to go through every server and look for classified documents.”

Solution

The most robust data security platform

The Varonis Data Security Platform gives the Security Manager heightened visibility and control over data.

DatAdvantage shows where the company is most at risk, with at-a-glance insight as to who has permission to access sensitive files, who actually accesses those files, and when files have been moved or deleted.

With DatAdvantage support for Windows, Exchange, Directory Services, SharePoint, and OneDrive, the Security Manager can follow a unified audit trail of events throughout their environment.

Data Classification Engine looks inside files and identifies at-risk sensitive data. **Policy Pack** enhances Data Classification Engine with CCPA patterns, enabling the Security Manager to locate and lock down regulated data.

When it comes to satisfying compliance requests, **DatAnswers** has been invaluable. Its intuitive search and exporting capability make it easy to find, move, or copy files to send to legal and compliance.

> “We got DatAnswers to be compliant with CCPA. DatAnswers enables us to tell regulators that we have the ability to look up all of the information on Jane Doe. I can locate it and delete it if she asks.”

When the FBI alerted the company to a possible unemployment fraud scheme, the Security Manager used DatAnswers to cross-check the information provided against employee records to determine that the claims weren’t coming from the company. An investigation that could have taken days was wrapped up within 20 minutes.

DatAlert and **Edge** help the company protect sensitive data against insider and outsider threats. Real-time alerting on file activity combined w¬ith perimeter telemetry mitigate the risk posed by ransomware, exfiltration attempts, and human error.

> “Varonis feels like an extra security team member—it’s great at telling me what I need to pay attention to without making a lot of ‘false noise.’
>
> That’s without mentioning the value of Varonis’ Incident Response team. That’s an extension of your security team right there. Varonis has the best support out of any vendor I’ve worked with.”

Most importantly, **Automation Engine** helps solve potentially major issues inherited through M&A activity—like the 30,000 broken permissions. Manual clean up is never time- or cost-effective. Automation Engine helps the company safely and automatically execute on large-scale remediation projects.

> “Varonis is great at telling me what I need to pay attention to without making a lot of ‘false noise’ … and they have the best support out of any vendor I’ve worked with.”

Results

Fixing 30,000 broken permissions in days, not years

Varonis helps the Security Manager tighten data security and streamline data governance. Its intuitive reports show them where they're most at risk, and what to prioritize.

> "The reports we use regularly expose too much open access, privilege creep, and exposed classified data. By figuring out where that data is, we can get it locked down properly."

Varonis adds to peace of mind when it comes to mergers and acquisitions. **With Varonis, it's possible to clean up 30,000 broken permissions within one week**—so even if they inherit an untidy infrastructure, remediation is fast and easy.

> "I calculated how long it would take to fix 30,000 permissions. If I cleaned up broken permissions every day for eight hours a day, it would take me three years. With Varonis, it takes under a week.
>
> When it comes to data governance, you can hire three extra bodies or you can have one product take care of it for you. Varonis will quickly pay for itself, even if all you focus on is low-hanging fruit. There is absolutely nothing to lose by trialing Varonis."

Varonis is quickly becoming ubiquitous, company-wide. Both the security team and the IT team are being trained to better maintain file health and proactively defend sensitive data.

When it comes to CCPA compliance, the company has never had tighter control or more visibility over their infrastructure.

> "From an overall compliance perspective, being able to report back and being compliant with the CCPA ... we did not have that ability before Varonis."

"When it comes to data governance, you can hire three extra bodies or you can have one product take care of it for you. There is absolutely nothing to lose by trialing Varonis."

Simplify security and data governance.

Take control of your environment, enforce compliance, and mitigate risk with Varonis.

REQUEST A DEMO