



How Varonis Helped a Public School System Investigate a Potential Data Breach



Varonis does all the aggregate work for me of classifying data in our file server, SharePoint, OneDrive, and our entire Microsoft 365 environment, and making sure our information is secure.

About this case study:

Our customer is a public school system in the U.S. We have happily accommodated their request for anonymity.



Highlights

Challenges

- Knowing where sensitive data exists in their environment and who can access it
- Securing on-prem and cloud Microsoft environments
- Investigating if sensitive data was leaked from their system

Solution

Varonis Data Security Platform:

- **DatAdvantage** gives complete visibility and control over your critical data and IT infrastructure
- **Data Classification Engine** finds and classifies sensitive data automatically
- **DatAlert** monitors and alerts on abnormal behavior on critical systems

Results

- Confirmed that the school hadn't suffered a data breach
- Locked down sensitive files on prem and in the cloud
- Growing use of Microsoft 365 with confidence

Challenges

Protecting sensitive data

Before Varonis, a U.S. public school system (anonymous by request) had trouble answering critical questions about sensitive data. They realized that they needed deeper insight into user activity, especially surrounding Personal Identifiable Information (PII), in order to better secure student data, delete stale data, and satisfy compliance requirements.

But limited time and tight budgets proved constant barriers to managing PII and other sensitive data. A small team with limited resources was tasked with handling the entire district's data governance. They needed a solution to serve as a long-term force multiplier, because they couldn't afford to hire more people or spend a lot of time in training.

“

“More than anything, we needed to track down all of our PII and anything else that might be sensitive—student information, social security numbers, and that kind of thing,” explains a Security SysAdmin.

Knowing that sensitive data needed to be secured across Microsoft environments on prem and in the cloud, the school system decided to perform a Proof of Concept of Varonis.

Varonis offered the visibility they needed to classify sensitive data, the ability to lock it down, and alerting that would help them proactively protect data against ransomware.



“Varonis flagged all this data that was almost a decade old and alerted us to at-risk areas. The risk assessment made us aware of just how much PII and other data we were holding.”

When the school system faced an incident where employee data may have been compromised and used to falsely file for unemployment benefits, they jumped into action.

“More than anything, we needed to track down all of our PII and anything else that might be sensitive.”

Solution

Protecting employee and student PII at scale

The school decided to adopt three Varonis solutions: DatAdvantage, Data Classification Engine, and DatAlert.

Their goal was to better answer questions around sensitive data, proactively protect data against insider and outsider threats, and determine if any sensitive data was leaked.

DatAdvantage is the heart of the Varonis Data Security Platform. Modules for Windows, Directory Services, and Microsoft 365 give the admins visibility into the school system's hybrid infrastructure. Sysadmins can now answer critical questions like who's accessing data and where users are over permissioned, and then safely lock down access.

Data Classification Engine automatically finds and classifies sensitive data across the school's on-prem and cloud environments. With insight into which files have high concentrations of sensitive records, sysadmins can visualize data risk and prioritize remediation projects.



“We’re finally comfortable knowing where we have sensitive data, having gone through the entirety of our SharePoint, OneDrive, and primary file server and classified everything that needs to be classified.”

DatAlert monitors file shares for suspicious activity on file and email systems. Varonis helped the school system implement DatAlert in their environment and reduce the signal-to-noise on alerts so that only high-priority alerts get surfaced.



“Checking in on the alerts that come in has become a daily habit. It’s great to go in and see that the vast majority of issues we need to fix pertain to stale data.”

When DatAlert does detect a problem, Varonis' Incident Response team leaps into action to help the school's sysadmins investigate and resolve the potential issue.



“DatAlert detected something that might have been malware in our file server. The Incident Response team helped me immediately and the issue was resolved within an hour. It’s amazing—almost like we have Varonis as part of our team.”

“We’re finally comfortable knowing where we have sensitive data, having gone through the entirety of our SharePoint, OneDrive, and primary file server and classified everything that needs to be classified.”

Results

Proving that no PII was leaked

Armed with a comprehensive report on user activity around sensitive data, the school's sysadmins were able to prove that no PII was exposed and that employee data used in the unemployment scam hadn't leaked from their system.

The evidence was clear—there hadn't been a breach.

Vindicated, the sysadmins started using Varonis to reduce future risk. They began locking down sensitive data. Being able to safely grow their presence in Microsoft 365 helps keep classes in session, even during the pandemic.



“Varonis does all the aggregate work for me of classifying data in our file server, SharePoint, OneDrive, and our entire Microsoft 365 environment, and making sure our information is secure.”

At the same time, having proof of compliance coupled with high-fidelity alerting helps the IT team prove value to the entire school district. It also helps them with cyber insurance negotiations, as they try to secure more favorable rates.

Despite all of these steps, the Security SysAdmin says that they've only scratched the surface of what's possible with Varonis.

“I looked at what Varonis was capable of and thought, ‘Wow. This is so powerful.’ Then I realized that I was only looking at one product—and there's even more it can do.”



Varonis—see what you've been missing.

Confidently answer questions around your critical data and protect your data from compromise.

[Request a demo](#)