



How Varonis Automation Engine Helps a U.S. University Reduce Its Attack Surface by 99.9%

CASE STUDY



“We had 84,000 folders with open access. Within a week of turning on Automation Engine, we brought that number down to 51—reducing our liability footprint by 99.94%.”



ABOUT THIS CASE STUDY:

Our client is a liberal arts university in the U.S. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Understanding who has access to sensitive data and proving that protective measures are in place
- Discovering data to comply with data subject access requests (DSARs)
- Complying with data privacy regulations including:
 - + Gramm-Leach-Bliley Act (GLBA)
 - + Sarbanes-Oxley Act (SOX)
 - + General Data Protection Regulation (GDPR)

SOLUTION

The most robust data security platform:

- **DatAdvantage** to audit and remediate who has access to sensitive folders
- **Data Classification Engine** to locate and classify sensitive student and faculty information
- **Automation Engine** to safely remove global access from tens of thousands of folders within a few days
- **DatAlert** helped detect a credential stuffing attack

RESULTS

- Attack surface reduced by 99.94%
- A major cyberattack prevented and tracked to its source
- Enhanced ability to prove compliance with data privacy regulations and fulfill DSARs

Challenges

Proving compliance and mitigating the risk of data breaches

Stale data opens the door to data breaches, and data breaches pose a major threat—especially to universities and colleges. Learning institutes house everything from student financial data to personally identifiable information (PII) to proprietary research.

That was the challenge facing the CTO of a major liberal arts university in the U.S. (anonymous by request). With almost five terabytes of unstructured data on their servers, they didn't have the resources or workforce required to find where sensitive information lived and who had access to it.



“Before we purchased Varonis, we had no way to understand our unstructured data. We lacked the tools to implement a good data governance policy. We couldn't even locate stale data, or see how much of our stale data was sensitive.”

Should a worst-case scenario occur, the CTO and their team would need to be able to prove to auditors that the university had taken every possible step to mitigate the risk of data breaches—something they couldn't do before Varonis.

“

“If we couldn’t tell somebody where their data lives and who had access to it, how could we hope to answer an auditor in the event of a data breach? Juries don’t look favorably on businesses that don’t take every reasonable precaution to protect private data.”

Learning institutes need to understand compliance requirements that extend beyond state lines. For example, if a student is a European citizen and they submit a data subject access request, the university is responsible for discovering exactly where their data lives, who has access to it, and fulfilling their request requirements.

Colleges and universities also need to be able to prove compliance with a myriad of national and international data privacy regulations.

“

“We have to comply with the GLBA, SOX, and any other federal regulations that deal with how we handle student financial aid and personally identifiable information. We also have international students, and we need to comply with regulations like GDPR too.”

”

“Juries don’t look favorably on businesses that don’t take every reasonable precaution to protect private data.”

Solution

Proving compliance and mitigating the risk of data breaches

The university's first priority was protecting its students, so they adopted two products that form the backbone of Varonis' solution.

DatAdvantage for Windows maps out who can access and who does access data across their on-premises data stores and email systems. If users ever have too much access, it safely automates changes to control lists and security groups.

Data Classification Engine shows where data is most at risk. With it, the CTO was able to automatically locate and classify sensitive data that lived in the university's storage area network (SAN).



“Even I was surprised by the amount of duplicate and stale sensitive data that lived throughout our SAN. Fortunately, Varonis is fire-and-forget. It automatically filters for sensitive data and points us to places where we're at risk, so we don't have to think about it.”

With DatAdvantage and Data Classification Engine, the CTO discovered something alarming: over 84,000 folders open to everyone, including 11,000 folders containing sensitive data.

Remediation was too big of a job for their small team. Fortunately, Varonis Automation Engine allows the CTO and their team to safely remove global access en masse with the click of a button.



“Maintaining a network without Varonis is like walking toward a cliff—especially if you're trying to protect user privacy. Without a way to identify and classify unstructured data, you're one wrong step away from disaster.”

Varonis helps stop a brute-force cyberattack

During a proof of concept of another product, DatAlert, a Varonis technician noticed something strange: a report of 29 failed authentication attempts with an invalid username.

The Varonis Incident Response team quickly traced the problem to a single server configured to allow users remote access to network resources. They realized that they were witnessing a credential stuffing attack in action.

Luckily, the university's strict password requirements prevented a data breach and Varonis helped them discover and fix the problem. Without Varonis, the attack would have gone unnoticed.



“Someone was definitely trying to get in with a stale account that might have been stolen. We have deletion procedures for these accounts, but one slipped through the cracks. Varonis helped us identify the threat, fix the vulnerability, and put our minds at ease.”

According to the CTO, it's that level of support and responsiveness that makes Varonis such an invaluable partner. And, they say, it's granular insight—like the ability to trace an attack to its source—that makes Varonis such an important part of the university's security solution.



“I have a Varonis alerts folder in my Outlook and I review it every day to understand what's going on in my environment.”

“If I ever have a problem, I can count on Varonis' truly excellent after-sale support. If I need a question answered, I need an answer now. Varonis' team provides those answers when I need them.”



“Varonis is fire-and-forget. It automatically filters for sensitive data and points us to places where we’re at risk, so we don’t have to think about it.”

Results

Attack surface decreased by 99.9%

Before Varonis, 95% of the university’s folders were open to every employee in the organization. Tens of thousands of folders—and hundreds of thousands of files—were vulnerable.

Using Automation Engine, the CTO and their team reduced the amount of exposed files to less than 0.1% in just a few days.



“We had 84,000 folders with open access. Within a week of turning on Automation Engine, we brought that number down to 51—reducing our liability footprint by 99.94%.”

The university now has 360-degree visibility into their unstructured data. If they get audited or if a student submits a data subject access request, they can almost effortlessly point to what they’re storing and prove that they know where data lives and who has access to it.

That visibility, the CTO says, is invaluable.

“

“The biggest threat facing most companies—especially higher education—is that they can’t see where unstructured data lives. They’re lost in the dark and blind to potential threats. Varonis shines a light on your unstructured data.”

When it comes to mitigating risk, proving compliance, and protecting the PII of its students and faculty, the CTO can’t imagine how higher education institutions can feel secure if they don’t have a solution like Varonis.

“

“I love Varonis. Their products make life easier. Their people are smart as whips and they really care about you. They really want to see their product succeed in your environment.”

”

“The biggest threat facing most businesses—especially in higher education—is that they can’t see where unstructured data lives. They’re lost in the dark and blind to potential threats. Varonis shines a light on your unstructured data.”



Protect sensitive data. Automate compliance.

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

REQUEST A DEMO