How Varonis Helps a U.S. Cultural Institution Protect Against Cyberattacks

> Our threat factor is 25x higher than most other institutions our size. With Varonis, we're alerted to abnormalities early so we can correct them immediately—and I can sleep at night.

About this case study:

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

HIGHLIGHTS

Challenges

- Protecting against constant cyber threats
- Improving a time-consuming audit process
- Finding a security platform to protect data in the cloud

Solution

The **Varonis Data Security Platform:**

- Gives complete visibility and control over critical data in Google Drive, Zoom, and Box
- Finds and classifies sensitive data automatically
- Repairs and maintains file system permissions
- Monitors and detects abnormal behavior in critical systems

Results

- 72% reduction in broken permissions
- Greater protection from yberattacks
- More visibility into SaaS ecosystem

CHALLENGES

High level of threats from outside actors

One U.S. cultural institution lives under constant threat of outsider attacks. With that risk top of mind, protecting donor privacy is the security team's highest mandate.

Their security team built an audit process to help identify and defend sensitive data. But there was a catch: the process was rigorous and inefficient. A complete audit would have taken weeks—time the security team couldn't spare.

We talked with Michael Trofi, from Trofi Security, who has more than 30 years in the security space providing vCISO, SOC, audit, and assessment services.

> **"We never had enough time to do the audit properly, so we were always afraid that we missed things."**

A data breach was a worst-case scenario. If donors' PII was exposed, they could be targeted by attackers.

> **"The worst thing that could happen is that a spreadsheet with donor information gets leaked."**

The institution needed to know: how big was the risk? To answer that question and gain a true-to-life data vulnerability report, they engaged Varonis for a free Data Risk Assessment.

The results were sobering—the customer had a huge amount of stale data in the cloud and on-prem and an alarming amount of open access. The issues were more than the lean security team was equipped to handle on its own.

> **“Discovery scans during an audit showed we had a lot of information that was shared out. I knew there was a problem, but it was far worse than I thought.”**

Fortunately, Varonis brings automated data security to cloud repositories, SaaS apps, and on-prem data stores—taking the burden off of security teams so they can stay ahead of ever-growing data and sharing.

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

“We’re always under threat. We receive threats that are on par with three-letter government agencies.”

SOLUTION

Protecting donor information

The **Varonis Data Security Platform** forms the bedrock of the Varonis Data Security Platform. With these products, the institution's security team can see the true extent of data exposure and gain more control over critical data in the cloud and on-prem.

According to the CISO:

> **"We tend to keep things around forever. But this pushed us to create new policies around archiving data to reduce the risk of data leakage and minimize the threat footprint."**

The cultural institution also implemented data classification for Windows and SharePoint to find and classify sensitive data that might put donors at risk.

With Varonis, risk remediation is faster and more efficient. Varonis allowed the institution to accelerate their risk reduction efforts by analyzing who actually needed access to data and removing access from everyone else. This helps control access to sensitive data and dramatically reduces the potential damage a nefarious actor could do.

Extending protection to the cloud

Next, the security team rolled out **Varonis for Google Drive**. In just 15 minutes, they could see what sensitive information had been saved in Google Drive and how it was being shared.

This gave the security team visibility that was orders of magnitude greater than what they had before. But with that visibility came new surprises, according to the CISO:

> **"We discovered that a good percentage of the staff was sharing personal folders out to their personal emails. When an employee leaves, we disable their accounts—but they still had access to their data. It was eye-opening."**

It was a seismic problem the IT team didn't know about before. They leapt into action, creating new data retention policies and setting up shared drives with stricter security. They also reoriented all IT staff with best practices.

In addition to **Varonis for Google Drive**, the cultural institution also adopted **Varonis for Box** and **Zoom**. These additions will help protect the confidentiality of data, eliminate exposure, and accelerate cross-cloud investigations.

Real-time alerting on all data, all the time

With access to data locked down, there was still one thing left to address: detecting external threats.

The cultural institution needed to know when user behavior put data at risk. And they needed the ability to stop malicious attacks in their tracks. That's where Varonis comes in.

> **"Data loss is something that used to keep me up at night. Users tend to click on a lot of emails and bad things. But Varonis detects ransomware signatures and shuts them down automatically."**

"We had no insight into who was sharing what on Google. Varonis classified our data and gave us visibility we didn't have before."

RESULTS

A cultural institution is free to continue its important work

Today, the cultural institution's file shares are more secure and require far less manual upkeep. Audits that used to take weeks are now completed with one click—and cleaning-up permissions is just as easy.

Varonis helped the CISO and their security team proactively identify risk and then take steps to train other staff to be more secure in their online communication and file sharing. Their efforts have been rewarded with a steep decline in alerts, according to the CISO:

> **"We now identify data in the cloud and on-prem to see where PII data is flowing or stored so we can follow best practices around data privacy."**

When the CISO performed a penetration test, the blue team (simulating a defensive security team) used Varonis to catch and stop everything that the red team (simulating malicious hackers) could throw at them.

> **"We conducted a penetration test and caught everything we tested. It confirmed that our cyber defenses are working."**

Even in a worst-case scenario, the cultural institution's good data hygiene has effectively minimized the blast radius of any attack. They decreased the number of folders with stale data by 54% and the number of stale users by 44% in just seven months.

They've also reduced the number of folders with broken permissions by 72% in the same timeframe.

Today the CISO feels good about the work they've done to protect this important cultural institution.

> **"Most security officers assume that if they haven't been breached or lost any data, everything must be okay. But in reality, it isn't."**

“Varonis shows you security weaknesses you didn’t think you had. And you can’t fix what you don’t know.”

Find and fix your data security weaknesses.

Request a demo