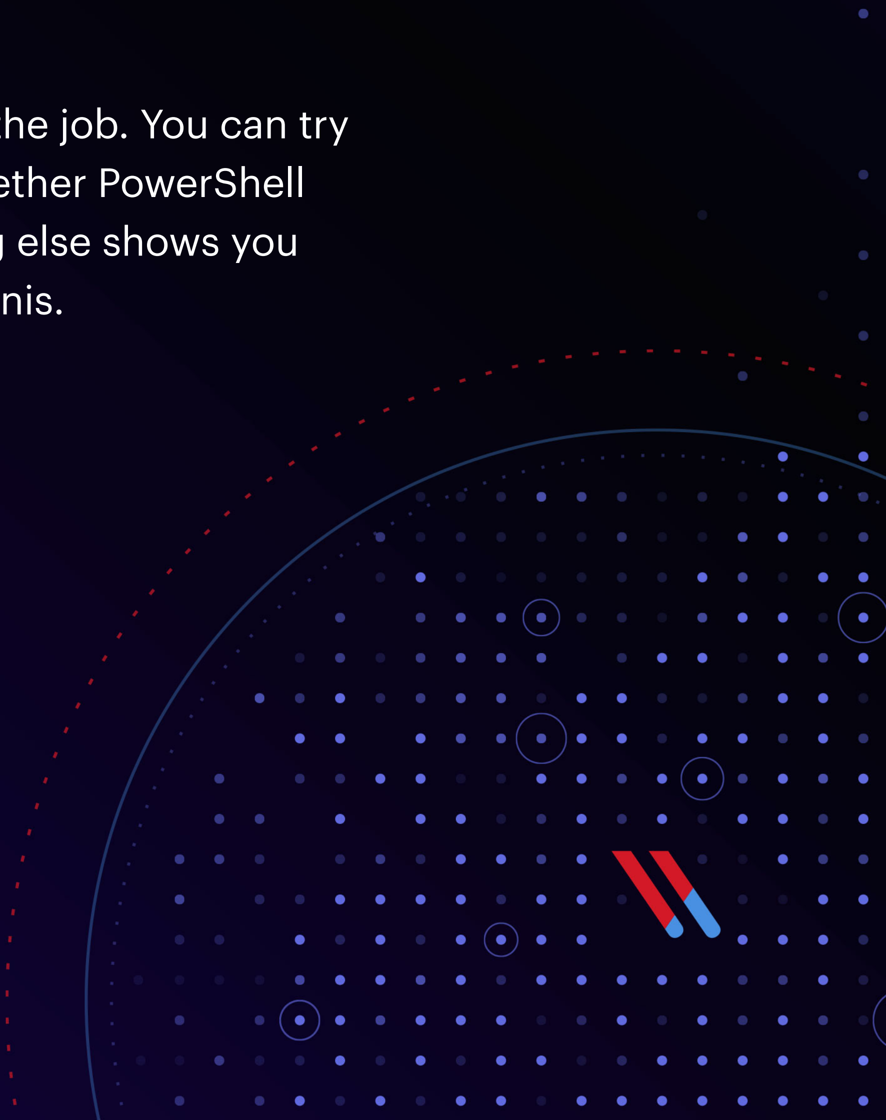
VARONIS + Where Technology Means More®

How a Liberal Arts University Safeguards Its Hybrid Environment with Varonis

> Varonis is the best tool for the job. You can try to use difficult-to-hack-together PowerShell scripts instead, but nothing else shows you the overall picture like Varonis.



About this case study:

Our customer is a liberal arts university in the U.S. We have happily accommodated their request for anonymity.

Highlights

Challenges

- Prioritizing data remediation on-prem and in Microsoft 365
- Managing external sharing and data exposure
- Answering threats like insider attacks and ransomware

Solution

ePlus

- Served as a key partner by conducting a POC to evaluate and adopt the solution best aligned to their environment.

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
- **Edge** detects and helps prevent DNS exfiltration attempts

Results

- Proper visibility and reporting into all shared folder permissions
- Protection of sensitive data stored on-premise and in Microsoft 365
- Prevention and detection vs. insider and external threats

Challenges

Protecting data against ransomware attacks

A private university in the U.S. (anonymous by request) needed to mitigate the risk posed by threats like ransomware. Protecting sensitive data and student information was the top priority—the school's reputation and revenue were at stake.

After weighing the options, the university's security engineers realized that the best defense was proactive, mitigative action. They needed visibility into their environment in order to monitor user activity for the telltale signs of a cyberattack.

A security engineer says that's why they chose Varonis:

> **"There are a number of tools that can look for ransomware attacks—but they only show you activity on the endpoint, like a virus that's already on your system. Varonis is the only solution that's looking at how data is manipulated."**

The university's environment had grown quite complicated over the years—especially with a growing reliance on the cloud. Consequently, they had difficulty prioritizing data in their environment and no way of monitoring user activity across on-prem and cloud platforms. This complicated the team's efforts to manage external sharing and data exposure.

> “There’s an awful lot of events and log data that can be easily missed in an environment that isn’t monitored. It’s a large blind spot that I was looking to get some insight on.”

A Proof of Concept (POC) revealed the extent of the issues—and gave the security engineer the evidence they needed to convince leadership of the necessity of Varonis.

> “When we first set up Varonis, it surfaced a lot of things that we didn’t realize were issues—like a user accounts with blank passwords.”

“There are a number of tools that can look for ransomware, but they only show you activity on the endpoint—like a virus that’s already on your system. Varonis is the only solution that’s looking at how data is manipulated.”

Solution

Proactive mitigation + advanced detection and response

One of Varonis' key partners, **ePlus Security**, a leading technology advisor and integrator, was closely involved in the process of conducting a proof of concept that helped the company evaluate and adopt the specific modules that best aligned to their environment.

After the POC, the university decided to harden its on-prem defenses by purchasing **DatAdvantage** for Windows and Directory Services. DatAdvantage gives the security team the critical visibility they didn't have before.

> **"We wanted behavior-based observations and insights, the ability to look into activity on our file shares, and visibility into Active Directory and cloud activity. Varonis was the best solution that met those needs."**

The user-friendly dashboards provide simple visualizations of existing permission structures and where users have too much access. When data is overexposed, it enables the security team to quickly and safely remediate access.

> **"Varonis is the best tool for the job. You can try to use difficult-to-hack-together PowerShell scripts instead, but nothing else shows you the overall picture like Varonis."**

The university also purchased **Data Classification Engine** for Windows and SharePoint. Now they're able to identify large concentrations of sensitive information, including PII, PCI, and compliance data under the Gramm-Leach-Bliley Act (GLBA) and the Family Educational Rights and Privacy Act (FERPA).

> “We can see where PII, PCI, and educational FERPA data is stored. We can dig into inherited access and gain a really quick report view in Varonis.”

DatAlert and **Edge**, which help prevent data exfiltration and inappropriate access, round out the Varonis security lineup. Varonis equips security engineers with rich, detailed alerts whenever it detects suspicious activity—and gives the security team crucial context to detect and stop threats.

> “It’s important to have high-fidelity alerts that don’t have a lot of noise. I’ve worked with the IR team a fair amount in tuning and adjusting those alerts—and the support from the IR team has been spectacular. It’s probably the best support team I’ve ever worked with.

All of these solutions help the university proactively lock down on-prem sensitive data and harden its environment. Now they’re able to catch potential ransomware and other threats early and solve issues before they take root.

“We wanted behavior-based observations and insights, the ability to look into activity on our file shares, and visibility into Active Directory and cloud activity. Varonis was the best solution that met those needs.”

Results

Protection for sensitive data wherever it lives

With their on-prem environment on lock, the university is now turning attention to the cloud environment. They recently completed a POC of **DatAdvantage** for Microsoft 365, which supports SharePoint and OneDrive, and **DatAdvantage Cloud** for Zoom, AWS, and Google Drive—all services that students rely on daily.

When they add these modules to their security lineup, the university will finally have 360° visibility into its hybrid environment. Every time data is touched, they'll be able to see who, what, when, and where in real-time.

> **"The dashboard, the alerts, and the insights it surfaces help you when you need to start an investigation. Varonis has all the things you need and it bridges the gaps you didn't even know about."**

Having this visibility is make-or-break when it comes to defeating threats like ransomware—and it's more important now than ever before. According to CSO, research and education institutions suffered an average of 1,605 attacks **every week** in 2021—a 75% increase over 2020.

Universities continue to be prime targets for cybercriminals, specifically because their security teams are traditionally understaffed and underfunded. But for this university, Varonis enables the small team to stay one step ahead of threats.

> **"Varonis is extremely valuable, especially for a small team like ours, because it's a force multiplier. With Varonis, a few people can perform powerful searches and actions without having to hire six additional data analysts."**

Leadership and the security team also gain peace of mind. They know that if the university ever does face a serious threat, Varonis' Incident Response team will help them solve the incident at a moment's notice.

“Varonis is extremely valuable, especially for a small team like ours, because it’s a force multiplier. With Varonis, a few people can perform really powerful searches and actions without having to hire six additional data analysts.”

VARONIS

Don’t leave your sensitive data exposed.

Protect your hybrid environment with Varonis.

Request a demo