How a U.S. University Protects Their Hybrid Environment Against Ransomware Attacks

> Varonis makes it easy to monitor our hybrid environment. We can go to one place and get all the alerts for both Microsoft 365 and on-premises systems. It puts it all in one place and centralizes our administration.

About this case study:

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

HIGHLIGHTS

Challenges

- Adapting to an exponentially increased attack surface
- Defending their hybrid environment from cyberattacks
- Securing sensitive student information in Microsoft 365 and on-premises

Solution

The Varonis Data Security Platform:

- Maps data access activity across file and email systems
- Finds and classifies sensitive data
- Ensures compliance with CCPA and GDPR
- Monitors and alerts on abnormal behavior on critical systems
- Detects and helps prevent DNS exfiltration attempts

Results

- Real-time alerts help detect and prevent ransomware attacks
- Built-in reports make it easy to focus remediation efforts and prepare for accreditation
- Automatically enforced data security policies and compliance with GDPR and CCPA requirements

CHALLENGES

Gaining crucial visibility to prevent ransomware

In 2024, the mean cost for higher education organizations to **recover from a ransomware attack** was more than $4M, almost four times higher than the amount reported in 2023.

One university in the U.S. (anonymous by request) had the misfortune of being hit by a ransomware attack twice within just a few years. With student privacy and the university's reputation on the line, they couldn't afford a third attack.

As the IT Assistant Director explains:

> **"It's scary. All of our data is precious to us, but especially financial records — student loans and grants — and our online portals including student grades. It forced us to make some strong decisions on where we needed to go."**

No business has the luxury of shutting down for weeks to try and recover from a malicious attack. This is especially true for universities, which need to be up and running at all times.

> **"We're a seven-day-a-week shop. It's not limited to our brick-and-mortar location; we have portals that students need to access from across the world. We need to make sure everything — from our phone systems to our VPN — is up all the time."**

But defending a hybrid environment against future attacks is difficult. The university has remote students accessing data stores through Microsoft 365 and on-premises.

In an environment like this, every student faces the risk of being targeted for an attack.

IT security needed more visibility into where sensitive data was being stored and who was accessing it. If they couldn't identify at-risk data, they wouldn't be able to defend it.

> **"A recent virus showed us that we didn't have insight into our data, where it was, or how it was being protected. If you can't see all your data, you won't know if you're under attack. How will you know the state of your files? Or what you need to restore?"**

The need for increased visibility led the university's IT Assistant Director to Varonis.

"A recent virus showed us that we didn't have insight into our data, where it was, or how it was being protected. If you can't see all your data, you won't know if you're under attack."

SOLUTION

Enforce least privilege and protect sensitive data

Varonis provides critical insight into the university's hybrid environment, including where data is stored, whether it's sensitive, how vulnerable it is, and which users can — and do — access it.

During a Proof of Concept, Varonis demonstrated how the cloud-native Data Security Platform provides visibility into hybrid environments, enabling the university's IT security team to pinpoint where there is excessive access to sensitive data and remediate automatically.

Additionally, Varonis monitors Entra ID and Active Directory activity to protect the "keys to the kingdom." Varonis helps IT security weed out vulnerabilities, including still-active accounts from previous administrations belonging to faculty who had long since left.

Varonis for SharePoint Online and OneDrive reveal where the university's sensitive data is overexposed through shared documents in Microsoft 365 and provides insight into how to remediate access to better protect their shared data. Varonis for Exchange Online monitors university email systems and public folders, granting insight into where sensitive data is being stored, shared, and accessed across all users' inboxes.

> **"We have thousands of students with personal details, like financial aid information, that could be compromised. Being able to use Varonis to monitor access and how data is being accessed has taught us how to structure security groups and user accounts, manage access and permissions, and better protect our data."**

The Varonis unified platform combs cloud and on-premises systems for sensitive data, like financial information and personally identifiable information (PII).

> **"Wherever sensitive data is, it has to be monitored and protected. Especially student emails — there's a lot of personal information and data, and we need to make sure it's kept safe."**

Varonis' library of prebuilt rules and patterns automatically discover data regulated by specific policies, including the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR).

> **"We are challenged by many data privacy regulations. That includes international regulations like GDPR, as we have students that actually are in Europe or may travel to Europe."**

Safeguard data with advanced threat detection and response

The IT Assistant Director didn't want to be caught unprepared by another ransomware attack. In addition to the risk-reducing solutions above, they also took steps to detect, defeat, and prevent future ransomware attacks.

With Varonis, the university's security team receives alerts of abnormal user behavior and file activity. This includes suspicious data access attempts, login attempts from new devices and locations, unusual download/upload activity, lateral movement, and mass file encryption or deletion. This allows the security team to lock data down while they investigate the potential threat.

> **"Varonis monitors all of our Microsoft 365 activity. We get alerts if there's a suspicious login or suspicious activity in a student email account, for example. Without Varonis, we would not have anywhere near the insight into user activity that we have now."**

Varonis helps prevent insidious threats that often go unnoticed. APT intrusions and data exfiltration attempts are often disguised as normal network traffic. Varonis alerts you to those threats.

> **"We were concerned about DNS requests — and the possibility that we were being probed for another attack. Varonis's team jumped in and helped us track and understand what was going on."**

Varonis integrates seamlessly with other security and storage platforms to provide the most comprehensive security solution possible.

> **"One of the great things about Varonis is the company's relationships with other security providers. For example, we use Zscaler, which basically provides a firewall in the cloud. Varonis integrates with Zcaler — and that's outstanding."**

RESULTS

Data security for a hybrid environment

Even with remote students accessing Microsoft 365 from around the world, Varonis helps guard the university's hybrid environment.

> **"Varonis makes it easy to monitor our hybrid environment. We can go to one place and get all the alerts for both Microsoft 365 and on-premises systems. It puts it all in one place and centralizes our administration."**

Varonis gives the security team the visibility they need to mitigate future risk — and saves them time in the process. No more hunting for a needle in a haystack; now they find and fix issues in minutes.

> **"Every day, 24/7, Varonis automatically probes our networks and finds hidden vulnerabilities. It saves us countless hours."**

Built-in reports make it easy to prioritize risk remediation and fix the most vulnerable or sensitive areas first.

> **"We use Varonis to run reports to present to the team that's preparing for our accreditation. It clearly lays out our security posture and how our data is being protected, where it is, and who's accessing it. Varonis collects all of that information."**

And, while they hope to never face another cyberattack, the security team is prepared — and Varonis' Incident Response team is just a phone call away, ready to provide backup.

> **"The value of Varonis' team is equal to the value of the product. They bring experience and knowledge that would take us countless hours of research to try to understand. Knowing that we have backup — that's invaluable — and they're just a phone call away."**

Your data. Our mission.

Varonis right-sizes permissions, finds and remediates exposed sensitive data, and detects abnormal behavior across hybrid environments.

Request a demo