VARONIS

How Varonis Saved a U.S. K–12 School District from Ransomware Nine Times in Five Years

> “When someone asks me about protecting unstructured data or stopping ransomware, the first word out of my mouth is, ‘Varonis.’ When it comes to data protection, it’s my first and only recommendation.”

About this case study:

Our customer is a U.S. school district. We have happily accommodated their request for anonymity.

HIGHLIGHTS

Challenges

+ Protecting student data against ransomware
+ Achieving FERPA and CIPA compliance
+ Reducing the school district's attack surface by locking down open accessSolution

Solution

The Varonis Data Security Platform:

+ Provides complete visibility and control over your critical data and IT infrastructure
+ Finds and classifies sensitive data automatically
+ Monitors and alerts on abnormal behavior on critical systems

Results

+ Detected and prevented 9 ransomware attacks in 5 years
+ Locked down 99.9% of sensitive data
+ Enforced policies to achieve and maintain compliance

CHALLENGES

Protecting a school district from ransomware

U.S. school districts are under attack.

In 2023, over 4 million records were compromised in third-party breaches and ransomware attacks. Add short staffing, tight budgets,and often outdated (or non-existent) security software into the mix, and schools are facing the perfect storm for ransomware attacks.

To gain a better understanding of the growing threat and help prepare for it, one school district (anonymous by request) hired a security specialist. This is what the specialist noticed:

> **"The district was completely unprepared to deal with ransomware. Their idea of security was antivirus and firewall."**
>
> **"When I came in, they asked, 'How do we protect ourselves?' I said, 'You need Varonis.'"**

The district needed to protect the personal and financial information of staff and students and comply with the Family Educational Rights and Privacy Act (FERPA) and the Children's Internet Protection Act (CIPA).

The specialist knew that in its current state, the school district wouldn't stand a chance against a ransomware attack. So they recommended three things:

+ Implementing software to help shorthanded IT staff gain visibility and control over their environment, including the ability to backup and easily restore critical files.
+ Implementing an alerting system to help detect and stop ransomware before it can escalate.
+ Locking down open access and enforcing least privilege, especially in Active Directory.

> **"There weren't any ACLs or hierarchical access structures to sensitive data. One of the payroll people had everybody's social security numbers and driver's license information stored in a personal folder. And in terms of open access, we had almost 80,000 files that anybody could access...students, teachers, anyone."**

In fact, **almost 90% of the school district's folders were open to everyone**. If they didn't reduce their blast radius, the potential cost in both money and reputation was astronomical. And without automation, cleaning up this open access would take years.

> **"I said, 'Look, you either pay for Varonis now or you hire more people. But locking down unstructured data is an immense project. You're not going to find enough security people to do what Varonis does.'"**

SOLUTION

Risk mitigation + threat detection and response

The specialist recommended the **Varonis Data Security Platform** because it combines proactive data protection and data-centric threat detection and response.

With Varonis, the school district was able to quickly lock down open access. Varonis' dashboard enabled them to quickly determine who had access to critical folders vs. who actually needed access, and then limit permissions on a need-to-know basis.

According to the specialist:

> **"I focused primarily on the district office, which houses the HIPAA and regulated payroll, accounting, and HR data."**
>
> **"I also restricted Active Directory access to just three people. I pushed everybody else out and locked that information down, and I made sure that Varonis alerted me if somebody was going in there."**

Enforcing least privilege in directory services was especially critical: every user authenticates to Active Directory or LDAP, and nearly every ACL, mailbox, and SharePoint site refer to users and groups in these directories for authentication and access control.

If an attacker manages to compromise an Active Directory account, they effectively gain the "keys to the kingdom" — and they're able to steal all kinds of data. Varonis helps mitigate the risk of this happening.

Varonis also helped the specialist focus their remediation efforts on the most at-risk areas. Varonis pinpointed sensitive data in their environment, including student PII, social security numbers, credit card details, and data protected under HIPAA, FERPA, and CIPA.

Armed with these insights, the specialist made a push to reduce open access on this critical information, thereby dramatically reducing the school district's blast radius.

> **"Before Varonis, it was like the Wild West. Everyone had access to almost everything. I've since reduced open access to almost nothing."**

Varonis also helps the school district with threat detection and response—and that decision proved critical. The Data Security Platform monitors file activity for signs of abnormal behavior, like a large number of files being encrypted all at once.

Varonis contextualizes those alerts and enables the security specialist to drill down into the threat. Importantly, Varonis can also automate responses to threats like ransomware, which saves precious time when minutes matter.

And that's exactly what happened to this school district — a ransomware attack — **not once, but nine times in five years.**

> **"Varonis has an alert feature that lets you execute scripts through PowerShell. It disables the account automatically and puts a denial on all of its file shares. That feature alone saved the district at least nine times — maybe more."**

Without Varonis, recovery would have taken weeks and it would have been impossible to determine exactly what information the attackers had compromised. But with Varonis, they stopped the attacks and restored critical files from backup by the end of the day.

"If I didn't have Varonis, the attackers would have encrypted all the files throughout the district."

RESULTS

99.9% of sensitive data locked down

Purchasing the **Varonis Data Security Platform** was a big decision, but one that wound up saving the school district hundreds of thousands of dollars. It helped protect student data, faculty data, financial data, and ultimately the district's reputation.

> **"When someone asks me about protecting unstructured data or stopping ransomware, the first word out of my mouth is, 'Varonis.' When it comes to data protection it's my first and only recommendation."**

School systems are still notoriously understaffed and underfunded, making it hard to fight the rising tide of security threats. But now the early investment in Varonis is paying off for this school district.

> **"Our environment is down to 0.002% of sensitive folders with open access. And after this interview, I'm going to use Varonis to track down those last 12 folders and lock them down too."**

Varonis continues to empower the district's IT team to stay on top of data protection and compliance by automating the hardest parts of the job: permission remediation, plus threat detection and response.

With those major concerns handled, the security specialist can focus more time and energy on training others how to responsibly handle data in their environment.

> **"Varonis has freed me from having to worry about malicious attacks like ransomware, so I can focus on the process- and policy-driven changes that need to take place."**

Your Data. Our Mission.

Varonis helps you achieve compliance and minimize your blast radius.

Request a demo