VARONIS

How Varonis Helps a U.S. County Fight Ransomware Attacks

> “The best thing about Varonis is that it simplifies life. Varonis gives me all of the visibility I need in one easy-to-read pane of glass. Beyond that, I’m glad to have the Incident Response team—they made triage during the incident a heck of a lot easier.

About this case study:

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

Highlights

Challenges

- Taking mitigative action to prevent data loss
- Implementing incident discovery and response procedures
- Achieving PII, PCI, and HIPAA compliance

Solution

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
- **Policy Pack** enhances Data Classification Engine with p atterns related to specific data privacy regulations
- **DatAnswers** makes data easily searchable
- **DatAlert** monitors and alerts on abnormal behavior on critical systems

Results

- Quickly recovered from a Microsoft 365 breach
- Reducing risk by locking down sensitive data
- Taking steps to enforce regulatory compliance

Challenges

Protecting a county against data loss and reputation damage

A U.S. county (anonymous by request) hired a new Network Manager to help them tackle a major problem: ransomware.

The county had been targeted by multiple attacks over a short time. The Network Manager was tasked with helping prevent future attacks and minimize the risk of data loss.

But there was a problem. The county had no visibility into its data stores, so the Network Manager had no way to tell what had been compromised or even where sensitive data lived.

> **"We had a bunch of CryptoLocker attacks. There were three in a matter of a few months. I was tasked with helping the county recover from those, but there was no way to do it."**

Searching for a solution led the Network Manager to Varonis.

> **"I figured there had to be a way to identify data and recover from CryptoLocker. When I found Varonis, I realized that it would show us what was happening in our environment and help us prevent attacks like this in the first place."**

The Network Manager also realized that Varonis would help them on their journey to become more compliant. As a county, they had every type of sensitive data to protect:

- Personal Identifiable Information (PII) including social security numbers and taxpayer information
- Payment Card Industry (PCI) data from different payment sources
- Health department data protected under the Health Insurance Portability and Accountability Act (HIPAA)

But enforcing compliance with a two-person team was an overwhelming prospect without a solution like Varonis.

> **“The newest concern is compliance with the Criminal Justice Information Services (CJIS) regulations. They’re coming down hard right now if you’re non-compliant. PCI and HIPAA are two big ones, and there’s so much information that it can overload a small department that doesn’t have Varonis.”**

“We had a bunch of CryptoLocker attacks. There were three in a matter of a few months. I was tasked with helping the county recover from those, but there was no way to do it.”

Solution

Data-first defense backed by a team of experts

Since adopting the **Varonis Data Security Platform** in 2014, the county continues to add Varonis products to its security stack to tighten its defenses:

- **DatAdvantage for Windows, Directory Services, Exchange Online, OneDrive, and SharePoint Online** – gives them complete visibility and control over critical data in their hybrid environment.
- **Data Classification Engine for Windows, SharePoint, OneDrive, and SharePoint Online** – finds and classifies sensitive data on prem and in Microsoft 365.
- **Policy Pack** – enhances Data Classification Engine with patterns related to specific data privacy regulations.
- **DatAnswers** – makes data easily searchable, simplifying regulatory compliance, especially Data Subject Access Requests (DSARs).
- **DatAlert** – monitors and alerts on abnormal behavior, including ransomware and other cyberattacks.

> **“We’ve got all the modules, especially for Microsoft 365. One of the reasons is compliance, but another big one is that we had all of these breaches after moving to the cloud. It gives us that further insight into how far a bad actor got: Did they just get into email or did they get all the way into OneDrive and start creating fake shares for themselves?”**

The county relies heavily on Microsoft 365 and a lot of their data lives in Exchange Online, SharePoint Online, and OneDrive. With Varonis, they’re now actively monitoring and alerting on more than 7 TB of data—over 12 million files.

Having Varonis in place proved crucial when the county was targeted by another ransomware attack. The Network Manager recalls the incident vividly:

> **“The hardest thing to fix is user behavior. Sure enough, an internal user got an email from someone that they trusted and clicked the link. It prompted them to input their Microsoft 365 credentials. Next thing you know, DatAlert is warning us that a device is logging in from another country.”**

The Network Manager describes it as a “panic attack.” The two-person team scrambled to stay ahead of the spreading ransomware, but they didn’t know exactly how to stop it. So they reached out to Varonis for help.

> **“Thirty minutes later, we had seven people from the Incident Response team on a call. They were digging through Varonis logs and providing instructions on what to do next. That had a huge calming effect—they really saved our bacon.”**

While Varonis automatically disabled compromised accounts, the IR team worked tirelessly alongside the county’s Network Managers to prevent the ransomware’s spread and recover encrypted data.

> **“At one point, my director came in and asked, ‘Are we going to be OK? Should I contact our insurance company?’ And I was able to say, ‘I think Varonis has us covered.’”**

“Thirty minutes later, we had seven people from the Incident Response team on a call. That had a huge calming effect—they really saved our bacon.”

Results

Stopping a Microsoft 365 breach in its tracks

The county's Network Manager says that having the Varonis Incident Response team on call has already paid for itself.

> **"The biggest thing for us is having the Incident Response team available and working with us on the security alert side of things. Honestly, Varonis is well worth the money just for Incident Response."**

Varonis helped the county detect ransomware on their servers, dig into the threat, and take action on the alerts. Having a complete record of everything that was encrypted and a comprehensive log of every file touched made recovery quick and painless, especially compared to past attacks.

With Varonis' help, the county was able to recover from the attack without falling back on their cybersecurity insurance coverage, and they avoided costly business disruptions, too.

> **"You won't truly know how far a hacker managed to get unless you're able to monitor individual access to OneDrive and SharePoint files. When you have a Microsoft 365 breach, you need that visibility."**

But of course, that's not the only benefit of Varonis. Varonis is also helping the county lock down its sensitive data and enforce compliance.

Already, they have eliminated on-prem global access and locked down highly regulated data. Now they're doing the same in their Microsoft 365 environment.

Locking down sensitive data severely reduces the risk posed by potential data breaches and it can also limit how far a ransomware attack is allowed to spread. It's a crucial step for limiting the blast radius, improving security posture, and preventing future data loss.

> **"The best thing about Varonis is that it simplifies life. Varonis gives me the visibility I need in one easy-to-read pane of glass. Beyond that, I'm glad to have the Incident Response team—they made triage during the incident a heck of a lot easier."**

“You won’t truly know how far a hacker managed to get unless you’re able to monitor individual access to OneDrive and SharePoint files. When you have a Microsoft 365 breach, you need that visibility.”

VARONIS

Protect sensitive data from ransomware attacks.

Gain rapid detection, proactive mitigation, and data-driven recovery.

Request a demo