How a Major American Retail Chain Stopped a Potential Data Breach in its Tracks with Varonis

CASE STUDY

"I saw the attack happening. The Incident Response team saw it happening. They immediately got the machine off of our network. The first thing we did after the upgrade was **set up an alert to ensure that it would never happen again**."

ABOUT THIS CASE STUDY:

Our client is a large U.S.-based retailer. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Protecting the sensitive data of users and customers
- Ensuring PCI compliance
- Gaining visibility into Active Directory to find at-risk areas and proactively prevent attacks

SOLUTION

The most robust data security platform:

- **DatAdvantage for Windows and Directory Services** provides crucial visibility and audit trails
- **Data Classification Engine** locates PCI data and facilitates compliance
- **Data Transport Engine** automatically migrates and deletes stale data
- **DatAlert Suite** warns users when systems are at-risk or under attack

RESULTS

- A major hacking attempt stopped within minutes of being detected
- Data security for over 1,500 users and 100,000s of customers
- 40+ hours saved every week and fewer interruptions for IT team
- Increased PCI compliance, accuracy and visibility

Challenges

Protecting users and customers from bad actors

When a U.S. retail chain (anonymous by request) with over 1,000 locations nationwide was targeted as the victim of a hacking attempt, the IT admin thanked their lucky stars that they had Varonis protecting their systems.

> “Around the time employees began working from home, someone’s PC was logging in and trying to connect to our network. Only, it wasn’t them. Somebody from another country had accessed their home computer,” they explain.

As luck would have it, the attack occurred during a call with Varonis’ Incident Response team. The IT admin was in the process of adding a new module to their security lineup—**DatAdvantage for Directory Services to support Active Directory.**

They knew that Active Directory was essentially the “keys to the kingdom.” If a bad actor gained access, the sensitive data of over 1,500 users and hundreds of thousands of customers would be at risk.

> “We’re a retailer, so we need to be PCI compliant. We were using Varonis primarily to find PCI data and remove it from open access folders. But we wanted to mitigate our risk even further and keep our customers secure, hence Varonis for Active Directory.”

The IT admin already understood the need for 360-degree visibility into Active Directory, but it’s hard to imagine a better demonstration of value than **stopping a security breach in progress during the upgrade.**

> “We were looking at Active Directory. I saw the attack happening. The Incident Response team saw it happening. They immediately got that machine off of our network. The first thing we did after the upgrade was set up an alert to ensure that it would never happen again.”

That story has a happy ending. The Incident Response team helped the affected user harden their home router and taught them how to dial in more securely. But the IT admin shudders to think what could have happened without proactive action.

> “If things weren’t caught in time—and someone got in and started doing something to our files, folders or network, and we didn’t know about it and weren’t able to stop it—that would be huge. We might not even be able to recover from something like that.”

"Someone's PC was logging in and trying to connect to our network. Only, it wasn't them. Somebody from another country had accessed their home computer."

Solution

A suite of security products all working in harmony

DatAdvantage for Directory Services is the latest solution adopted by this retailer, but it's not the only Varonis product they employ.

They started out with **DatAdvantage for Windows**, which maps access and permissions across file systems. It shows the IT admin where users have too much permission and allows them to safely automate changes to access control lists.

"Being able to easily and quickly identify user data on our network—where it's stored, what they're touching, who has access—and being able to audit and report on that information is important to every security professional and every business."

At the same time, they began using **Data Classification Engine** to find and remediate at-risk folders. Data Classification Engine automatically detects overexposed PCI data, and enables the IT admin to lock it down without interrupting business.

When sensitive data needs to be relocated or archived, **Data Transport Engine** automates the process. Data Transport Engine ensures that data is moved where it needs to go, even cross-domain or cross-platform. It also cleans up stale data automatically, simplifying regulatory compliance.

> “We completed data migration department-by-department and Varonis helped us identify and delete terabytes of stale data. It also gave management a window into what their employees were doing and how they were adjusting their projects to delete stale, sensitive data.”

DatAlert Suite ties everything together and acts as an advance warning system when Varonis detects potential threats to enterprise data. With DatAlert, the IT admin will never again be taken by surprise by a bad actor trying to gain network access through a user’s computer.

In fact, DatAlert recently helped the IT admin detect and resolve another situation that would have put the entire company at much higher risk.

> “Someone was mistakenly given a password that would never expire on a shared PC. We received an alert about that and fixed it within the hour. Without Varonis, we would have had a giant hole in our security and never even known about it.”

In the event that the IT admin can't solve something right away, they're glad to know that the Varonis Incident Response team is standing by and ready to help.

> "To be able to email or call someone from Varonis and get a response back—not just the same day, but often within minutes—that means everything to me. Varonis' support is in a league of its own."

"To be able to email or call someone from Varonis and get a response back—not just the same day, but often within minutes—that means everything to me."

Results

Time savings + enhanced data security for users and customers

The retail chain doesn't take data security lightly.

They would be willing to invest in however many solutions it would take to protect their users and loyal customers. But what makes Varonis the perfect solution is that it both **protects their sensitive data and saves the IT team over 40 work hours every week.**

> "Without Varonis, we would need at least one full-time employee watching our systems. Their whole job would be scanning through logs manually—and they wouldn't be as thorough as Varonis."

Every day, Varonis' user-friendly platform saves the IT team additional minutes that add up to hours. Where other solutions are cobbled together through acquisitions, every Varonis product is built from the ground up using a common code base. That means less time switching between software and piecing together reports.

> "You don't want to spend all day hopping between different products with different log-ins and passwords to understand what's going on with your data security. You just want a system that quickly does what it's supposed to and lets you generate comprehensive reports you can hand to management. That's Varonis."

While Varonis saves the IT team time and effort, it also helps the company gain a single, unified view of their systems' security. The IT team rests easier knowing that Varonis is keeping a watchful eye on their network and Active Directory.

“We have good visibility into who and what is logging onto our network. We instantly know about threatening behavior, including someone trying to hack an account over and over until it gets locked out. We have the insight we need to take action.”

“We instantly know about threatening behavior, including someone trying to hack an account over and over until it gets locked out. We have the insight we need to take action.”

Gain the visibility you need to protect employees and customers.

Audit activity in Active Directory and lock down sensitive data with Varonis.

REQUEST A DEMO