How Varonis Helps Virginia Credit Union Watch for Stealthy Threats

CASE STUDY

"We found a legacy security group that was probably created years ago that provided our desktop users with excessive permissions on accounts in Active Directory. **If DatAlert hadn't told us about it, I'm not sure we would have ever found it."**

Virginia Credit Union is a member-owned, not-for-profit financial cooperative with over 300,000 members.

HIGHLIGHTS

CHALLENGES

- Monitoring and protecting critical user accounts and data across Windows, NetApp and Active Directory
- Employees moving to remote work left potential security gaps
- SIEM-created event logs lacked critical context

SOLUTION

The most robust data security platform:

- DatAdvantage for Windows audits file access and reviews access permissions for remediation
- DatAdvantage for Directory Services gives visibility into Active Directory
- Data Classification Engine scans data stores and locates sensitive data
- DatAlert Suite monitors files and email systems for signs of ransomware and other threats
- Edge (evaluation) monitors threats on the perimeter and provides further context to alerts
- Complimentary Incident Response support to investigate potential threats

RESULTS

- Immediate visibility across disparate data sources
- Quickly pinpointed a serious security issue with DatAlert's threat models
- DatAlert threat detection cuts through noisy SIEM logs to focus on alerts that matter

Challenges

From data access governance to alerting on potential threats

Virginia Credit Union (VACU) started working with Varonis in 2012. Since then, the credit union has been relying on the Varonis Data Security Platform to support their data access governance program:

- DatAdvantage for Windows provides visibility by mapping permissions and user access history across the credit union's Windows environment.
- Data Classification Engine automatically scans their files for sensitive and regulated data, like account and routing numbers.

When Ruben Justiniano moved from supporting technology governance to the Cybersecurity Operations Team as Data Security Engineer at VACU, he decided they needed an additional solution in their arsenal.

So in 2019, they added DatAlert to ensure they would be alerted to suspicious activity in their environment as quickly as possible.

While Ruben had a ton of experience using Varonis to classify and secure data, DatAlert was a new solution for VACU. To get up and running as quickly as possible, he worked with Varonis' complimentary Incident Response team to fine tune and customize DatAlert.

> “Once we put DatAlert in, we had Varonis help us tune out the noisy stuff. Just like any platform, it will throw a lot of alerts — but very quickly, with the help of the Varonis Incident Response team, we were able to customize DatAlert in our environment with exclusions and filtering within their threat models... From there, we were getting only a handful of alerts a day.”

When the fine-tuning process was complete, DatAlert began monitoring their environment and building baseline behavioral models on what typical activity looked like.

According to Ruben, “[DatAlert] started to clue us in on what our users typically do.” And that was insight the credit union didn’t have before.

“[Very] quickly, with the help of the Varonis Incident Response team, we were able to customize DatAlert in our environment with exclusions and filtering within their threat models.”

Solution

Stopping potential issues in their tracks

After Ruben and the Varonis IR team customized DatAlert for the credit union, it didn't take long before it started flagging potential issues in their environment.

One morning, DatAlert notified Ruben to excessive Active Directory permissions on a legacy security group — a serious security gap that could have given a successful attacker the ability to move laterally within the network and escalate privileges.

> "Shortly after we finished the tuning process, I came in one morning and saw an alert. A privileged account had its password reset."

Using Varonis, Ruben was able to quickly zero in and understand the issue.

> "I started to look into the alert and noticed the account that did the reset was a user's standard account, which should be used for day-to-day activities — not things like password resets or permission changes in AD."

Fortunately, the issue wasn't a breach but an account misconfiguration — an issue that, if not corrected, could have been exploited by a hacker or an employee with bad intentions.

“We found a legacy security group that was probably created years ago that provided our desktop folks with really excessive permissions on accounts in Active Directory. Honestly, if DatAlert hadn’t told us about it, I’m not sure we would have ever found it.”

“If a malicious threat actor got inside and was to compromise one of those desktop users — not even an administrative account — they would have been able to do some pretty big damage there.”

“Honestly, if DatAlert hadn’t told us about it, I’m not sure we would have ever found it.”

Remote work shift leads to an Edge test drive

In early 2020, organizations around the world scrambled to transition to an all-remote workforce and reliance on collaboration tools like Microsoft Teams skyrocketed.

With no time to waste, Ruben took Varonis up on their offer to try out Edge at no cost.

> “When the pandemic hit, we had to move extremely quickly to get our workforce predominately working from home. Edge became an attractive option for us to monitor VPN connectivity, web proxies, and also DNS.”

The added visibility, according to Ruben, sheds light on potential threats and unusual activity from their network perimeter.

> “Varonis allowed us to get a lot of insight into what types of activities our remote users are doing. As soon as we put Edge in, I was getting daily alerts on abnormal user behavior because folks were uploading a lot of data to their WebEx sessions."

Beyond alerting to suspicious activities, the Edge evaluation helped the credit union identify and shore up potential gaps in their security.

> “Edge provided us with insight into service accounts accessing the web — applications running off a service account that pass some information to the internet for analytics. We’ve been able to find those and lock them down. Now we have the visibility we need without having to comb through the laborious logs of our web proxy.”

"When the pandemic hit, we had to move extremely quickly to get our workforce predominately working from home. Edge became an attractive option for us to monitor VPN connectivity, web proxies, and also DNS."

Complementing their SIEM with meaningful insights

Like most organizations, VACU uses a SIEM to capture event logs. While these logs can contain valuable information, they can generate a sea of data that must be analyzed by security staff.

"We have a love-hate relationship with our SIEM — it is only going to do what you have the time, money and resources to dedicate to configuring and tuning it."

Unlike a SIEM, Varonis cuts through the noise and adds critical context to event logs — and that boosts visibility and surfaces alerts that matter.

"The benefit of Varonis, from a cybersecurity ops and incident response perspective, is that right after implementation it is going to do those correlations and provide the immediate visibility you need."

Compared to configuring their SIEM, rolling out Varonis was simple. Ruben didn't have to spend a lot of time trying to figure out what Varonis should be monitoring, which had to be done when rolling out their SIEM.

And, according to Ruben, finding misconfiguration and operational issues would be virtually impossible to do without Varonis.

> "All of the heavy lifting is done by the software — they've already got it preconfigured for the things you want to pay attention to."
>
> "With Varonis, correlations are already in place. It's already going to be looking at all of these disparate systems and from the start will tell you what you need to look for."

According to Ruben, organizations should have both a SIEM and Varonis in place.

> "But if you don't have both yet, or you don't have either one, I would tell you to get Varonis first, because that is going to provide you with that baseline for your active directory, unstructured data, Exchange, and perimeter telemetry."

"The benefit of Varonis, from a cybersecurity ops and incident response perspective, is that right after implementation it is going to do those correlations and provide the immediate visibility you need."

A team that has your back

As an IT and cybersecurity professional with nearly 20 years of experience, Ruben knows about working with software vendors. But they didn't all set him up for success the way Varonis did.

> "Some of these platforms promise a lot of things. Varonis' support has been completely on point — every implementation, the follow-ups afterwards — it's not the situation where they just put it in place and then walk away. Varonis has had outstanding response times and support for our organization."

Ruben recommends taking advantage of the complimentary support Varonis offers: "You'll start getting value out of platform faster, and you'll be more successful as a result."

For Ruben, Varonis' hands-on customer support includes not just the Incident Response team, but the whole Varonis team.

> "Our sales representative and our sales engineer, and the entire support team, any time we've had an issue, have been really quick to help us. Sometimes they've even helped us fix issues with things we had misconfigured in our environment."

"Varonis' support has been completely on point – every implementation, the follow-ups afterwards — it's not the situation where they just put it in place and then walk away."

Results

Keeping a watchful eye on users and accounts

Like many companies, the credit union is gaining peace of mind knowing that Varonis is monitoring for issues around the clock. Thanks to Varonis, they can...

- **Uncover hidden account issues that put them at risk.** Varonis combs your environment and pinpoints misconfigured accounts that leave security gaps.
- **Safeguard their most sensitive data.** Locking down critical data mitigates the risk posed by insider and outsider threats, including cyberattacks.
- **Complement their SIEM investment.** Why drown in event logs? Varonis adds context and shines light on only the events that matter most.
- **A team they can rely on.** Complimentary support from the Varonis Incident Response team is only a phone call away.

Varonis helps the Cybersecurity Lead save time too.

With Varonis, the credit union was able to support not only its data access governance program, but also watch for advanced threats from the network perimeter that could otherwise go undetected.

> According to Ruben: “Varonis does a really good job of automating the process of keeping track of service accounts, privileged accounts, executive account — those accounts you really care about that tend to have the most permissions.”

> “Varonis helped me on the data governance side with data security and data classification, and now on the cybersecurity operations side with DatAlert. It’s the first console that I use in the morning and it’s helped us close a lot of gaps in terms of alerting on potential threats in real time.”

Zero in on the alerts that matter and start making sense of your SIEM logs

Varonis helps separate the signal from the noise, so you can focus your time on solving real issues, faster.

REQUEST A DEMO