VARONIS

How Varonis Helps a U.S. Federal Credit Union Protect Sensitive Data & Safeguard Against Cyberthreats

CASE STUDY

“We use a lot of solutions for data security, but our other tools would be lost without Varonis. It’s the glue that holds our data security systems together.”

ABOUT THIS CASE STUDY:

About this case study: Our client is a respected U.S. federal credit union. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Protecting personal and financial information of members
- Gaining visibility into which files have been accessed & shared
- Placing stricter controls over who has access to sensitive files

SOLUTION

The most robust data security platform, fully integrated with their SIEM:

- **DatAdvantage** for Windows for visibility into file access
- **DatAlert** to detect potential malware or internal data leaks
- **Data Classification Engine** for identifying sensitive data on-premises and in the cloud

RESULTS

- Sensitive data protection for over 10,000 end users
- Clear audit trails that make threat detection and regulatory compliance easy
- Ongoing and agile support from Varonis's responsive team

Challenges

Data protection and threat detection and response

Data security should be a priority for every business, but for respected federal credit unions, it's non-negotiable.

That's why one credit union's Cybersecurity Analyst (who wished to remain anonymous) says his company adopted Varonis back in 2010, and why they still trust Varonis for data protection and threat detection and response.

> "Being a financial institution, we have to protect our member information—their bank accounts, social security numbers, and other personal data. Remaining compliant and affirming the trust our members place in us? That's really important."

When they first adopted Varonis, their infrastructure team wanted a clearer audit trail. They needed more visibility into which folders were being accessed and by whom.

> "Varonis brought a lot of clarity to our data security. Before Varonis, we didn't have a way to track which files were open on our shared drive. We didn't know who was supposed to have access versus who was actually accessing certain data."

Once they had more visibility into their data infrastructure, the company shifted their focus to tighter security.

Their goals were simple:

- Clean up access controls on folders that had either been over-shared or were open to all employees.
- Lock down critical data sets.
- Develop a systematic approach to identifying and stopping potential insider threats before they became serious.

Varonis was the perfect solution for all of their data security and threat identification and prevention needs.

> “Being a financial institution, we have to protect our members’ information—their bank accounts, social security numbers, and other personal data.”

Solution

Intuitive data auditing, a detailed alert system, and advanced data classification

At the heart of Varonis' Data Security Platform is DatAdvantage, which maps out who does and who doesn't have access to sensitive data across all file systems, both on-premises and in the cloud.

DatAdvantage allows the credit union to visualize permissions via an intuitive dashboard, audit every file touched, and remediate permissions based on individual user needs.

> "When we need to look at what files a user has touched or shared, we rely on Varonis. It's essential for getting to the bottom of suspicious activity, like someone downloading or uploading a bunch of files from our shared drive."

Importantly, Varonis is also compatible with Splunk, their Security Information and Event Management System (SIEM). Splunk captures, indexes, and correlates real-time data about what's happening on the credit union's network.

With Varonis DatAlert functionality integrated into Splunk, they are able to easily navigate the sea of information their SIEM provides and drill down into each context-rich alert for additional insight.

> "Varonis saves us a lot of time. We don't have to waste time hunting for relevant information with Varonis connecting the dots for us—and that gives us tremendous peace of mind."

Gaining visibility into security events in real time has been very useful for the credit union's infrastructure team. Now, they're focused entirely on cleaning up file access and increasing data security.

Varonis Data Classification Engine, which automatically scans and classifies sensitive information regardless of whether it is stored in the cloud or on-premises, has been essential for this process.

> "Without Varonis, we wouldn't know these open files existed. Now, with their help, we're identifying every vulnerability and finding ways to fix them. Even their initial scans during an onsite data review of our files were SO helpful."

> "When we need to look at what files a user has touched or shared, we rely on Varonis. It's essential for getting to the bottom of suspicious activity, like someone downloading or uploading a bunch of files from our shared drive."

Results

Over 10,000 end users protected

When asked why the credit union has trusted Varonis to protect their sensitive user data for almost a decade, their response was simple:

> “We use a lot of solutions for data security, but our other tools would be lost without Varonis. It’s the glue that holds our data security systems together.”

Today, the credit union relies on DatAdvantage for Windows and the DatAlert Suite to safeguard the information of over 10,000 end users. Varonis has also helped them identify sensitive information in order to increase data security.

> “Varonis is great—especially if you’re concerned about security on your shared drives. It gives you so much clarity into who is accessing each file, and which data is at risk.”

On a day-to-day basis, Varonis is the solution they trust to identify suspicious activity and proactively identify and eliminate potential threats, so bad actors can’t catch them by surprise.

> “The other day, Varonis alerted me to someone accessing a systems admin tool. Within minutes, I was able to identify the user, check out their permissions, and ask why they’d accessed the file. Without Varonis, we wouldn’t have even known about the event.”

While that situation turned out to be benign, and the credit union has never experienced a major threat, they’re glad to know that if something ever does happen, they have Varonis protecting their sensitive user data.

> “Varonis is great—especially if you’re concerned about security on your shared drives. It gives you so much clarity into who is accessing each file, and which data is at risk.”