VARONIS

How Varonis Helps a UK Credit Union Protect the Personal Data of Over 500,000 Members

CASE STUDY

“Varonis helps us along our journey to become fully GDPR compliant. It provides us with a structured format to look at our data estate in a prioritized manner—and it has already saved us a lot of time.”

ABOUT THIS CASE STUDY:

Our client is a UK Credit Union. We have happily accommodated their request to anonymize the names of the people interviewed and their company.

HIGHLIGHTS

CHALLENGES

- Ensuring compliance with GDPR requirements
- Implementing CIS Controls to defend against cyberattacks, insider threats & data breaches
- Acquiring software to make data management easy & intuitive

SOLUTION

The most robust data security platform:

- **DatAdvantage** for Windows helps monitor data access
- **Data Classification Engine** for Windows & SharePoint automatically classifies GDPR protected data
- **DatAlert** provides continuous file monitoring and alerting on critical files

RESULTS

- Over £100,000 in storage costs saved by gaining visibility into stale/unused data
- Reduced risk and improved access controls across share network
- CIS Controls necessary to becoming more GDPR compliant

Challenges

Maturing data security & meeting GDPR requirements

In the UK, the General Data Protection Regulation (GDPR) strictly regulates how companies manage customer data. Non-compliance with GDPR can result in fines of up to €20 million or 4% of annual turnover.

One organization impacted by the new legislation was a credit union in the UK (anonymous by request). The credit union manages all of the savings, investments, and mortgages of over 500,000 members.

Before GDPR came into effect, the organization had experienced a period of rapid growth. As a result, they'd collected and stored a lot of personally identifiable information (PII) and other sensitive data.

But as the organization's Data Privacy Analyst explains, effectively managing that data after the fact was easier said than done:

> "We had data shares that had been there for years, but no way to know what type of data was there or who had access to it. We also didn't have an easy way to find and remove stale PCI or other sensitive data."

Under GDPR guidelines, companies can only store personal data that's absolutely necessary, relevant, and limited to the original purpose that it's collected for. They can also only store data for as long as necessary for that purpose.

Knowing they would never be able to manually manage all of their members' data, the credit union created a new security maturity program. The goal was to find a solution to...

1. Assist them in implementing CIS Controls™—standards for defending against cyberattacks, insider threats, and data breaches.
2. Simplify data management to ensure that they meet GDPR compliance standards as quickly as possible.

According to the Data Privacy Analyst:

> "We were looking for a solution that would help us manage personal data and lock down our infrastructure's security."

> "We had data shares that had been there for years, but no way to know what type of data was there or who had access to it. We also didn't have an easy way to find and remove stale PCI or other sensitive data."

Solution

Varonis products that meet or exceed the requirements of CIS security controls

Varonis was able to prove that their products meet or exceed the requirements of all 20 of the CIS Security Controls the credit union was seeking to implement.

For example, the credit union wanted Control #13 (Data Protection) in place, to ensure data privacy and integrity. Varonis products that facilitate this control include:

- **DatAdvantage** – detects stale and unused data, allowing for automatic or manually deletion, quarantine, or migration.
- **Data Classification Engine** – scans data stores to identify PII, PHI, other information protected under GDPR. Results are viewable through the DatAdvantage UI and on a daily report.
- **DatAlert** – detects unauthorized or unusual data access. This includes abnormally high numbers of file modifications, abnormal access attempts, and the early warning signs of exfiltration.

Being able to easily implement controls and accurately monitor data was a necessary first step on the road to GDPR compliance.

> “The first thing we did was deploy Varonis on all of our data shares. We looked at who had access and tightened permissions on open shares. Now this is one of our controls that we are making sure we’re compliant on.”

Varonis helps the IT team identify and eliminate stale data, including potentially sensitive data they didn’t even know they had, which might have resulted in GDPR non-compliance.

> “We use Varonis to scan our data estate for personal data. Then we generate reports highlighting where that data fits. We use those reports to decide whether it falls within our data retention policy or, if it doesn’t, whether we should get rid of it or just remove unnecessary sensitive data.”
>
> “I like that it’s easy to classify what needs to be archived or deleted. The reports clearly show us when data is old or not needed anymore. That makes it easy to go through and remove it from our data shares.”

DatAlert enables the IT team to monitor file shares for vulnerabilities and anomalies. When it detects a potential problem, they’re able to quickly pivot, understand the issue, and take remedial steps.

Even though the Data Security Analyst reviewed dozens of different solutions, they say that the decision to partner with Varonis was easy—especially after seeing the platform’s granular insights and user-friendly interface.

> “We looked at several different companies and reviewed their capabilities. Varonis ticks all the boxes and the support we receive from them during the proof of concept all the way through to now has been amazing.”

“The first thing we did was deploy Varonis on all of our data shares. We looked at who had access and tightened permissions on open shares. Now this is one of our controls that we’re making sure we’re compliant on.”

Results

Everything they need to achieve GDPR compliance

According to the Data Security Analyst, Varonis has already helped the credit union save over £100,000 in storage costs, specifically because it gave them more visibility into their stale and unused data stores.

> “Thanks to Varonis, we haven’t needed to invest in additional storage. We’ve been able to invest those savings in other areas.”

Finding and eliminating that data manually would have been a tall order. With Varonis, data cleanup is almost effortless.

> “Varonis saves us an astronomical amount of time finding and eliminating sensitive data. I honestly don’t think we could even do it without Varonis.”

But while the immediate time and cost savings are great, the most important thing Varonis has done for the credit union is pave the road for GDPR compliance.

Heightened visibility into the organization’s data management has been a lifesaver. And, with proper CIS Security Controls in place, it has a robust defense and early warning system to help it defend against cyberthreats and data breaches.

> “Varonis helps us along our journey to become fully GDPR compliant. It provides us with a structured format to look at our data estate in a prioritized manner—and it has already saved us a lot of time.”

“Varonis saves us an astronomical amount of time finding and eliminating sensitive data. I honestly don’t think we could even do it without Varonis.”

VARONIS

Are your file shares risking the security of your company—and its customers?

Compliance doesn’t have to be hard with Varonis to help you protect sensitive data.

REQUEST A DEMO