



How Chemung Canal Trust Company is Operationalizing Labeling With Varonis



“We hadn’t really looked at Purview until we had Varonis. Our labeling project came up during our Varonis deployment. Our Varonis deployment engineer did a tremendous job outlining the different benefits and brought us up to speed.”

HIGHLIGHTS

Challenges

- + Visibility into regulated and sensitive data
- + SOX, GLBA, and NY DFS compliance
- + Locking down sharing links

Solution

Varonis' cloud-native Data Security Platform:

- + Powerful automation that fixes security issues without human intervention
- + Visibility and control across all enterprise data in M365 and Windows
- + Easy integration between Varonis and Microsoft Purview
- + Real-time alerts on potential threats
- + Support via Proactive Incident Response

Results

- + Classified 350k+ sensitive files
- + Labelling sensitive files across their data estate
- + Identified and remediated anonymous sharing links
- + Implemented external sharing best practices

CHALLENGES

Data classification and security for a trusted financial institution

Chemung Canal Trust Company (CCTC) is New York state's oldest locally-owned and -managed community bank, serving communities in central NY and northern Pennsylvania since 1833. Along with being a full-service financial institution, CCTC provides trust and investment services nationwide.

Like all banks, CCTC must secure sensitive personal and financial data. The bank must comply with regulations like SOX and GLBA and must audit data access continuously.

Josiah Bennett, the Security Analyst at CCTC, knew the power of Varonis from his experience at a prior institution and knew he wanted to bring Varonis to CCTC. On his experience with Varonis previously, Josiah explained:

"Varonis helped us figure out what data we had, helped us classify it, and put controls around that data. We also liked many of the reports that came out of Varonis. If we looked at the Varonis dashboards and saw something we needed to investigate, Varonis would take us right to what we needed to see. Varonis is easy to use to get the reports and information we need."

When it came time to evaluate solutions to secure data in CCTC's hybrid Microsoft 365 and Windows environment, Josiah and the team knew Varonis could do the job.

"We looked at a few different products. After having our experience with Varonis, we knew they could give us everything that we needed in a timely manner."

SOLUTION

Gaining control of a complex hybrid environment

Varonis' cloud-native platform helps the CCTC team gain real-time visibility into their Microsoft 365 environment and on-prem file shares. Varonis classifies all the data in their hybrid environment, maps out permissions, and identifies and remediates overexposed information automatically.

In addition to Varonis' out-of-the-box classification rules, CCTC created custom rules to meet their specific requirements.

According to Josiah:

“We created classification rules to identify data that would come up during audits. We created other classification rules for internal-only documents that cannot be shared publicly.”

Labeling with Varonis + Microsoft Purview

Before Varonis, CCTC had Microsoft Purview but hadn't considered embarking on a labeling project.

According to Josiah:

“We hadn't really looked at Purview until we had Varonis. Our labeling project came up during our Varonis deployment. Our Varonis deployment engineer did a tremendous job outlining the different benefits and brought us up to speed.”

Now that they have Varonis and Microsoft Purview, CCTC is doing what most companies can only dream of — they are in the process of labeling all their information across their data estate.

When the project is complete, the CCTC team will be able to save time preparing for audits. The team will be able to easily pull reports from Varonis with all the information they need.

“We want to restrict access to certain documents and make sure that anything that should be ‘internal only’ stays internal. We will run a query in Varonis and have it pull the data with that label for the audit. That will save us a lot of time, because it takes us hours to compile all of the documentation we need for audits.”

With Varonis, CCTC is operationalizing Purview labels — a feat they hadn't even considered previously — to help them ensure they have the proper safeguards to protect regulated data.


Gaining control of sharing links

Collaboration links can be great for business productivity, but it can also make it easy for employees to overexpose potentially sensitive information.

With Varonis, Josiah and the team gained visibility and control of risky collaboration links. Moreover, they implemented sharing best practices, like disabling anonymous sharing and preventing guests from sharing data they do not own.

According to Josiah:

“Microsoft makes it so you can collaborate with anyone all the time. During our deployment with Varonis, we locked sharing links down by default and restricted the sharing employees could do.”



“We want to restrict access to certain documents and make sure that anything that should be ‘internal only’ stays internal.”

RESULTS

Right-sizing permissions to least privilege

Many organizations face the problem of permission sprawl as users accumulate access. Without automation, it's virtually impossible to right-size that access over time as users change roles and come and go.

With Varonis, CCTC continues to evolve its data security posture. Varonis provides visibility into sensitive information across its hybrid data estate, with valuable insights on data use, permissions, and sharing links that can expose information.

Importantly, CCTC can proactively reduce permissions and keep them that way with automation.

According to Josiah:

"We found a lot of sensitive data through our deployment with Varonis. We can see where sensitive data is overexposed and rein in those permissions when people haven't accessed that data regularly and don't necessarily need access."

"Varonis improved our security posture considerably."

Alerting and support from a world-class IR team

Minutes matter when it comes to stopping potential threats. The customer worked with the Varonis Incident Response Team to set up and operationalize automated threat detection and alerting scripts to help stop suspicious activity.

Varonis is watching CCTC's environment for anomalous activity and helping to keep data safe.

"Varonis alerted us to pentest activity, and we took those alerts and sent them to the pentesters and said, 'We've seen this. Can you confirm that this is you?' Varonis gives us visibility into the activity taken on our data."

What's more, the company can call Varonis' global team of incident responders to assist if a potential incident occurs.

Visibility and control over sensitive data

According to the security analyst, Varonis' contribution is like night and day.

Without Varonis, tasks like determining which users can access what files and completing audit reports would be far more time-consuming.

Deploying and operationalizing Varonis played a major role in transforming CCTC's security. The customer is proactively reducing their risk and ensuring compliance with regulations with automation.

According to Josiah:

"Before we had Varonis, we didn't have real visibility into our environment. Varonis allows us to classify our data and gain perspective on what we have — we know who is using Teams to share files and who is saving folders and files. Varonis saves us a lot of time."



"Varonis gives us visibility into the activity taken on our data."



Shift your labelling project into high gear.

Varonis makes it possible to label all the information across your data estate.

[Request a demo](#)