VARONIS

Why Hanmi Bank Switched from a Point Tool to Varonis Data Security Platform

> The key to data security is that to protect sensitive data, you need to know where it lives. Varonis does that for us.

Highlights

Challenges

- Point tool was unable to fully scan the bank's data stores
- The bank lacked the visibility needed for CCPA compliance
- They weren't receiving the support they needed

Solution

Varonis Data Security Platform:

- **DatAdvantage** gives complete visibility and control over your critical data and IT infrastructure
- **Data Classification Engine** finds and classifies sensitive data automatically
- **Policy Pack** enhances Data Classification Engine with CCPA and GDPR patterns
- **DatAlert** monitors and alerts on abnormal behavior on critical systems
- **Automation Engine** automatically repairs and maintains file system permissions
- **Data Transport Engine** enforces rules for data movement and migration
- **DatAnswers** helps fulfill DSARs quickly

Results

- Successfully classified sensitive data
- Removed excessive access from their entire environment with no scalability issues
- Achieved CCPA compliance
- Receives ongoing support from the Varonis team

Challenges

Lack of support from a file auditing point solution

Hanmi Bank was trying to achieve California Consumer Privacy Act (CCPA) compliance. They needed to be able to scan their environment and find regulated data, including SSNs, driver's licenses, ABA numbers, and other personal identifiable information.

The team had tried to use a point tool for two years. But during that time, they were never able to fully identify all of the sensitive data that needed protection—which led to incomplete and inaccurate reporting. What's more, the tool could not scale to meet the team's growing demands.

> **"We only had six servers at the time—it wasn't a big environment. But the software was not able to complete a full scan," explains the VP of IT Infrastructure, Layla Khorsand. "Also, every time we needed to reboot something, we had to stop the scan and restart it from the beginning. So I had to babysit it."**

> **"We tried using the tool for almost two years before we decided it wasn't working. The product struggled to complete even the initial scans for sensitive data," confirms Navneeth Naidu, CTO.**

VARONIS

A lack of much-needed support was the final straw. The IT team was very frustrated—something had to change.

> **"Every single time a scan failed, the provider blamed something else. There was always 'another issue' with our environment. So we pulled the plug," says Layla.**

"We tried using the tool for almost two years. The product struggled to complete even the initial scans for sensitive data."

Solution

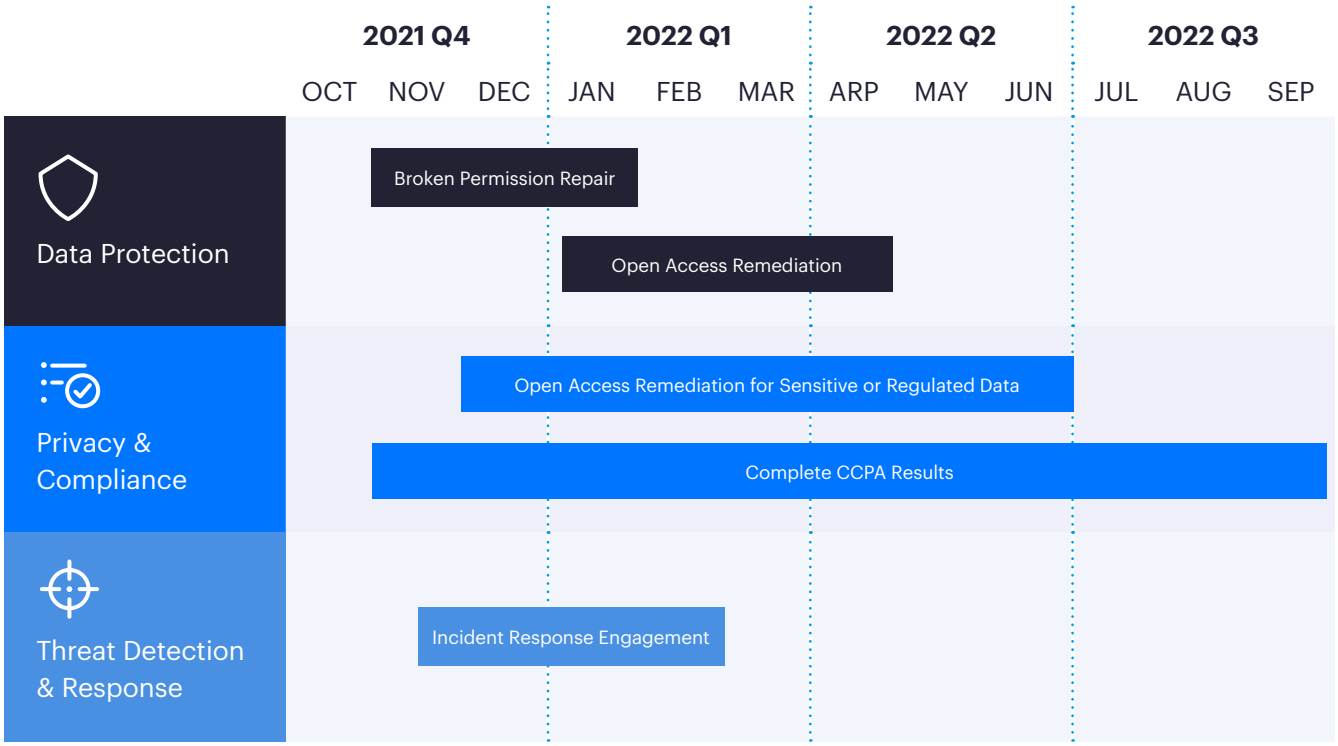
Seamless implementation and a true partnership

In need of a new cybersecurity solution, the company decided to try Varonis. The VP of Infrastructure was "very skeptical" after the previous experience, but Varonis' Proof of Concept laid her fears to rest.

> **"Once we switched to Varonis, it took less than two weeks to run a full scan of our environment. We haven't had any issues since implementation," says Layla.**

On top of a comprehensive product suite, Varonis also had a proven Operational Plan that gave them measurable milestones to meet their goal. They realized CCPA compliance was more than just checking a box and felt Varonis understood exactly how to get them there.

Operational Plan



VARONIS

360° visibility into enterprise data

DatAdvantage provides continuous monitoring of the bank's data stores on-prem and in the cloud, which includes over 2.6 million folders and 20.5 million permissions. With modules for Windows, Directory Services, Microsoft 365, Azure, and Exchange Online, the bank finally has 360° visibility into their network.

During the initial scan, DatAdvantage identified a number of red flags, including a lot of sensitive files with open access. If left untended, these files could be exploited by bad actors or ransomware gangs to gain access to the bank's sensitive data.

The bank's IT team uses **Data Classification Engine**, which identifies sensitive data, to help prioritize remediation. **Policy Pack** further enhances these insights by identifying sensitive information that falls under CCPA.

They also set up **DatAlert** to monitor for suspicious activity. When Varonis detects a deviation from normal behavior, DatAlert enables the IT team to drill into the alert, lock out potentially compromised accounts, and stop the threat in its tracks.

> **"Varonis gives us the ability to pinpoint where sensitive data is and gives us the ability to control it in our environment. We also have improved ransomware protection, because we can act quickly to disable users when Varonis alerts us that abnormal activity is happening," says Navneeth.**

Advanced compliance controls

Armed with the knowledge of where sensitive data lives and what's at risk, the IT team then used Varonis solutions to begin locking down data and fulfilling CCPA obligations.

Automation Engine is helping the team to automate the remediation of overexposed data that's open to everyone in the company. With the click of a button, the team enabled self-healing permissions to automatically remove global access groups. A remediation project that might have taken years was wrapped up in months.

The next step: auto-enforcing good data retention policies. **Data Transport Engine** helps with this by automatically moving data to more secure locations, quarantining exposed sensitive files, and deleting stale, risky data.

And when the IT team needs to locate specific folders, or when a customer submits a Data Subject Access Request (DSAR), **DatAnswers** makes it easy to locate the corresponding files in seconds.

> **"As a bank, knowing where data is and who has access to it is critical. CCPA requires you to be able to know where sensitive data lives and label that data. And, as part of ITGC control, you need to tightly control user access. Varonis gives us that ability," says Navneeth.**

"Once we switched to Varonis, it took less than two weeks to run a full scan of our environment."

Results

CCPA compliance + always-on support

For this community bank, the difference between their point tool and Varonis has been night and day. Navneeth says that there's no comparison between the two:

> **"I would definitely recommend Varonis because it's very user-friendly, it works, and the team is great. Everyone we've gotten to know through Varonis has been amazing."**

Layla agrees that the best part about working with Varonis has been the incredible partnership.

> **"You feel like you're getting first-class support. Our engineer makes life so much easier. I emailed him yesterday and he sent me a Zoom link right away. We were connected almost immediately," says Layla.**

At the end of the day, the most important thing is the efficacy of the product—and that's where Varonis shines. From the initial scan of the bank's infrastructure to all the remediation efforts that followed, Varonis saves time for the IT team and helps them with their compliance efforts.

> **"Varonis was able to complete the initial scan in no time, and that's where the point tool was struggling," Navneeth says.**

> **"I had to babysit the point tool. I don't need to do that with Varonis. If we ever need to reboot something, Varonis just picks up where it left off automatically. Varonis saves me a lot of time so I can get to the other things that I need to do. It does exactly what it promises," says Layla.**

Now, the bank has successfully classified all of its data. They have the tools they need to achieve CCPA compliance. And they've been able to operationalize their existing security stack to better protect data against threats like ransomware.

> **"The key to data security is that to protect sensitive data, you need to know where it lives. Varonis does that for us. It also lets us look at who has access to our data and quickly respond to threats like ransomware by shutting down suspicious activity," says Navneeth.**

Looking back, the difference between Varonis and their previous point tool is night and day. Before, they struggled to scale, missed data during classification, and settled for incomplete reports. With Varonis, they never have to worry about data that slips through the classification cracks.

Combined with unparalleled monitoring, advanced threat detection and response, automated remediation of overexposed information, and support for data subject requests (and more), the team has an all-in-one data security solution they can rely on.

"I would definitely recommend Varonis because it's very user-friendly, it works, and the team is great. Everyone we've gotten to know through Varonis has been amazing."

Get the data protection you need, backed by a team you can rely on.

Request a demo