How an Industry-Leading Agricultural Company Uses Varonis to Mitigate Ransomware & Insider Threats

CASE STUDY

"Preventing a catastrophic outage is the primary benefit. Built-in auditing is a big plus. Being able to enforce data security policies and alarm against worrying user behavior is another benefit. Varonis is well worth the expenditure."

ABOUT THIS CASE STUDY:

Our client is an industry-leading agricultural company.
We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Gaining visibility into Active Directory and file servers
- Reporting and alerting in real-time
- Guarding against ransomware and insider threats

SOLUTION

Varonis Data Security Platform:

- **DatAdvantage** maps data access activity
- **Data Classification Engine** finds and classifies sensitive data
- **DatAlert** monitors and alerts on critical systems

RESULTS

- Accurate and up-to-date audit reports generated 92% faster
- Data monitoring and alerting mitigates the risk of insider threats and ransomware
- Increased visibility + support give peace of mind

Challenges

Homing in on overexposure to mitigate risk

Ask any IT or security professional what keeps them up at night and they'll most likely say the same thing:

> "Ransomware—the massive encryption of our data that would impact our ability to operate and make decisions. That... and how quickly it can spread," says a Senior Network Strategist.

The strategist, who requested anonymity, is part of a team responsible for proactively defending the sensitive data of an industry-leading agricultural company.

But not every threat is external. When a critical HR folder containing sensitive files went missing, the security team used **Varonis** to investigate the incident, find the missing folder, and determine if anything had been leaked:

- **Data Classification Engine** helped the team find the missing data in an open access folder.
- **DatAdvantage** showed who had moved the folder and a record of who had accessed it since the move.

> "Where there's smoke, there's fire. When we see alerts in Varonis, we're able to turn dials on certain critical data points within our environment. If changes are made, or something goes missing, Varonis lets us know."

IT security traced the incident back to a simple mistake—the VP of Human Resources had accidentally dragged the folder to a new location, making it over-accessible. Fortunately, no data had been compromised and Varonis made remediation fast and easy.

But this incident begged the question: What about next time? What if the next threat began maliciously deleting data? What would they do if ransomware snuck through their defenses and began moving or encrypting data en masse?

> “Realizing that someone could just mass move critical data and we would never know was a significant catalyst for permanently adopting a solution like Varonis. Without it, we’d be completely blind to what users were doing on our file shares.”

The incident stressed the need for visibility into what was happening on file servers and Active Directory. Varonis helps shine a light on their environments.

> “Where there’s smoke, there’s fire. When we see alerts in Varonis, we’re able to turn dials on certain critical data points within our environment.”

Solution

Discovering where data is overexposed and locking it down

In addition to **DatAdvantage** and **Data Classification Engine**, the company adopted Varonis DatAlert.

DatAlert detects and alerts on suspicious activity that may indicate a threat. Prioritized alerts enable deep investigation and quick action.

Using these solutions, the security team has built rule sets to mitigate company risk while minimizing false red flags.

> “Varonis gives us the ability to customize our alerting and reporting. By building different rules, we can get notified immediately if changes are made to critical file folders.”

Even potentially small issues don’t slip by unnoticed. The company’s IT Manager says that Varonis has helped alert them to users who might not be following best policy. With this knowledge, they can curb potentially harmful behavior before it escalates.

Now, both legal and HR receive notifications when access is granted to certain folders. Additionally, the company is able to quickly and easily report on who has access for various business units any time an auditor requests the information.

Always-on data monitoring and alerting help prevent the “disappearing HR folder” incident from recurring.

> “You know where your data is, what it is, and who has access. Varonis even tracks potential issues: If someone from HR exports a detail into an Excel spreadsheet to create a report, but leaves that data in the wrong place, we know about it.”

Varonis reports have even been baked into the company’s regular auditing processes. For example, as part of their regular daily process, the accounts payable (AP) department loads debit and credit information into their SAP system. Using Varonis, the security team monitors the file that the AP department uploads and creates a report to verify that no one is altering that data at any point during the process.

> “A breach could mean a loss of millions of dollars. So we’ve made it an audit requirement that these reports come out of Varonis to make sure that everything is on the up and up.”

“Varonis gives us the ability to customize our alerting and reporting. By building different rules, we can get notified immediately if changes are made to critical file folders.”

Results

Increased efficiency and data security confidence

According to the company's IT Manager, Varonis provides increased efficiency and tremendous peace of mind.

In terms of efficiency, they say that audits and reports that used to take hours are now prepared in minutes:

> "We don't have to do manual ad hoc reports in PowerShell or take screenshots in Active Directory and plug it into spreadsheets anymore. You're looking at huge time savings—a few hours down to maybe 15 minutes."

The peace of mind comes from Varonis' powerful mitigative capabilities and from knowing that the Incident Response team is always standing by to support the company's internal security team.

> "Varonis is by far one of the best vendors that we deal with—and we deal with all the Microsofts and Citrixs and Veritas and Symantecs of the world.
>
> Varonis' team is always available to assist. They're there for both detection and analysis, and eradication and recovery. The support and timeliness is noticeably better."

Before Varonis, one accidentally-moved folder could have spelled disaster. Now, the company is proactively reducing the risk of human error, while simultaneously taking steps to mitigating the threat posed by potentially malicious insiders and ransomware.

> "When I report to the risk committee, Varonis is nicely positioned as a risk mitigator in our organization. Preventing a catastrophic outage is the primary benefit. Built-in auditing is a big plus. Being able to enforce data security policies and alarm against worrying user behavior is another benefit. Varonis is well worth the expenditure."

"Varonis is by far one of the best vendors that we deal with—and we deal with all the Microsofts and Citrixs and Veritas and Symantecs of the world. The support and timeliness is noticeably better."

Mitigate ransomware and insider threats.

Varonis gives you visibility and control over your sensitive data.

REQUEST A DEMO