How a Top U.S. Airline is Making a Worry-Free Transition to OneDrive Thanks to Varonis

CASE STUDY

"It doesn't matter what your company does—if you have sensitive files to protect, you should have Varonis."

Challenges

Gaining more visibility into file shares

When a top U.S. airline (which has requested anonymity) adopted Varonis, they needed a solution that would help them protect their data and monitor all of their on-premises file servers.

To learn more about the issue they were facing, we spoke with the Senior Manager in charge of information security and compliance and the Senior Analyst for security and incident response.

> "
>
> "The main problem we were facing was that, quite frequently, file shares would be modified and no one would know who had done it," explains the Senior Manager.
>
> "Without file monitoring we couldn't see who was changing sensitive files or where they were located. We were being blindsided," the Senior Analyst adds.

As the company continued to grow, senior leaders had also decided to switch from on-premises storage to the Microsoft Office 365 cloud in order to facilitate collaboration and protect sensitive data.

But it wasn't until the airline began doing a proof of concept (POC) with OneDrive and implementing a proactive disaster recovery (DR) process that they realized the full extent of the issue.

"We didn't realize how many people were keeping information in their personal folders. For example, when our travel department received booking requests for executives, there were people who would save that information in plain text in their folders. It was a big eye-opener for us."

In fact, if it wasn't for Varonis, they might never have known how much sensitive data was unsecured. If they'd run afoul of a security breach and were found to be non-compliant, they could have faced fines of up to $100,000 every month.

"We're a public company, so we need to be PCI certified and SOC 2 compliant. Having more visibility and control is essential from both a legal and a financial aspect."

"Without file monitoring, we couldn't see who was changing sensitive files or where they were located. We were being blindsided."

Solution

Cleaning up on-premises data & protecting sensitive files in onedrive

The first thing the airline did was use Varonis DatAdvantage and Data Classification Engine to clean up data in their physical servers.

DatAdvantage automatically catalogs all user accounts, group memberships, and their permissions to data and resources. It also tracks account activity, allowing monitoring and immediate response whenever someone accesses or modifies sensitive files.

Data Classification Engine scans and classifies all sensitive and regulated information, regardless of whether it's stored on-premises, in file shares, NAS devices, SharePoint, or Microsoft 365.

"

"Varonis gave us so much visibility into our network. It's incredible. We were able to clean up files that we wouldn't have even known existed, and it definitely aided with PCI compliance."

"And the reports are great for forensics. It keeps a log of all user activity so you can easily track what's happening."

The airline also began testing OneDrive with Varonis to protect their sensitive files in the cloud.

"

"We wouldn't even be considering OneDrive if we didn't have Varonis in place."

VARONIS

"

"OneDrive is huge and its current monitoring capabilities are limited. We need the visibility and insights Varonis provides—especially in terms of what data people are storing and a forensic trail we can follow if they start saving data to personal drives."

DatAlert Provides the Data Analyst with alerts whenever it detects potential suspicious activity and allows him to investigate each report in granular detail. With it, he has all the insights he needs to ensure that the airline's sensitive data is protected.

"

"I look at DatAlert every day. I have it open as we speak. I get a notification any time a sensitive file is shared externally, and Varonis tells me whether or not the shared file contains any sensitive information."

"I've started using DatAlert to create reports and sending them to myself, so I can parse through all of the valuable information. Whatever I want to know, it's in there—who has administrative privileges, what accounts they have, if their password is expired, who's been accessing Active Directory and more."

DatAlert's wealth of information is so thorough that it's now become the pillar around which they're building out all of their in-house incident response (IR) capabilities.

"

"Luckily, we haven't had any major incidents that required a swift response. But we're confident that Varonis' alerts would help us catch suspicious activity and facilitate our internal response plan."

VARONIS

"We wouldn't even be considering OneDrive if we didn't have Varonis in place."

Results

File security on-premises and in the cloud

The airline is currently in the midst of their domain migration as they move all of their on-premises data to OneDrive. During this transition, they've ramped up their use of Varonis.

> "Our confidence is high when it comes to Varonis. It's easy to implement and intuitive to understand. The alert dashboard clearly shows me what I should be paying attention to—top alerted devices, top alerted threat models, and things like that."

And whenever they don't understand something, Varonis' support team is always on hand to help them through it.

> "I've only had to reach out to support a few times, but it's always been great. They always get back to me quickly with step-by-step instructions. Every issue has been resolved without hassle."

Varonis gives the airline confidence they won't sacrifice data security during their move to OneDrive.

"

"We wouldn't be moving our files to the cloud if we weren't completely confident in Varonis. With it, we know our file integrity is intact and our network is secure. Were I to make a lateral move to another company, I would mandate Varonis."

They're also thinking ahead and preparing for pending regulation changes, such as the California Consumer Privacy Act (CCPA), and other data privacy acts that will inevitably be introduced in the years to come.

When it comes to maintaining compliance and protecting sensitive data, they highly recommend Varonis.

"

"Varonis is already doing a great job protecting our file shares. Now we're using it to prepare for some of the stricter data regulations being introduced."

"

"I would highly, highly recommend it for gaining more visibility into your systems. It doesn't matter what your company does—if you have sensitive files to protect, you should have Varonis."

VARONIS

See where you're exposed.
Simplify compliance.

Varonis takes the stress and worry out of data protection, threat detection and response, and regulatory compliance.

REQUEST A DEMO