



How Varonis Helps a Top-20 U.S. Builder Shield Office 365 Users From Cyberthreats

CASE STUDY



“Like any solution in my team’s stack, it comes down to the efficacy of the product. Varonis does exactly what it promises to do—and we receive great support from their team.”



ABOUT THIS CASE STUDY:

Our client is a top-20 U.S. builder, developer, and engineering services provider. We have happily accommodated their request to anonymize all names and places.

HIGHLIGHTS

CHALLENGES

- Ensuring that data governance measures kept up with expansion into the Office 365 cloud
- Mitigating the risk of data breaches for online data stores
- Introducing data privacy measures to preempt regulatory requirements (GDPR, CCPA, etc.)

SOLUTION

The most robust data security platform:

- **DatAdvantage** for Windows, Directory Services, OneDrive, and SharePoint Online gives more visibility and control
- **Data Classification Engine** helps locate and lock down sensitive data (PII, PHI, etc.)
- **DatAlert Suite** provides advanced warning against anomalous behavior

RESULTS

- Varonis was able to detect and prevent the early stages of unauthorized access during pentests
- More security and peace of mind while expanding their hybrid IT environment
- Hours saved every week for the cybersecurity team

Challenges

Gaining visibility into Office 365 environment

When a top-20 builder based in the U.S. (anonymous by request) began a company-wide rollout of Office 365, it needed to ensure that sensitive data could be easily located and remain secure in the cloud.

As the company's Senior Security Lead says:



“Corporate took notice as operating and business service groups began using SharePoint Online and OneDrive. The problem was that they were expanding more rapidly than their governance could allow for. We needed a way to monitor SharePoint and OneDrive the same way we were monitoring our internal file system.”

For years, this builder had been leveraging Varonis products—DatAdvantage and Data Classification Engine—to identify, isolate, and lock down sensitive data like PII and financial information on-premises.



“Data Classification Engine was helping us search for sensitive data stored internally. DatAdvantage gave us an audit trail to follow and helped us understand who was the originator of content, which was very helpful from a legal and HR perspective.”

Now they wanted that same peace of mind in their cloud environment. Having witnessed Varonis in action, they had the confidence they needed to move forward.

“

“The request came in to get a better handle on what was going on in our cloud environment. Fortunately, we knew what Varonis was doing for us internally—and we knew it could be doing the exact same thing in Office 365.”

”

“We needed a way to monitor SharePoint and OneDrive the same way we were monitoring our internal file system.”

Solution

Data security—on-prem and in the cloud

This company conducts annual third-party penetration tests, or “pentests,” against their environment. They also conduct pentests whenever they consider new security solutions.

During these ethical hacks, pentesters try to elevate themselves in the environment to see what they can access without being detected.



The Senior Security Lead explains, “The crown jewels a hacker will go for is Domain Admin Rights or Enterprise Admin Rights. But when our pentesters try to self-elevate in DA groups, we have DatAlert watching them.”

“We have the capabilities to stop [that level of] unauthorized access and conduct further forensics if we need it. Varonis has definitely proven its value in mock real-event scenarios.”

Three Varonis products in particular help the company lock down and safeguard its sensitive data:

1

DatAdvantage for Directory Services, OneDrive, and SharePoint Online gives them maximum visibility and control both on-premises and in the cloud.



“DatAdvantage answers crucial questions about our content: Who put it there? Who last modified it? Who has access to it? It gives us good visibility into the audit of data.”

- 2 **Data Classification Engine for SharePoint Online** pinpoints where sensitive data lives in the cloud and gauge its risk level.



“We use it to hunt sensitive data in our environment. It helps us look at the cross-section of where we have sensitive data that might not be as protected as it should be, or that was accidentally put in the wrong folder.”

- 3 **DatAlert Suite** allows them to monitor folders and detect threats before they turn into major data breaches.



“DatAlert is the canary in the coal mine that warns us when something is wrong. From latent traces of malware to users being added or removed from protected groups, it tells us what we should be paying attention to.”

By combining knowledge of directory services and file server activity, Varonis provides advanced threat detection and well-rounded protection for sensitive data, wherever it lives.



“We have the capabilities to stop unauthorized access and conduct further forensics if we need it. Varonis has definitely proven its value in mock real-event scenarios.”

Results

More security and hours saved every week

According to the Senior Security Lead, Varonis is this company's best defense for detecting and preventing potential threats before they spiral into data breaches.



“Like any solution in my team's stack, it comes down to the efficacy of the product. Varonis does exactly what it promises to do—and we receive great support from their team.”

Having Varonis for OneDrive and SharePoint Online gave this company peace of mind during their Office 365 rollout. Now, it's saving hours every week for this company's IT team.



“DatAdvantage saves us a ridiculous amount of time during audits. We've saved hours on discovery and manually piecing together permissions and ACLs in Active Directory.”

“Without DatAlert and Data Classification Engine, we'd have to write our own anomalous behavior detection [scripts] and manually hunt through our folders for sensitive information. That saves time too.”

Fewer hours spent on tedious tasks, like permissions and access control list (ACL) clean-up, means more time for mission-critical tasks.

“

“Cybersecurity team hours are finite and they’re valuable. Having Varonis to free those up for other efforts is great.”

This company is now in the midst of expanding its Varonis lineup by adding DatAnswers to their security stack. They want to ensure that they continue to comply with regulations such as the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), and stay ahead of any new data privacy acts that may get introduced.

“

“Our Enterprise Risk Committee is currently evaluating our exposure to CCPA and GDPR. Any recommendations handed down by that committee will obviously be fueled by a technical solution. That will be where Varonis comes in.”

“Varonis will play a large role in helping us find personally identifiable information, see where it’s exposed in our unstructured data, and mitigate the risk.”

”

“Cybersecurity team hours are finite and they’re valuable. Having Varonis to free those up for other efforts is great.”



Step up the security of your hybrid IT environment.

Using Office 365 alongside on-premises data stores leaves gaps in your data security. Varonis helps you solve them.

[REQUEST A DEMO](#)