How Varonis Enables a U.S. Commodities Trader to Move to Office 365 with Confidence

CASE STUDY

“The combination of Varonis’ audit-level capability and proactive real-time detection is an enormous empowerment to any CISO—regardless of business, vertical, or core operations. Without Varonis, I wouldn’t be able to do my job.”

ABOUT THIS CASE STUDY:

Our client is a U.S. Commodities Trader in the NYC metro area. We have happily accommodated their request to anonymize names and places.

HIGHLIGHTS

CHALLENGES

- Mitigating the risk of data breaches from insider and outsider threats
- Migrating to the Office 365 cloud with the highest level of data security possible
- Ensuring compliance with national and international regulatory requirements

SOLUTION

The most robust data security platform:

- **DatAdvantage** audits who has access and who does access data in the cloud and on-prem
- **Data Classification Engine** locates and classifies sensitive data
- **Data Classification Policy Pack** identifies data protected under the CCPA and GDPR
- **DatAlert Suite** monitors and alerts on potential insider threats, outsider threats, and at-risk areas

RESULTS

- Access control remediation to safeguard sensitive folders
- Visibility into data infrastructure as they migrate to the cloud
- Worry-free compliance with data privacy acts and regulatory authorities: CCPA, GDPR, NERC, FERC, ENISA, and more

Challenges

Applying due diligence before moving data to the cloud

When asked about the most common threat facing modern businesses, the Chief Information Security Officer (CISO) of a U.S. commodities trader in the NYC metro area said:

> "With cloud storage, we've entered a new era that a lot of people aren't prepared for. Entering into the cloud without applying due diligence opens up a business to risk—and it's the most common issue I see."

Many decision-makers move to Office 365 without understanding all the risks involved. They don't have baseline controls in place to restrict access to sensitive data, including PII, trading algorithms, strategies, mergers, and acquisitions.

If the company can't trace where sensitive data lives, who owns it, and who has access, they have no hope of catching data breaches until it's too late. And if they move that data to the cloud, their attack surface increases exponentially.

> "It's not the cloud service provider's responsibility to automatically fix data security. We've seen numerous examples of data breaches caused by now-infamous configuration mistakes."

While outsider threats are always top-of-mind for the CISO, they say the more insidious threats often come from within.

> "87% of insider data breaches are non-malicious—they're caused by users with too much access, former employees whose permissions were never revoked, or even orphan files. These pose a massive risk."
>
> "Malicious insiders are the minority. However, the threat they pose is the most damaging—especially when there are no controls in place that would prevent them from making impactful actions."

Data breaches can have disastrous consequences on companies. In today's digital landscape, stale data and lax cybersecurity standards could collapse business empires.

> "The fines for failing to protect user privacy—they're not small. In the EU, you could pay up to 4% of the global revenue of your company."

"Entering into the cloud without applying due diligence opens a business up to risk—and it's the most common issue I see."

Solution

Visibility and alerting in the cloud and on-premises

DatAdvantage for Windows and Directory Services supports the commodities trader's on-premises data stores and email. Combined with **Data Classification Engine**, the CISO has a complete and panoramic view of data access.

This visibility is crucial for educating department heads about data ownership and working with them to automate changes to control lists and security groups.

> "In 99% of cases, the reaction is the same—anger, surprise, a sharp exclamation of 'This person shouldn't have access' or 'That person left months ago.' With Varonis, I can visualize the extent to which we're at risk on a single screen."

As the company expands its use of Office 365, they've added OneDrive support to DatAdvantage too.

> "With the expansion of cloud operations, the emphasis falls more and more on visibility of what's happening in the cloud."

For a business with a huge global presence, having this increased visibility into their cloud environment is non-negotiable—especially given the numerous data privacy acts and regulatory authorities their operations in North America and the EU are subject to.

Varonis Policy Pack enhances Data Classification Engine in order to simplify compliance. With hundreds of pre-built patterns, it's easy to quickly and accurately discover protected data.

> "As data privacy regulations change, it's not always possible to keep track of the specifics. Varonis does it for us with off-the-shelf data classification."

The final solution they use—**DatAlert Suite**—ties everything together. Continuous monitoring of on-prem and cloud systems enables the CISO to assess at-risk areas and proactively address potential threats before they escalate.

> "Varonis allows you to customize alerts based on threat scenarios. It's the key solution we use to associate the type of alerts with the actor and the value of the data they're attempting to access. Basically, it gives you a rich snapshot of everything going on in your environment and it enables you to dig deeper into the incident if you need to."

"As data privacy regulations change, it's not always possible to keep track of the specifics. Varonis does it for us with off-the-shelf data classification."

Results

Worry-free cloud migration and enhanced regulatory compliance

With Varonis, the CISO has been able to pin down data owners and then work with them to define the classification ratings of their critical files. From there, they can remediate excess controls, mitigating the risk of insider threats and data breaches. They say:

> "The combination of Varonis' audit-level capability and proactive real-time detection is an enormous empowerment to any CISO—regardless of business, vertical or core operations. Without Varonis, I wouldn't be able to do my job."

The high-level insight Varonis provides into the company's data stores, access controls, and at-risk areas gives the CISO peace of mind as the company expands its use of Office 365.

> "Without Varonis, every decision is reactive—Microsoft tools don't give you the same level of visibility. With Varonis, we can make strategic decisions to proactively defend our data. Varonis gives us a competitive edge."

With Varonis, the CISO also has peace of mind that the company isn't on the wrong end of compliance regulations, even when requirements change unexpectedly.

The company uses Varonis to comply with a variety of state and federal regulations, including those laid out by the North American Electric Regulatory Corporation (NERC), Federal Energy Regulatory Commission (FERC), and California Consumer Privacy Act (CCPA).

And, because their operations extend into the EU, they also have to consider various international regulations, such as the General Data Protection Regulation (GDPR) and the European Union Agency for Cybersecurity (ENISA) requirements.

> "Data privacy regulations are complex entities. If you get subpoenaed for your data or hit with a data subject access request, you need to be able to quickly retrieve that data or your business is going to suffer. You can't do that with a Windows Explorer search—you need a solution like Varonis."

"With Varonis, we can make strategic decisions to proactively defend our data. Varonis gives us a competitive edge."

Migrate to Office 365 with confidence.

Varonis shows you where sensitive data lives, where it's overexposed, and where you're at risk of non-compliance.

REQUEST A DEMO