VARONIS CASE STUDY

A Financial Services Design and Distribution Firm

> *“Varonis DatAdvantage helped us reduce a process that previously took 30 hours to less than 90 minutes. To be able to do that kind of analysis and have that level of security is a powerful statement of how valuable Varonis is as a product.”*

—Director of Infrastructure Technology

THE CUSTOMER

A Financial Services Design and Distribution Firm

INDUSTRY

Finance

PRODUCTS

DatAdvantage for Windows, DatAlert, Data Classification Framework

This Varonis customer is a leading financial services design and distribution organization with more than 100 member firms across more than 30 U.S. states, the United Kingdom, and the United Arab Emirates.

BUSINESS REQUIREMENTS

Visibility into Windows File Server Permissions

The company needed a solution that could support the future migration of file servers and files from an Active Directory domain that belonged to a member firm it eventually acquired. The company's IT team wanted greater visibility across both file systems so that they could better plan and map the migration of the acquired firm's data.

PREVENT INSIDER THREATS

The company wanted a solution that could monitor insider activity behavior to help detect and arrest mass deletions and employees taking intellectual property to a competitor.

GET AHEAD OF POTENTIAL DATA BREACHES

Malware and ransomware are on the rise, so the financial services firm required a solution that could quickly alert the IT staff to unusual file access behavior, like rapid encryption of files stored on its servers.

FIND AND LOCKDOWN SENSITIVE INFORMATION

The company wanted to find where its most sensitive data was located and determine if any of it was stale so that they could reduce risk and save on storage costs at the same time.

ENABLE COMPLIANCE

The company must be prepared to answer questions from regulatory bodies (i.e. FINRA and SEC) such as, "Do you have a process around managing security? Do you have a process around managing file access?" These entities also required the firm to prove the effectiveness around processes such as file access permissions and auditing.

THE SOLUTION

DatAdvantage for Windows

The company initially purchased DatAdvantage for Windows to support the migration of file servers, and files from an Active Directory domain, that belonged to a member firm it eventually acquired. DatAdvantage gave the firm much needed visibility across both file systems so that it could best plan and map the migration of all of the other firm's unstructured data.

According to the firm's director of infrastructure technology, *"Immediately after the initial DatAdvantage roll out, we came to realize how truly valuable this solution is because it helped us learn two things: First, our file security and file permissions, at least for the group that we were migrating, needed to be upgraded and corrected before we did the migration. Second, Varonis helped us reduce the chance of insider threats. Varonis was a perfect win because its solutions made it super easy to A, identify our problems and B, to fix them."*

During this Active Directory migration, shortly after putting DatAdvantage in place, we had two relatively senior level employees leave the company and go work for what we considered a direct competitor. Obviously there was some concern associated with the potential loss of intellectual property – even though we didn't necessarily have any suspicions about these individuals, we still wanted to make sure that company data didn't leave with them."

We are fortunate to have Varonis in place because it helped us discover that one of our network folders containing about 10,000 files had been completely deleted. Before DatAdvantage, we didn't know any of the information around 'the what' and 'the why' these files were deleted from a shared directory space."

The director of infrastructure technology's first question was, *'Was this folder being used by other people and was there anything that other people expected to be there that was suddenly missing?' Varonis helped us quickly see who was using those files by giving us a log in history, and then see everything that happened with those deleted files over the period of time in which we were interested. I was quickly able to discover that there were only two people who had accessed those files: One was an executive administrator, and the other was the individual who departed the company. I validated with other users that nobody was missing any data, and even though the folder itself was accessible by multiple people, it had not been accessed by anybody but those two individuals. Just by looking at the nature of the files that the second individual had looked at, I could see that they were employee performance review type files that an executive administrator would be expected to be able to handle and review once they were completed.*

This insight helped me determine that this individual was using that shared folder as his 'personal online drive' for his files. As a result of some other forensic things that we did, we drew the conclusion that from his perspective, he was merely cleaning up. Yes, he made some poor choices, but he had no intention of deleting maliciously or stealing any intellectual property.

So, in this case, Varonis DatAdvantage helped clear the individual's name – the software helped us reduce a 30 or so hour process (involving a costly forensics investigation), to less than 90 minutes. We wouldn't have been able to come to such a definitive conclusion without it - that kind of analysis and to have that level security is a powerful statement of how valuable Varonis is as a product."

DATALERT

Varonis DatAlert gives the firm the ability to detect potential security breaches with real-time alerting based on file activity, Active Directory changes, permissions changes, and other events. Alert criteria and output are easily configurable so that the right people and systems can be notified about the right things, at the right times, and in the right ways.

The firm's director of infrastructure technology said, *"Any IT person will freely admit that he or she is deathly afraid of being impacted by a ransomware such as CryptoLocker. We configured DatAdvantage with DatAlert to detect and disable an account that is encrypting files. Once it hits a threshold, of say, 200 files encrypted within a minute period of time, we're able to disable that account to prevent our corporate information stores from being encrypted.*

This just one way we've used DatAlert. We are continuing down the path of migrating two different Active Directory file structures into a single file server, so we will almost certainly use Varonis to do that copy, as well as in the event of that migration, as well as using it for file permissions, and file security, etc."

VARONIS DATA CLASSIFICATION FRAMEWORK

The firm principally works in the life insurance space, and has a fair amount of protected health information as well as personal identifiable information that it must protect. The Varonis Data Classification Framework helped quickly discover where sensitive information was vulnerable and who was touching it - and locked it down without interrupting business.

After parsing through the company's file servers, the Data Classification Framework helped the firm uncover three terabytes of unstructured data that was classified as PHI and PII. According to the firm's director of infrastructure technology, "*Before implementing Varonis, I think we assumed that we had virtually no PHI or PII on our file server, from a company perspective there was a perception that most of the data was in our databases.*

And then of course, because we replicated that data down to our disaster recovery data center, it finally sized at around six terabytes of unstructured data that we needed to protect. *Now that we have that level of visibility, our records management organization is interested in leveraging Varonis to classify other data such as intellectual property.*

For next year we're considering classifying SharePoint data, and looking into ways to get better synergy between our records management effort and our classification efforts."

RESULTS

DISCOVER

DatAdvantage helped the customer **discover** that one of its network folders containing about **10,000 files** had been completely deleted.

REDUCE

DatAdvantage helped the customer **reduce** a **30 hour** process to just under **90 minutes.**

LEARN

DatAdvantage helped the customer **learn that 52% of its unstructured data** hadn't been touched in **24 months**.

A PROACTIVE APPROACH TO PREVENTING INSIDER THREATS

The firm's director of infrastructure technology said, *"Think about really truly understanding the labor and the opportunity costs involved with an insider threat. Think about the costs associated with going through the process the old-fashioned way, and not being able to come up with evidence that can draw a conclusion with the intent of the individual, versus the cost of implementing Varonis, and using it on demand, and just making these things non-events.*

The value of the Varonis software and its capabilities have more than paid for itself. Most companies don't think about cost of labor involved with an insider threat, but it's an important factor. I appreciate having Varonis in place and running upfront what I need it to do quickly and easily.

Varonis is a no-brainer. With its log reports I can quickly provide concrete, indisputable evidence in a court case for example, that the insider threat involved activity such as copying files or malicious intent. It'll stand up in a court of law, to the extent that the evidence will be able to prove or disprove anything – and could certainly reduce the amount of time it takes to litigate such a case."

AN AUTOMATED AND EFFICIENT PROCESS FOR MANAGING REGULATORY COMPLIANCE DEMANDS

"Compliance requirements are getting more and more mature, so managing them effectively is an ongoing effort and something we are very proactive about. If a regulatory body requests an audit and has a list of questions for us, we'll narrow the scope of the question down to the specific group that's being audited. So if it's our brokerage group, then the audit questions apply only to that group. Many of these entities are very process oriented, and will ask, 'Do you have a process around managing file access? Our answer is, 'Yes, we do.' They also want to see how effective our processes are around, for example, file access permissions and auditing file access. Varonis has helped us put some of those pieces in place so that we can react quickly and efficiently.

The foundational element in any of these, whether it's file access, whether it's a HIPAA control program, once again comes back to 'Do you know what information you have, do you know where it is and do you know who has access?' Thanks to Varonis we're able to address all of these questions quickly and easily at the drop of a hat."

SENSITIVE DATA IS LOCATED AND STALE DATA IS ELIMINATED

"As a company we're trying to get to the point where we can intelligently archive our unstructured data that we think still has residual value but is not currently being used. Varonis has shined a spotlight on something that's never had light on it before – the software's ability to show us 'files accessed' and "last used," has resulted in us learning that 52% of our unstructured data hasn't been touched in 24 months.

The first question is, 'If you're not using it in 24 months, how much of it is relevant?' The second question is, 'Why am I keeping it on primary storage? Why don't I start thinking about moving it to less expensive storage, and doing something different about it?'

Some folks think there's no risk of keeping data forever, which can be a struggle for us. We have several terabytes of data locally in the corporate office – it's not so large that we can't secure a single file server and storage system, and put protection around it. But the question is, if we have sensitive data, protected health information and stuff like that, should we move it separately? How do you architect security around a small set of data that's interspersed with a slightly larger but not an overly large storage system? Do we need to separate it? Do we just put encryption across everything?

By using Varonis to get better visibility into these things, we can formulate policies around what do we do with sensitive data, what do we do with data that's no longer being actively used, and how do we put it in near-line storage instead of online storage - which will ultimately improve our cost structure, support structure, and our security.

ABOUT VARONIS

Varonis is the leading provider of software solutions for unstructured, human-generated enterprise data. Varonis provides an innovative software platform that allows enterprises to map, analyze, manage and migrate their unstructured data. Varonis specializes in human-generated data, a type of unstructured data that includes an enterprise's spreadsheets, word processing documents, presentations, audio files, video files, emails, text messages and any other data created by employees. This data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property and numerous other forms of vital information. IT and business personnel deploy Varonis software for a variety of use cases, including data governance, data security, archiving, file synchronization, enhanced mobile data accessibility and information collaboration.

Free 30-day assessment:

WITHIN HOURS OF INSTALLATION

You can instantly conduct a permissions audit: File and folder access permissions and how those map to specific users and groups. You can even generate reports.

WITHIN A DAY OF INSTALLATION

Varonis DatAdvantage will begin to show you which users are accessing the data, and how.

WITHIN 3 WEEKS OF INSTALLATION

Varonis DatAdvantage will actually make highly reliable recommendations about how to limit access to files and folders to just those users who need it for their jobs.

START YOUR FREE TRIAL