



# VARONIS CASE STUDY

Loyola University Maryland



# LOYOLA

UNIVERSITY MARYLAND

*“A real differentiator between Varonis DatAdvantage and the other solutions we explored was the breadth of features that it offers. It finds your sensitive data, gives you the ability to track it and assess it against baseline end-user activity, and automatically alerts you when abnormal behaviors begin to happen. DatAdvantage allows us to see what’s happening and gives us the ability to take action if we need to.”*

—Louise Finn  
CIO, Loyola University Maryland

# THE CUSTOMER

## LOYOLA UNIVERSITY MARYLAND

### **LOCATION**

Baltimore, Maryland

### **INDUSTRY**

Education

Founded in 1853, Loyola University Maryland is a Jesuit, Catholic university in Baltimore, Maryland.



# CUSTOMER CHALLENGE

Loyola University Maryland feared the possibility of falling victim to a fate that other major universities around them had experienced: a major data breach. In the months following the early 2014 attack on a large university nearby, Loyola University Maryland's CIO Louise Finn proactively explored various solutions that could mitigate risk in the event of a similar attack, but the technologies she probed could not provide reliable and detailed insights.

*According to Finn, "A top priority of ours was to ensure that any Personally Identifiable Information (PII) of our staff and students that lived across our many bio-systems was locked down. We need to know where it is at all times, who has access to it, and ensure that it's well-protected."*

The university was about to sign on the dotted line with another solution but after conducting a 30-day DatAdvantage pilot with multiple staff members, the Loyola University Maryland IT team quickly identified that DatAdvantage would provide them so much more. They were amazed with the level of accuracy and breadth of features. Loyola made its decision on Varonis because its solution provided many features other vendors do not, such as:

- Complete visibility into who has access to data and what data any user or group has access to (bi-directional visibility)
- An audit trail of all file activity, including who opens, creates, deletes, moves and modifies files (without requiring native auditing)
- The ability to identify excessive permissions, and simulate and execute permissions changes
- The ability to identify data owners
- Automated alerts on anomalous user behavior compared with historical access patterns
- The ability to identify stale data
- All in a single view



As for the implementation, the full install only took a few hours. Dave Arnett, the university's Associate Director of Servers and Storage added, "Technically I didn't have to do very much at all. It was very nice."

*"A real differentiator between DatAdvantage and the other solutions we explored was the breadth of features that it offers. It finds your sensitive data, gives you the ability to track it and assess it against baseline end-user activity, and automatically alerts you when abnormal behaviors begin to happen," explained Finn. "If an employee is leaving the institution they often decide to download whatever they want, maybe not realizing those files belong to the university. DatAdvantage allows us to see what's happening, giving us the ability to take action if we need to."*

Tom Podles, Director of Infrastructure at Loyola University Maryland, said, *"There are two things that you want to do for security. You want to prevent people who aren't supposed to get to your sensitive data, from getting to your sensitive data. But you also need to be able to audit your data inventory to moderate access and ensure that those who need access to the data have it, and that they are using it correctly. Varonis is one of the few security solutions that actually does both."*



# RESULTS

## Reduced Risk and Improved Productivity

Before Varonis, Loyola University Maryland had no way of identifying where all of its potentially vulnerable PII data specifically lived on their network. After installing Varonis DatAdvantage the IT team was able to identify all instances of PII data and found that they could eliminate almost all of the social security numbers that were saved. This both mitigated risk and greatly reduced the company's use of storage space.

According to Dave Opitz Sr. Security Analyst for Technology Services at the university, *"One important task that we have been able to accomplish is reducing our use of file storage. We have been running a trial of Varonis on SharePoint, and it turns out we've been able to eliminate almost all instances of social security numbers saved. We've already deleted 90% of these unnecessary instances, and are currently working on the last 10%."*

Additionally, the level of functionality and information that DatAdvantage provided the Loyola University Maryland IT team was previously unobtainable. Without DatAdvantage, IT would have had to manually go through each folder if they wanted the level of accurate insight that Varonis provides—a futile task.

*"The new insights allow us to quickly prioritize our security efforts and educate employees on data storage practices,"* added Opitz.



## WHAT'S NEXT?

The university also purchased Varonis [DataPrivilege](#) in addition to DatAdvantage and will roll it out in the very near future. The plan is for IT to work with the university's different departments to clean up file shares, delete stale data, assign permissions, and rework their general data practices, then introduce DataPrivilege, which will give users the ability to easily review, grant, and revoke access through an easy-to-use web application—without IT's assistance. The university expects DataPrivilege to not only reduce IT burden, but also save time while allowing users to make measurably better access control decisions.

For more information on Varonis' solution portfolio, please visit [www.varonis.com](http://www.varonis.com) and join the conversation on [Facebook](#), [LinkedIn](#), [Twitter](#), and [YouTube](#).

Get a free security assessment [here](#).

# 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](#)