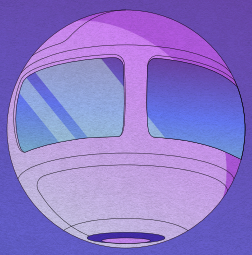
cyera

Case Study

How a Leading Academic Medical Center Achieved Real-Time Data Visibility and Solved a 1,000-Hour DLP Stalemate with Cyera



"A lot of companies, when they get too big, don't listen to you anymore. Cyera actually listens." - CISO at a Leading Academic Medical Center.

An Associate Vice President and CISO at a Leading Academic Medical Center manages an information security program covering healthcare, research, and education. This environment requires protecting a large volume of PHI, research data, and student records (FERPA) across a complex ecosystem that includes Azure, AWS, Citrix NetScaler, and Epic EMR. As a heavy Microsoft shop leveraging E5 licensing and Azure as its primary cloud provider, the team faced a critical challenge: protecting a sprawling, multi-platform environment containing billions of sensitive records while lacking a clear data inventory or the ability to classify data at scale.

The Challenge: Filling the “Space in the Middle”

"You know you have critical data, you know you want to protect it... But you have all the space in the middle where you have a bunch of questions that you can't answer without a tool like Cyera."

No Data Inventory:	The team managed sensitive data like PHI, PII, FERPA records, and research data. But without automation, the environment's massive scale made it impossible to comprehensively map and monitor data using traditional manual methods. They had a general sense of where the data lived, but securing it at scale was an entirely different challenge.
Modernizing Data Classification:	Legacy policies relied on manual user classification, an industry-wide challenge at this scale, where automated oversight is required for accuracy and consistency.
OneDrive Oversharing With No Proof:	The team suspected that sensitive files were shared via open links but lacked evidence to support that. Without proof, justifying new controls was difficult.

The Root Problem Manual Efforts Couldn't Solve:

The team spent over 1,000 hours across multiple cycles of Microsoft DLP projects. These projects were repeatedly tabled because legacy tools could not provide the deep data context required to solve the root problem. Despite extensive effort, these technical limitations prevented the projects from delivering the desired risk reduction.

Static Rules That Couldn't Scale:

While this Leading Academic Medical Center had existing DLP rules for Outlook, they did not yet extend to file-sharing environments. Simple patterns like MRN numbers were caught in emails, sensitive files were being shared through open OneDrive links, and the team needed better visibility and controls to address this.

Scale That Made Manual Work Impossible:

Billions of records made manual inventory impossible. No staffing model could keep up. Automation was the only way forward.

Manual classification couldn't keep up with the amount of data being generated. Even with a solid policy in place, the team faced a growing visibility gap. Automation became the only way to close it.

The Solution: Machine Hours Over Man Hours

The CISO shifted the strategy from a human-led effort to AI and Machine Learning automation.

Automated Classification:

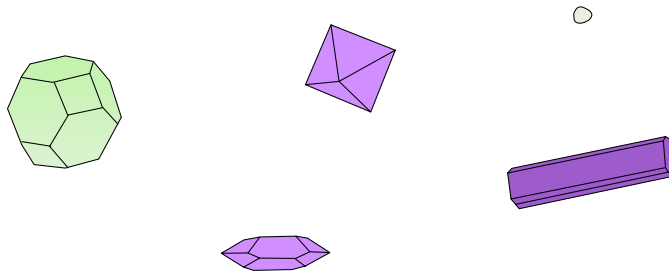
The company updated its data policy to have Cyera's AI handle inventorying and classifying data. The team recognized that manual inventory was not realistic given the scale. Machine hours, not human hours, made the difference.

Unified Enforcement:

By combining DSPM and Omni DLP, the team could send richer data context to Microsoft Purview. This made enforcement more accurate and adaptable as the environment changed.

Strategic Integration:

The platform integrated seamlessly with Azure, M365, and the company's identity management solution (Saviynt), ensuring a unified approach across connected environments.



The Results: Visibility in a Week, Risk Reduction that Compounds

Within the first week of scanning, the team already had actionable findings. The CISO brought the results to the Chief Data Officer and CIO directly: "I've seen it, now you guys are gonna see it, because we have a problem, we need to fix it. We all have skin in the game."

Within a week of deployment, Cyera surfaced insights about the company's sensitive data that would have been impossible to uncover through manual reviews alone. The team gained a clear view of where personal information was stored and identified potential risk areas:

Cyera's initial scan categorized thousands of security findings, enabling the team to focus its immediate efforts on the top 30% of critical high-risk exposures.

Moving from manual guesswork to automated visibility made a noticeable difference for the team: **"My stress level has gone down since having Cyera here, because it helps me to get a hold of where my data is and how to protect it"** - CISO at a Leading Academic Medical Center

The team acted quickly to close externally shared OneDrive links that posed a risk of exposing sensitive information, including patient data. Then they proactively secured these records, significantly reducing its exposure.

During the initial scan, Cyera surfaced orphaned EDW production environments that the current data team had actively been trying to locate. This allowed security and data teams to align on a shared consolidation effort, extending Cyera's value well beyond security.

Cyera identified data stores that remained active beyond the company's employee offboarding timeline, giving the team the visibility needed to strengthen their data lifecycle management process over time."

"A lot of companies, when they get too big, don't listen to you anymore. Cyera actually listens." **- CISO at a Leading Academic Medical Center.**

Choosing Cyera: Lessons Learned

"You need machine learning, you need AI to be able to make data decisions, and inventory and classify your data. So I think that Cyera has the best product to do that today."

Several factors shaped their decision to move forward with Cyera:

First, Cyera integrates directly with Microsoft environments.	Azure, M365, and Purview operate as a connected workflow rather than isolated tools. That integration is essential for teams already invested in Microsoft: **"Having Cyera interface directly with Microsoft products, and having that partnership, is vital to us."**
Second, a point solution for DSPM is not enough.	Without a complete approach, teams manage rules manually and miss context. Cyera's end-to-end coverage avoids these gaps and delivers more reliable results.
Cyera's proactive investment in integrations, including Microsoft and Saviynt, was a deciding factor.	**"Cyera having an aggressive approach to getting value-add integrations is very, very important to the product."** - CISO at a Leading Academic Medical Center
Finally, success depends on building relationships across the organization. Bringing together data officers, CIOs, and security teams creates shared ownership and leads to better outcomes:	"If you can build relationships with your data officer and with your CIO to try to bridge the gap and say, hey, we've all got a vested interest in this, how do we solve it together? That's a winning strategy."

Explore What's Possible with Cyera

Whether your world revolves around healthcare, research, education, or all of the above, Cyera empowers you with automated discovery, intelligent classification, and robust DLP so you can finally deliver on the promise of true data protection.

Book a demo →

"Most executives are not going to understand the value of DSPM, but the value is that you're able to reasonably say our critical data is protected."