CYERA

Turning Data Noise into Actionable Security: Lessons from a Leading Financial Institution

“We had a need to do document retention... Cyera helped us discover the data, tag it, and move it into quarantine.”

Security leader, U.S. financial institution

Managing data across a large financial services organization quickly becomes unmanageable without the right tools. Over time, redundant and outdated files pile up, Microsoft 365 sharing becomes scattered, and legacy file shares remain. The result is a lack of clarity about what data to keep, protect, or remove.

The team wasn’t starting from scratch. They had tried another data security platform, but it never got off the ground, leaving them with stalled initiatives and no clear path forward. **They needed a partner to help untangle the noise, not just another tool.**

1. The Challenge: Data everywhere, clarity nowhere

The institution faced both strategic and tactical problems that made progress difficult:

- **Document retention was stuck:** ROT data lived across file shares and M365, and the organization had no systematic way to identify, tag, or retire? it.
- **Their previous platform failed:** A legacy solution sat unused, so it couldn’t be operationalized or tuned for their environment.
- **DLP alerts drowned out real signals:** Thousands of false positives obscured the few risky events that truly mattered.
- **M365 exposure was unclear:** Guest and 3rd party sharing kept happening, but the team couldn’t see how many files were shared or what access users had.
- **Cross-functional alignment was impossible without shared visibility:** Security, privacy, and data governance each had requirements, but they lacked a reliable data foundation to make decisions.

“DLP creates a lot of noise... and with that noise comes a lot of work.”

- *Security leader, U.S. financial institution*

The problem was not a lack of data. The problem was **a lack of insight.**

Turning Data Noise into Actionable Security: Lessons from a Leading Financial Institution

2. The Solution: Automated discovery, smarter DLP, and a partner willing to build with them

a. When the institution partnered with Cyera, they weren't just seeking technology. They were looking for a **path forward.**

Cyera helped the team with:

- Discovering where data lived across cloud and on-prem systems
- Tagging files according to retention rules
- Building a quarantine workflow that didn't previously exist

Over six months, the teams worked side by side to design a model the institution could actually put into practice.

> "Some of this functionality didn't exist, but the team was willing to build that capability while we partnered together"
>
> - *Security leader, U.S. financial institution*

b. Transforming DLP from noise to clarity

The real DLP problem was not missing alerts, but being buried under too many.
With Omni DLP, they saw:

- About 16,000 false-positive events reduced to just a handful
- AI distinguishing normal business activity from abnormal patterns
- A dramatic reduction in analyst time spent chasing non-issues

This shift alone gave the security team hours back each week and changed how they approached data risk.

Turning Data Noise into Actionable Security: Lessons from a Leading Financial Institution

c. Microsoft 365 visibility that drives action

Cyera helped them answer previously unanswerable questions:

- Which users are exposing data to guests or third parties?
- How many files are impacted?
- What type of data is at risk?
- What remediation will help?

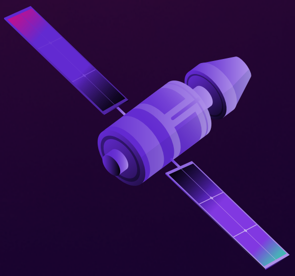
With this clarity, the team could prioritize issues and take action directly inside the platform.

d. Coverage from cloud to file shares

Although their long-term strategy was cloud-first, Windows file shares remained entrenched in day-to-day operations. Cyera supported both, giving the customer a unified view of data risk across environments.

3. The Results: A modernized data-security program that finally moves forward

- This wasn't just about new tools. It **changed how security, privacy, and governance teams worked together.**
- **A document retention program that actually shipped:** After years of stalled progress, the institution finally completed its retention initiative by combining discovery, tagging, and quarantine workflows to classify and route data.
- **Massive reduction in DLP noise:** What once was overwhelming became manageable. Analysts no longer sifted through thousands of false alerts. They focused on real issues.
- **Faster, clearer decision-making** The team could now:
  - Identify risky users and overshared files
  - Understand exposure at a glance
  - Prioritize insider-risk related data issues
  - Route fixes through Jira or direct platform workflows



CYERA

Turning Data Noise into Actionable Security: Lessons from a Leading Financial Institution

- **Cross-team alignment rooted in shared insight**

Privacy, cybersecurity, and governance finally operated from the same understanding of:

- What data exists
- What must be kept
- What can be removed
- What must be protected

"We focus on what's most important - insider risk, fraud, and the data that can be misused. And then we drive it based on risk."

- *Security leader, U.S. financial institution*

- **A simpler, more intuitive experience:** Instead of slow setups and steep learning curves, the institution used a platform that made data security feel accessible even as requirements grew.

"You point, click, you go. Everything's a very clean layout."

- *Security leader, U.S. financial institution*

Why This Financial Institution Chose Cyera

It wasn't just the platform, it was the partnership: "They were willing to tune the tool, discover, build automation that didn't exist... and that really stood out for us." - Security leader, U.S. financial institution

Here's what changed for their team:

- They built a foundation to make DSPM and DLP part of daily operations.
- AI helped cut through noise and highlight real risks, so teams could focus on what matters.
- They gained visibility across cloud, M365, and on-prem environments.
- Remediation fit into their existing workflows, so teams didn't have to reinvent how they work.
- Their approach could flex as new risks emerged, including challenges like AI misuse.

Explore What's Possible with Cyera

See how organizations reduce risk, strengthen governance, and protect what matters with Cyera.
Book a demo