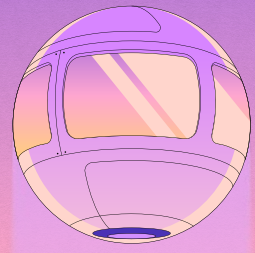


From Alert to Evidence in One Day:

How a Global Media Company Investigated 6,854 Files with Cyera Omni DLP

Cyera helped a global media company catch an insider data leak and gave its security, privacy, and legal teams the evidence to act.



“Before Omni DLP, my team spent most of the week chasing alerts that turned out to be nothing. Now we see context on every alert, like what the data is and who touched it. We’ve cut false positives, and I trust the alerts we do get.” - Director of Data Security, Global Media Company

Same Day

first file-level report delivered after discovery and escalation

6,854

incidents in the full report, across the same number of unique files

Expedited

resolution—from detection to comprehensive evidence to support investigation

1 Engineer

reviewed alerts and caught the data of exposure

At this global media and entertainment company, a finance intern—on their last day on the job—shared thousands of sensitive internal documents from their corporate OneDrive account to a personal external email domain. They used a second destination in an apparent attempt to hide this activity. All this took place within a short window of time on a single day. At first, nobody at the company was aware of the serious incident. That is, until a data security engineer consulted his Cyera dashboard and spotted the insider threat within just 24 hours.

He discovered that contracts, acquisition agreements, payment authorizations, talent and writer deals, and forwarded email threads were exposed, with many containing personally identifiable information (PII) and financial data. This incident could easily be missed because the files were left as OneDrive shares rather than email attachments—and the user had legitimate business reasons to touch many of these folders. The incident was quickly resolved through Cyera’s data-centric visibility into user behavior combined with AI-powered classification, continuous tracking of data exposures, and automated remediation.

Collaborating with the Right Partner Accelerates Data Risk Investigation

The organization sought answers to four critical questions:

- What data was exfiltrated?
- Who was impacted?
- What permissions were granted to the user?
- What activities was the user engaged in prior to the incident?

Cyera analysts were assembled the very afternoon that the incident was detected. The internal data security engineer led the effort from his side. After discovering the incident, he escalated it, and engaged other relevant internal and external teams. The investigation became a coordinated effort involving multiple people and leveraging three key data security layers: Cyera Omni DLP, Cyera DSPM, and Cyera Access trail.

Omni DLP: Transforming Alerts into Evidence	DSPM's Data Classification: Revealing What's Inside	Access Trail: Triggering Incident Response
• Created a file-level report from the alert, with details like file names, hashes, destinations, severity, and links to each document. • Reran the report when the scope expanded to include every event the user created beyond the initial PII-focused set.	• Cross-referenced files with DSPM to indicate which ones were scanned and what sensitive data they held. • Flagged files that had not yet been classified for rescanning.	• Backfilled Access Trail to uncover user behaviors before the incident, such as file sharing and chatting with external users in Microsoft Teams. • Prepared to run AI-powered Investigation Agent as a next step to get an enriched view of the user's activity and determine risk.

Cyera Delivers a Swift Evidence-Backed Verdict: Insider Data Exfiltration

In a matter of days after the incident was discovered, it was resolved through the accurate detective work by Cyera and the organization's internal team. Here's how the series of events unfolded:

Days 1 & 2 Mass sharing on the intern's last day	Omni DLP flagged 6,854 files that were shared from OneDrive to an external personal domain within roughly two hours, raising high- and critical-severity alerts on each unique file.
--	---

Day 3

Detection by the data security engineer

During his morning review of the Omni DLP queue in the unified console, he found a flood of alerts tied to a single identity. Next, using Cyera's AI-powered severity rating, he queried the tool in plain English to find out whether the alerts were bugs, false positives, or real events. Using business context, such as the identity of the person connected with the access, data sensitivity ratings, and exposure conditions, Cyera automatically logged the incident as a real event that demanded immediate attention.

Days 4

Delivering the full picture

When the customer asked for a thorough audit of the user's activities, Cyera delivered a comprehensive report that was handed off to the SOC, legal and privacy teams for further action. To build the report, DSPM's classification engine used machine learning to provide precise, granular details on the exfiltrated data, including type, location, sensitivity level, and business risk. Access Trail quickly pinpointed the intern who accessed the files, the exact time, the sensitive data involved, and how they gained access, which, in this instance, appeared to be legitimate, but only on the surface.

Days 4

Read-out and closure

Cyera security analysts stepped in to assist with the investigation, walking the internal team through the findings in a formal Incident Materiality Assessment. With defensible evidence in hand, the security operation center (SOC), legal, and privacy moved the investigation forward to prioritize and remediate the issue to eliminate root causes and define stronger data privacy policies.

Thousands of Alerts Build the Case

Cyera's detailed reports anticipated questions for the investigation team before they even asked them, accelerating the process for legal and other teams. Access Trail audits provided precise insights into user activity: time-stamped records of when they accessed sensitive data, how they gained access, the actions they took (downloads, sharing, transfers), and how that data moved across the environment. The initial report focused on PII, showing 989 incidents. Later, when the scope of the project expanded to all sensitive data, the second report discovered 6,854 incidents, matching the identical number of unique files. This discovery made it obvious that the intern was responsible for exfiltrating this data set.

The clear takeaway from this story is that, when you combine a vigilant data security engineer, proactive internal teams, and Cyera, it's a winning combination for quickly identifying and resolving insider threats.

For more information visit cyera.com or book a demo

Book a demo

