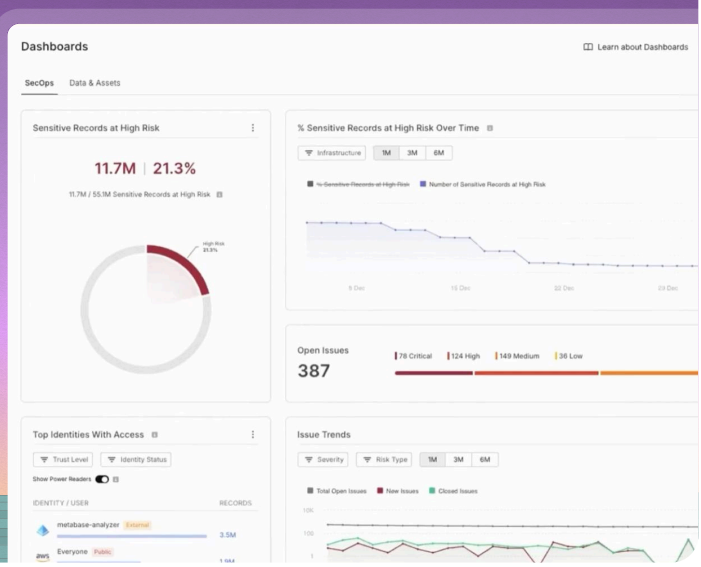
cyera

Solution Brief

CYERA PLATFORM

Protect Your Data Everywhere It Lives and Moves

The difference is shared data intelligence between Cyera DSPM and Omni DLP.



Two Halves of the Same Problem

The data security problem has two halves: data at rest and data in motion. DSPM answers the first half: what sensitive data exists, where it lives, who can reach it, and what risk state it's in. DLP answers the second half: where that data goes, how it moves, and whether it should. But you're only ever seeing half of the story — and half of the blast radius.

Challenges for Security Teams

Visibility is fragmented.	DSPM shows you who has access to sensitive data. DLP shows you who is acting on that access. But when those signals live in separate tools, you're connecting the dots manually while the clock runs - and by the time you do, the window to act has closed.
IP is impossible to define.	Product formulas, M&A deal structures, engineering source code - the data that defines your business has no generic pattern, no industry keyword, no fingerprint for what isn't known. If DLP can't define it, it can't protect it.
No labels, no coverage.	Most enforcement depends on labels that were applied incorrectly - or never applied at all. DSPM finds those gaps and fixes them. But for formats that can never receive a label only DLP can enforce directly on content.
AI amplifies data debt.	AI tools inherit access to data at rest - turning years of overpermissive access and unclassified files into immediate exposure. When that data moves through prompts, responses, and models, it doesn't just leak - it may be gone permanently.

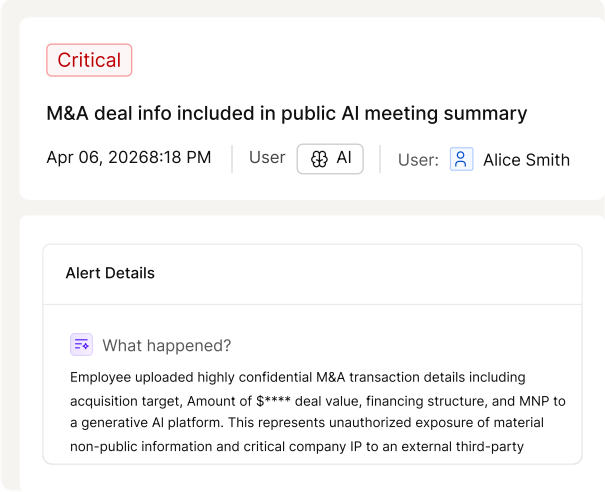
The Cyera Difference

What's missing is shared data intelligence to connect the two halves. Cyera DSPM understands not just where sensitive data lives, but what kind of data it is, why it matters to the business, and who can access and use it. Cyera Omni DLP extends that understanding to the moment data moves - so every investigation is grounded in the same view of your data. Here are four ways organizations are leveraging their data intelligence with Cyera.

Insider Risk

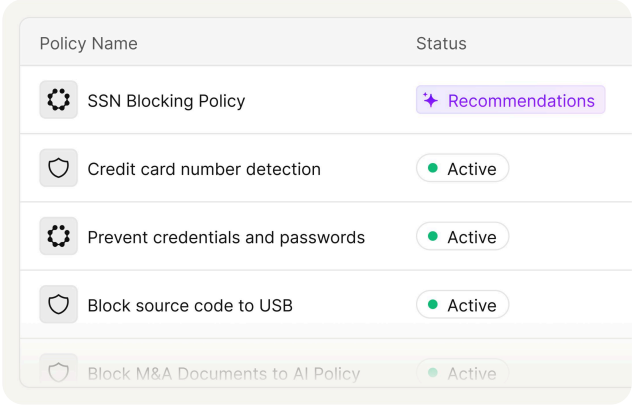
Cyera approaches insider risk by starting with the data: what it is, who can access it, and what activity is happening around it - so investigations are grounded in business impact, not just volume or isolated behaviors. Security teams can act on two fronts. The first is proactive: identifying repeat offenders or risky team patterns for targeted training. The second is urgent: triaging high-risk employees based on sensitive data access and recent activity, then investigating for common offboarding patterns like pre-exit data hoarding, exfiltration to personal email, and uploads to cloud storage.

- DSPM inventories data at rest and exposure, providing the sensitivity and business context needed to prioritize investigation.
- DSPM's Access Trail module provides a full activity record of what was accessed, when, and from where so you can reconstruct what happened.
- Omni DLP surfaces abnormal behaviors by correlating data movement with data sensitivity and identity context so you can focus on the riskiest users.



DLP Operationalization

DLP generates more alerts than teams can investigate and the policies driving them don't accurately reflect what's valuable to the business. Omni DLP is the missing intelligence layer that changes this: orchestrating alerts and policies across your stack, enriching every event with context, and connecting enforcement to what truly matters. When data starts moving, DSPM adds the blast radius perspective so every investigation reveals the full scope of what's at risk - not just what a rule matched. The result: less noise, fewer gaps, and analysts focused on high-impact incidents.

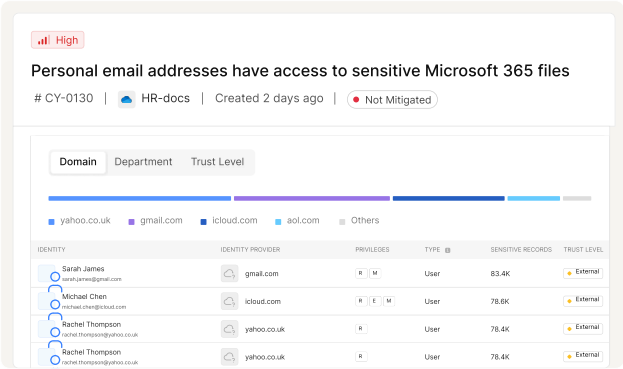


- Omni DLP turns DSPM's learned classifications into recommended policies so your crown-jewel data is covered - even when they can't be expressed with regex and keywords.
- Every DLP alert arrives enriched with the full story - who the user is, what data they can access, and what they did with it before the incident - so investigations start with context.
- Omni DLP highlights which policies are noisy vs. effective, so teams prioritize tuning that measurably improves risk reduction without more effort.

Purview Optimization

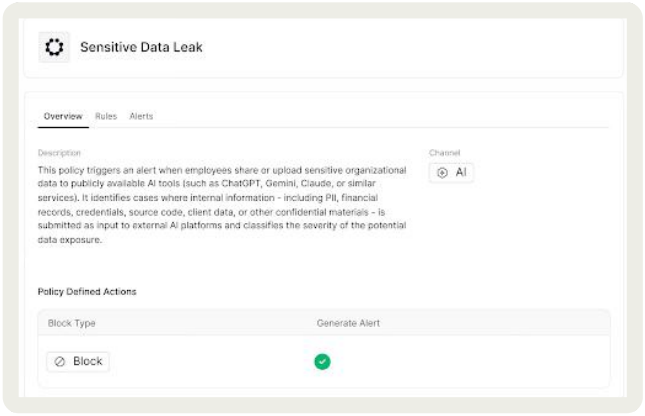
Cyera DSPM continuously classifies data in SharePoint and OneDrive, validates label accuracy, and corrects gaps at scale - so Purview DLP enforces on labels it can actually trust. Where labels can't apply or data moves outside the Microsoft estate, Omni DLP extends protection with label-independent detection and policy recommendations so coverage doesn't break. Teams lean on this for Copilot readiness, ensuring sensitive content is correctly labeled (and protected even when it can't be labeled) before Copilot inherits access and surfaces it broadly.

- Cyera DSPM detects missing, incorrect, and under-labeled files and remediates to the right MIP label - so labels become a dependable "source of truth," not a user-generated guess.
- Cyera Omni DLP protects sensitive data that labels can't cover (unlabelable file types) and controls exfiltration beyond M365 - so enforcement isn't blind when data leaves SharePoint/OneDrive or moves through non-Microsoft channels.



AI Data Readiness and Protection

Cyera governs AI at the data level: what sensitive data your AI tools can actually reach, which identities are driving that access, and what happens when it moves through them. DSPM has already mapped which sensitive data lives in the environments your AI tools access, and which human and machine identities connect to it. Omni DLP extends that foundation into runtime controls, intercepting prompts to analyze conversational context and intent before and after data is shared with enterprise AI applications - including ChatGPT, Claude, Gemini, and Microsoft 365 Copilot. Cyera Browser Shield adds coverage for browser-based AI applicaitons.



- Turn DSPM's AI asset inventory into active governance. The tools you've already mapped - and the identities accessing them - become the basis for runtime policy.
- Policies are tuned to user role and data sensitivity, not applied uniformly across all AI activity.
- Alert, notify, or block when prompts carry risky content - without restricting access to sanctioned AI tools for legitimate use.

For more information visit cyera.com or book a demo

Book a demo →