

Improve cyber resilience with DSPM

Cyera and Cohesity bring together DSPM and AI-powered data protection to eliminate blind spots, accelerate cyber recovery, and reduce risk

The challenge: Sensitive data silos and fragmented visibility

Organizations are sitting on massive volumes of data. While primary data gets much of the attention when it comes to protection and security measure, much of an organization's data estate is often invisible, under-protected and poorly governed. Specifically, backup datasets frequent contain sensitive information such as PII, intellectual property, and other business critical data. Many organizations can't see inside their backups to classify or govern sensitive content, creating a huge blind spot that increases risk and hampers cyber recovery. To make matters more challenging, traditional Data Security Posture Management (DSPM) tools lack the visibility over backup datasets, meaning that organizations are operating with blind spots in security, compliance, and recovery readiness.

The result?

- Undetected data residency violations.
- Compliance gaps.
- Sensitive data exposed at rest and during recovery.
- Slow, chaotic incident response during cyber events.

Solution: Cyera intelligence, embedded into the Cohesity platform

Cyera is a pioneer in DSPM, providing unmatched real-time visibility and AI-powered classification of sensitive data so organizations can confidently reduce risk with precision. Cohesity, in partnership with Cyera, embeds DSPM directly into backup operations, delivering a policy-driven, risk-aware, and cost-optimized approach to backup security and compliance. Together, Cohesity and Cyera give organizations the seamless integration to deliver a smarter, comprehensive approach to protecting your entire data estate and establishing a cyber resilience strategy.

Resilience = visibility + action

Building a cyber resiliency strategy starts with getting total visibility over your sensitive data. What sensitive data do you have? Where is it stored? Who has access to it? How is it being protected? It is important to have this visibility across not only your primary datasets but the mountains of secondary data in your backups and archives. The integration between Cyera and Cohesity allows organizations to get the rich insights and context about all your data directly in Cohesity's management console.

Key Benefits

- Identify protection gaps for critical workload
- Secure and compliant recovery of sensitive data
- Improve visibility into sensitive content across backups
- Reduce storage and compliance costs
- Accelerated cyber incident response

Objects	Protection Status	DSPM Tags	Security Violations
S3_Bucket-1	Unprotected	Financial • Credit Card Number 100	Credit card number in plain text Critical
S3_Bucket-2	Unprotected	Business & IP • Employee ID 2K • Stale	36% of records not accessed since last 3 years Medium
EC2_VM-Prod	Protected	Personal • German Driver's License 31	European personal data stored outside of EU High
OneDrive-Albert_Flores	Protected	Business & IP • Employee ID 2K	EU citizen data recovered outside of EU High
sharepoint-st1-Finance	Protected	Personal • Username 8 • Stale	Sensitive data accessible by inactive users Critical
sharepoint-st1-Prod	Unprotected	Financial • Credit Card Number 100 • Stale	20% of records not accessed since last 3 years Medium
RDS_DB	Unprotected	Personal • Username 5 • Password 5	Credentials in plain text Critical

Figure 1: Get rich insights and contexts about what sensitive data is present.

Uses cases powered by Cohesity + Cyera

1. Deep data discovery across backups

- Unified data intelligence from Cohesity and Cyera offers full visibility into data sensitivity, access patterns, ownership, and more.
- Cohesity correlates Cyera's DSPM insights to improve the security posture of your secondary data.

2. Accelerated incident response

- Correlate threat signals from both Cohesity and Cyera to enhance risk visibility.
- Enable rapid breach response with prioritized threat hunting and forensic analysis.
- Meet regulatory expectations (e.g., SEC disclosures) by quickly understanding the blast radius of an incident.

3. Compliant and secure recovery

- Prioritize recovery of critical and active workloads.
- Enforce compliance by avoiding unauthorized access or exposure of sensitive data during recovery.
- Flag compromised or infected files in your secondary datasets.

4. Risk identification

- Automatically detect unprotected sensitive assets.
- Close protection gaps with automated policy enforcement.
- Ensure backups are aligned with data compliance frameworks (e.g., GDPR, HIPAA).

5. Cost optimization

- Identify Redundant, Obsolete, or Trivial (ROT) and stale data.
- Automate tiering and deletion of ROT data once the data is securely protected by Cohesity.
- Reduce storage costs and risk by minimizing unnecessary exposure of ROT data.

How it works

Cyera continuously discovers, classifies, and contextualizes sensitive data, pinpointing unprotected or "shadow" data and categorizing it by residency, duplication and sensitivity. This intelligence seamlessly feeds into Cohesity Data Cloud, enabling users to automatically tag high-risk data across all their secondary datasets. This brings together visibility, risk reduction, and cyber-recovery readiness into alignment to empower your organization's cyber resilience.

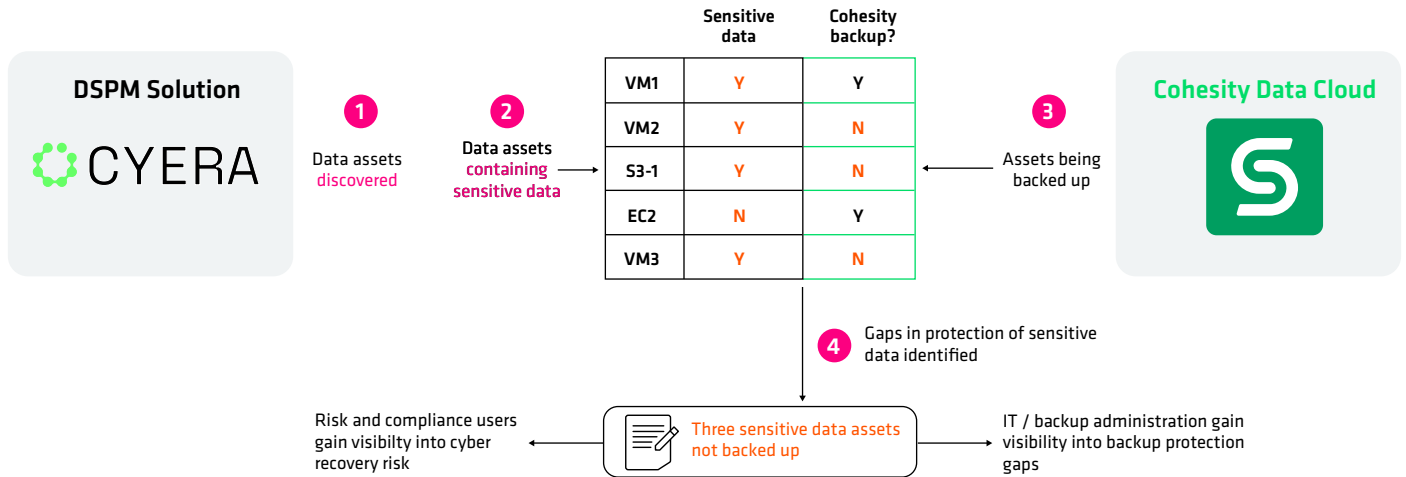


Figure 2: Cohesity and DSPM partners help customers prioritize critical workloads to protect and secure.

Strengthen your cyber resilience today

In today's hybrid, multi-cloud, and AI-driven enterprises, data sprawl is inevitable, but risk isn't. By integrating Cyera's DSPM capabilities with Cohesity's industry-

leading data protection platform, organizations can turn data silos into security-aware, compliance-ready assets without compromising performance, agility, or cost.

Learn more at <https://www.cohesity.com/partners/cyera/>

© 2025 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY

[cohesity.com](https://www.cohesity.com)

1-855-926-4374

2625 Augustine Drive, Santa Clara, CA 95054

3000060-003-EN 9-2025