COHESITY

Integrate Wiz DSPM with Cohesity Data Cloud

Version 1.1

August 2025

ABSTRACT

To ensure the security of your data, both in flight and at rest, Cohesity supports AES-256 software encryption using an internal Key Management Service (KMS) that automatically generates keys and stores them internally. However, by managing your encryption keys in a centrally managed external KMS like IBM Security Guardium Key Lifecycle Manager, you can significantly enhance security, streamline key management, and provide robust cryptographic capabilities and resilience against insider threats. This guide will walk you through the process of setting up IBM Security Guardium Key Lifecycle Manager 4.2.1 as your external KMS in Cohesity, which is compliant with KMIP 1.4.

Table of Contents

Figures

Introduction

Organizations face a significant challenge when it comes to the visibility of critical data across a growing multitude of repositories. Accelerating cloud adoption, compounded by an explosion of microservices and a high rate of change (driven by modern DevOps practices), puts customers at risk of significant data sprawl. Due to these visibility gaps, critical and sensitive data becomes hidden from IT teams and often goes unprotected.

According to a recent data breach survey, 82 percent of breaches involve data stored in cloud environments. The Cost of a Data Breach Report 2023 study found that the average cost of a data breach reached an all-time high of $4.45 million.

The need for DSPM capabilities and modern data security and management services has never been greater. DSPM gives customers a deep understanding of their sensitive data, who has access to it, how it is being used, and where it is stored. With Cohesity's modern data security and management technology, customers have a strong cyber resilience posture.

This guide explains how you can integrate the Wiz DSPM, a leading cloud security platform, with Cohesity Data Cloud to accelerate the protection of sensitive and vulnerable data assets and provides customers to prioritize protecting cloud workloads with critical risks, increasing their resilience in the face of potential attacks.

Wiz DSPM Overview

Data security posture management (DSPM) is designed to continuously monitor an organization's data security policies and procedures to detect vulnerabilities and potential risks.

According to Gartner, “Data security posture management (DSPM) provides visibility as to where sensitive data is, who has access to that data, how it has been used, and what the security posture of the data stored or application is.”

Wiz — a leading cloud security platform continuously analyzes configurations, vulnerabilities, sensitive data exposures, secrets, and more across workloads in the cloud to identify the critical issues that combine to represent the real risk. As an example, Wiz scans your cloud to identify all the workloads that exist and then scans these workloads to identify sensitive data like protected health information (PHI) that, combined with other risks like misconfigurations, puts customers at high risk of exfiltration and extortion. Wiz gets you ahead of data exposure with a comprehensive platform that dramatically reduces the time it takes to identify and fix data issues.

To learn more about Wiz Data protection capabilities, refer to Wiz.com.

Cohesity Data Cloud Overview

Cohesity Data Cloud is a unified platform for securing, managing, and extracting value from your data, that reduces your attack surface, lowers costs, and minimizes risk. Cohesity Data Cloud is available as self-managed software and SaaS with rich features, including.

- **Modern Backup and Recovery**—The most comprehensive, modern, web-scale data management and backup and recovery solution to protect cloud-native, SaaS, and on-prem data at scale. You get instant recovery at scale and with direct metadata snapshots (so that each backup performs like a synthetic full), the ability to instantly put backed-up file shares online, and continuous data protection (CDP).
- **Traditional and Modern Workloads**—Support for VMs, databases, files, containers, cloud-native, SaaS, Storage, and traditional workloads.
- **Defend Against Ransomware Attacks**—Multilayered security architecture with Zero Trust Security, including granular RBAC, MFA, SSO, immutable snapshots, and ML-based ransomware attack detection. Protect and recover against ransomware with threat protection, cyber vaulting, and ML-powered data classification.
- **Threat Protection and Data Classification**—Highly curated and managed threat feeds, trained with ML, threat detection and response to your specific needs by augmenting the extensive library of over 117,000 behavioral patterns, create multiple YARA rules defining Indicators of Compromise (IOC), or import custom rules. Highly accurate NLP and ML-based engine classify sensitive data, automatically or on-demand, including personally identifiable information (PII), PCI, and HIPAA.
- **Global Search and Unified Management**—Reduce recovery point objectives to minutes by eliminating slow-to-access, chain-based backups. A single management platform offering multilayered security architecture, unifying operations with integrated solutions for backup, CDP, DR, search, ransomware attack detection, and vulnerability scanning into a single scalable environment.
- **Cloud Vault**—Cohesity FortKnox is a SaaS cyber vaulting and recovery solution that gives your data additional layers of managed security and protection against cybersecurity threats. To learn more, refer to Cohesity product documentation.
- **Cloud Archive**—Policy-based data archival to meet long-term data retention, compliance, and regulatory requirements.
- **Cohesity Cloud Services**—Cohesity-managed data security and management with SaaS that runs multiple cloud data services, including backup, cyber vaulting, threat defense, data classification, DR, and more on a single multi-cloud platform.
- **Cohesity Gaia**—combines generative AI with your enterprise data. Unlock data insights by bringing retrieval augmented generation (RAG) AI and large language models (LLMs) to enterprise data within Cohesity. Ask natural language questions and get context-rich answers.
- **Business Continuity**—Simplify business continuity and disaster recovery with automated failover and failback orchestration for your mission-critical workloads. Get your critical applications online after a breach or outage through automated orchestration.
- **Security Integrations**—Cohesity integrates with leading perimeter and end-point security vendors, giving you greater visibility and actionable alerts in your Security Operations Center (SOC).

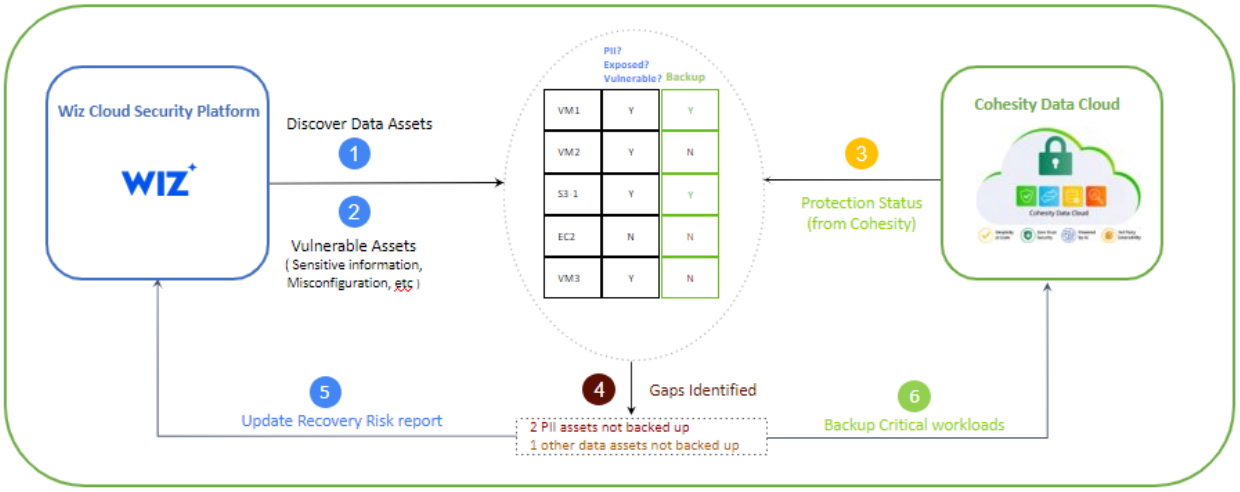
- **Deployment**—Software-defined solution for on-premises, public cloud, backup as a service, and edge sites.
- **API-first Extensibility**—Derive business insights with the Cohesity Marketplace partner ecosystem. Streamline operations and easily integrate on-prem and cloud environments with pre-built automated workflows and API integrations.

To learn more about how Cohesity provides **AI-powered data security and management**, refer to Cohesity.com.

Cohesity Wiz DSPM Integration Overview

Cohesity's integration with Wiz is bidirectional and comprehensive. It involves the ingestion of Wiz's findings, encompassing data sensitivity, security exposures like toxic combinations and cloud misconfigurations, and detected threats. These insights are presented through tags, allowing users to review them alongside the current protection status of each data object on the **Sensitive Data Posture page** within the **Security Center**. Moreover, Cohesity enriches Wiz with metadata about assets not protected by Cohesity and utilizes the Wiz Security Graph. This bidirectional integration empowers users to generate reports and execute queries for spanning all their cloud accounts within Wiz, enhancing the overall security and management capabilities. It helps inform data protection priorities and expedite action so customers can recover critical workloads when needed.

Figure 1: Cohesity-Wiz DSPM Integration



Integration Benefits

Wiz DSPM integration with Cohesity Data Cloud enables organizations to accelerate the protection of sensitive and vulnerable data assets. By integrating Cohesity with Wiz DSPM, customers can achieve below benefits:

- **Discover sensitive data across cloud assets:** Gain visibility into your cloud workloads with sensitive data correlated with an exposure path that attackers can exploit.
- **Identify data protection gaps:** Identify gaps in safeguarding your cloud workloads. Recognizing these gaps informs data protection priorities, ensuring that you can efficiently recover essential workloads when needed.
- **Report on cyber recovery risk:** By combining the capabilities of DSPM solutions with Cohesity, you can augment your assessment of data security posture with your ability to recover. This results in a more comprehensive understanding of cybersecurity risks and, as a result, more robust protection.

Prerequisites & Considerations

You have to meet the following prerequisites before starting the integration.

- Gather the details from your Wiz accounts team.
  - Client ID
  - Client Secret
  - Token URL
  - API Endpoint URL
- License entitlement to DataProtect is required. License for Cohesity Data Hawk is optional and enables additional sensitive data visibility.
- Register your cloud account as a source on Cohesity DataProtect as a Service.

Understand the following **considerations** before you integrate Wiz with Cohesity Data Cloud—

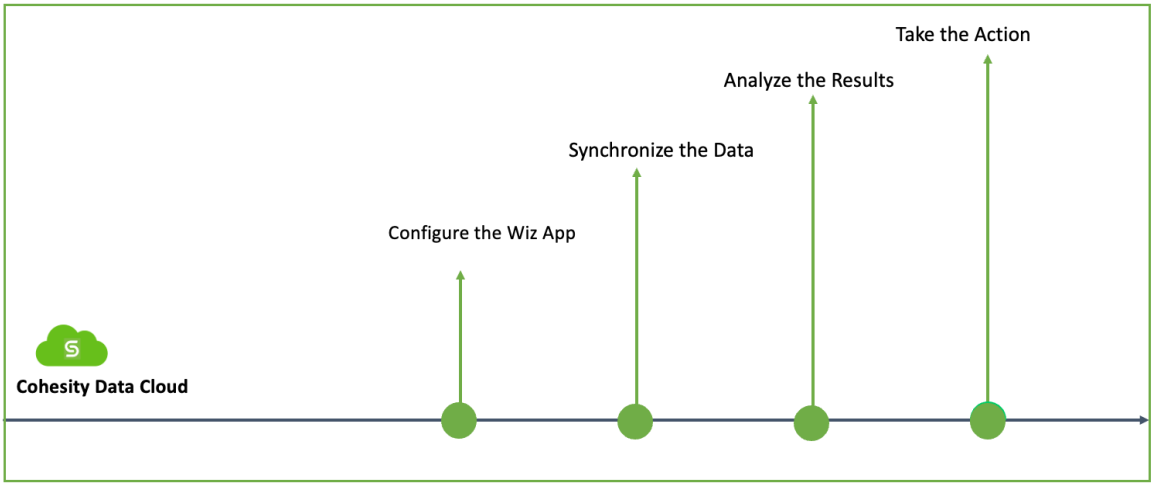
- Supported workloads are AWS RDS objects.
- Register the workload on the Wiz DSPM.

Configure the Wiz DSPM Integration

You can now integrate Security Center with the Wiz DSPM platform from the Cohesity Marketplace. The integration enables you to automatically identify any gaps in the protection of sensitive cloud data within accounts that Cohesity can see, assets at risk based on sensitive data classification, and exposure attack path from Wiz. It helps to prioritize data protection and enables quick action to recover important workloads as needed.

To integrate with **Cohesity Data Cloud with Wiz DSPM**, perform the following steps:

Figure 2: Configuration Workflow



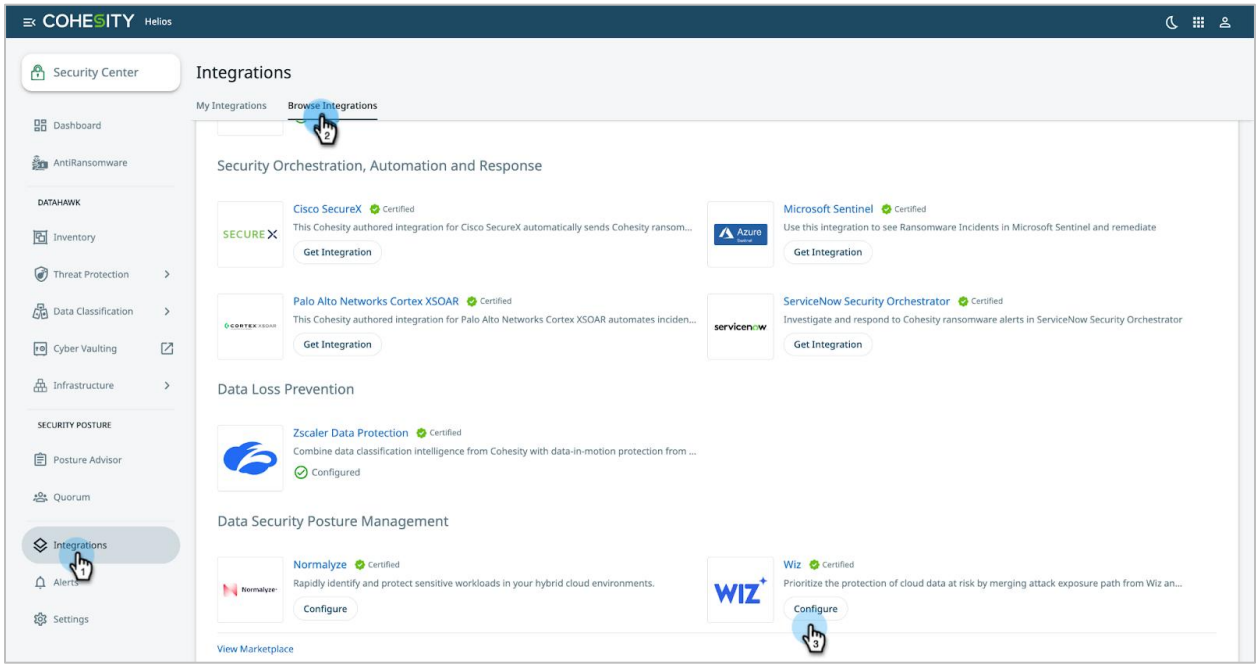
NOTE: Refer to the Prerequisites before you start the configuration.

Configure the WIZ Integration App

Cohesity has developed an integration app that allows users to browse directly from the Cohesity Security Center.

To integrate Cohesity Data Cloud with Wiz DSPM:

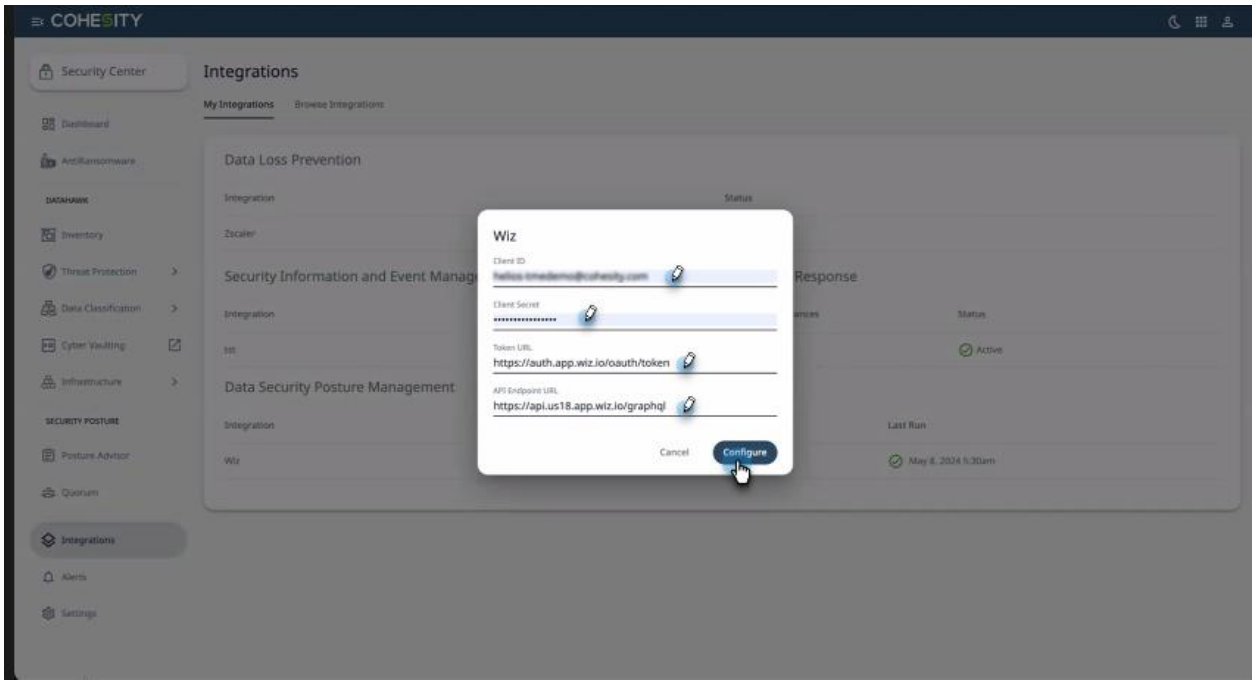
1. Login to the **Cohesity Data Cloud.**
2. From the **Security Center**, select **Integrations**>**Browse Integrations**.



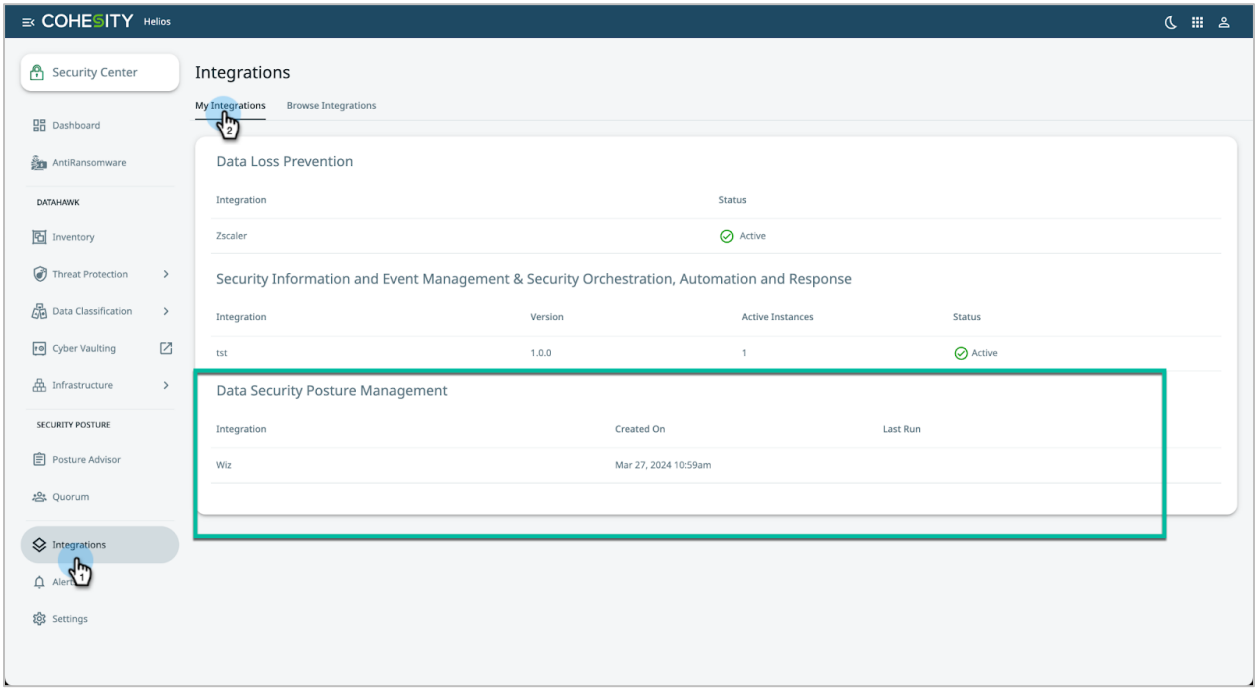
3. Under the **Data Security Posture Management** section, click **Configure** under the listed **Wiz** application.

4. On the **Wiz** dialog, enter the following details that you had obtained for your Wiz account team and click **Configure.**

   a. Client ID
   b. Client Secret
   c. Token URL
   d. API Endpoint URL



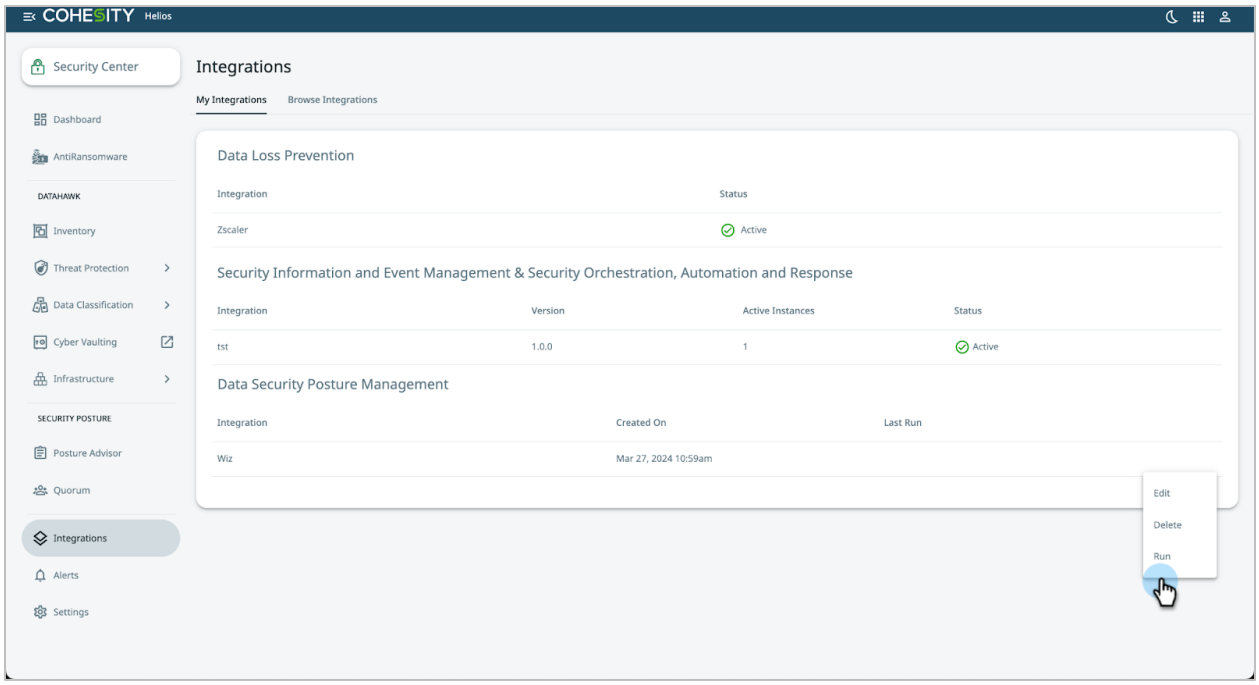
5. The integration between Wiz and Cohesity is successful.



Synchronize the Data

After the integration, you can manually initiate a sync operation, and the DSPM tag is shown with tags from Wiz. By default, the sync occurs at UTC +00:00 hr daily.

After syncing the data from Wiz, Cohesity ingests the Wiz findings on cloud workloads in the form of DSPM Tags, which indicate data sensitivity and contextual information like security risks such as cloud misconfiguration and detected threats. To fetch the latest data from Wiz, click the actions menu (:) next to the **Wiz** app and select **Run**.



Analyze the Results

Wiz reports cloud workloads with sensitive data (PII data) along with contextual risk information like the toxic combination, vulnerability threat detection, and cloud misconfiguration. Cohesity ingests the Wiz findings on cloud workloads in the form of DSPM tags, and Cohesity pushes the workload protection status to Wiz Dashboard.

You can view this data on the **Data Classification** > **Sensitive Data Posture** page in the **Security Center**. Using these details, you can protect the workloads with sensitive data using Cohesity DataProtect.

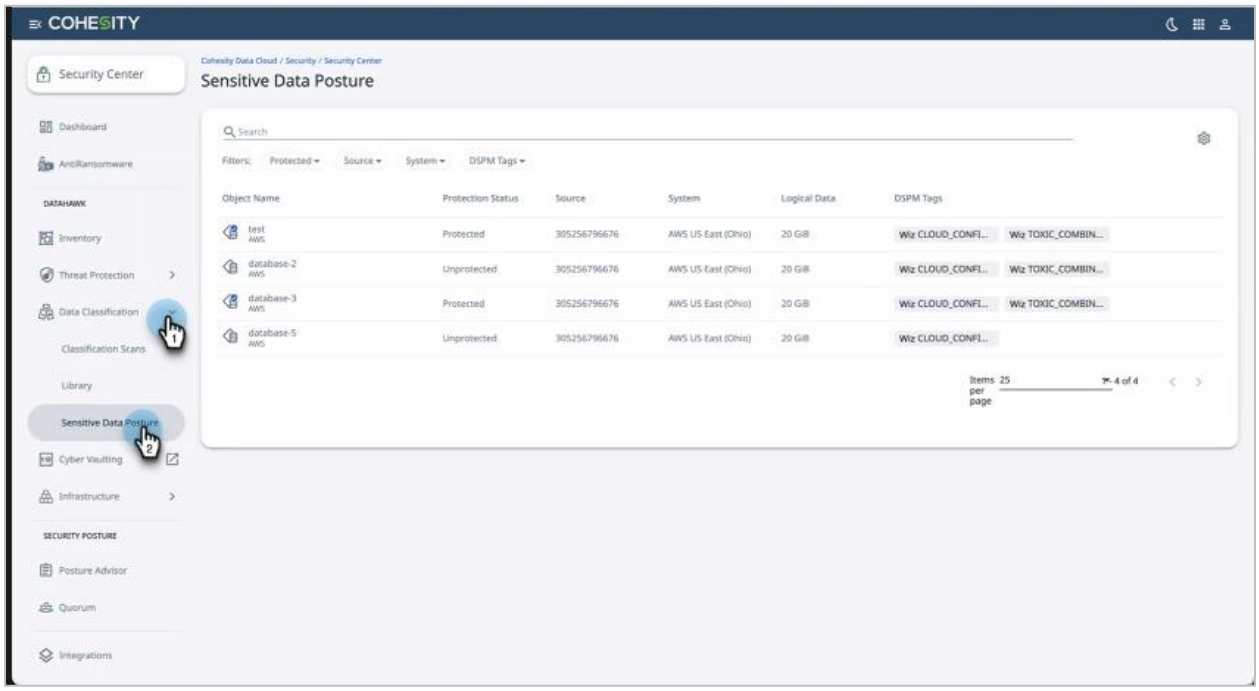
The **Sensitive Data Posture** page shows only the objects registered on Cohesity DataProtect that have Wiz DSPM tags.

The following table describes the data displayed in the **Sensitive Data Posture** page:

- **Object Name**-The cloud data asset discovered by Wiz that contains sensitive data or security vulnerabilities.
- **Protection Status**- The protection status of the object.
- **Source**-The source of the object.

- **System**-The system on which the source is hosted.
- **Logical Data-** The combined total of data in the protected or unprotected objects.
- **DSPM Tags**- The tags applied by Wiz on the object. Refer to Appendix A for a description of each tag mapped to the issue type.

NOTE: The custom tags pushed from Cohesity to Wiz can take up to 24 hours to process, as Wiz runs a scan every 24 hours.



Take the Action

Once you analyze protection gaps for workloads, especially those that contain sensitive data, ensure you regularly backup critical workloads to avoid the risks and help organizations protect critical workloads more quickly. To protect and back up the sensitive workload, add a workload to the Protection Group and select the appropriate protection policy.

To add or edit a Protection Group for supported workloads (Amazon RDS), refer to Protect Your Amazon RDS Instances.

Conclusion

Cyber resiliency is all about minimizing the disruption to an organization's business processes and minimizing data loss during a cyberattack. The integration with Wiz further strengthens our offering, providing enhanced visibility into your critical and vulnerable data and increased flexibility in maintaining your cyber recovery capabilities.

Appendix A: Supported Wiz DSPM Tags

You can configure the Wiz DSPM platform with different types of policies (rules) that generate issues (findings) when there is a violation. Based on the issue types, they can be categorized as **DSPM Tags** in the **Cohesity Security Centre** dashboard.

DSPM Tag	Wiz Rule Violation	Description
Toxic Combination	Control Rules Violation	Wiz comes with hundreds of built-in Controls rule, each of which combines a Security Graph query defining a risk (e.g., "publicly exposed VM with effective global permissions") with a severity level (Critical, High, Medium, Low, or Info). *Publicly exposed, highly privileged, serverless can be invoked by unauthenticated users.* *Admin service account can be assumed by an internal vulnerable unprivileged VM instance.* *Critical/High severity vulnerability detected on an internal VM instance.* When an issue is generated by the above Controls, we show this tag in our UI.
Threat Detection	Threat Detection Rule Violation	Wiz comes with a set of out-of-the-box Threat Detection Rules, each of which detects potential threats in your environment. Threat Detection Rules are assessed in near real-time and are based on Cloud Events and the Runtime Sensor. These rules correlate all events collected by Wiz, e.g., cloud audit logs, CSP detection tools, Runtime Sensor, Admission Controller, and more. Cloud Rules—Cloud Rules monitor events in a cloud environment to detect threats, unexpected events, unauthorized access, or risky configuration changes in near real-time. Runtime Sensor—The Wiz Runtime Sensor is an optional cloud-native detection and response eBPF-based executable designed to offer real-time visibility into cloud and Kubernetes workloads.
Cloud Configuration	Cloud Configuration Rule Violation	A Cloud Configuration Rule is a configuration check that applies to a specific cloud resource type—if a resource does not pass a Rule, a Configuration Finding is generated and associated with the resource on the Security Graph.

Appendix B: Glossary

Terms	Description
DSPM	Data security posture management (DSPM) is designed to continuously monitor an organization's data security policies and procedures to detect vulnerabilities and potential risks. According to Gartner, “Data security posture management (DSPM) provides visibility as to where sensitive data is, who has access to that data, how it has been used, and what the security posture of the data stored or application is.”
MITRE ATT&CK	A globally accessible knowledge base of adversary tactics and techniques based on real-world observations and a foundation for developing specific threat models and methodologies
MTTD	Mean Time To Detect **(MTTD)** measures the average time it takes to detect an incident or disruption.
MTTR	Mean Time To Recover **(MTTR)** measures the average time it takes to respond to and resolve an incident or disruption.
RPO	Recovery Point Objective **(RPO)** is the maximum acceptable amount of data loss an organization can tolerate before harming the business. RPO is calculated in the time between the downtime event and the last backup.
RTO	Recovery Time Objective (**RTO**) is the maximum acceptable amount of time that can pass before an organization restores functionality to an application, service, data, or other digital asset inaccessible due to an outage or data loss incident.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Security Center of Excellence Team – Focuses on Cohesity Security solutions and integrations.

Other essential contributors included:

- Surya Swaminathan, Principal Solutions Architect
- Rob Young, Product Manager, Competitive Intelligence
- Kamal Deka, Senior Product Manager
- Sheetal Venkatesh, Product Management
- Karthick Radhakrishnan, Director, Solutions Architecture
- Subash Babu, Staff Technology Editor

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.1	Aug 2025	Republished with latest template
1.0	May 2024	First release

ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 42 of the Fortune 100.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.