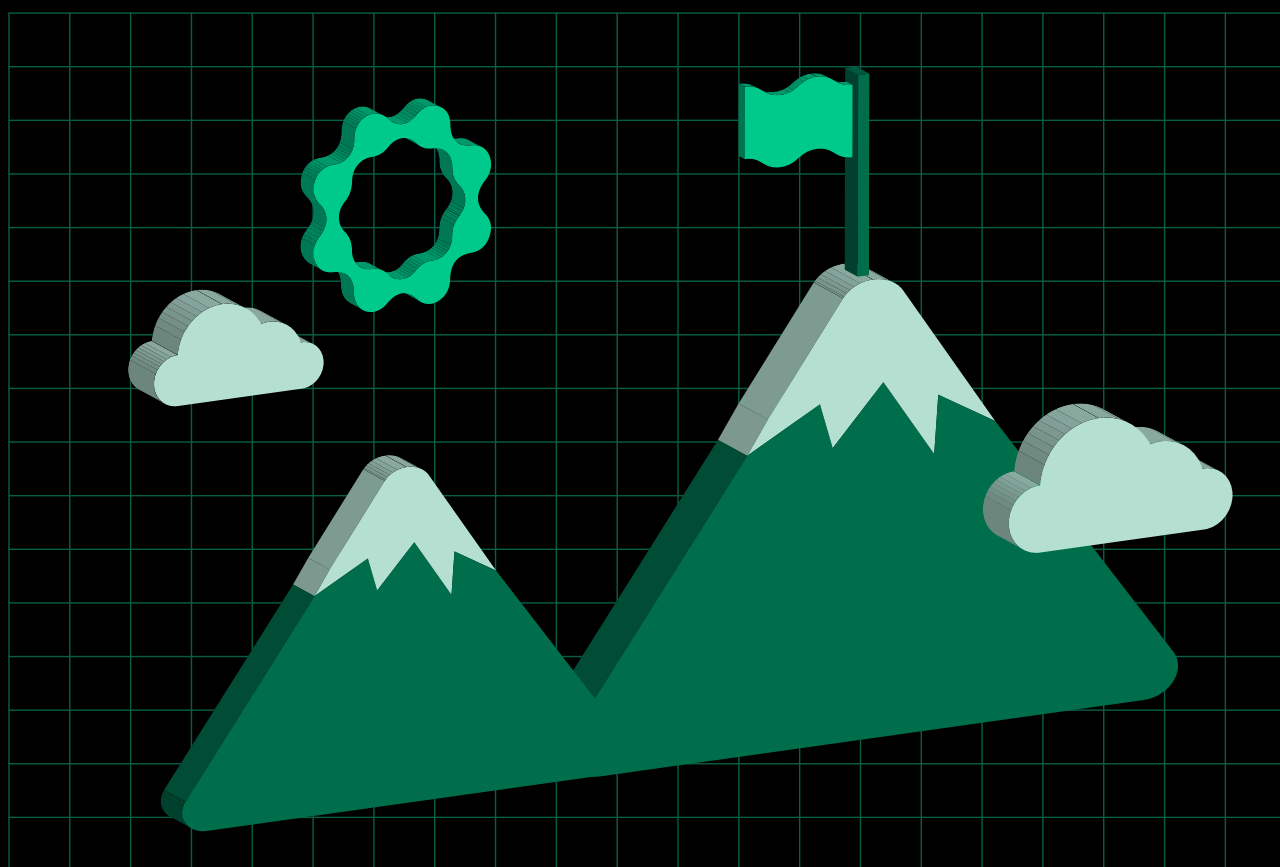# 5 Cloud Data Security Challenges And How Teams Eliminate Them with Cyera

# 5 Cloud Data Security Challenges And How Teams Eliminate Them with Cyera

Cloud adoption shows no signs or slowing or stopping, largely due to the immense benefits organizations gain by moving to the cloud. On average, organizations stand to save 15-40% on infrastructure costs by migrating to the cloud, according to recent reports.

But alongside these benefits come new challenges. Data sprawl, ghost data, and a larger attack surface become powerful obstacles when securing a cloud environment, and solving these challenges is an essential priority for any team with cloud infrastructure.

Multiple solution categories for cloud security exist, but there is an all-inclusive solution: **Data Security Posture Management (DSPM).**

As a new innovation in data security, DSPM solutions are purpose-built to help you understand the data you manage, and what's at risk. Cyera helps you protect yourself from breaches and data leaks, detect threats and respond to attacks faster, prioritize remediation efforts based on business risk, and increase your team's productivity by simplifying time consuming tasks like incident response triage and compliance and privacy audits.

Cyera takes a cloud-native approach to protecting data. Our DSPM solution is agentless, dynamically discovers all of your data stores, and uses intelligent automation to accurately classify and add context to your sensitive data. Backed by Sequoia, Accel, and others, and trusted by brands like Takeda, Cboe, and LifeLabs, Cyera is solving data security challenges and empowering security teams to partner with the business in order to leverage data, securely. Here's how.

# Complete Data Protection
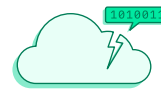# in a Unified Cloud-Native Platform

With Cyera, security teams can consolidate multiple siloed and limited solutions into a data security platform that encompasses:
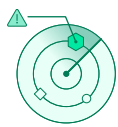


**1** Sensitive data discovery and classification
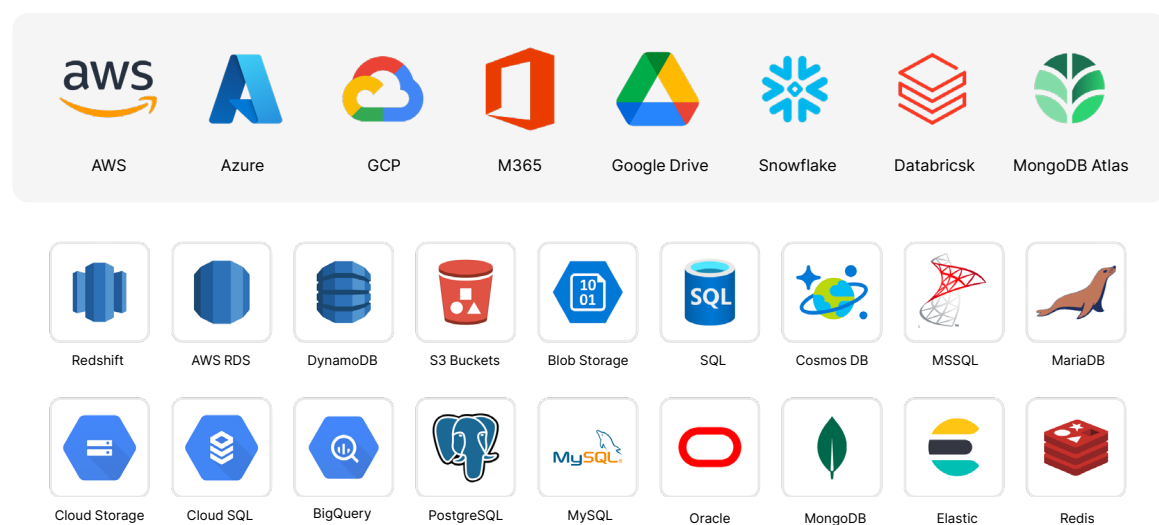


**2** Data security posture management



**3** Cloud Data Loss Prevention

**Cyera is the only DSPM solution on the market that includes all of these capabilities and more.**

Cyera empowers security teams with the ability to discover, understand, and protect cloud data without the complexity, cost, or operational overhead of legacy data protection solutions.

Our agentless technology dynamically discovers all structured and unstructured data across IaaS, PaaS, and SaaS data stores including:

| AWS | Azure | GCP | M365 | Google Drive | Snowflake | Databricsk | MongoDB Atlas |

| Redshift | AWS RDS | DynamoDB | S3 Buckets | Blob Storage | SQL | Cosmos DB | MSSQL | MariaDB |

| Cloud Storage | Cloud SQL | BigQuery | PostgreSQL | MySQL | Oracle | MongoDB | Elastic | Redis |

**1**

## CHALLENGE

**Discover and Classify Sensitive Data**

## SOLUTION

Cyera's DSPM solution starts by dynamically discovering where sensitive data lives, and the value it represents by:

- **Identifying sensitive data and where it resides.** Cyera automatically identifies data stores that contain sensitive data, both structured and unstructured, and continuously scans your environments to detect changes to your data store inventory.

- **Classifying sensitive data to determine how to handle it.** Cyera's powerful ML and NLP algorithms parse structured and unstructured data, looking for sensitive data. The platform then applies labels to categorize the data to enable data loss prevention and protection.

- **Providing critical context on the company's unique data.** Sensitive data like credit card numbers or account numbers is easy to detect and classify. However sensitive customer, employee, or corporate data isn't always obvious to machines. Cyera's advanced classification engine gives data an identity. This enables people, processes, and technology to make decisions about how to handle a piece of data appropriately.

- **Building a foundation for data protection.** Cyera enables security teams to reduce the attack surface, maintain operational resilience and preparedness, and optimize costs by defining data protection controls - taking into account security, privacy, and other regulatory frameworks, data backup and management policies, and the environments where data can exist based on its sensitivity and value to the business.DSS, GLBA, HITECH, NIST, SOX, and more
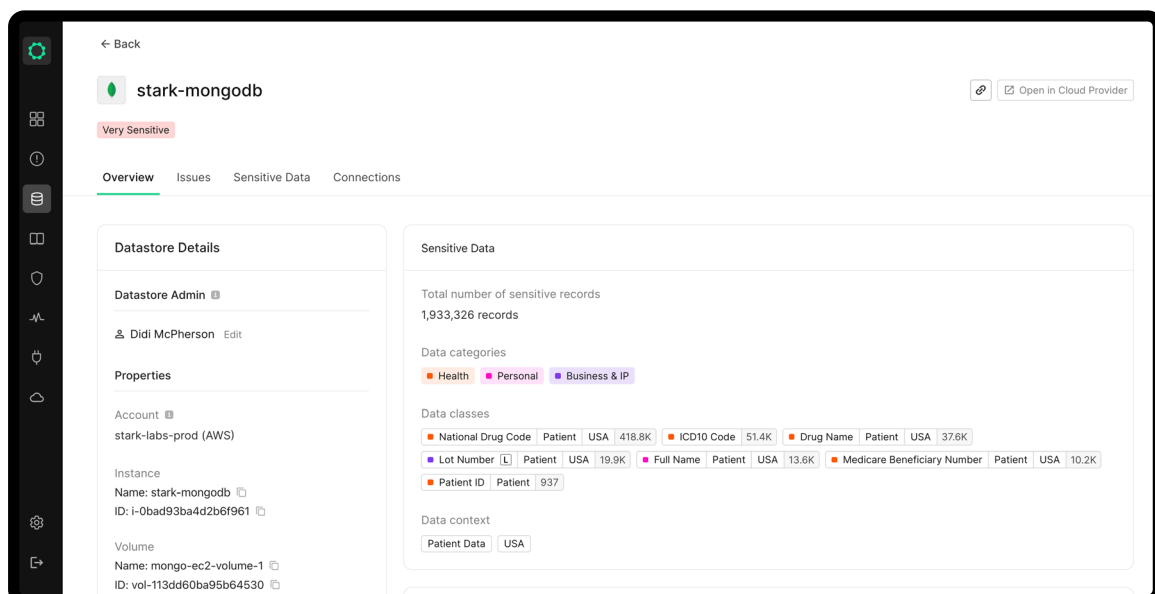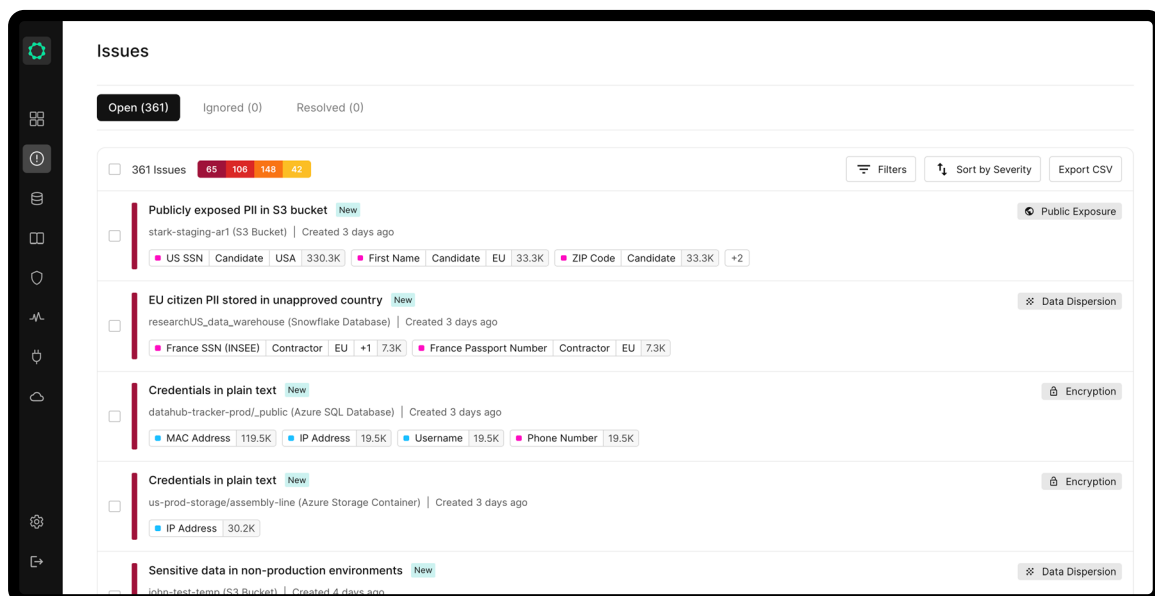
**CHALLENGE**

## Reduce the Attack Surface

**SOLUTION**

Cyera's DSPM solution highlights data protection issues, and prioritizes the appropriate actions to establish and maintain a strong data security posture by:

- **Maintaining a comprehensive cloud-sensitive data inventory:** Cyera creates a dynamic cloud data inventory, with data risk assessments that empower security teams to work with business stakeholders to drive awareness and action.

- **Evaluating sensitive structured and unstructured data posture across IaaS, PaaS, and SaaS:** Cyera automatically identifies sensitive data security issues based on the environment, identities and access to the data.

- **Contextualizing risk relative to security, privacy, and other regulatory frameworks:** Cyera's unified policy engine evaluates data security posture challenges based on established frameworks including GDPR, CCPA, HIPAA, PCI DSS, GLBA, HITECH, NIST, SOX, and more

- **Prioritizing the most pressing secure data exposures:** Cyera's policy engine scores risk and prioritizes alerts to pragmatically identify the issues that have the largest impact on your organization.

3

**Ensure Real-Time Detection and Response**

Cyera's DSPM solution contextualizes the risk of sensitive data exposure to accelerate responses to security issues by:

- **Integrating response guidance and workflows.** Cyera supports prevention, detection and response and streamlines operations by making it easier to understand risk and the appropriate action to take.

- **Highlight required, relevant data for accurate and more rapid alert triage.** Cyera's advanced analytics correlate data context into prioritized alerts based on established security and risk frameworks. The result is faster, more accurate responses.

- **Provide integrated response options.** Cyera helps security teams resolve alerts quickly with integrated configuration recommendations and guided and best practices to drive swift action. Integrations also bring much needed data context to your SIEM or SOAR solutions to improve your overall security posture.

**4**
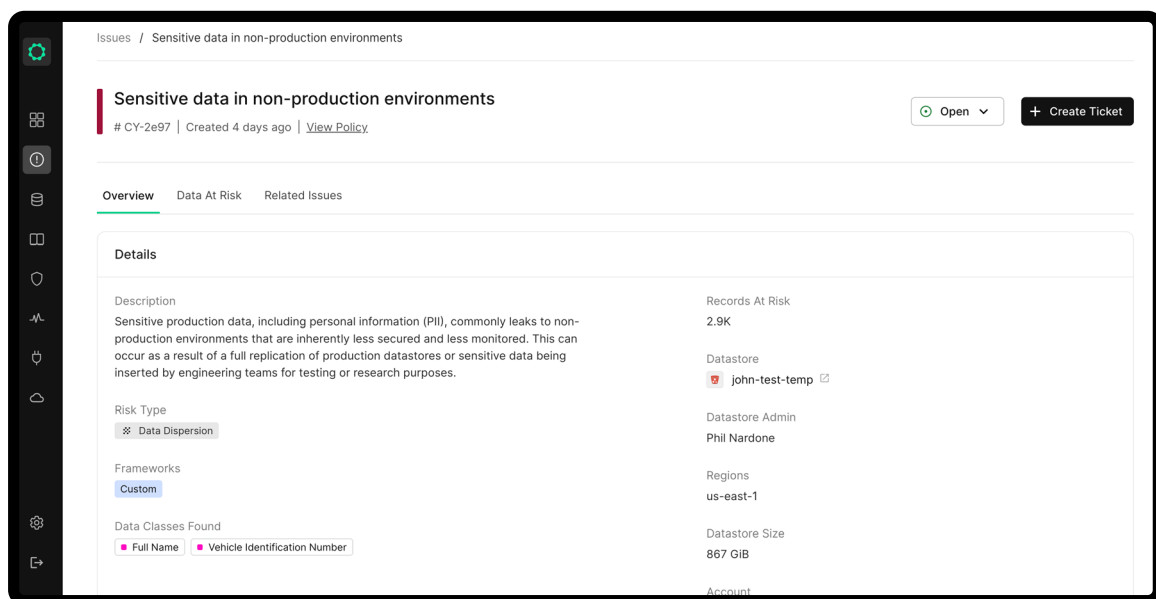
## Automate Risk Remediation Workflows

**SOLUTION**

Cyera's DSPM solution provides actionable guidance, with toolchain integrations that allow security teams to automate remediate workflows:

- **Track risks, and partner with the business to facilitate regulatory compliance.** Powerful, actionable alerts include context on why data is at risk, and the steps security teams can take to enforce security controls and response decisions.

- **Accelerate security exposure remediation.** Cyera's automated risk assessments enable security teams to respond faster, shortening response times with built-in remediation guidance.

- **Automate remediation workflows with toolchain integrations.** Reduce the total cost of managing security exposure, and improve your security teams' efficiency, with powerful integrations into common security tools. Cyera reduces the training and skills needed to complete operations, enabling teams to orchestrate and automate repetitive tasks.
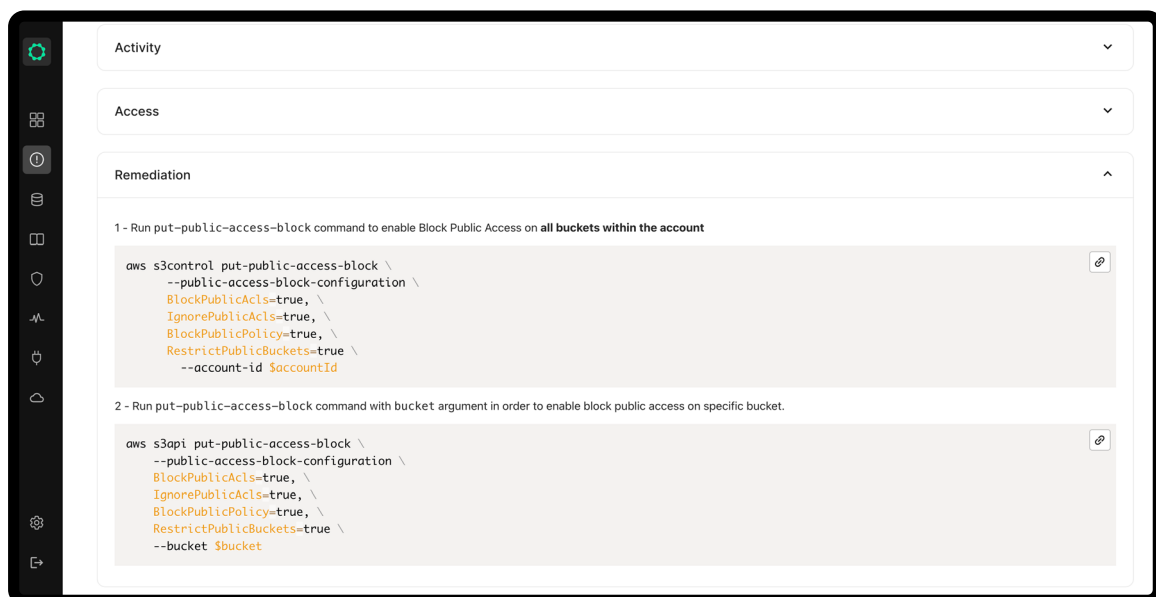
**CHALLENGE**

## Maintain Operational Resilience and Preparedness

**SOLUTION**

Cyera's DSPM solution empowers security teams to act as an ally, and an extension of the business:

- **Build strong policies:** Nobody can predict future threats, but Cyera helps security teams prepare for the future by focusing on reducing the impact of inevitable exposures by building strong data security policies and enabling distributed data protection decision making.

- **Maintain a resilient posture:** Cyera provides proactive monitoring, continuous data risk assessments, and integrated issue responses, including the ability to quickly provide critical sensitive data context to security operations teams during a zero day exposure or attack.

- **Implement adaptable controls:** Business transformation and organizational changes are frequent causes of expanded attack surfaces and necessitate new or improved security controls. Cyera helps you prepare for the unexpected by improving your awareness of where data is created, changed, or when new process or application changes expose you to new risks.
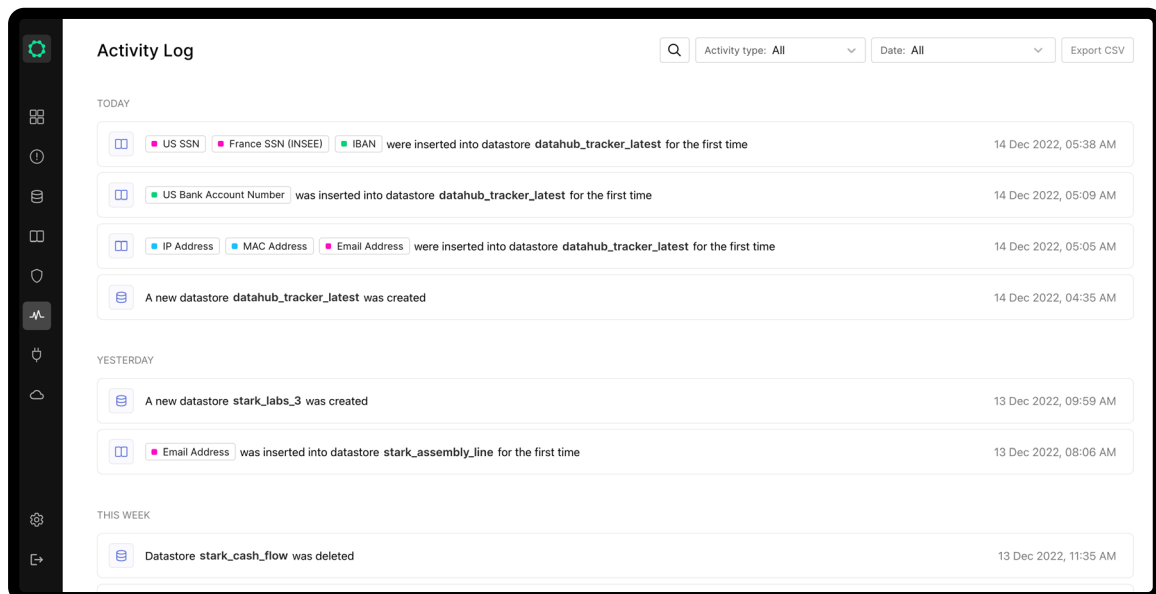
# Improve your cloud data security posture with Cyera

**Cyera is building the next generation of data security.** Our data security platform empowers teams across the business to collaborate and share data effectively, highlighting data security, privacy, and governance challenges in context, with actionable guidance to remediate issues fast. With Cyera, security teams will benefit from a complete understanding of their data, identities and access to improve their security posture, with powerful data discovery and classification, data loss prevention, and data access governance solutions together in a single platform.

## About Cyera

Cyera is the cloud data security and privacy company that gives businesses context and control over their cloud data. The company's mission is to empower its customers to enable innovation, securely. As the industry's most advanced cloud data protection platform, Cyera instantly provides companies a strong baseline for all security, risk management, privacy, and compliance efforts and ensures the entire organization operates with the same policies and guardrails. Backed by leading investors including Sequoia, Accel, and Cyberstarts, Cyera is defining the way companies do cloud data security. To learn more, visit www.cyera.io.