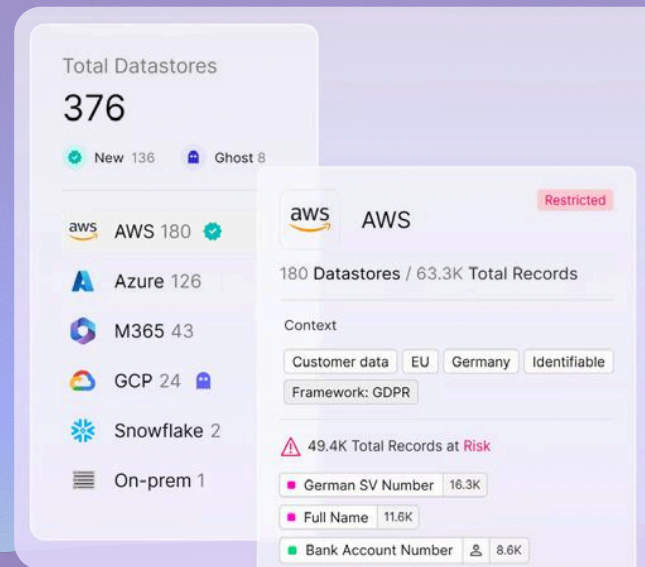


Enhancing Cloud Data Security with Cyera's DSPM and AWS Integration



As cloud adoption accelerates across industries, so does the complexity of securing sensitive data.

Enterprises are moving critical workloads to AWS for scalability and agility, but they often lack adequate visibility into where their data resides, who has access to it, and how it's protected. This blind spot exposes organizations to serious risks, including data breaches, regulatory violations, and unintentional exposure to generative AI models like Amazon Bedrock or Amazon Q.

To address these concerns, a new category of data-centric protection has emerged: Data Security Posture Management (DSPM). DSPM enables organizations to continuously monitor, assess, and improve how sensitive data is stored, accessed, and governed across cloud environments.

Leading this transformation is Cyera, an AI-Native Data Security Platform, supported by the AWS Global Startup Program, that integrates DSPM with advanced automation and deep connectivity to AWS.

Key Challenges in Cloud Data Security



Fragmented Data Visibility

Modern cloud environments are dynamic. New AWS services, ephemeral workloads, and data replication across regions and environments make it nearly impossible to maintain an accurate updated inventory of sensitive data. Traditional discovery tools are manual, siloed, slow, and lack precise classification and scale, leaving organizations blind to risks in production systems.



Complex Access Management

Managing permissions in AWS can be challenging. IAM roles, identity-based and resource-based policies, and service-linked roles often result in excessive access permissions, especially in complex, multi-account environments. Without unified visibility into these controls, organizations struggle to enforce least-privilege access, increasing the risk of unauthorized data exposure.



Gaps in Security Assurance

Cloud misconfigurations continue to be a leading cause of data breaches. Although AWS offers robust native security services, many organizations face challenges in identifying and correlating risk signals and enforcing consistent policies. As data moves through services like Amazon S3, Redshift, or Bedrock, it becomes increasingly difficult to maintain continuous security and compliance.

Traditional discovery tools are manual, siloed, slow, and lack precise classification and scale, leaving organizations blind to risks in production systems

Cyera's DSPM Solution

Cyera platform addresses these concerns by delivering an end-to-end, AI-native solution that unifies visibility, access intelligence, and monitoring across cloud and on-prem environments.

Automated Data Discovery and Classification

Cyera uses agentless integrations to continuously and rapidly scan cloud-native services and infrastructure. Unlike traditional scanning tools, there's no setup delay or periodic limitation — classification is real-time and scalable. Importantly, customers don't need to define rules or what to look for. Cyera's AI-native platform autonomously learns from your environment, discovers new and sensitive data, and presents results as learned data types — eliminating manual configuration and streamlining classification workflows.

With this dynamic data inventory, security teams can immediately understand where their most sensitive data is stored, how it's being used, and whether it's exposed or at risk.

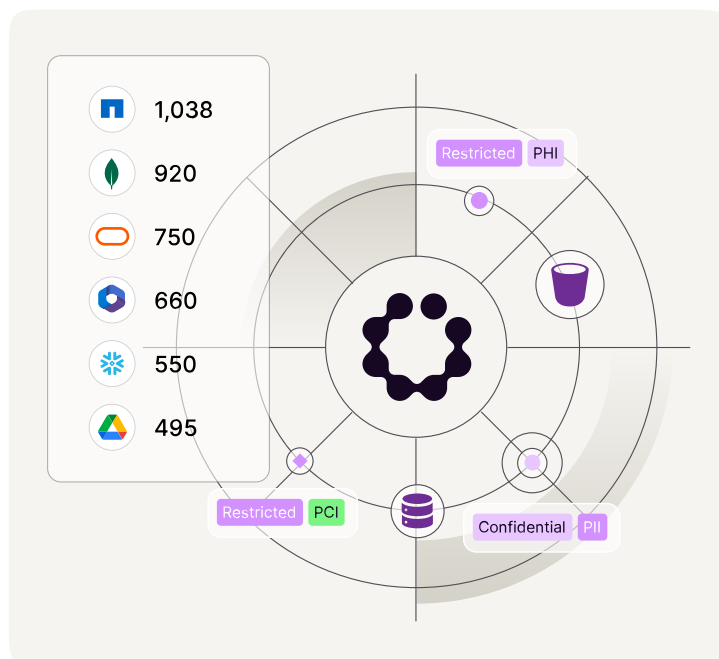


Access Mapping and Risk Identification

Cyera integrates identity and access telemetry to map which human and machine identities have access to what data. It flags excessive or high-risk permissions and correlates them to both human users and non-human identities, such as applications or services. Risk prioritization is contextual, highlighting data that is exposed to the internet, unencrypted, or accessible by third-party vendors or generative AI services.

Automated Remediation and Continuous Monitoring

Cyera stands out from traditional tools by generating alerts and providing automated, policy-driven solutions to address misconfigurations. Whether applying encryption to unprotected S3 buckets or revoking unused access, Cyera enables teams to resolve issues quickly before they escalate into incidents. It continually analyzes your data's compliance posture, ensuring findings align with important standards such as SOC 2, HIPAA, GDPR, and PCI DSS.



Security teams can immediately understand where their most sensitive data is stored, how it's being used, and whether it's exposed or at risk



Seamless Integration with AWS

Cyera's native integration with AWS services enhances the platform's ability to secure data without slowing down development or operations.

AWS Security Hub

Enriches Security Hub findings with data classification insights and consolidates Cyera DSPM insights into a centralized console for security operations

AWS IAM

Provides comprehensive access pattern analysis, enabling organizations to adopt and maintain a least-privilege access model, especially for sensitive data

Cyera for Amazon Bedrock

Identifies the Amazon Bedrock identities accessing sensitive data, empowering customers to make informed decisions about data access for Bedrock applications

This deep integration enables Cyera's DSPM intelligence to complement existing AWS security infrastructure and tooling — allowing for scalable enforcement and enterprise-grade observability.

Cloud security starts with knowing your data. Cyera provides a single, AI-native platform to continuously discover, classify, and protect sensitive data across AWS and beyond. Cyera is DSPM by design, not an add-on. Its native architecture delivers real-time, risk-aware data security with built-in classification, access mapping, and automated remediation.

Why Cyera?

Agentless
discovery,
faster data
visibility

AI-powered
classification
with 95%
precision

Automated risk
identification
and
prioritization

AI-powered
data loss
prevention for
data in motion

Unmatched
scale to match
your data
growth

As cloud environments evolve, so must your data security strategy. Cyera, in partnership with AWS, enables you to secure what matters most — intelligently, continuously, and at scale.

Visit cyera.com to request a personalized demo and see how Cyera can help protect your business-critical data in the cloud.

Book a demo

