CYERA

Why DSPM is Core to Every Enterprise Data Security Program

Traditional security measures can't keep up with the data deluge

In the modern, cloud-centric world, sensitive information can be created anywhere and end up anywhere—sometimes in places we don't even know exist. If you don't know where your sensitive data is, who has access to it, and what's being done with it, security teams are left guessing, and that's dangerous. After all, you can't secure what you can't see, and you can't manage risks you don't know about.

Data is created everywhere.

In so many forms.

We don't have a clear view of what data lives where, how sensitive it is, and how well it is protected.

83%

of data security professionals acknowledge that a lack of visibility into data is weakening the overall security posture of enterprises. - Cyera 2024 DSPM Adoption Report

The Benefits of Data-First Approach

Data Security Posture Management (DSPM) focuses on understanding where data lives, how sensitive it is, how it can be accessed, and how well it is protected. DSPM helps CISOs and security staff understand the heterogeneous, distributed data landscape so concrete steps can be taken to improve data security.

Moving from Strengthening Perimeters to Improving Data Security

Securing the perimeter doesn't work when data lives everywhere. **Instead security teams should focus on the data itself.** DSPM provides a comprehensive inventory of your data landscape and relevant aspects of security such as identity, configurations, and permissions so you know how to protect it, regardless of where it resides or what form it takes. Think of DSPM like an interactive map for your data. It shows you where everything is and also tells you what's important and what needs your attention. The data inventory provides the clarity and insights needed to develop an effective data security strategy.

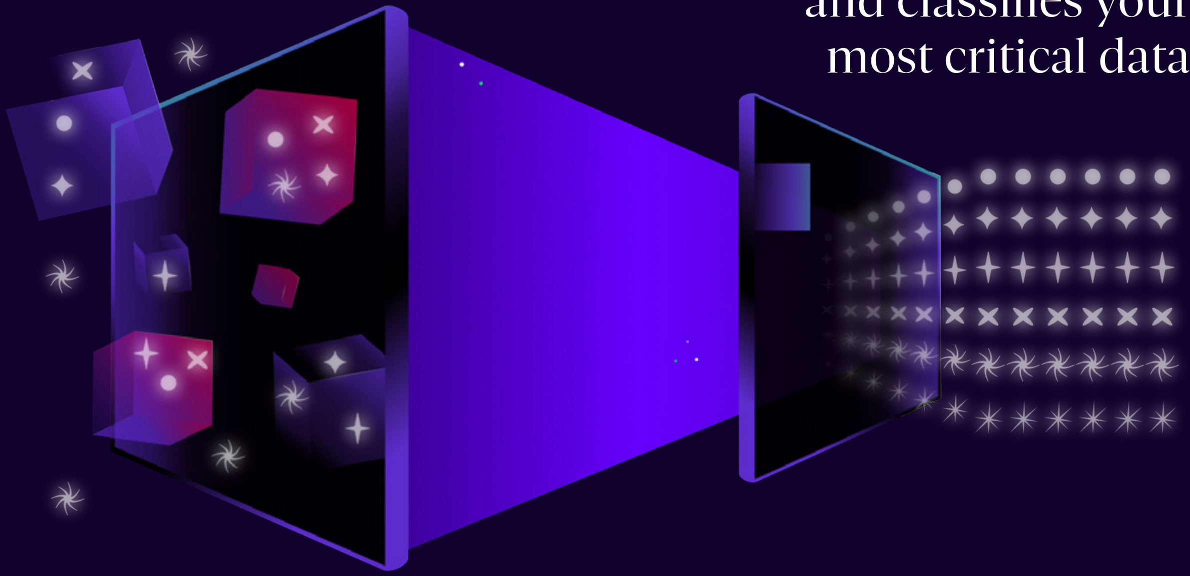
Reduce Your Attack Surface and Cut Costs by Pruning Data

Most companies store data that is old, duplicated, or unnecessary, but deleting it without clear visibility is not for the faint of heart. Hoarding data increases both costs and your data attack surface. DSPM helps you find and classify unneeded data, giving you the confidence to take action that will save you money and reduce risks.

DSPM finds and classifies your most critical data

Data Types

- ● Business
- ✦ Financial
- ✦ Health
- ✕ IT & Security
- ✳ Personal
- ✳ Duplicate



DSPM is the foundation for data security success

Unlike any other data security platform, DSPM surveys the entire data landscape, which helps spot issues early, and enables effective response. This big picture view helps CISOs and security experts provide precise answers and powerful capabilities to address the most critical data security questions.

DSPM Answers Fundamental Data Security Questions

Discover

What data do we have and where is it?
DSPM discovers, tracks, and monitors your most important data, on-premises, in the cloud, and in critical SaaS apps. It keeps your data inventory up-to-date, so you always know what data you have and where it is.

Classify

How can we categorize sensitive information?
DSPM uses AI to classify what data is most sensitive, which data presents risk, and which data is less important, clarifying the context in which the data is used.

Comply

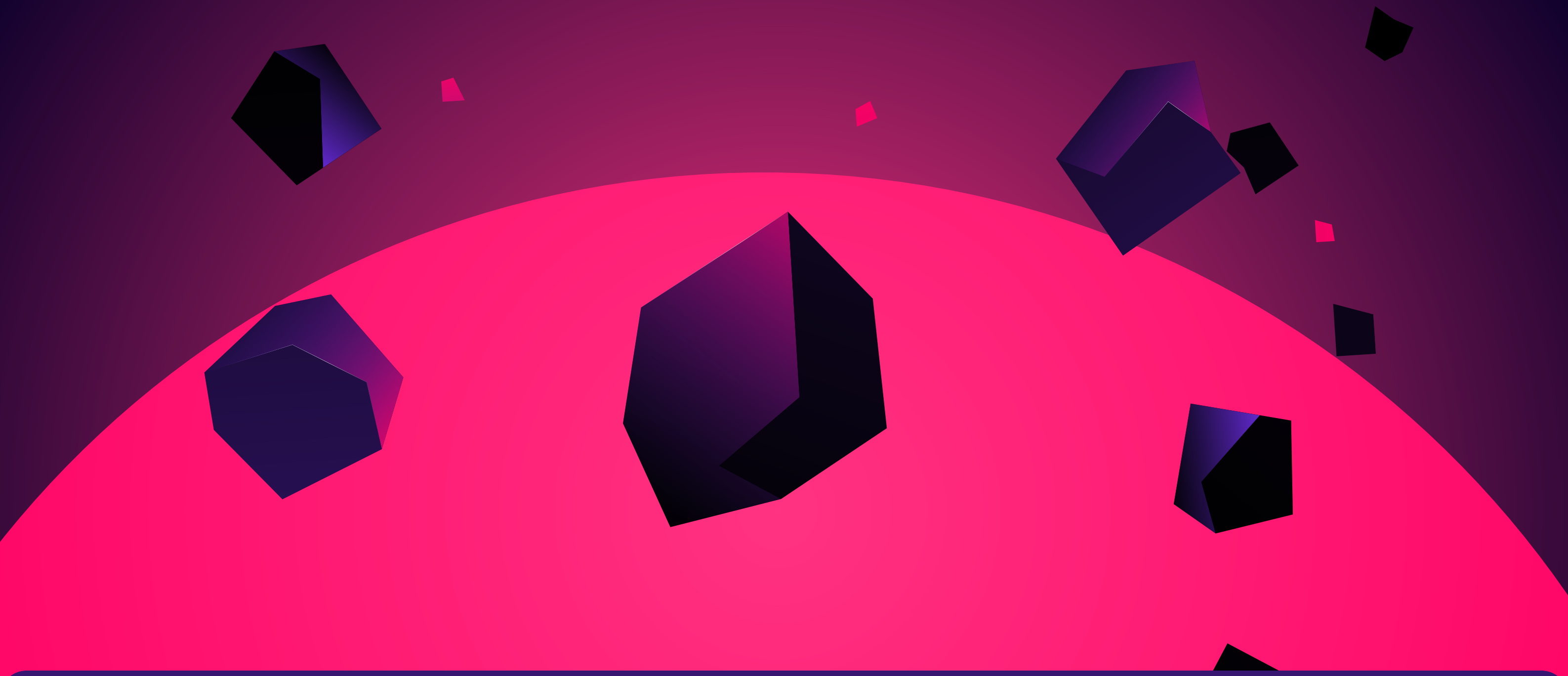
How can we comply with critical regulations?
DSPM provides the necessary visibility to identify if data is at risk for a compliance violation and provides evidence for demonstrating compliance.

Respond

What data risks demand immediate attention?
DSPM identifies data security issues so they can be corrected, improving your data security posture. If an incident occurs, the data involved can be quickly identified.

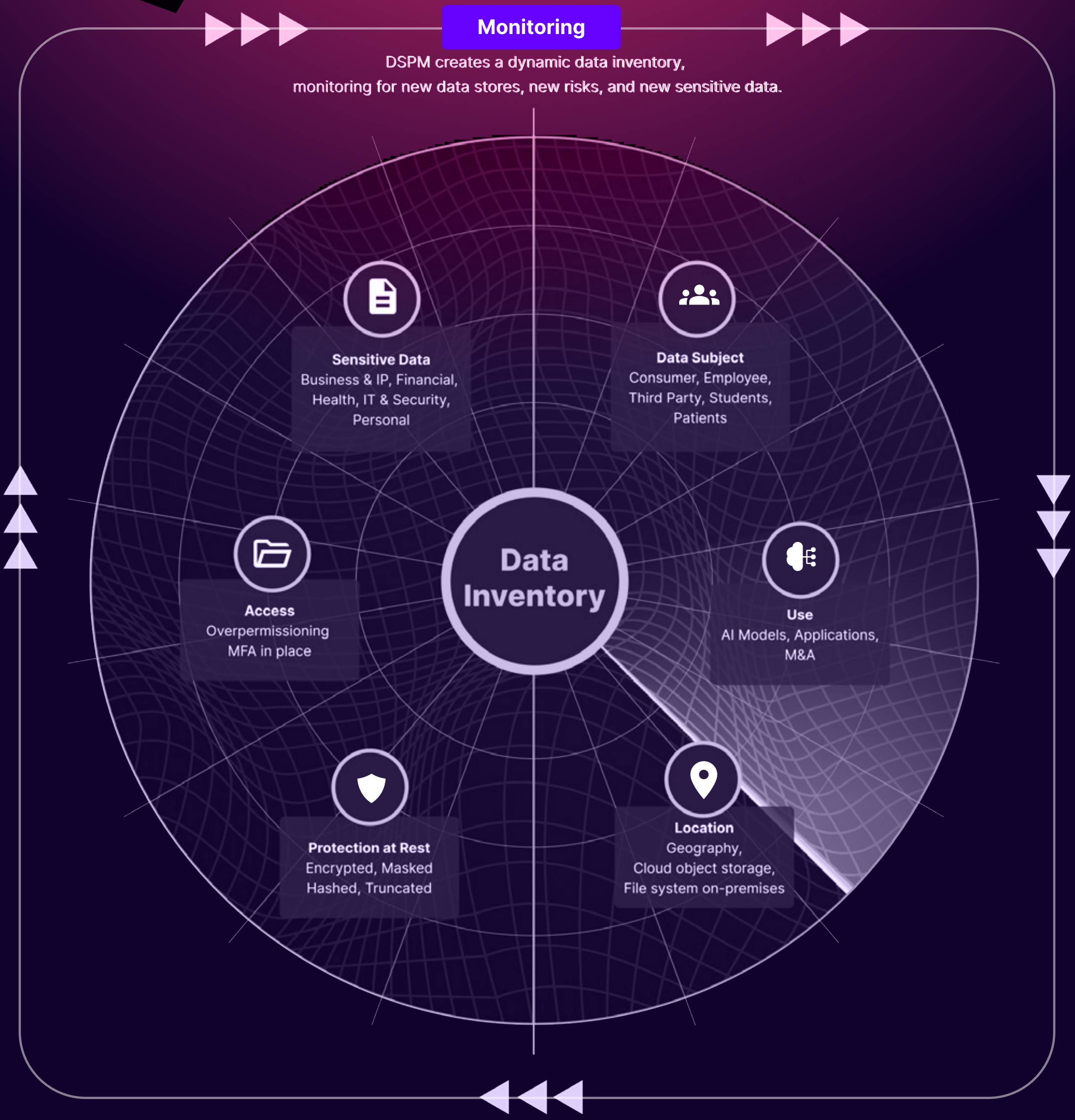
Leverage

How can we accelerate data-dependent initiatives?
DSPM reduces friction, enabling data to be put to use rapidly and safely in a wide variety of use cases, including AI applications.



DSPM Creates a Detailed, Comprehensive Data Inventory

DSPM provides visibility into all important dimensions of data, serving as the foundation of a proactive, data-centric security strategy. It helps you see and secure your data, no matter where it lives, giving you the clarity and context needed to protect your most valuable asset—data—effectively.



Monitoring

DSPM creates a dynamic data inventory, monitoring for new data stores, new risks, and new sensitive data.

Data Inventory

Sensitive Data
Business & IP, Financial, Health, IT & Security, Personal

Data Subject
Consumer, Employee, Third Party, Students, Patients

Access
Overpermissioning
MFA in place

Use
AI Models, Applications, M&A

Protection at Rest
Encrypted, Masked
Hashed, Truncated

Location
Geography,
Cloud object storage,
File system on-premises

Finding Gaps in Existing Security Measures

Essential security measures like encryption, access controls, backups, and secret keys are necessary, but they're not enough. They often leave gaps that can be exploited. DSPM creates a comprehensive data security inventory that classifies data by sensitivity and tracks how it is protected. With that information, CISOs can determine if encryption, access controls, backups, or secret keys are properly focused and configured. In this way, DSPM turns basic security measures into more proactive tools, helping you hunt down and fix issues before they become problems.

Encryption

It's difficult to ensure critical data is encrypted if you can't find it. DSPM helps by highlighting unencrypted sensitive data.

Access

It's common to have too many people with access to sensitive data. DSPM points out where access should be restricted.

Backup

Backups are vital, but they only work when they are configured correctly. DSPM helps find your most critical data and determine if backups are in place.

Keys

By integrating with DSPM, Key Secret Management solutions can help ensure that sensitive keys are not only stored securely but also tied to the specific data they are meant to protect.

Making Advanced Security Tools More Effective

Advanced and sophisticated tools like DLP, IAM, SIEM, SOAR, CASB, DAM, PAM, and TPRM struggle without a complete data inventory. DSPM informs these tools with greater context around data, providing the visibility and confidence needed to improve implementation and configuration to make them more effective. Ultimately, this reduces false positives and limits alert fatigue.

Data Loss Prevention (DLP)

Traditional DLP solutions often struggle with a high volume of false positives due to a lack of context about the data they're protecting. DSPM's precise classification reduces false positives that hinder the success of DLP systems.

Identity & Access Management (IAM)

IAM systems often lack granular visibility into data. DSPM helps IAM systems understand what data should and shouldn't be accessed, enabling you to put proper permissions in place.

Security Information & Event Management (SIEM)

SIEM systems can lead to alert fatigue. DSPM allows them to understand the sensitivity, type, and location of data involved in security events, making the alerts more meaningful.

Security Orchestration, Automation, & Response (SOAR)

SOAR helps automate incident response, but often lacks data context to prioritize actions. DSPM enables SOAR solutions to trigger more precise and effective remediation workflows.

Cloud Access Security Broker (CASB)

CASB secures cloud applications but lacks visibility into the data it protects. DSPM enhances CASB by classifying cloud data, ensuring policies are aligned with data sensitivity and compliance needs.

Database Activity Monitoring (DAM)

DAM provides monitoring but lacks broader context of data sensitivity and risk. DSPM enhances DAM by classifying the data within databases, enabling more informed monitoring and protection.

Privileged Access Management (PAM)

PAM controls and monitors elevated access to critical systems. With DSPM, PAM can enable more granular permissions, allowing privileged users access to only necessary sensitive data.

Third-Party Risk Management (TPRM)

A successful TPRM program requires insight into which third parties have access to sensitive data. DSPM informs TPRM tools by providing visibility into which third parties are accessing sensitive data.

Improving Modern Data Security Capabilities with DSPM

The most recent generation of security technologies like CSPM, XDR, SASE, ZTNA, and CWPP tackle modern challenges. Even still, these and other modern security solutions need a solid understanding of the data they're protecting.

Cloud Security Posture Management (CSPM)

CSPM secures cloud configurations, but overlooks data sensitivity and lacks precise data classification capabilities. DSPM identifies the sensitive data across infrastructures, enabling more informed and prioritized configurations.

Extended Detection & Response (XDR)

XDR relies on context to detect and mitigate threats effectively. DSPM adds data sensitivity and classification insights, enabling XDR platforms to better prioritize and respond to risks.

Secure Access Service Edge (SASE)

DSPM complements SASE by helping protect the data itself across all environments, not just ensuring that network traffic or access points are secure.

Zero Trust Network Access (ZTNA)

ZTNA limits network access but lacks visibility into the data being accessed. DSPM helps ensure sensitive data is only accessible to authorized users.

Cloud Workload Protection Platform (CWPP)

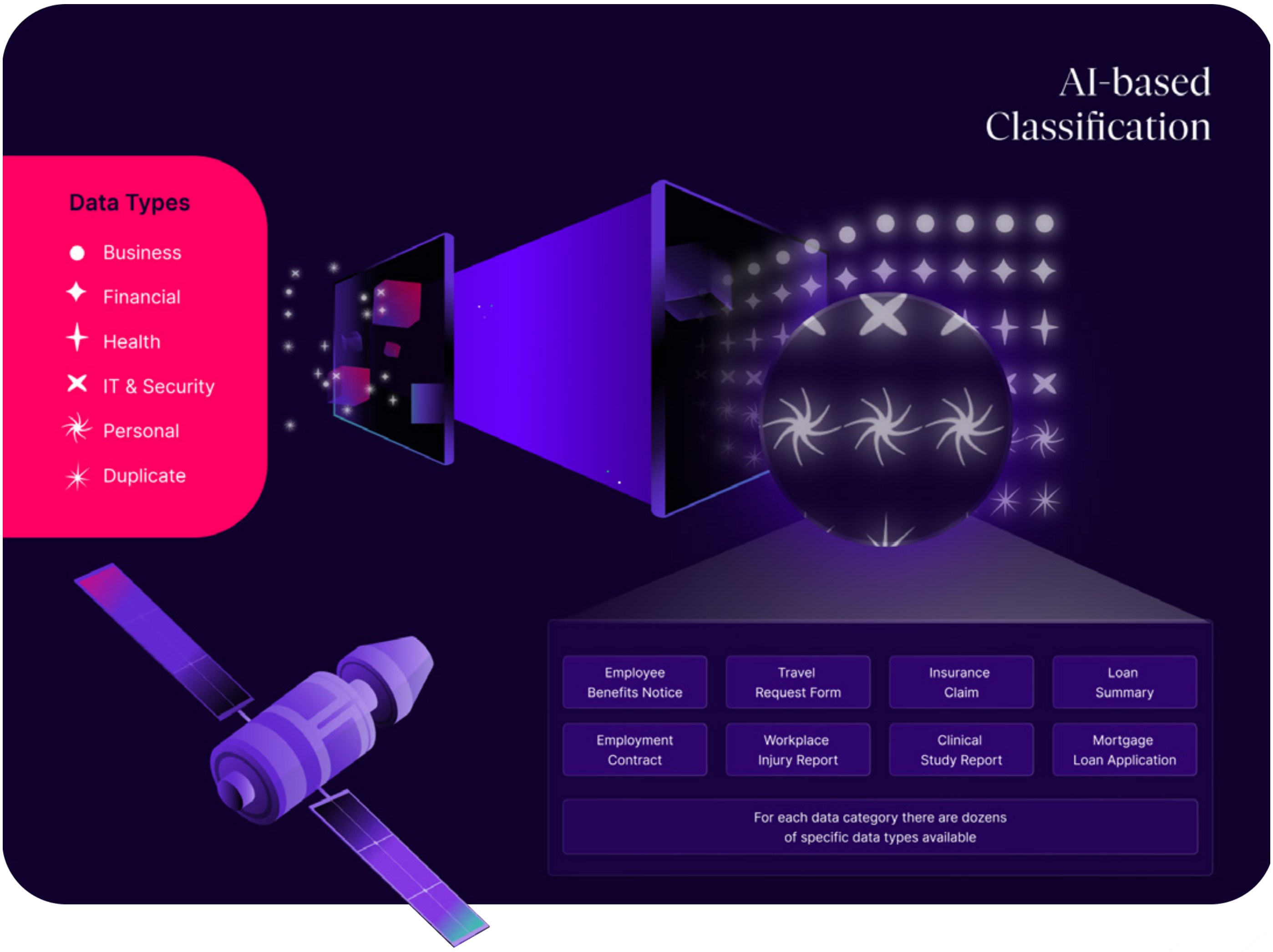
CWPP protects workloads but misses data sensitivity. DSPM classifies cloud data to align security with its importance.

Enterprise Digital Rights Management (EDRM)

EDRM solutions need to understand the sensitivity of data (an area where DSPM excels) in order to properly deploy its protection capabilities.

Why Cyera for DSPM?

Cyera uses AI-powered classification to understand and interpret data contextually, much like a human analyst. Our LLMs leverage vast amounts of training data to develop a nuanced understanding of language, patterns, and context, enabling them to classify data and assess its sensitivity with high precision. These LLMs are trained incrementally on diverse datasets, allowing them to recognize and understand a wide range of data types and structures, and even auto-learn new data.



AI-based Classification

Data Types

- ● Business
- ✦ Financial
- + Health
- ✕ IT & Security
- ✳ Personal
- ✳ Duplicate

Employee Benefits Notice

Travel Request Form

Insurance Claim

Loan Summary

Employment Contract

Workplace Injury Report

Clinical Study Report

Mortgage Loan Application

For each data category there are dozens of specific data types available

Cyera's AI-powered classification helps you:

- Uncover data unique to your business through unsupervised learning of new classifiers.

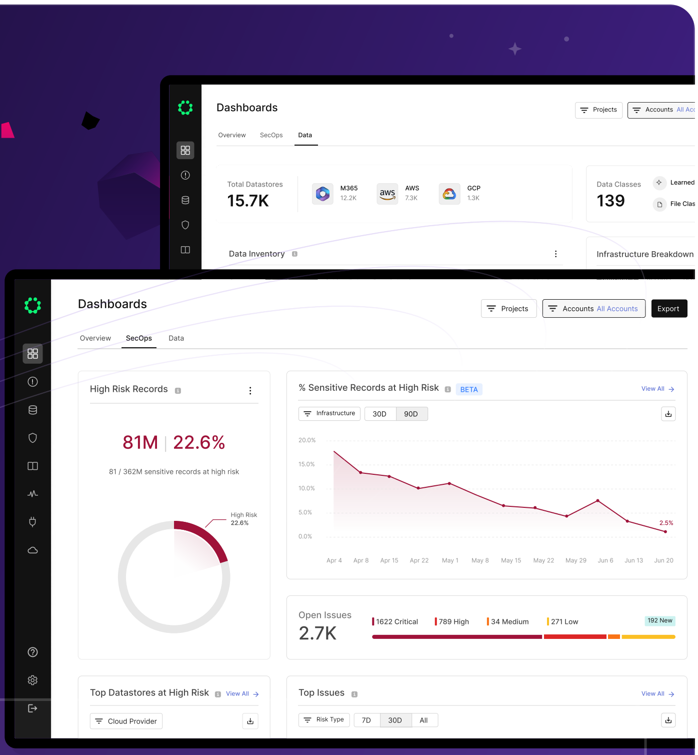
- Gain data context, such as location, sensitivity, type, applicable laws, identifiability, and security controls.

- Enhance visibility into sensitive data access, security configurations, and data risks to make better decisions across your security landscape.

> Marrying unsupervised learning, RegEx, pattern matching, and heuristics is an incredibly powerful combination that breaks new ground in data classification.

The Cyera Data Security Platform

Fuel business growth by pioneering the discovery and security of its most vital resource: data.



Protect Your Dataverse.

Organizations struggle to understand their data—what they have, where it resides, its security posture, and who has access. Cyera provides clarity with automated discovery and AI-powered classification, identifying data risks and protecting data in motion to strengthen security and help ensure safe, compliant access to data for your business.

Discover data risks at scale, and with speed

Cloud adoption creates immense data sprawl. Control this complexity with continuous data discovery, enabling visibility across environments to reduce risk and enhance compliance.

Classify data with high precision, and rich context

Given the abundance of data, you need to know which data is most sensitive, and understand key context to help you better protect it. AI-powered classification can help.

Finally connect data and identity security

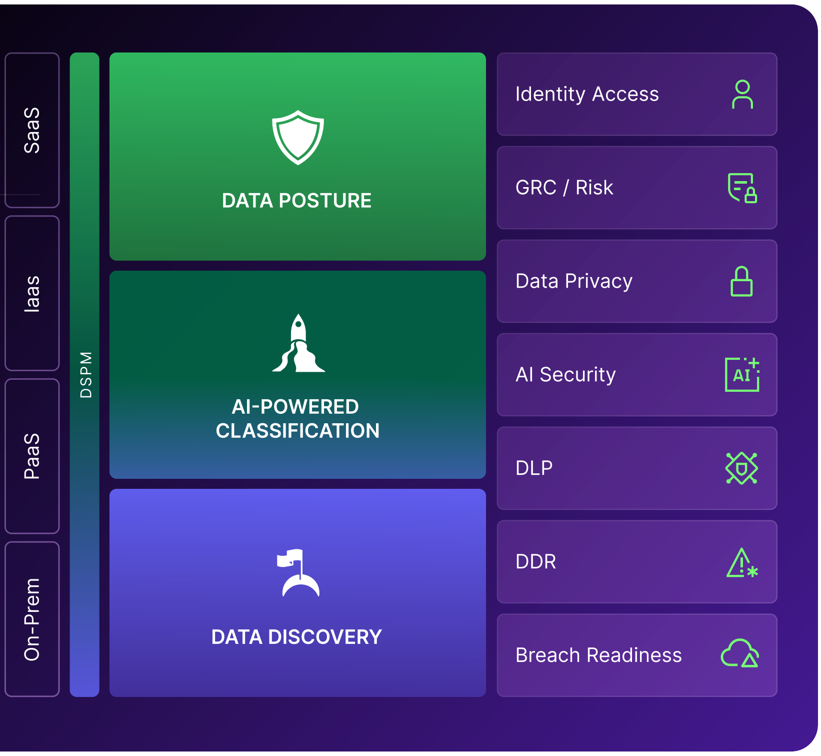
Data and identity go hand in hand. View identity through the lens of data for the first time so you know who – or what – is accessing critical data.

Protect data in motion with intelligent data loss prevention

Legacy DLP solutions weren't designed for the AI era. Detect, monitor, and protect critical data in motion with AI-powered data loss prevention.

A Unified Platform for Everything Data Security

From ground to cloud, Cyera powers your data security mission with a single platform designed to eliminate your most critical data risks—efficiently and effectively.



Data Security Posture Management (DSPM)

Discover and classify your sensitive data, determine what's at risk, and monitor it over time.

Data Governance, Risk & Compliance

Track data controls and policies for a risk-based approach to data governance and compliance.

AI Security

Leverage AI–responsibly and securely. Stop unauthorized data from entering AI models or copilots.

Data Detection and Response (DDR)

Continuously detect and respond to threats like unauthorized access, data exfiltration, and more.

Identity Access

Gain clarity into the human and non-human identities with access to sensitive data.

Data Privacy

Build a personal data inventory, identify privacy risks, and demonstrate privacy compliance.

Data Loss Prevention (DLP)

Layer AI-powered data loss prevention on top of DSPM capabilities to protect sensitive data in motion.

Breach Readiness

Conduct tabletop exercises, define recovery plans, and set materiality criteria for faster breach response.

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

For more information visit cyera.io or scan→

CYERA

CYERA.IO