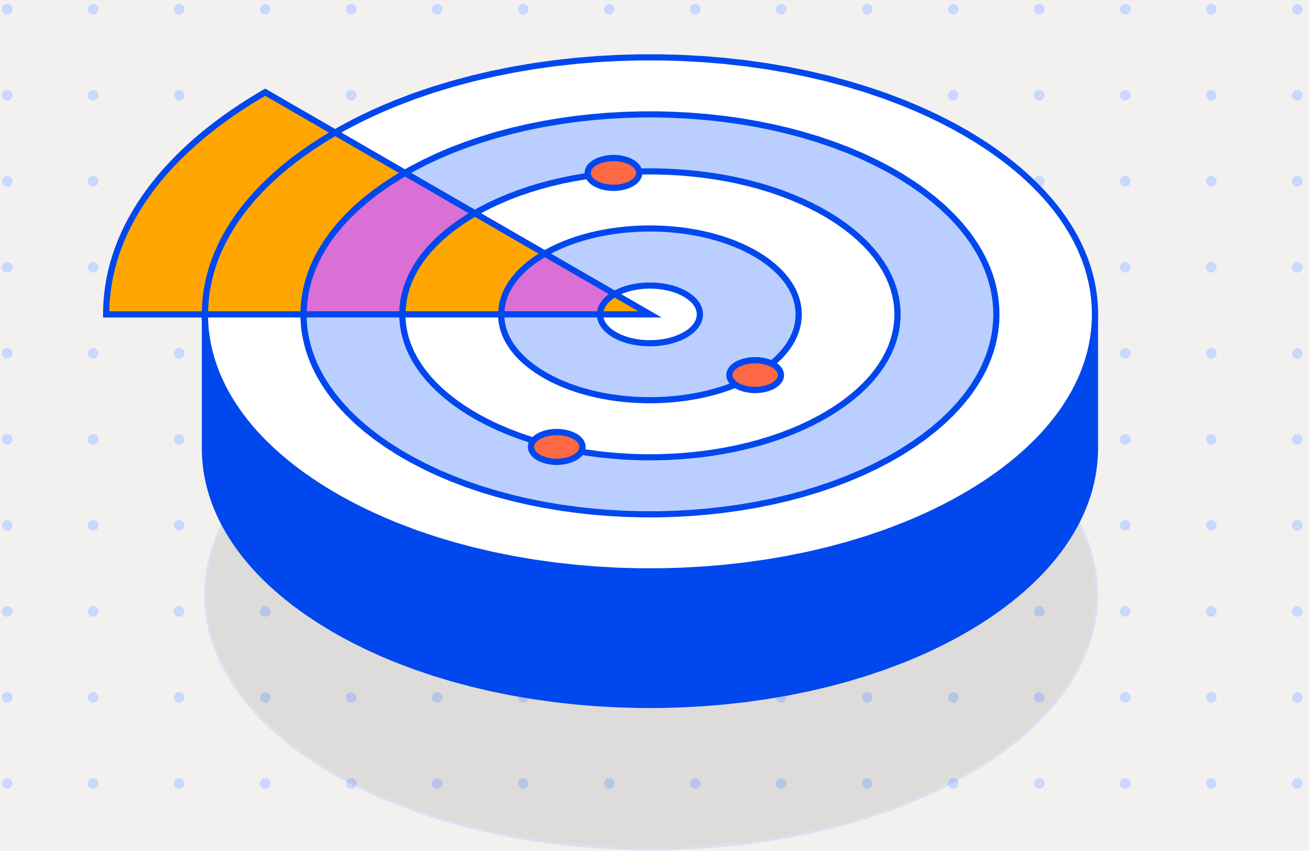
cyberhaven

Core Capabilities of AI-Native, Modern DSPM



Modern data security depends on more than discovery or classification alone. Next-generation DSPM transforms visibility into actionable insight, enabling teams to understand, manage, and protect sensitive data across increasingly complex environments. Understanding these capabilities is critical for evaluating DSPM solutions and ensuring alignment with your organization's risk posture.

01 Data Discovery: Finding Sensitive Data Everywhere

The foundation of DSPM is knowing where your data resides. Modern platforms connect to every data source across the organization, including:

- Cloud infrastructure (AWS, Azure, GCP)
- SaaS applications (collaboration tools, CRM, ticketing systems)
- On-prem databases and file shares
- Employee endpoints
- Generative AI tools used by employees

Discovery must be continuous. Scheduled scans cannot keep pace with the rapid creation, replication, and transformation of data. Continuous discovery ensures that newly created data, changes to existing data, and shadow copies are detected as soon as they appear, reducing exposure before it becomes a risk.

02 Data Classification: Understanding What the Data Is

Knowing where data lives is only the first step. Modern DSPM platforms classify data with precision, moving beyond pattern-based or rule-heavy approaches. AI-driven classification enables:

- Higher accuracy with fewer false positives
- Semantic understanding beyond simple regex rules
- Sensitivity assessment in context of business use, not just content patterns

This capability is especially critical for unstructured data and AI-generated content, where sensitivity is determined by use, not form.

The Value of AI-Driven Data Understanding

AI-Driven Data Understanding moves DSPM beyond static labels and fragmented discovery. It combines deep semantic analysis with continuous context and lineage so you can:

- **See what data truly is, not just where it sits.** AI analyzes content and context to improve accuracy and reduce false positives.
- **Distinguish meaningful risk from benign noise.** Provenance and access history help separate internal corporate data from public or low-risk information.
- **Understand how data changes and moves.** Contextual lineage reveals how sensitive information evolves as it flows across endpoints, SaaS, cloud, and AI workflows.
- **Inform smarter protection and prioritization.** Rich context enables policies that align with business risk, not just pattern matches.

03 Contextual Data Understanding: Beyond Labels

Classification alone cannot reveal risk. Modern DSPM enriches data with context, helping teams understand:

- **Provenance:** Was data internally created or sourced externally?
- **Exposure:** Who can access it—internal users, external collaborators, or the public?
- **Location:** Endpoint, SaaS, cloud storage, or on-prem systems
- **Structure:** Document, spreadsheet, database record, or raw text
- **Management status:** Whether the system holding the data is managed or unmanaged

Context lets DSPM differentiate risk between seemingly identical data. For example, an internal document on a managed laptop poses far less risk than the same document publicly shared from a SaaS platform

04 Data Lineage: Tracking How Data Moves and Transforms

Lineage tracks data throughout its lifecycle, showing how it moves and changes across systems. For example, sensitive data might be:

- Created on an employee endpoint
- Uploaded to a collaboration platform
- Exported into cloud storage
- Copied into documents or spreadsheets
- Fed into AI tools that generate derivatives

Without lineage, these actions appear as disconnected events. With lineage, DSPM reveals hidden risk paths, shadow copies, and downstream exposure that static tools cannot detect.

Effortless Experience: DSPM Should Fuel Innovation, Not Hinder It

Modern DSPM provides visibility while enabling teams to protect data comfortably. By unifying discovery, classification, and enforcement into a single workflow, teams can:

- **See and act on risk instantly.**
One platform, one view, no fragmented dashboards.
- **Reduce noise and false positives.**
Context-rich AI insight highlights what truly matters.
- **Move faster with confidence.**
Automated policies and continuous monitoring let teams focus on decisions, not busywork.

Simplify operations at scale. Unified controls mean fewer tools, less manual effort, and consistent enforcement across endpoints, SaaS, cloud, and AI workflows.

Outcome: Security teams gain clarity, confidence, and control without the complexity and friction of legacy systems.

05 Data Risk Assessment and Prioritization

Effective DSPM continuously evaluates risk across multiple dimensions:

- Public exposure or misconfigured access
- Overly permissive entitlements
- Cross-border data transfers
- Dormant or orphaned sensitive data
- Risky movement patterns

Instead of generating thousands of alerts, modern DSPM correlates sensitivity, access, exposure, and usage to prioritize the issues that matter most. This helps teams focus on actionable risk instead of drowning in dashboards.

06 DSPM and Generative AI: Protecting Data in AI Workflows

AI fundamentally changes how data risk manifests. Employees interact with AI to summarize, analyze, and generate content, producing new derivatives and sharing sensitive data outside controlled systems. Next-generation DSPM provides:

- Detection of sensitive data being fed into AI tools
- Tracking of AI-generated outputs across environments
- Visibility into AI workflows that create unacceptable risk
- Enforcement based on data sensitivity and context

Without DSPM visibility into AI-driven data flows, organizations are blind to one of the fastest-growing sources of exposure.

07 Identity and Access: Understanding Who Can Touch the Data

Modern DSPM integrates identity, access, and data into a unified model, linking datasets, datastores, human identities, service accounts, and AI-driven entities. This transforms posture from a static view of "where sensitive data lives" into a dynamic understanding of "who can interact with it and under what conditions."

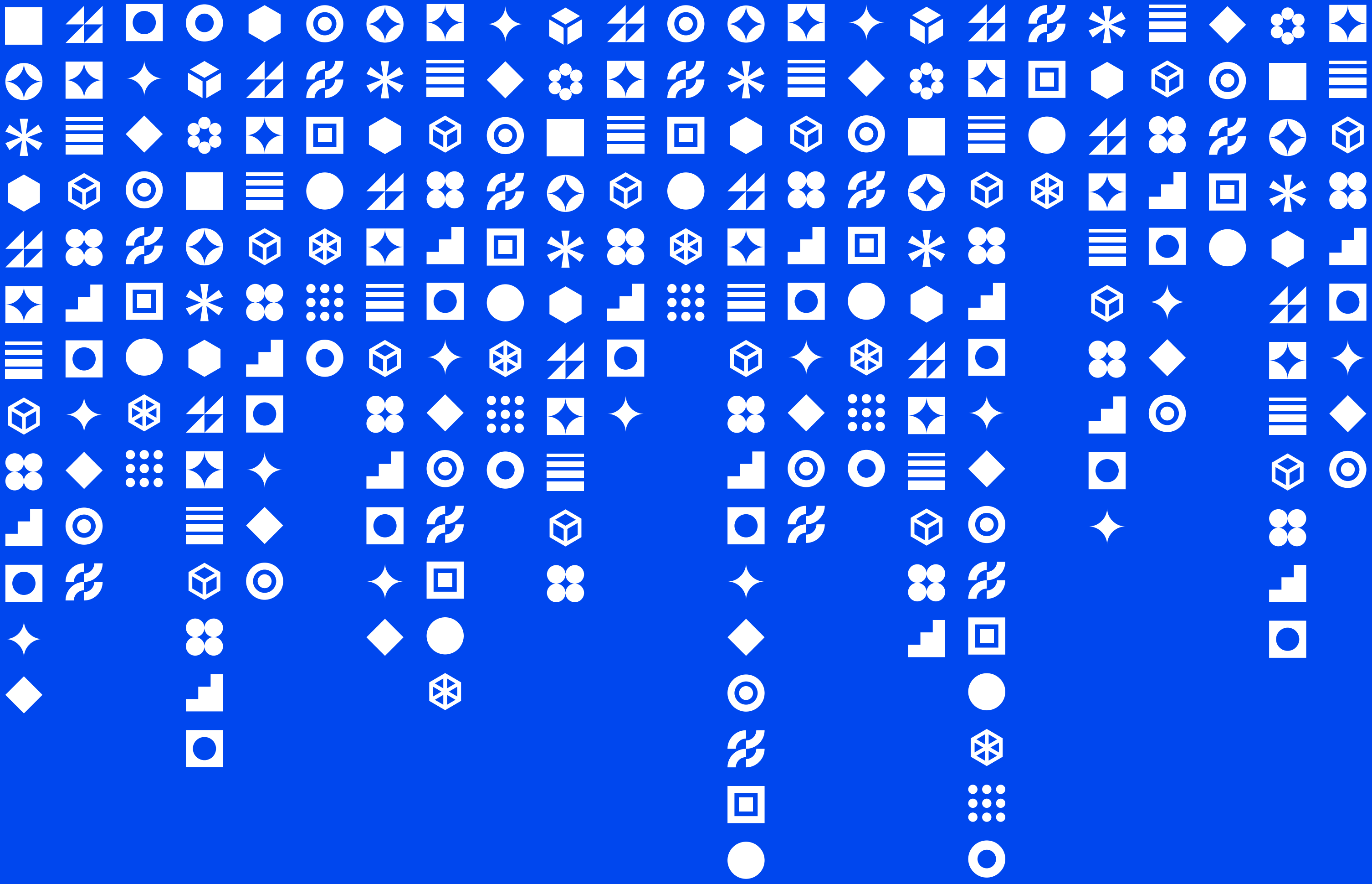
This enables organizations to answer critical risk questions out of the box, including:

- Which sensitive datasets are accessible to large groups of users or the entire organization?
- What customer or regulated data can contractors or external collaborators access?
- Which sensitive data is exposed to non-human identities, such as service accounts or AI agents?
- If a specific identity is compromised, what data could it reach?

By mapping access relationships directly to sensitive data, DSPM surfaces identities with excessive or risky permissions and allows teams to drill into access patterns, usage behavior, and downstream exposure. This eliminates the need to rely on fragmented IAM tools or manual analysis to understand blast radius.

Core Capabilities of DSPM

Capability	What It Does	Why It Matters
1. **Continuous Data Discovery**	Finds sensitive data wherever it lives: cloud, SaaS, endpoints, on-prem, and AI tools	Reduces blind spots and shadow copies before they become risk
2. **AI-Driven Data Classification**	Identifies sensitive and regulated data using semantic and contextual analysis	Improves accuracy, reduces false positives, and captures fragmented/ unstructured data
3. **Contextual Data Understanding**	Enriches data with provenance, exposure, location, structure, and system status	Differentiates risk between similar data and informs prioritization
4. **Data Lineage**	Tracks how data moves and transforms across systems, workflows, and AI outputs	Reveals hidden exposure paths and downstream risk invisible to traditional tools
5. **Risk Assessment & Prioritization**	Continuously evaluates exposure, access, entitlements, and movement patterns	Focuses teams on actionable issues instead of overwhelming dashboards
6. **AI-Aware Data Protection**	Monitors sensitive data usage in AI workflows and tracks AI-generated derivatives	Prevents high-risk AI interactions and maintains control over emerging data flows
7. **Identity & Access Context**	Maps who can access sensitive data across human identities, service accounts, and AI agents.	Shows who can touch data and how broadly, enabling accurate prioritization and faster breach impact analysis.
8. **Stopping Data Loss**	Take action, automatically, through natively integrated DLP capabilities.	Turns visibility into action by stopping data exfiltration at the source.



The Cyberhaven Difference

The future of data security demands more than visibility. It requires control, context, and the ability to act at the speed of modern work. Cyberhaven approaches this challenge by unifying discovery, classification, enforcement, and AI-aware protection into a single platform. By addressing both the complexity of data and the pace of AI-driven workflows, Cyberhaven empowers security teams to reduce risk without adding operational friction.

Learn more about Cyberhaven DSPM