veeam



Anatomy of a Modern DSPM:

10 Core Capabilities Powering Data-Centric Security

Why data and AI security matters:

43%

say AI adoption is outpacing their ability to secure data and models.

(Veeam Data Trust and Resilience Report 2026)

68%

of organizations have experienced data leaks linked to AI tool usage, and only 23% have formal security policies in place.

(Metomic, State of Data Security Report)

$4.99M

is the average global cost of a data breach: A 12% year-over-year increase and a record high.

(IBM/Ponemon Institute, Cost of a Data Breach Report 2026)

10 core capabilities of a modern DSPM

1 Automated data discovery and classification

The challenge

Sensitive data sprawls across SaaS, multicloud, and on-premises systems. Shadow and dark data remain invisible, leading to blind spots, accidental exposure, and compliance violations. Legacy regex methods generate false positives and inconsistent labeling.

The capability in action

AI-powered discovery and context-aware classification provide comprehensive visibility into both structured and unstructured data. Sensitive data like PII, PHI, and PCI is accurately identified, eliminating noise and enabling downstream security, risk, and compliance controls.

2 Contextual data and AI intelligence

The challenge

Fragmented data signals, such as entitlements, usage, and risks, are scattered across silos. Without a unified context, organizations cannot prioritize effectively, resulting in delayed remediation and missed compliance gaps.

The capability in action

DSPM leverages knowledge graphs to correlate metadata, access, and regulatory context into a unified source of truth. This transforms raw signals into actionable intelligence, empowering security, compliance, and business teams to make precise, timely risk decisions.

3 Toxic combinations of risks

The challenge

Isolated alerts often seem harmless. A misconfigured bucket, a sensitive dataset, or a new AI model may not raise alarms individually, but together they form a critical vulnerability.

The capability in action

DSPM automatically detects and prioritizes these compound risks, uncovering threats like AI models accessing exposed sensitive data. Organizations can also define custom risk rules aligned to their unique business context.

4 Security posture management

The challenge

Teams drown in alerts from misconfigurations (e.g., exposed S3 buckets or over-permissive entitlements). Without a sensitive data context, they cannot distinguish trivial from critical risks, wasting time while breaches loom.

The capability in action

DSPM continuously scans configurations across SaaS, cloud, and hybrid environments. By correlating misconfigurations with the presence of sensitive data, it prioritizes what truly matters and enables proactive remediation.

5 Data access intelligence and controls

The challenge

Excessive entitlements and poorly governed access expose sensitive information. Static IAM visibility cannot capture risky access patterns, especially in AI-driven environments like copilots.

The capability in action

DSPM builds a normalized knowledge graph of entitlements and tracks usage. It enforces least-privilege access and provides fine-grained controls (for example, row-level filtering and dynamic masking). This ensures secure and compliant data is available to teams.

6 ROT data minimization

The challenge

Redundant, obsolete, and trivial (ROT) data silently accumulates, driving up storage and backup costs, expanding the attack surface, and increasing compliance liabilities (e.g., GDPR retention rules). It also contaminates GenAI training data.

The capability in action

DSPM uses policy-driven automation to detect, categorize, and remediate ROT data. By continuously cleaning stale data, organizations reduce costs, shrink breach risk, and improve the quality of AI initiatives.

> Cleaner data isn't just a security win, it's a resilience win. Less redundant and obsolete data means smaller, faster, less expensive backups and a smaller recovery surface if something goes wrong. DSPM's ROT cleanup and Veeam's data resilience platform address two sides of the same cost-and-risk equation.

7 AI data security

The challenge

AI is moving into the enterprise faster than security teams can keep up. That speed and scale means any small gap in data security gets exposed and amplified. Generic guardrails and point solutions don't fix the underlying problem, as they don't secure the data itself.

The capability in action

DSPM discovers AI agents and models across the environment and maps them to the data they touch, revealing risks like data exposure, mishandling of regulated data, and inappropriate access. It applies controls at the data level through a single policy engine that spans both AI models and data systems, then runs compliance checks to validate that the data is safe. The result: Validated, safe data that lets the enterprise move faster, and more safely, with AI.

8 Compliance automation

The challenge

Compliance teams rely on spreadsheets, attestations, and siloed tools. Manual workflows for overlapping frameworks such as GDPR, EU AI Act, and CCPA are slow, error-prone, and unsustainable at scale.

The capability in action

DSPM streamlines compliance via automated control mapping, testing, and reporting across data and AI environments. Real-time compliance dashboards, evidence workflows, and persona-based reporting reduce audit prep from quarters to months.

9 Automated remediation

The challenge

Manual remediation is slow, fragmented, and risky. Security issues linger because fixes require coordination across multiple teams.

The capability in action

DSPM orchestrates policy-driven remediation, automatically fixing common risks and generating federated tickets for complex ones. Integrations with platforms like ServiceNow, Jira, and Slack ensure remediation is embedded into existing enterprise workflows.

10 Breach management

The challenge

During a breach, teams find it hard to identify which data and users were exposed and what regulatory notifications are required. This creates costly delays and compliance failures.

The capability in action

DSPM automates breach impact analysis, mapping data to individuals, jurisdictions, and regulations. It calculates potential penalties, orchestrates notifications, and generates authoritative incident reports, accelerating incident response and minimizing impact.

> Knowing what was exposed is only half the incident response story; getting back online with clean, verified data is the other half. DSPM tells you what happened and who to notify. Meanwhile, Veeam's ransomware recovery and radical resilience capabilities get the business back up and running fast.

Move from risk to resilience with Securiti DSPM

DSPM addresses the root causes of data risk: Lack of visibility, poor context, alert fatigue, weak access controls, AI misuse, and compliance complexity. By solving these problems, DSPM helps enterprises move from reactive firefighting to a proactive data and AI security posture, accelerating AI innovation and business growth with confidence.

A strong data security posture tells you where your risk lives. A resilient backup and recovery strategy makes sure that risk never becomes a business-ending event.

Get guidance on why DSPM matters now: How it discovers sensitive data, detects risks, and orchestrates remediation in your environment.