netskope

White Paper

Netskope One DSPM: Unlocking Modern Data Security

Discover, Classify, and Secure Data at Rest, in Motion, and in Use

Table of Contents

WHERE IS YOUR DATA? IS IT SECURE?

Data is the lifeblood of organizations, fueling innovation, growth, and business-critical decision-making. But as data flows faster and further across cloud environments, on-premises systems, and sprawling data lakes, new complexities emerge:

- Sensitive data is scattered across environments, creating blind spots and increasing the risk of exposures.
- Shadow and abandoned data, often unmonitored, amplifies vulnerabilities and leaves organizations unaware of hidden risks.
- While transformative, AI models bring their own risks through data imprinting and unchecked real-time interactions.

Every security leader must ask the following questions: "Where is my data, and is it secure?" Without clear answers, the risks grow exponentially; data breaches, misconfigurations, and overexposed access are just the beginning. This is where data security posture Management (DSPM) becomes a change agent for organizational data strategy.

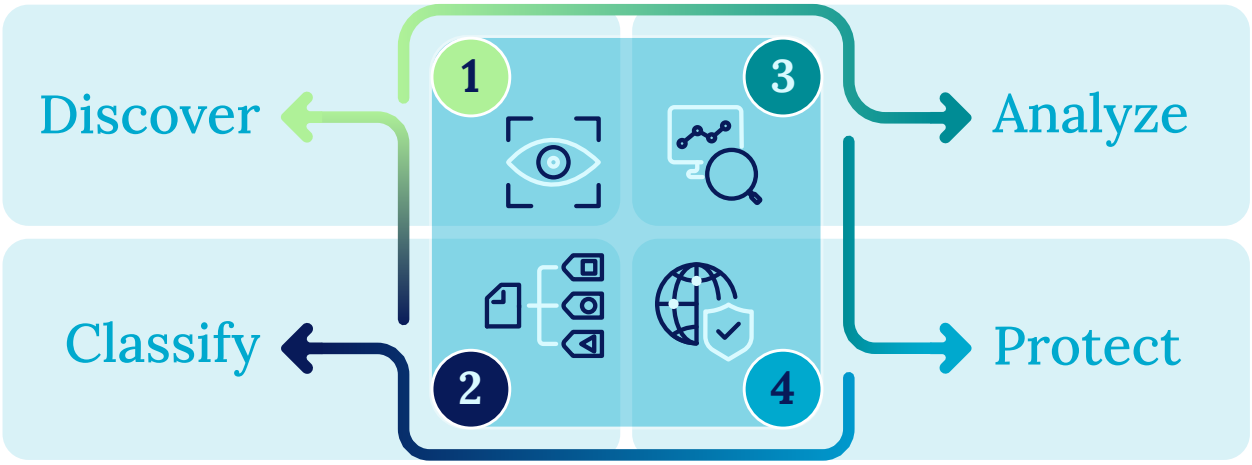
What Is DSPM?

At its core, DSPM solves one of the most pressing challenges in cybersecurity: achieving complete visibility into sensitive data while ensuring it's protected against vulnerabilities and misuse.

Traditional data protection tools often can't see where data resides or how it's accessed across vast hybrid environments. DSPM changes that by:

1. Discovering and mapping data across cloud, on-premises, and hybrid environments, including structured, unstructured, and also shadow data.
2. Classifying and tagging sensitive information to ensure critical data gets prioritized for protection.
3. Assessing risk posture to detect misconfigurations, excess access, and policy violations.
4. Automating remediation to close gaps quickly and minimize risk exposure.

With DSPM, you're not guessing about your security posture; instead you're seeing it, understanding it, and improving it in real time.



NETSKOPE ONE DSPM: THE FOUNDATION OF MODERN DATA SECURITY

Netskope One DSPM, part of the Netskope One platform, provides the foundation for a complete and proactive data security strategy by delivering capabilities to:

Discover: Automatically locate and map all structured, unstructured, and shadow data stores.

Classify: Accurately identify and tag sensitive data to align with business value and regulatory frameworks (e.g., GDPR, CCPA, HIPAA).

Analyze: Continuously assess configurations, permissions, and risks to eliminate vulnerabilities.

Protect: Automate remediation workflows to enforce policies and reduce the attack surface.

By answering **"Where is my data?"** and **"How secure is it?"** Netskope One DSPM empowers security teams to focus on what matters most: protecting critical data assets and reducing risk.

Netskope One DSPM forms part of the Netskope One Data Security solution and is a core component of the single Netskope One platform. Netskope One DSPM and Netskope One DLP work hand in hand to provide a complete data security solution, exchanging data between components to holistically deal with the data at rest and data in motion problem.

Let's take a closer look at the core capabilities of Netskope One DSPM. What are the tools and processes that set it apart and enable organizations to achieve complete visibility, control, and remediation?

1. DATA DISCOVERY: ELIMINATE UNKNOWN UNKNOWNS

The first step to securing your data is knowing where it lives. Netskope One DSPM automatically discovers structured and unstructured data across cloud, on-premises, and hybrid environments like AWS, Azure, Snowflake, and more.

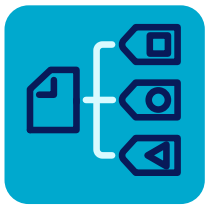
- Identify shadow data lurking in forgotten repositories.
- Detect orphaned data stores created during mergers, acquisitions, or decentralized team activity.
- Eliminate risky silos and blind spots that leave sensitive data exposed.

Example Use Case:

Data often falls through the cracks in organizations undergoing mergers or with decentralized operations. Netskope One DSPM acts like radar, detecting forgotten or unsanctioned data repositories and bringing them back under governance.

Outcome

You gain **complete visibility** into your data landscape, eliminating the unknown unknowns that attackers exploit.



2. DATA CLASSIFICATION & TAGGING: UNDERSTAND WHAT MATTERS MOST

Not all data is created equal. Netskope One DSPM helps you understand and prioritize by:

- Classifying data based on sensitivity, such as PII, PHI, intellectual property, etc.
- Tagging data to meet compliance regulations like GDPR, HIPAA, CCPA, and other frameworks.

Why It Matters:

Accurate classification gives security teams a clear roadmap to prioritize critical data. It simplifies audits, enhances compliance posture, and ensures you focus on protection where needed most.

3. CONFIGURATION & ACCESS ANALYSIS: CONTROL WHO CAN ACCESS WHAT

Data misconfigurations and excessive access are among the top causes of breaches today. Netskope One DSPM continuously analyzes:

- Data store configurations to identify vulnerabilities like open S3 buckets, improper encryption, or publicly accessible databases.
- Access permissions to enforce least privilege and eliminate insider risks or over-permissioned access.

Example Use Case:

Is your AI team accessing training datasets containing sensitive PII? Netskope One DSPM ensures access policies align with business requirements and security standards.

Outcome

You regain control over who can access what, reducing the risk of breaches caused by misconfigurations or excessive permissions.

4. RISK DETECTION & AUTOMATED REMEDIATION: FIX PROBLEMS FAST

Staying ahead of threats requires more than just detection—it requires action. Netskope One DSPM:

- Flags risk like misconfigurations, policy violations, and suspicious data activity.
- Provides remediation playbooks to guide security teams in resolving issues.
- Enables automated workflows to fix problems without manual intervention.

Key Benefit:

Your security team moves from reactive firefighting to proactive problem-solving. By addressing risks quickly, Netskope One DSPM reduces the attack surface and strengthens data resilience without slowing down business operations.

Outcome

Issues are resolved faster and smarter, empowering security teams to focus on strategic priorities.

With these core capabilities, discovery, classification, access control, and risk remediation, Netskope One DSPM lays the foundation for a secure, well-governed data environment. But this isn't just about visibility. It's about turning insights into action and giving your security team the tools they need to mitigate risks, ensure compliance, and unlock the full potential of your data. This becomes even more critical as businesses go deeper and deeper with AI, where data security challenges are evolving at an unprecedented pace. Let's explore how DSPM can address these emerging risks and protect the data powering your AI initiatives.

HOW NETSKOPE ONE DSPM PROTECTS AI TRAINING DATA

As organizations increasingly refine AI models with proprietary data, the complexities of managing sensitive information in AI workflows create unique challenges. Traditional DSPM solutions often fall short when it comes to addressing the specific risks associated with AI, leaving gaps in real-time monitoring, data imprinting, and access governance. Netskope One DSPM directly addresses these AI-specific risks with precision and control.

Unique AI-Specific Challenges:

1. **Data Imprinting:** AI models can unintentionally retain or "memorize" sensitive information from training datasets, creating a risk of inadvertent disclosure during model deployment.
2. **Real-Time Access Risks**: Each real-time data pull for AI training or inference increases the attack surface, as sensitive datasets are constantly accessed across distributed environments.

How Netskope One DSPM Solves AI-Specific Risks:

1. **Real-Time Monitoring for AI Pipelines:** Netskope One DSPM continuously monitors data usage in AI workflows, detecting potential misconfigurations, suspicious activity, or overexposed datasets. Unlike traditional DSPM tools that focus on static data at rest, Netskope One DSPM provides real-time insights into how data is accessed and manipulated during AI model training and inference.

   Example Use Case: If an unauthorized user or system attempts to pull sensitive data from a training dataset, Netskope One DSPM immediately flags the activity, preventing unauthorized access before it escalates.

2. **Preventing Data Imprinting Risks:** By providing granular visibility and control over training datasets, Netskope One DSPM ensures that only sanitized and properly governed data is used in AI workflows. This reduces the likelihood of sensitive information being inadvertently "memorized" by AI models.

   Key Differentiator: Netskope One DSPM goes beyond standard discovery and classification by continuously analyzing access patterns and data usage, ensuring that sensitive data is protected throughout the entire AI life cycle.

3. **Automated Access Controls:** With dynamic enforcement of least-privilege access policies, Netskope One DSPM ensures that only authorized users and systems can access AI training datasets. It minimizes insider risks and protects against accidental overexposure.

   Example Use Case: Netskope One DSPM can enforce strict access controls to ensure only specific data scientists working on a project can access sensitive datasets while other team members are restricted.

4. **Shadow Data Discovery in AI Pipelines:** AI workflows often pull from multiple data sources, including shadow or forgotten ungoverned and vulnerable repositories. Netskope One DSPM discovers and integrates these data sources into governance frameworks, ensuring they don't become points of failure.

   Outcome: Organizations gain full visibility into every dataset feeding their AI models, eliminating blind spots and reducing compliance risks.

Unleashing AI Innovation Without Security Compromise

Netskope One DSPM provides the visibility, control, and protection organizations need to innovate confidently with AI. Its ability to monitor real-time data usage, prevent data imprinting, and enforce dynamic access controls ensures that AI models are trained securely, responsibly, and in compliance with regulatory standards. This level of precision and adaptability is unmatched in the industry, positioning Netskope One DSPM as the ideal solution for balancing AI innovation with data security.

KEY USE CASES OF NETSKOPE ONE DSPM

AI innovation depends on securing the data that powers it, and Netskope One DSPM ensures organizations can confidently innovate while maintaining full life-cycle data security. However, protecting AI workflows is just one piece of the puzzle. Effective data security requires a broader, more comprehensive approach that safeguards AI pipelines and addresses visibility gaps, access risks, compliance challenges, and proactive risk remediation.

This is where Netskope One DSPM shines, offering targeted solutions to the most pressing data security challenges organizations face today. Let's explore the key use cases demonstrating the platform's transformative capabilities.

1 **Visibility into Data Risk**

Uncover shadow data, orphaned repositories, and other blind spots to ensure full visibility across cloud, on-premises, and hybrid environments.

Example: A decentralized organization with data scattered across teams can use Netskope One DSPM to discover and bring unmonitored data under governance, reducing potential risk exposure.

2 **Access Management**

Identify and minimize over-permissioned access to enforce least-privilege principles and reduce insider threats.

Example: A finance team's shared drive containing sensitive payroll data is overexposed to employees outside the department. Netskope One DSPM detects this misconfiguration and enforces tighter access controls.

3 **Streamlined Compliance**

Automate data classification and enforce compliance policies for regulations such as GDPR, HIPAA, and CCPA, simplifying audits and mitigating regulatory risks.

Example: A company handling EU customer data uses Netskope One DSPM to classify and tag sensitive PII, automatically flagging and remediating any violations of GDPR data storage policies.

4 **AI Training Data Security**

Secure sensitive datasets for AI model training by providing visibility, access control, and continuous monitoring.

Example: AI teams accessing proprietary datasets for model training are monitored to ensure no unauthorized access or data leakage, safeguarding the integrity of the AI pipeline.

5 **Automated Risk Remediation**

Continuously detect and resolve misconfigurations, policy violations, and risky data usage with automated workflows and remediation playbooks.

Example: Netskope One DSPM automatically identifies an exposed S3 bucket containing customer records, applies the appropriate permissions, and notifies the security team—all without interrupting operations.

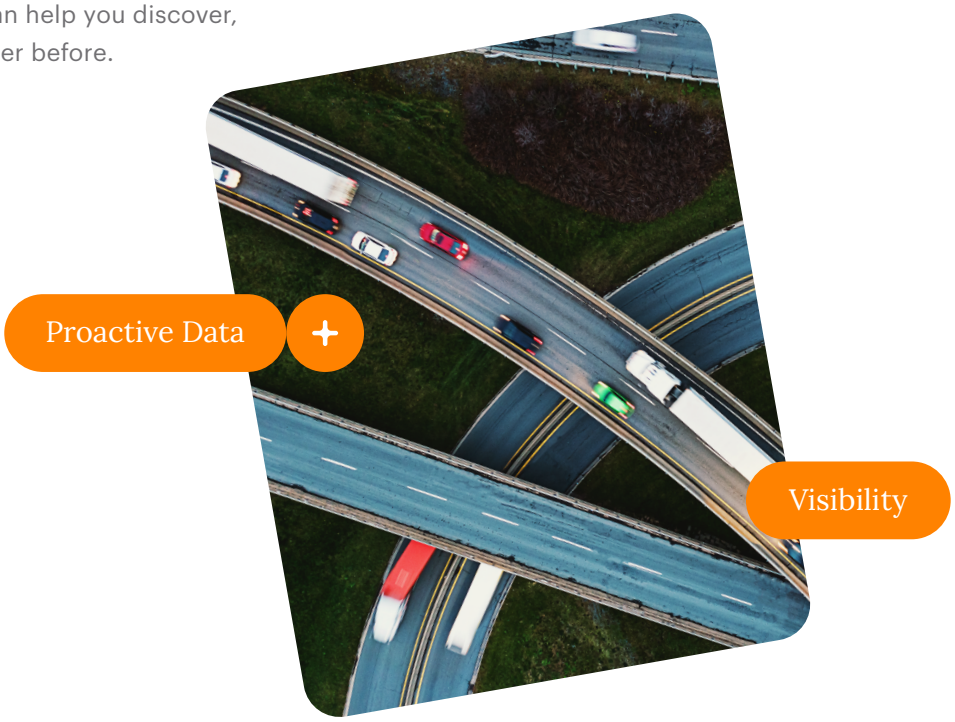
Netskope One DSPM addresses key use cases that help organizations maintain control, reduce risk, and ensure compliance, empowering security teams to stay ahead of evolving threats.

THE FUTURE OF DATA SECURITY STARTS WITH VISIBILITY

When moving into modern data security, from shadow data and misconfigurations to the risks inherent in AI innovation, one truth remains clear: effective data security starts with visibility. Without knowing where your data resides, how it's classified, and who can access it, you can't protect it.

Netskope One DSPM provides the foundation security teams need to take control of their data, wherever it lives. By combining comprehensive discovery, automated classification, access management, and real-time risk remediation, Netskope One DSPM goes beyond solving today's challenges to future-proof your data strategy. From ensuring compliance to protecting sensitive AI training data, our platform empowers organizations to stay ahead of emerging threats while confidently driving innovation.

Ready to see how Netskope One DSPM can uplevel your organization's data security? Request a meeting with us today, and let us show you how we can help you discover, secure, and govern your data like never before.



Interested in learning more?

Request a demo

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.