netskope

Whitepaper

Fixing the Broken Promise of Data Governance

Netskope One Data Security

TABLE OF CONTENTS

INTRODUCTION

Data drives the world. Competitive edge lies in how effectively enterprises manage, secure, and govern their data. Accenture says 70% of the world's most valuable corporations are data-driven, a significant leap from just 30% in 2008. However, as enterprises collect, store, and analyze increasing volumes of sensitive information, data governance programs often fail to deliver on their promise.

Data governance has devolved into a manual, disconnected, and reactive check-box exercise for many organizations. One financial services leader explained this frustration:

> "We've been up and down with data governance a few times in the past few years. There was a governance office. We 'check-boxed' our way through it, and it was ultimately seen as more of a barrier than a benefit."

Financial Services Enterprise, December 2024

This broken promise of data governance stems from outdated approaches that rely on manual processes, siloed teams, and periodic audits. Enterprises need a proactive solution that integrates and automates data security and governance into everyday workflows. This is where data security posture management (DSPM) serves to optimize data governance, ensuring that sensitive data is continuously monitored, assessed, and protected across its entire life cycle.

of the world's most valuable corporations are data driven, a significant leap from just 30% in 2008.

Accenture

First, What Is DSPM?

Data security posture management (DSPM) automates the core functions of data governance by providing real-time visibility and actionable insights across all environments: cloud, on-premises, and hybrid. It replaces manual, siloed governance practices with continuous monitoring and automated enforcement, enabling enterprises to:

- **Discover and classify** sensitive data across structured and unstructured formats
- **Assess and prioritize** security risks, including misconfigurations, excessive permissions, and policy drift
- **Enforce compliance** with regulatory frameworks such as GDPR, HIPAA, and PCI DSS
- **Continuously protect** data at rest and in motion and integrate it with existing security tools like DLP and CASB

In essence, DSPM provides the real-time insights and automation needed to operationalize data governance effectively.

> Traditional governance models often fail due to fragmentation, manual processes, and reactive policies.

Data Governance Policies: More Than Just Access Control

Many people—and many commercial software solutions, for that matter—tend to oversimplify the role of data governance in managing access control. For example they may:

- Determine what kind of data resides where via data classification
- Manage who has access to a specific database, schema, or table
- Manage what type of permission they have (read, read/write)

Next-gen access control solutions might also include self-service portals for employees to request access and obfuscated access, where employees can access data. However, specific fields are masked or tokenized on the fly.

Access control is a necessary bedrock of good data governance programs, but, at the same time, access control is insufficient on its own. Let's explore some other types of data governance policies that enterprises have and how those policies can often end up as well-intended pieces of paper on someone's desk that aren't actually enforced, i.e., they never get operationalized.

Examples of

DATA GOVERNANCE POLICIES	DATA PRESERVATION POLICIES
All databases should be backed up every day.	A cloud database isn't configured to be backed up.
All databases in Region A should be replicated to Region B.	The replication script fails and no one notices.
Data should be retained for 2 years, then archived.	Data is kept beyond the retention period.
All data warehouse clusters should reside in this account and region.	Data warehouse cluster created in the wrong account and/or wrong region.

DATA SECURITY POLICIES	
All data stores should be encrypted at rest.	A cloud database isn't configured to be encrypted.
All data stores should be inaccessible from the public internet.	An S3 bucket or MongoDB instance is accessible to the public.
All data should be replaced with synthetic data when being copied over.	Script fails, production data ends up in staging environment.
When an employee is terminated, all the employee's database usernames should be deprovisioned.	Database usernames need to be manually deprovisioned, and a username doesn't get deprovisioned.

If a user hasn't accessed sensitive data stores in the last 2 months, their permission should be reduced.	Once granted permission, users have permanent access to data stores.
Only Marketing personnel should be able to generate customer lists with more than 100 rows.	A customer success representative downloads a list of 50,000 customers.
All database usernames should map to a service account or an employee identity.	An unrecognized database username has activity and doesn't map to an employee identity or a service account.
Summer interns and high-risk employees should not have access to highly sensitive data.	Someone inadvertently copies sensitive data to a schema that all employees have access to, including summer interns and high-risk employees.
Customers should only be able to access their own data.	Customer A is able to access Customer B's S3 bucket.

COMPLIANCE & PRIVACY POLICIES	
Schema A should never have PII in it.	Someone inadvertently copies PII into Schema A.
Type A data should never reside in the same table as Type B data.	Someone inadvertently copies Type A data into a table with Type B data.
Type A and Type B data should never appear together in query results.	Someone inadvertently issues a query that accesses 2 different tables and joins Type A and Type B data with an anonymous but unique identifier.
Data from this dataset should never be stored in this set of countries..	A table from the dataset in question is copied into a data store that resides in a restricted country.

Data from this dataset should never be handled by employees from this set of countries.	An employee from a restricted country accesses that dataset.
We should always know where sensitive data is.	A day after a sensitive data audit is completed.
No employees should be able to violate the privacy of any of our customers.	An employee looks up the records of his/her ex.
No employees should make material changes to records in this dataset.	An employee deletes records in that dataset.
Any employee adds several records in that dataset.	An employee makes material edits to records in that dataset.

DATA MANAGEMENT POLICIES	
All field names should adhere to this naming convention.	Field names that don't follow the naming convention are added.
All data stores/sets should have a Data Owner assigned to them.	Data stores/sets exist that have no data owner assigned to them.
Data Owners should always be aware of any/all fields in their respective datasets.	50 new fields were added to a dataset last month, and the Data Owner is unaware of them.
All data stores/sets should have the following metadata associated with them: ...	Multiple data stores/sets have no metadata associated with them.

All fields classified as this sensitive data type should have the following tags/metadata associated with them: ...	Inconsistent tagging across fields that have the same sensitive data type.
Fields that are entirely synthetic data should not be marked as sensitive.	Fields containing synthetic data are marked as sensitive.
Whenever a Data Steward changes the classification of a field, the Data Owner should review that new classification.	Data Owner does not know when a field is reclassified.
When data is copied to a different location, the metadata associated with the data should be copied with it.	Data is copied, but metadata isn't, resulting in multiple (conflicting) sets of metadata for the same field.

How DSPM Modernizes Data Governance

Traditional governance models often fail due to fragmentation, manual processes, and reactive policies. Data security posture management (DSPM) offers an evolving solution that automates and integrates governance processes across teams and tools.

Fragmentation and Data Silos

As organizations expand, data becomes dispersed across various departments, systems, and environments—on-premises, cloud, and hybrid. This fragmentation leads to data silos, hindering a unified view of sensitive information and resulting in redundant or inconsistent datasets. Such silos impede effective decision-making and create inefficiencies.

How DSPM Helps:
DSPM provides a comprehensive view of data across all environments, eliminating silos and ensuring consistency and transparency.

Manual Audits and Lack of Real-Time Monitoring

Traditional data governance often relies on periodic audits and manual reviews, leaving sensitive data vulnerable between assessments. This approach allows vulnerabilities to go undetected until they escalate into breaches or compliance failures.

How DSPM Helps:
DSPM introduces continuous monitoring, enabling real-time detection and remediation of risks, thereby maintaining constant protection of sensitive data.

Reactive Policies and Unenforced Standards

Organizations tend to react to incidents rather than proactively mitigate risks with real-time monitoring. Governance policies may exist as guidelines without operational enforcement mechanisms, leading to data protection gaps.

How DSPM Helps:
DSPM reshapes governance from a reactive to a proactive approach by automating policy enforcement and integrating security configurations with regulatory standards, ensuring adherence and reducing risks.

Over-Permissioned and Unmanaged Access

Excessive or outdated permissions granted to employees, contractors, and third-party partners increase the risk of insider threats and unauthorized access. These gaps complicate compliance efforts and heighten the likelihood of breaches.

How DSPM Helps:
DSPM continuously monitors access controls, identifies over-permissioned users, and dynamically updates permissions to ensure data is accessed only by authorized individuals.

Unclear Ownership and Responsibility

Data governance responsibilities are often dispersed across security, compliance, IT, and other teams. This leads to confusion and inefficiencies, and the lack of clear accountability results in miscommunication and gaps in governance policies.

How DSPM Helps:
DSPM fosters collaboration among these teams by providing integrated workflows, assigning clear ownership, aligning efforts, and bridging governance gaps.

Shadow IT and Unmanaged Data Sources

Employees adopting unauthorized software or cloud solutions create unmanaged data stores that evade traditional governance processes. These rogue data sources increase the risk of breaches and noncompliance.

How DSPM Helps:
DSPM discovers and governs shadow IT, ensuring complete visibility into all data sources, whether authorized or not.

Data Classification Challenges

Enterprises often struggle with classifying and prioritizing sensitive data, especially unstructured formats like emails or shared documents. Organizations can't apply appropriate protections without effective classification, leaving high-risk data vulnerable.

How DSPM Helps:
DSPM automates data classification, accurately identifying sensitive information and enabling efficient application of protections.

Difficulty Scaling Governance

As enterprises grow, scaling governance frameworks across diverse systems, regions, and teams becomes challenging. Manually managed governance processes can't keep pace with expansion, leading to inconsistent policies and gaps in data protection.

How DSPM Helps:
DSPM provides a scalable governance framework that adapts seamlessly to the needs of enterprises.

Insufficient Integration with Security Tools

Governance tools tend to lack integration with critical security solutions like data loss prevention (DLP), security information and event management (SIEM), or cloud access security brokers (CASB). This disconnect creates gaps in enforcement, leaving sensitive data exposed across its life cycle.

How DSPM Helps:
DSPM integrates with existing security ecosystems, bridging these gaps and enabling end-to-end governance.

As demonstrated, DSPM effectively addresses critical data governance challenges, evolving from a mere security tool to a comprehensive solution that automates and streamlines governance processes. While DSPM significantly enhances data governance, integrating it with DLP solutions offers a more holistic approach to data security. DLP prevents unauthorized data access and transfer, complementing DSPM's capabilities. Together, they form a cohesive strategy that safeguards sensitive information throughout its life cycle.

"Better Together"—Why DLP and DSPM Are Complementary

DLP Enforces Protections: Building on the foundation DSPM provides, DLP acts as the frontline defense, monitoring, detecting, and preventing data from leaving secure environments. DLP provides immediate, real-time protection by reacting to the risks DSPM identifies, ensuring data is handled and accessed appropriately. Whether preventing unauthorized sharing or stopping a sensitive file from being uploaded to an unapproved platform, DLP enforces critical security measures where they're most needed.

DSPM Provides a Foundation: Consider DSPM setting the groundwork for data security. It locates sensitive data and identifies vulnerabilities that may be hiding across environments. With this foundational visibility and understanding, DLP could determine where the most critical risks exist or how data is stored. DSPM ensures organizations have a clear map of their sensitive data assets, enabling precise and effective security strategies.

Together, They Cover the Full Life Cycle: DLP and DSPM complement each other by covering the entire data security life cycle. DSPM focuses on securing data at rest—where it resides within storage systems—while DLP actively safeguards data in motion, ensuring protection as data is accessed, shared, or transferred. This comprehensive approach ensures that sensitive information remains protected at every stage of its life cycle.

Together, DLP and DSPM Deliver Comprehensive Data Security

Real-Time Prevention (DLP): With DSPM's insights, DLP becomes strategically positioned to monitor and control sensitive data movements. For instance, if a user attempts to send sensitive information to an unauthorized destination, DLP can intercept and block the activity in real time, preventing potential data breaches or compliance violations.

Visibility and Discovery (DSPM): DSPM identifies and classifies sensitive data across structured and unstructured forms, offering a clear, actionable map of critical data assets and associated risks. By enabling precise insights, DSPM empowers security teams to focus DLP efforts on protecting the most sensitive and high-risk data.

Continuous Security and Compliance: DLP and DSPM ensure an ongoing, proactive approach to compliance and security. DSPM maintains visibility into security configurations and highlights vulnerabilities, while DLP adds an immediate layer of protection to prevent intentional or accidental data loss. This dual capability is vital for maintaining regulatory compliance and reducing risks.

Tomorrow's Data Governance: Telling the Full Data Story

Data governance challenges, fragmented systems, manual processes, and reactive policies have left enterprises struggling to meet the demands of complex data environments. As data grows exponentially and regulatory requirements tighten, more than traditional approaches are needed to ensure visibility, control, and protection.

DLP and DSPM: A Unified Approach

DLP and DSPM represent the future of data governance. DSPM maps and monitors data vulnerabilities, giving organizations a clear understanding of where sensitive information resides and the risks it faces. At the same time, DLP actively prevents data leaks, safeguarding information as it's accessed, shared, or moved. Together, they provide an end-to-end solution for data security, covering both data at rest and in motion.

More Than Security: A Data Governance Strategy

This unification isn't just about protecting data; it's about rethinking data governance entirely. DSPM lays the foundation by identifying, classifying, and securing sensitive data, ensuring enterprises have visibility and control. DLP builds on this by enforcing protections in real time, preventing unauthorized access and data loss. Together, they enable proactive governance, aligning security, compliance, and operational efficiency in previously unattainable ways.

Unlocking the Full Potential of Your Data

By integrating DLP and DSPM into a unified strategy, organizations can move beyond simply reacting to threats. They can embrace a proactive, scalable approach that matures their data governance frameworks. This unified approach ensures regulatory compliance, mitigates risks before they escalate, and fosters trust with customers and stakeholders. Ultimately, DLP and DSPM empower organizations to tell the whole data story, managing and protecting their data environments while unlocking their true business potential.

The time for tomorrow's data governance is now. By adopting a unified, automated approach with Netskope One Data Security, enterprises can break free from outdated methods and turn governance into a competitive advantage. This isn't just about securing data; it's about enabling businesses to thrive in a data-driven world.

For more information, visit www.netskope.com.

Data governance challenges, fragmented systems, manual processes, and reactive policies have left enterprises struggling to meet the demands of complex data environments.

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.