Executive Guide to DSPM: Visibility and Control over Sensitive Data

Let's play a game of two truths and a lie.

> "Data never dies."
>
> "You can't protect what you don't know."
>
> "It's impossible to protect all your data."

If you guessed the last statement is false, you're correct. But just because protecting your data is possible doesn't mean it's easy. Data, ubiquitous and valuable, is also highly vulnerable to risk. The proliferation of devices and cloud applications, coupled with regulatory complexities, make safeguarding data more challenging than ever. Beyond the sheer volume of data, protecting what you don't know exists or where it's stored becomes a daunting task. The risk of leaks and regulatory penalties escalate for "shadow data" or "dark data" stored across multiple cloud service platforms, leaving organizations exposed. In a time in which data breaches carry severe financial and reputational consequences, ignorance is not bliss and not an option.

In truth, visibility is everything. Securing data starts with identifying and understanding what you have. Data Security Posture Management, or DSPM, is a category aiding security teams to discover, classify and prioritize sensitive data across their entire infrastructure, from on-premises servers to endpoints and multiple cloud platforms.

It provides information about where sensitive data is stored, who has access and how they are using it. Some emerging DSPM solutions also provide automation to make it easier to remediate the risks.

This guide explains why DSPM is crucial for identifying potential data and compliance risks and staying ahead of them. We'll also discuss the distinct advantages provided by Forcepoint DSPM, combining the proactive discovery of data issues with preventive controls that continuously adapt as part of Forcepoint's full-lifecycle "Data Security Everywhere" capabilities.

What Does Data Security Posture Management Do?

Simply explained, DSPM is a technology and a risk-assessment framework for sensitive data in an organization. Core DSPM capabilities include:

→ Data discovery

→ Data classification

→ Risk assessment for files

→ Access and permissions management

DSPM
RAPID IDENTIFICATION AND CLASSIFICATION
A
B

DSPM allows users to visualize:

→ **Where** sensitive data is stored

→ **How** the data is used

→ **What** the security posture of the data is

→ **Who** has access to the data

→ **When** the data will need to be purged

Understanding DSPM

At its core, DSPM revolves around gaining visibility and control over your data landscape to achieve data security governance. It assists organizations in taking a more strategic view of data by recognizing that data risk equates to business risk. DSPM locates and identifies regulated data like Personally Identifiable Information (PII) or health records stored across networked folders, cloud directories and devices.

A DSPM solution assesses and classifies data posing significant risk, enabling you to devise and implement manual or automated processes to mitigate those risks. For instance, it can identify Redundant, Obsolete or Trivial (ROT) files, improper permission settings or misplaced data in Platform- and Infrastructure-as-a-Service (PaaS and IaaS) environments.

Once you discover this information you can take corrective steps, like resetting user permission levels, deleting the file or relocating it. Some DSPMs can automate these security actions to a degree.

The key benefits of DSPM

- → **Reduce risk:** Prevent breaches by uncovering and rectifying sensitive data misuse.
- → **Streamline compliance:** Attain true visibility and control over sensitive data for efficient data governance.
- → **Increase productivity and reduce costs:** Facilitate faster, safer data access and sharing for better innovation and collaboration; and potentially save on cyber insurance costs.

Risk Reduction

DSPM uncovers hidden data risks across your cloud and on-perm environments, helping organizations to operate more safely and efficiently.

→ By categorizing data based on sensitivity and potential impact, businesses allocate resources efficiently, tackling the most critical threats first.

→ Comprehensive visibility and monitoring cover structured and unstructured data, including sensitive data like PII, PCI and HIPAA information, along with access controls.

→ Data breach prevention becomes a reality through identifying and correcting misplaced or unused sensitive data.

Harnessing Artificial Intelligence and Machine Learning

Forcepoint DSPM leverages AI and Machine Learning to swiftly and accurately classify data security risks, allowing you to mitigate issues before attackers can exploit them.

Visibility and control: Integral to Forcepoint's "Data Security Everywhere" solutions, Forcepoint DSPM proactively discovers data issues in concert with Forcepoint ONE Data Security and Risk-Adaptive Protection, providing data controls while dynamically adapting to user actions and risk levels. This comprehensive approach enables organizations to make informed decisions and combine proactive security actions with strong data protection.

AI-powered data discovery and data classification: An intuitive analytics dashboard provides granular visibility into data risk factors, from duplicates to ROT data and over-permissioned access. Forcepoint DSPM quickly pinpoints data across cloud and on-premises data storage locations. It can scan approximately 1 million files per hour from a single data source, powered by advanced AI-mesh and ML technology working together as a sophisticated neural network. The AI mesh comprises many large language models that train dozens of generative AI models in identifying potential data risks.

Forcepoint also provides intelligent, automatic classification based on sensitivity levels. The AI-boosted classification speed and accuracy allow teams to prioritize policy enforcement and incident response efforts effectively. The AI-driven classification engine also uses ML to continuously boost accuracy and reduce false positives and negatives. Users can also train the AI model to create custom classifications based on specific needs, such as distinguishing between valuable intellectual property and common office files.

Real-time monitoring and data risk assessment: Discovery scans evaluating critical data sets can provide real-time alerts on data risks, enabling efficient analysis and automatic risk-issue repair.

Safely use GenAI apps: Leverage GenAI apps such as ChatGPT Enterprise, Microsoft Co-Pilot, Google's Gemini, and others to increase productivity while reducing data risk. Forcepoint DSPM provides visibility into who is using ChatGPT Enterprise, what prompts they are submitting, which files are being uploaded, what risks those files might pose, and any data sovereignty issues.

Simplify Compliance

Business data often contains highly sensitive information, requiring compliance with global privacy regulations. Companies must promptly disclose breaches or face substantial financial and reputational penalties. DSPM mitigates non-compliance risks by expediting auditing for PII requests and providing reporting capabilities and access controls aligned with local laws and data governance.

Forcepoint Advantages

Forcepoint DSPM enables organizations to demonstrate compliance with confidence, with its built-in Compliance Hub, automated reporting, and – when used together with Forcepoint ONE Data Security – enforcement capabilities.

Simplified data governance: A centralized data view makes it easier to implement and enforce data governance policies. The DSPM Compliance Hub provides a step-by-step wizard to apply actionable settings such as data storage locations by region, specific industries and compliance standards.

Automated reporting: Generating compliance reports saves time and resources during audits. Dashboards offer at-a-glance details ranging from data sovereignty by geographic region to users with access to sensitive data. Users can easily build custom use cases and reports, such as ransomware exposure analysis and data incidents, without requiring coding knowledge.

Workflow orchestration: Defining ownership and accountability for different data sets and categories streamlines compliance stakeholder alignment. Easily define ownership and accountability for different data sets to streamline the process of gaining stakeholder alignment. This brings more efficient workflow around actions performed on each data source and asset.

Streamlined compliance: Using Forcepoint DSPM combined with Forcepoint ONE Data Security provides access to over 1,700 templates, classifiers and policies that accelerate compliance with privacy regulations in over 80 countries and 150 regions.

Increase Productivity and Cost Savings

DSPM solutions offer tangible benefits, enhancing productivity and cost savings. DSPM enables security teams to focus their efforts on strategic initiatives rather than repetitive manual processes. The emerging use of AI and ML can eliminate or greatly reduce manual steps and accelerate discovery and classification processes.

Forcepoint Advantages

Reduced time for discovery and classification: Automate and accelerate data discovery and classification using AI and ML, identifying about 1 million files an hour and eliminating slow and error-prone manual processes.

Simplified data access management: Clear visibility into data ownership and location streamlines access permissions, minimizing delays and frustrations for employees who require data to do their jobs.

Increase productivity: Safely use GenAI apps such as ChatGPT Enterprise, Microsoft Co-Pilot, Google's Gemini, and others to increase productivity while reducing data risk.

Optimized data storage: Reduce storage costs by discovering ROT data across your environments.

See it. Control it. Protect it.

DSPM is a strategic imperative for modern businesses and governments. By empowering organizations to see, control and protect sensitive data, DSPM solutions enable businesses to mitigate risks, streamline compliance efforts and drive productivity and cost savings. As data remains pivotal for innovation and growth, investing in robust DSPM solutions like Forcepoint DSPM is essential to safeguarding your data.

Forcepoint DSPM sets itself apart with its unique “Data Security Everywhere” approach, bringing visibility and enforcement together. With lightning-fast deployment capabilities and AI-powered automation, Forcepoint DSPM discovers data risks, while ensuring effortless regulatory compliance. From discovery and classification to workflow orchestration and policy enforcement, Forcepoint DSPM provides protection across the data lifecycle. That’s the secret to simplicity.

Get visibility and control over your data today.

Talk to an Expert

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of Wsensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[FP-Executive Guide to DSPM-Ebook] 24Jul2024