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, the lack of insight into your data risk makes it a more daunting task: “dark data,” data that is unused and usually unknown and “shadow data,” duplicates stored in multiple cloud services or SaaS applications, can leave your organization exposed. In a time in which data breaches carry severe financial and reputational consequences, ignorance is not bliss and not an option.

Visibility is everything. Securing data starts with identifying and understanding what you have. Data Security Posture Management, or DSPM, is a solution aiding security teams to discover, classify prioritize, and—when necessary—to remediate sensitive data. When packaged with Data Detection and Response (DDR), DSPM with DDR brings continuous monitoring of data risk which enables reporting insights that help security teams dynamically detect and remediate data risk, reducing the threat of data breaches and non-compliance.

It opens a window into the entire organization’s data posture, from on-prem to multiple cloud locations, revealing where sensitive data is stored and how it is creating risk of data breaches and non-compliance to privacy regulations.

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 and DDR, combining the proactive discovery of data risks and breaches 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 and classification
- → Compliance management
- → Risk assessment for files
- → File risk remediation

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 Protected Health Information (PHI) stored across networked folders, cloud directories and devices.

A DSPM solution assesses and classifies data posing significant risk, enabling you to devise and implement 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.

The key benefits of DSPM

→ **Reduce risk:** Decrease risk of data breaches through posture management.

→ **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; streamline time- and resource-consuming investigations and remediation; and potentially save on cyber insurance costs.

Understanding DDR

DDR offers continuous threat detection and dynamic responses, providing robust defense against potential data breaches. DDR is a technology that continuously monitors data repositories looking for risky data changes that could indicate potential data breaches. It also analyzes data for context, to see how data is being accessed, updated and changed.

Utilizing AI Mesh technology, DDR ensures optimal data context, unique data lineage tracking, and dynamic visibility across cloud and endpoints. Alongside DSPM, DDR allows organizations to go further to detect breaches, helping to protect your data, reduce financial losses and maintain customer trust.

Beyond detecting potential data breaches, DDR helps security teams to respond dynamically to threats. It stands apart from competitive solutions by providing data context visibility and lineage tracking for unstructured data to ensure visibility in cloud environments.

The key benefits of DDR

→ **Reduce risk:** Continuous identification, monitoring, and response to potential data breaches.

→ **Streamline compliance:** Extensive visibility across cloud and endpoints to ensure data protection.

→ **Increase productivity:** AI Mesh helps optimize data context and reduce false positives when identifying potential data threats, helping security teams to focus resources.

How DSPM and DDR Work Together

Where DPSM provides a snapshot of your organization's data posture, DDR offers an ongoing view of data as it changes over time.

DSPM provides visibility to your organization's data through discovery, classification and prioritization of sensitive data. It also helps with remediation by removing or fixing risky data across cloud and endpoints. With DSPM, robust discovery and consistent classification are key—and that needs to occur across your organization's infrastructure including endpoints and cloud environments.

DDR works within the context of data-in-use. It actively monitors infrastructure to understand data as it changes, including how it's changing, permissions access and where it's being stored, copied or moved. Data context adds a new level of dynamic visibility, building on the data foundation supplied by DSPM. This dynamic visibility paves the way for data threat detection, allowing security teams to focus resources on the response part of the equation.

Ultimately, DSPM and DDR work together to provide a comprehensive view of your organization's data—both while it's at rest or while it's in use.

Risk Reduction

DSPM not only uncovers hidden data risks but also offers insights to prioritize remediation effectively. This helps organizations to run more safely and efficiently in multiple ways:

- By categorizing data based on sensitivity and potential impact, businesses allocate resources efficiently, tackling the most critical threats first.
- Comprehensive visibility and monitoring into sensitive data like PII, PCI and HIPAA information, along with access controls.
- Data breach prevention becomes a reality through identifying and remediating data that brings risk to the organization.

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 while DDR continuously monitors data in use—providing comprehensive visibility even while data is changing. Forcepoint DLP and Risk-Adaptive Protection add data controls that dynamically adapt 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 classification: At the heart of Forcepoint DSPM lies the AI Mesh, a highly networked classification architecture that uses a GenAI Small Language Model (SLM). The AI Mesh determines whether a piece of data is sensitive and/or critical based on AI classifiers and data science capabilities. These include deep neural network classifiers for sentiment analysis, light AI classifiers such as Bag of Words for determining topics, Bayesian Inference for predictive modeling of text and regex filters to delineate what text is classifiable. GenAI SLMs are nimbler and more efficient than LLMs, providing low-latency capabilities at a fraction of the resources their larger counterparts require.

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.

1/3

of breaches involve shadow data

IBM Cost of a Data Breach Report 2024

Simplify Compliance

Business data often contains highly sensitive information, requiring compliance with global privacy regulations. Maintaining a complete data posture that is in compliance with global privacy regulations like GDPR, CCPA and others can be incredibly complex and resource-intensive. These regulations require organizations to have a clear understanding of where sensitive data is stored, how it is processed and who has access to it.

137 out of 194

71% of countries have some form of legislation

Forcepoint Advantages

Forcepoint DSPM transforms the daunting task of maintaining compliance into a manageable process, empowering organizations to handle their data more efficiently and significantly reduce the risk of regulatory fines and breaches. This innovative solution is crafted to support organizations in adhering to privacy regulations through several essential features.

Automated Data Discovery and AI Classification: It uses an AI Mesh to automatically locate and categorize sensitive data across various environments, ensuring that all data is accounted for and managed according to regulatory standards.

Scheduled Scans and Alerts: The platform runs scans as frequently as needed, providing alerts based on the scan results. This flexibility allows organizations to build a secure data posture for compliance while also staying updated on their data compliance status as data changes without incurring additional charges.

Customizable Compliance Reporting: Forcepoint DSPM generates detailed, customizable reports that demonstrate compliance with specific regulations like GDPR and CCPA. These reports are essential for audits and can be tailored to meet the unique needs of different regulatory bodies.

Enforcement of Data Governance Policies: The platform allows organizations to enforce data governance policies consistently across all data assets and data locations from on-prem to multiple cloud locations. This ensures that data handling practices are aligned with regulatory requirements, reducing the risk of non-compliance.

Augment scans with Continuous Monitoring: As a DSPM add-on, Forcepoint DDR provides ongoing threat detection by dynamically monitoring your organization's data between scheduled DSPM scans. DDR actively monitors, scans and classifies data while it is in use.

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.

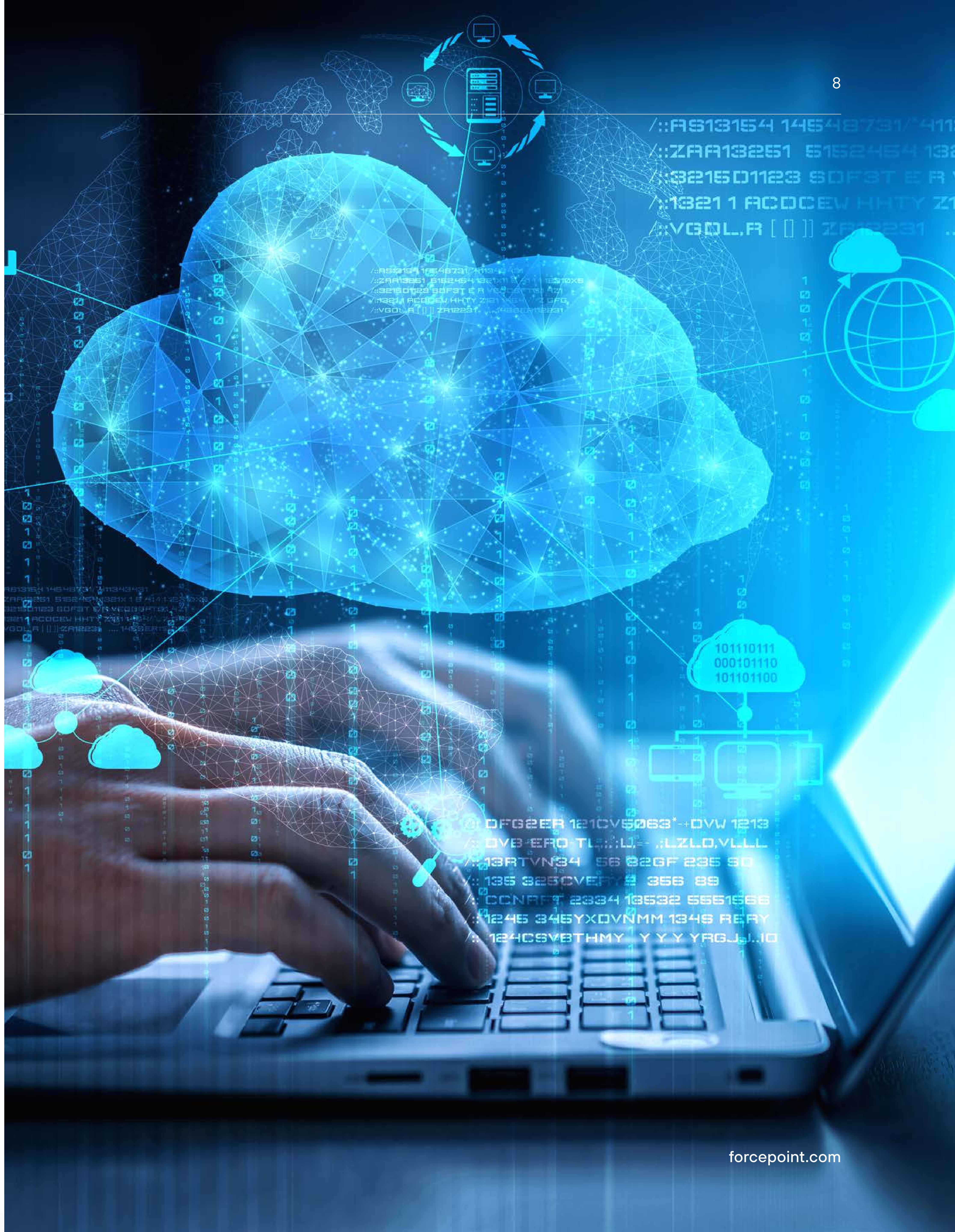
Forcepoint Advantages

Reduced time finding and classifying data: Automating data discovery and classification using AI and machine learning eliminates manual processes that can be slow and error-prone.

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.

Improved data security posture: Proactive identification and remediation of data security risks prevent costly breaches.

Optimized data storage: Automatically locate and remove ROT data, reducing storage costs.



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 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 deployment capabilities and AI-powered automation, Forcepoint DSPM stays ahead of emerging threats, while ensuring effortless regulatory compliance. From discovery and classification to automated remediation and policy enforcement, Forcepoint DSPM provides protection across the data lifecycle.

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, X and LinkedIn.

[FP-Executive Guide to DSPM-Ebook] 14Mar2025