Forcepoint DSPM

Powered by GetVisibility

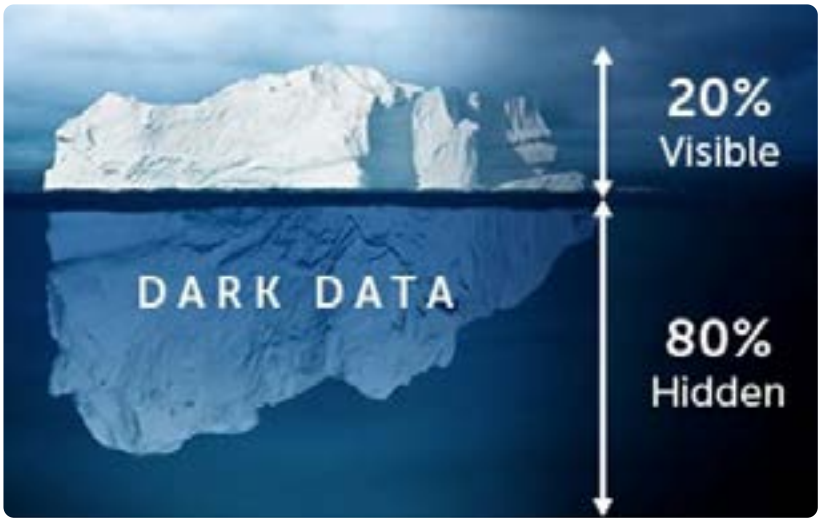
Forcepoint

Brochure

See. Secure. Simplify. Your complete data landscape.

Is your data at risk of crippling your business?

In today's digital world, protecting your organization's sensitive data is crucial. Data breaches and privacy regulation non-compliance can literally cripple your business. Both can be very costly in terms of fines, customer trust and even the ability to continue to do business. In recent years with digitalization and the growth of cloud applications and cloud storage, organizations are continuously constructing massive data ecosystems, housing diverse data types that include large amounts of sensitive information. Data today for most organizations is like a giant iceberg where the majority of the data is hidden. This is often described as "dark data" or "shadow data." It's unseen and unknown, yet it contains large amounts of sensitive information that organizations are directly responsible for. It's estimated that for most organizations approximately 80% of their data falls into this area of dark data.



DSPM (Data Security Posture Management) offers a comprehensive approach to securing your information from unauthorized access, disclosure, alteration or data destruction. Unlike other types of data security methods that focus on systems and devices, DSPM focuses on the entirety of an organization's data itself, ensuring compliance and mitigating the risk of data breaches.

According to IDC, 80% of data globally is unstructured and 90% of that data is not analyzed, also referred to as "dark data"[1]

94% of organizations are storing data in multiple cloud environments.[2]

Equifax settle a $1.4B lawsuit for its data breach[3] exacerbated by hackers accessing a shared drive storing multiple copies of employee usernames and passwords. The company lacked tools to detect and identify redundant and outdated files.

1 The Unseen Data Conundrum, Forbes, February 2022

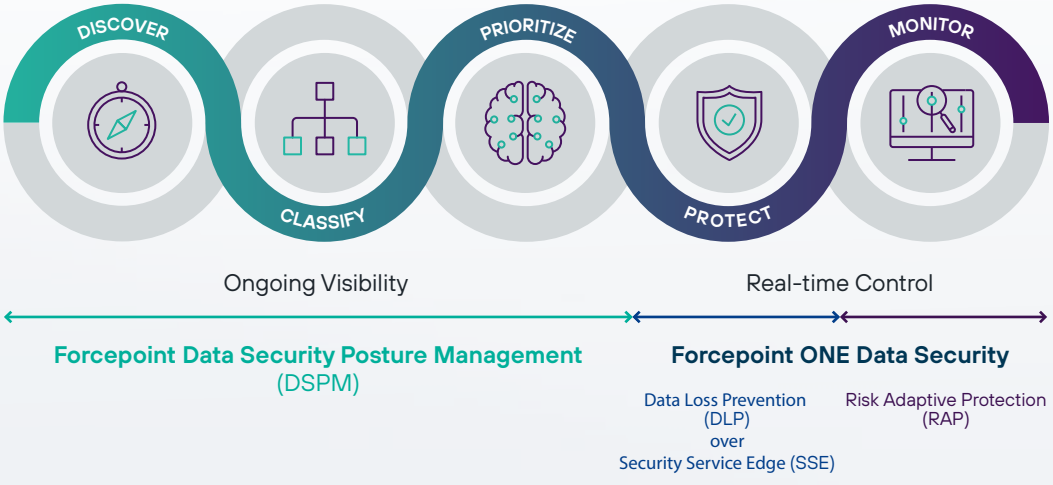
2 Dark Data: The Cloud's Unknown Security and Privacy Risk, Forbes, June 2023

3 Equifax agrees $1.38bn data breach lawsuit settlement, Finextra, January 2020

What does DSPM address?

- **Identifying sensitive data:** DSPM helps organizations identify sensitive data across multiple cloud environments and services as well as on-prem locations. This includes understanding where sensitive data resides, how it's accessed and who has permissions to interact with it.
- **Assessing vulnerability and risk:** DSPM assesses the vulnerability of sensitive data to security threats and the risk of regulatory non-compliance. By analyzing the security posture of data, organizations can proactively address potential risks.
- **Focusing on data at the source:** Unlike other data security tools that primarily secure devices, systems and applications, DSPM focuses directly on protecting the entirety of an organization's data. It aims to prevent data breaches and ensure compliance by securing the data at its core.
- **Addressing dark data and ROT data:** DSPM directly addresses dark data (data currently not seen or used in normal business processes). Similarly, DSPM can address ROT (redundant, outdated and trivial) data that also tends to proliferate across organizations as companies continue to hold on to large amounts of data for various reasons, thinking it will help them stay compliant. It actually creates even greater data risk, and DSPM helps manage this risk.
- **Addresses over-permissioned/over-exposed data:** Due to the way data proliferates through copying and editing new versions of data, permissions to data can often also explode into users, groups, and even to the entire organization. DSPM helps to enforce the "principle of least privilege" Zero Trust concept that dramatically reduces over-permissioned data as a way of preventing data breaches.
- **Multi-cloud and hybrid cloud environments:** As organizations adopt multi-cloud and hybrid cloud environments, the risk of data breaches increases dramatically. DSPM provides visibility and control over sensitive data across these diverse computing environments in addition to on-prem locations.

Forcepoint DSPM is designed for the modern organization that needs strong visibility and control of their business data. It provides visibility throughout their various cloud environments and servers to prevent data breaches and reduce the risk of non-compliance with privacy regulations. Forcepoint delivers full visibility and control across the data lifecycle, providing Data Security Everywhere by combining **proactive discovery of data risk** (DSPM) with **active controls over how data is used** (DLP and SSE) while **continuously adapting to each user's actions** (Risk-Adaptive Protection).



Unify visibility and control over your data landscape with Forcepoint DSPM

Managing and securing your organization's data has never been more complex. Forcepoint DSPM offers a powerful solution to gain comprehensive visibility and control over your data, regardless of location. With industry-leading discovery speeds, advanced AI-powered data classification and automated remediation capabilities, Forcepoint DSPM empowers you to make informed decisions about your data security posture and proactively address potential risks.

Key benefits of Forcepoint DSPM include:

Fast, comprehensive discovery: Across multiple clouds and on-prem, Forcepoint DSPM is able to scan 300 files per second, equivalent to approximately 1 million files per hour. It's not uncommon for organizations to have many terabytes and even some have petabytes of data they are responsible for. With this high-performance discovery, Forcepoint enables organizations to get a quick view of data across a massive data landscape. Unlike other DSPM providers, Forcepoint doesn't charge for discovery runs – customers can run discovery as often as they like with no additional charges.

AI-powered accuracy: Forcepoint DSPM discovers data across cloud and network sources and automatically classifies that data, utilizing an advanced AI classification engine. This engine has a massive number of dimensions, utilizing GenAI for training with synthetic data. There is a series of domain-specific GenAI models focused on different industries that collectively feed into the larger cloud model, creating what is called an "AI Mesh." In addition, specialized on-prem AI models are deployed for individual organizations that can then use machine learning (ML) to continuously boost its accuracy. Ultimately this high accuracy has enabled organizations that had trouble with other popular classification methods to dramatically reduce false positives/negatives, successfully protecting their intellectual property and saving large amounts in terms of time and resources.

Data visibility across your data landscape: Forcepoint DSPM allows you to inspect permissions for all files and users. Data admins can see which individuals have access to a file or fileshares across the organization. With a single click, you can immediately view permissions for all files that are scanned. Forcepoint DSPM provides reports in real time along with a dashboard with extensive details giving a birds-eye view into dark data, as well as providing an overview data risk assessment to help you understand the areas of highest data risk.

Automated remediation: As discovery and classification are occurring, Forcepoint DSPM can automate remediation in order to reduce data risk in real time. Forcepoint brings both manual and automated remediation for deduping, repairing of data permissions, and quarantining and moving files to correct locations from within the solution. It can also show incident alerts which can then be drilled down and inspected for further action.

Workflow orchestration: Easily define ownership and accountability for different data sets to streamline the process of gaining stakeholder alignment. This enables more efficient workflows around actions performed on each data source and asset. Effective remediation requires broad buy-in and collaboration beyond the security organization to the CDO/DataOps group as well as functions such as marketing, finance, DevOps and many others. Forcepoint DSPM looks at securing data posture not merely as a security issue but as a business priority. By designating data stakeholders and coordinating remediation rules with stakeholders, remediation can truly be successful.

Don’t let data risk cripple your business. Forcepoint can help!

In today’s digital age, data is an organization’s most valuable asset, but it can also be a significant liability if not properly managed. Forcepoint DSPM offers a proactive approach to securing your sensitive data, mitigating the risks of data breaches and ensuring regulatory compliance. By implementing Forcepoint DSPM, you can gain comprehensive visibility into your data landscape, identify and address vulnerabilities and proactively protect your organization from the financial and reputational damage caused by data breaches and regulatory non-compliance. Take control of your data security posture today. Start exploring how DSPM can safeguard your valuable information. Go to www.forcepoint.com/dspm to request a demo, or sign up for a free data risk assessment in which a security engineer can provide you a sample run of your own data to see what types of data risk you are facing right now.

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 sensitive 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-DSPM-Brochure] 16May2024