Forcepoint DSPM



Forcepoint

Brochure

AI Transformation Is the Next Evolution of Digital Transformation

Is your data safe in this new era?

Organizations across industries are grappling with AI transformation spurred by the promise of drastically increasing productivity. This AI enhanced era is marked by initiatives to onboard enterprise AI services, manage unsanctioned AI use, and mitigate risks associated with agentic AI activity. Across the board a key priority underpinning these efforts is visibility and control of how sensitive data is used. However, practically every organization struggles to gain consistent visibility, let alone control, of their data at scale. It is like an iceberg, where we only see a small fraction at the surface, with the vast majority imperceptible below the surface. This is often referred to as "dark data," it remains unseen and unknown, yet contains substantial amounts of sensitive information for which organization bear direct responsibility. Now, organizations are trying to figure out how to enable users to safely leverage AI while ensuring the protection of their sensitive data, but AI use itself is making the problem worse as it helps to create more data at unprecedented speed.



Data Security Posture Management (DSPM) 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 specific applications and devices, DSPM can see and control the entirety of an organization's data, whether in the cloud or on private networks, ensuring compliance and mitigating the risk of data breaches.



Share of organizations that reported an AI-related breach and lacked proper AI access controls[1]



Cost savings from extensive use of AI in security operations
Security teams extensively using AI and automation shortened their breach times by 65 days and lowered their average costs by USD 1.93 million compared to those that didn't use these solutions[1].



AT&T agreed to a $177 million class-action settlement tied to two 2024 breaches. The first breach exposed data including Social Security numbers for 73 million current and former customers, and the second involved unauthorized access to a workspace containing sensitive customer information sitting in a cloud environment without adequate monitoring[2].

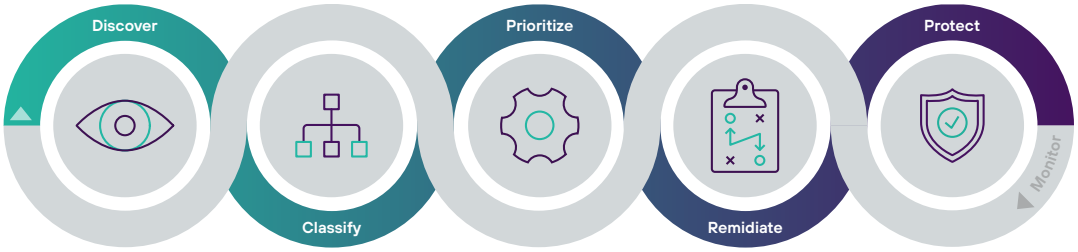
1 IBM's Cost of a Data Breach Report 2026
2 Top Class Actions **AT&T data breach class action settlement**

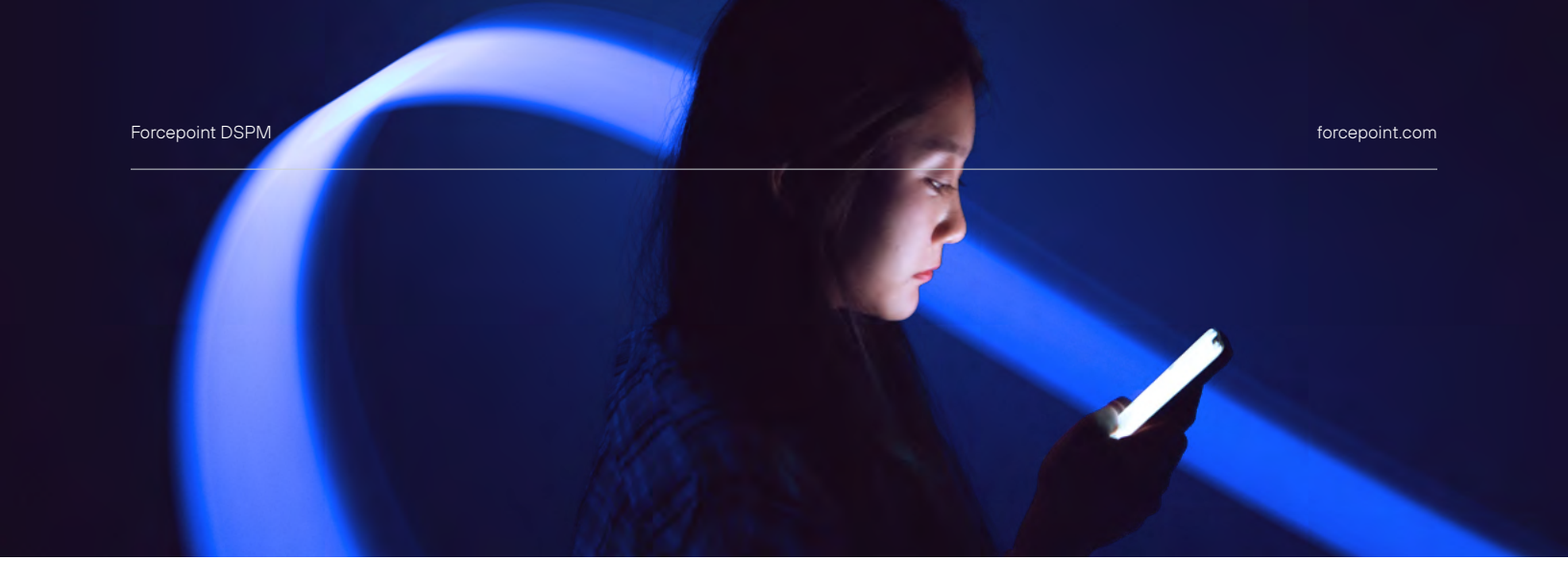
What does DSPM address?

- **AI transformation journey:** Unleash AI's potential with Forcepoint DSPM, safeguarding your data everywhere with our advanced AI Mesh technology. With centralized visibility and remediation from Forcepoint DSPM and real-time blocking controls from Forcepoint DLP, we secure your sensitive information across key channels including GenAI apps like ChatGPT, Copilot, Gemini, and many others— empowering bold innovation while boosting productivity and reducing risk.
- **Identifying sensitive data:** DSPM helps organizations identify sensitive data across multiple cloud environments and services as well as on-prem locations, including both structured and unstructured data. 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.
- **Continuous risk monitoring:** Forcepoint Data Detection and Response (DDR) add-on enables Forcepoint DSPM to detect and remediate new data risks as they are happening. No need to wait for the next complete DSPM scan, dynamically identify risks to your data security posture to remediate.

Forcepoint DSPM is designed for the modern organization that needs strong visibility and control of their sensitive data. It provides visibility throughout 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) **while continuously adapting to each user's actions** (Risk-Adaptive Protection). Gain dynamic discovery of data risk with continuous monitoring (Forcepoint DDR) to prevent data breaches and protect your data security posture.

AI-powered discovery, classification, orchestration





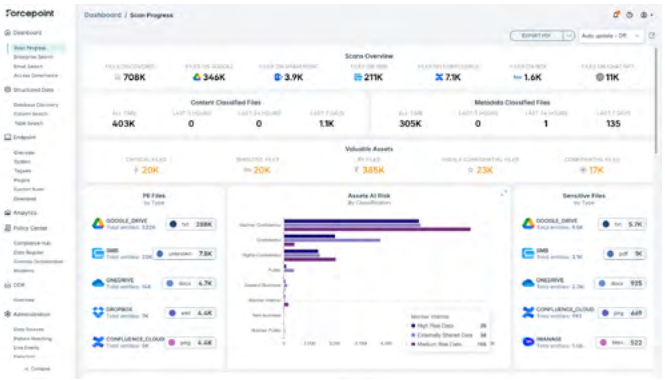
Unify visibility and control over your data landscape with Forcepoint DSPM

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 data classification using full content inspection powered by Forcepoint's AI Mesh and advanced DLP classifiers, 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: Forcepoint DSPM delivers rapid, high-performance scanning of files and databases across multi-cloud and on-premises environments, performing full content inspection rather than relying on simple metadata tagging or sampling-only approaches. This depth of analysis ensures sensitive data is accurately identified, not merely estimated. Forcepoint's high-performance discovery and classification enables organizations to gain rapid, comprehensive visibility into their data landscape at scale, spanning structured and unstructured repositories alike, including data residing in generative AI platforms such as ChatGPT Enterprise, Anthropic Claude, and Microsoft Copilot to help security teams stay ahead of emerging AI-driven data exposure risks.

AI Mesh enabled accuracy: Forcepoint DSPM discovers data across cloud and network sources and automatically classifies that data, utilizing an advanced AI classification engine. Forcepoint DSPM's AI Mesh empowers organizations with superior data classification accuracy. Its networked AI architecture, leveraging a GenAI Small Language Model (SLM) and Forcepoint's long trusted, curated DLP classifiers, efficiently captures context from unstructured text. Customizable and efficient, it ensures rapid, accurate classification without extensive training, enhancing trust and compliance. 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 files and databases across the organization. With a single click, you can immediately view permissions for all files that are scanned. Forcepoint DSPM provides 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.

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/Governance, Risk and Compliance (GRC) 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.

Forcepoint DDR: A powerful add-on to Forcepoint DSPM, is a key solution for addressing data breaches. It provides continuous threat detection and enhanced data risk visibility, ensuring that organizations can effectively see changes to data that are likely leading to data breaches as they are potentially happening. By leveraging AI-driven responses, Forcepoint DDR offers precise threat neutralization, helping organizations maintain robust security measures. Its extensive visibility across cloud and endpoints, combined with data lineage tracking, makes it an essential tool for safeguarding sensitive information, reducing financial losses, and maintaining customer trust.



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, all while securing your data in GenAI applications. 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.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint enables Self-Aware Data Security, an AI-native approach that helps enterprises and governments know their data everywhere, adapt to evolving risks and regulations in real-time, and protect at scale with a unified, single-policy framework. 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, LinkedIn, Instagram and YouTube.

©2026 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.
[FP-DSPM-Brochure-EN] 21Aug2026