proofpoint.

SOLUTION BRIEF

Data Security Posture Management

Securing your data ... wherever it is.

Addressing complexity

- Visibility and control

The explosion of data

The rise of AI platforms, Databases as a Service (DBaaS), and Continuous Integration/Continuous Development (CI/CD) practices has created complex, interconnected data landscapes and ever-growing data sprawl across cloud and hybrid environments. The pace of technological change has caused security teams to lose visibility into their most valuable and sensitive data. This lack of visibility creates regulatory compliance challenges and leaves organizations more vulnerable to attacks. Even with multitudes of security tools available, data breaches happen every day, proving that traditional security methods are no longer enough.

Human-centric risk

The risks from data visibility gaps are compounded when organizations don't have a clear understanding of which insiders have access to their critical data. In an effort to streamline workflows, insiders often create and use unauthorized data repositories, unapproved tools, and insecure data-sharing practices. At the same time, over-privileged accounts and system misconfigurations further increase vulnerability to cyber-attacks. Overburdened security and data teams may skip critical steps, such as classifying data before training AI models, inadvertently exposing sensitive information to unnecessary risks, a situation often worsened by development teams prioritizing speed over security.

Get visibility and control

Proofpoint Data Security Posture Management (DSPM) addresses the root cause of many breaches—blind spots in data environments—while prioritizing the reduction of human-centric risks in data security. By identifying where sensitive and valuable data resides and who has access, DSPM empowers security teams to close gaps and reduce the attack surface.

The solution excels in discovering and classifying data stores, prioritizing critical information, identifying risky and excessive access, detecting and remediating exposure risks, and streamlining compliance and auditing processes.

This solution set is part of Proofpoint's integrated Human-Centric Security platform, mitigating the four key areas of people-based risks.

$10.5T

The cost of cyberattacks on the global economy, by the end of 2024

83%

The percent of organizations that have experienced at least one breach related to access issues

Source: https://www.pingsafe.com/blog/cloud-security-statistics/

$4.35M

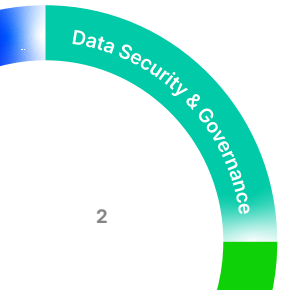
The average cost of a data breach—with public cloud breaches costing more

Central to the solution is the AI-powered agentless scanner, which accurately identifies and classifies valuable and sensitive data at scale across diverse environments with unparalleled speed and accuracy.

DSPM maps attack paths that could lead to breaches or data loss, illustrates how people and resources access data, and prioritizes risks by assigning monetary value to data. Results are presented through intuitive, real-time visualizations. Actionable insights and guided remediations integrate with alerts into service management platforms and help reduce attack surface such as over-permissioned access.

DSPM lowers operational costs by streamlining compliance across 500+ benchmarks and discovering forgotten data. Data discovery, classification, and risk prioritization capabilities inform and enhance existing security tools like Proofpoint DLP.

The solution ensures AI models use or train with the right data, enabling safe adoption and increased business agility. DSPM addresses the unique risks of AI-driven environments and secures data pipelines connected to LLMs like ChatGPT, Microsoft Copilot, and Amazon Bedrock.



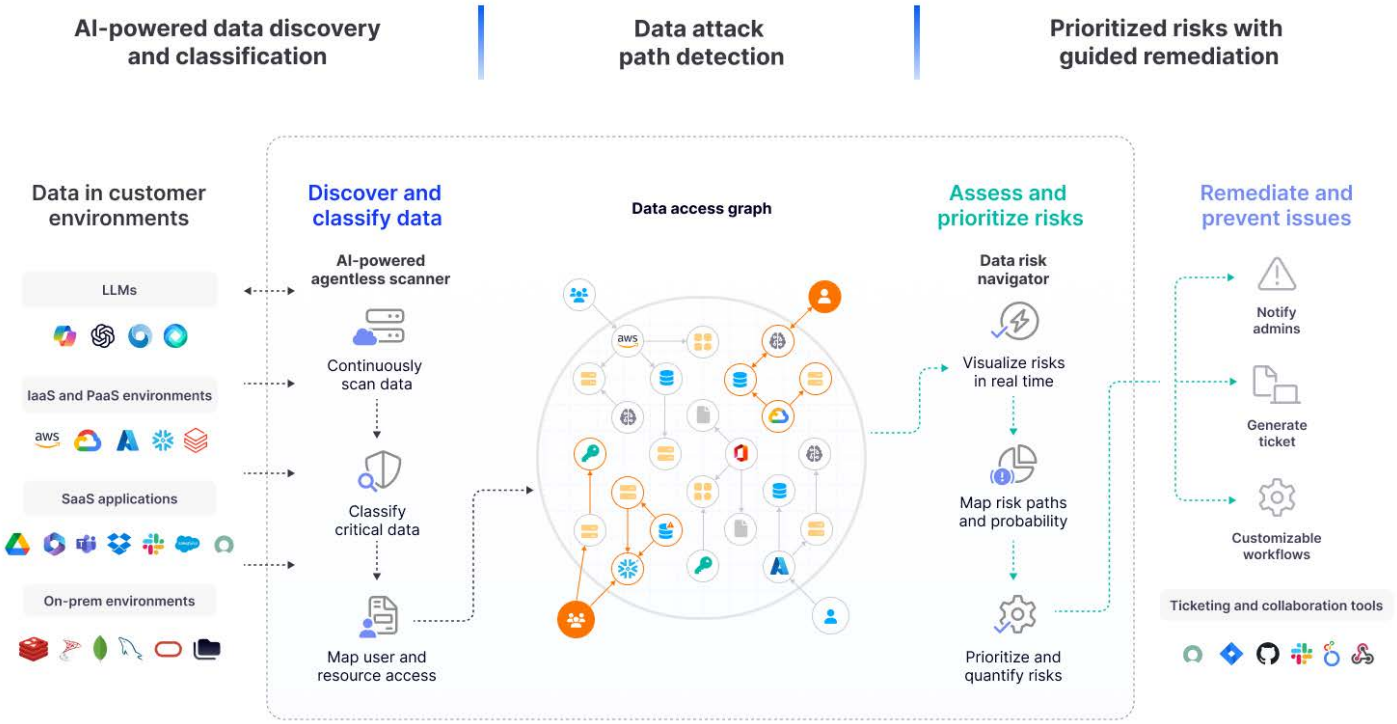
Unique capabilities

- Data context
- Data access governance
- Prioritized remediation

Unique capabilities

As shown below, DSPM enhances defenses by delivering clear and full visibility into valuable and sensitive data across SaaS, PaaS, public or multi-cloud, on-premises and hybrid environments and LLMs with the AI-powered agentless scanner. Data access graphs strengthen security further by reducing human-centric risks with least privilege enforcement and comprehensive data access governance. The data risk navigator analyzes data sensitivity, access patterns, and risk exposure to prioritize remediation based on data value and risk likelihood, helping teams protect critical data while reducing costs and shrinking the attack surface through optimized storage practices.

Proofpoint DSPM



Key Benefits

- Data visibility at scale
- Industry-leading accuracy

Discover and classify data

DSPM continuously discovers new data stores as they are instantiated across your distributed infrastructure. Our unique cloud orchestration architecture scans all entities in a single pass, making it more efficient than other tools.

Using the AI-powered and agentless scanner, DSPM delivers the most accurate classification of data in the market, employing a hybrid approach of regular expressions, natural language processing and large language models that optimizes performance and minimizes resource usage. Optical Character Recognition (OCR) ensures that non-digital assets like PDFs are properly classified before being stored and used.

Support for Microsoft Information Protection (MIP) sensitivity labels enables teams to enforce data governance policies, ensure compliance, and safeguard information against unauthorized access or misuse across Microsoft environments.

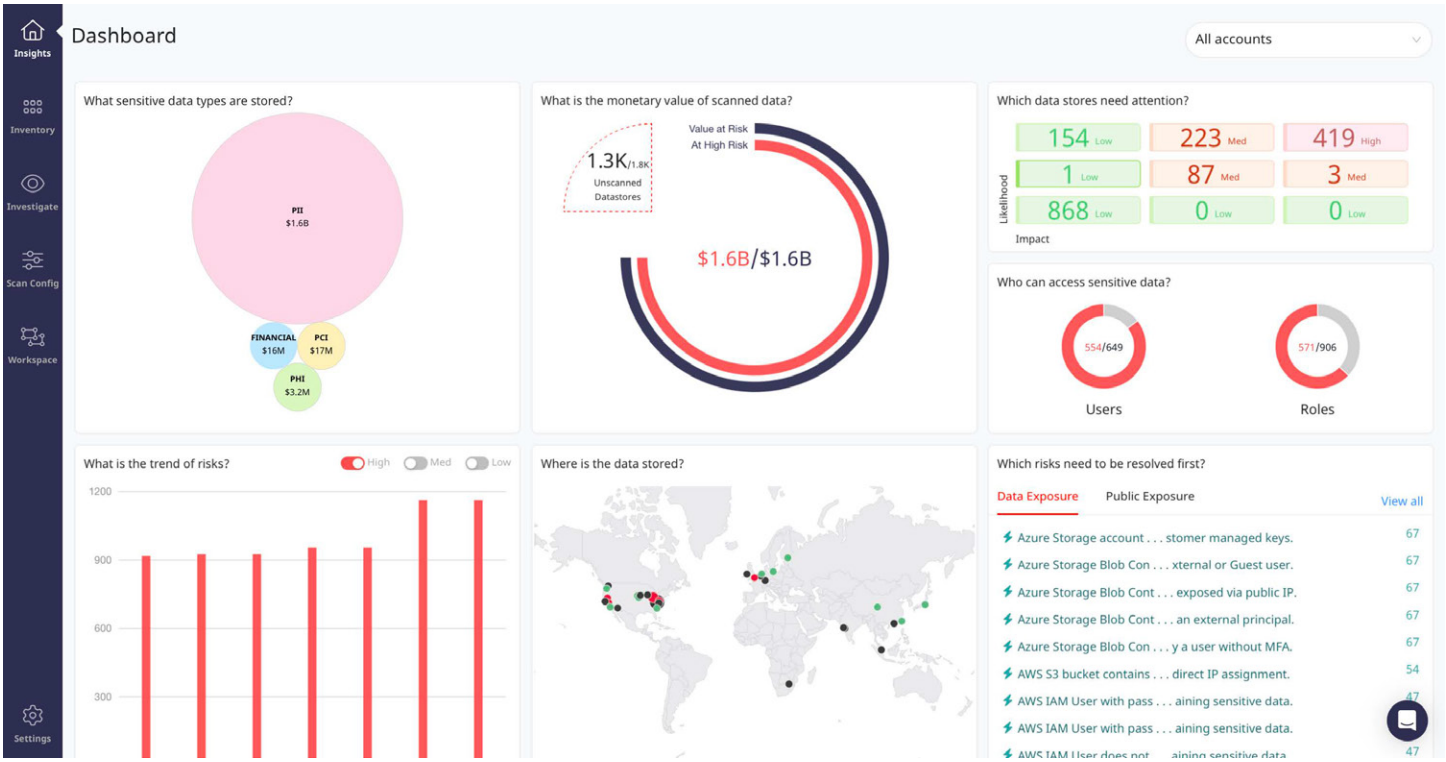


Figure 1: DSPM dashboard highlighting the types of valuable or sensitive data, its monetary value, its risk, and who can access it

Key benefits

- Prioritization of high-value data stores
- Reduced storage costs
- Reduced attack surface

Prioritize data stores

Data security teams constantly grapple with the huge number of data stores that they need to protect while realizing that not all data stores are created equal. Using unique data valuator technology, DSPM estimates the cost of breach for each data store, helping teams prioritize their security efforts around what matters most. Combined with insights about access and exposure risks, the robust risk matrix allows teams to focus on data stores that carry both a higher likelihood of risk and higher financial impact to the organization if breached.

DSPM identifies and eliminates unnecessary data stores, such as shadow, duplicate, and abandoned data, including stale backups and snapshots. This process reduces storage costs, shrinks the attack surface, and streamlines data management by ensuring only relevant, actively used data is maintained, ultimately enhancing security and optimizing storage practices.

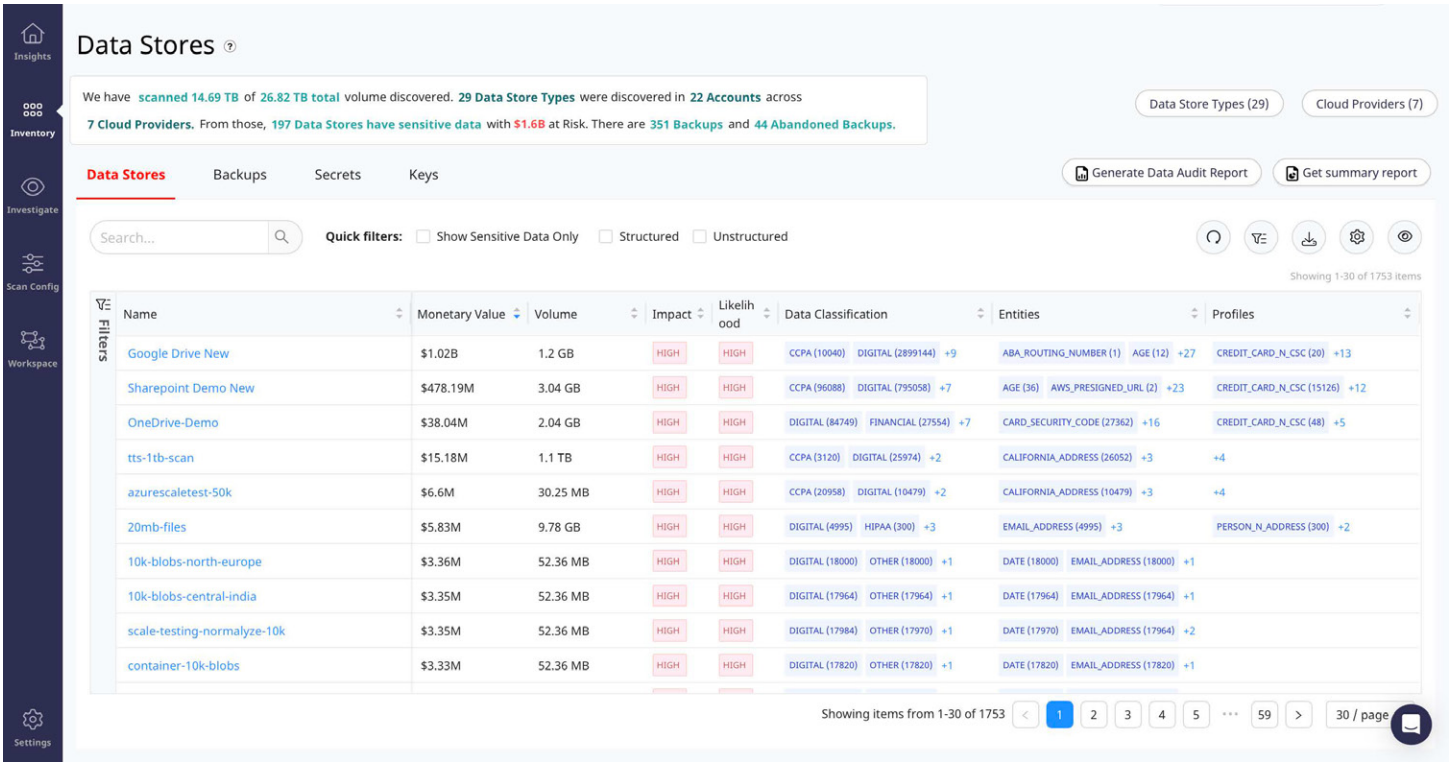


Figure 2: Data stores by monetary value and impact and likelihood of risks

Key benefits

- Reduced human-centric risk
- Zero Trust enablement

Least privilege access

DSPM supports least privilege access by identifying over-permissioned users and unused access across data stores, supporting comprehensive data access governance and forming the foundation for a Zero Trust model.

By analyzing IAM roles, permissions, database grants and other access controls for user and machine identities in near real time, DSPM quickly identifies who has what type of access to a given data store and visualizes those insights in data access graphs. By analyzing access logs, DSPM can conclude who is and who isn't making use of the permissions they have. Security and data teams can then quickly determine a large portion of user and machine identities that have permissions to access valuable or sensitive data but don't really need it. By removing those accesses, teams can achieve least privilege access to data and reduce potential attack surface.

Additionally, DSPM flags under-protected users and accounts across SaaS and PaaS apps, such as users with access to sensitive data who don't have MFA enabled or have been inactive more than 90 days; and accounts with more than 10 admin users.

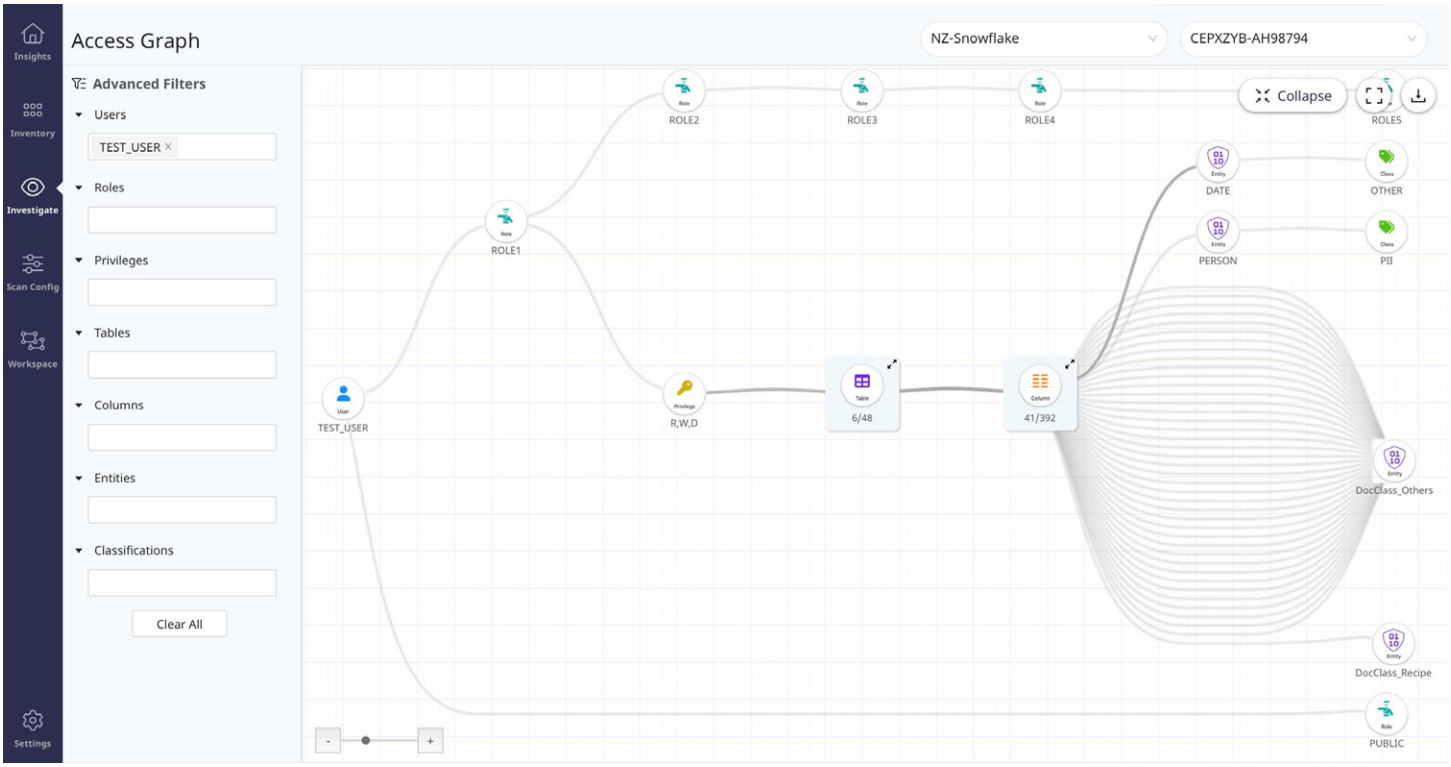


Figure 3: Users and roles with access to valuable or sensitive data

Key benefits

- Risk visualization and prioritization
- Faster remediation response times

Attack path detection

DSPM collects information about all compute resources, networking resources, and PaaS and SaaS services within the cloud provider and detects misconfigurations and vulnerabilities present in each of these resources. Organized as a graph within the solution, this information allows users to understand the paths a potential attacker could take to access sensitive data. By operating on a continuous, near real-time basis, the solution quickly detects changes that could increase data exposure. Detailed insights into data sensitivity, access patterns, and risk exposure enhance traditional DLP and DDR tools.

Guided remediation

Actionable insights and comprehensive recommendations for identified risks make it easy for the appropriate team to take action quickly. For example, risk in SaaS apps is reduced with the ability to remove public access links, organization-wide shares, and domain-wide access for Google Workspace and Microsoft 365.

Out-of-the-box integrations with third-party ticketing, notification and automation platforms help security operators collaborate with DevOps and platform engineering teams to remediate risks using existing workflows and reduce response times.

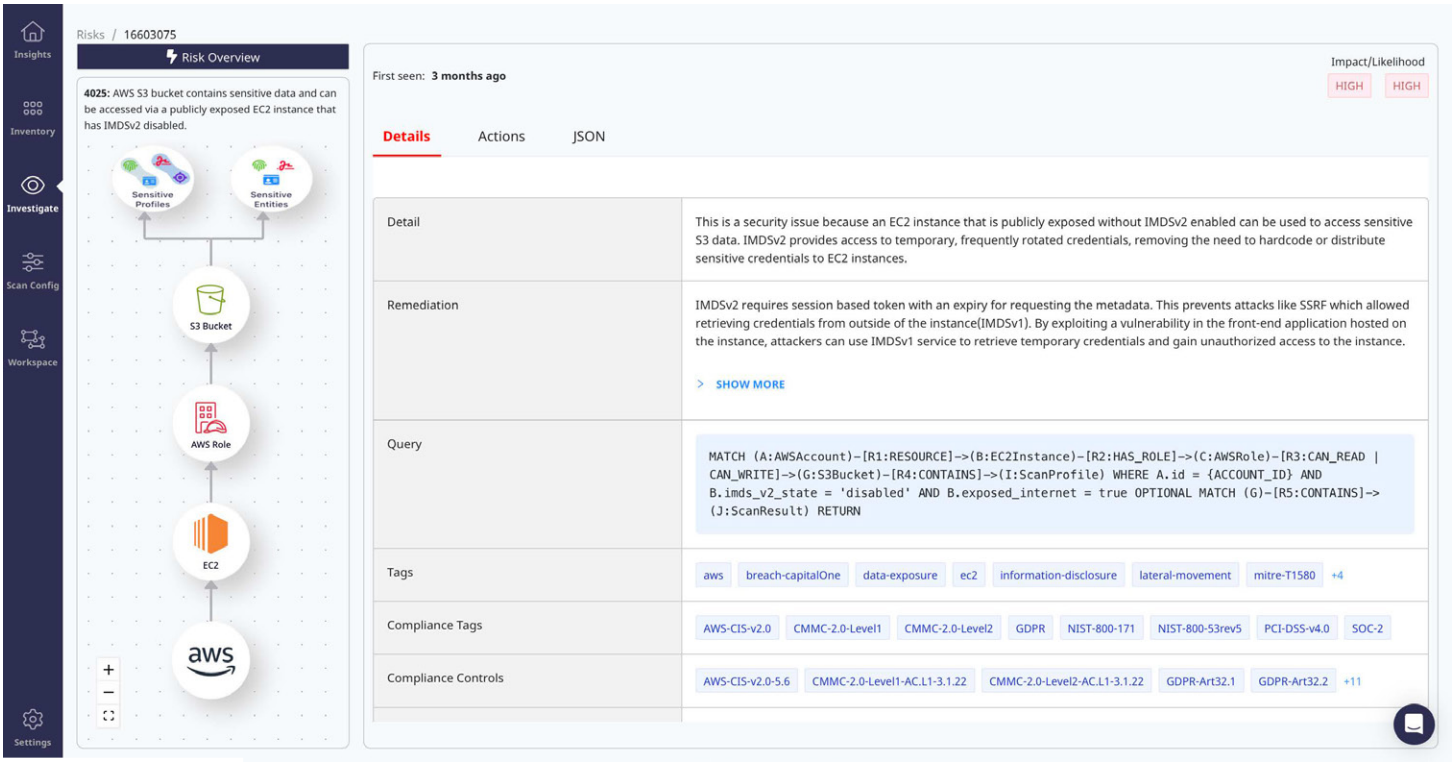


Figure 4: DSPM shows the data attack path. In this case a risky EC2 instance has access to an S3 bucket containing sensitive data. The details show guided remediation steps, and the actions panel enables remediation workflows including creating a JIRA ticket or notifying appropriate teams via Slack.

Key benefits

- Streamlined compliance

Continuous Compliance

DSPM continuously identifies and highlights data privacy gaps against over 500 regulatory compliance benchmarks including GDPR, HIPAA, NIST, CMMC, SOC2, and others. Compliance violations are tagged with both the applicable compliance framework and the individual control that has been violated, so analysts know the impact on their compliance posture.

Compliance reporting features allow organizations to view and report their compliance status across their entire infrastructure, offering detailed views by account, resource, and compliance framework. This enables teams to proactively address vulnerabilities and maintain continuous compliance, effectively preparing them for audits and ensuring ongoing data security.

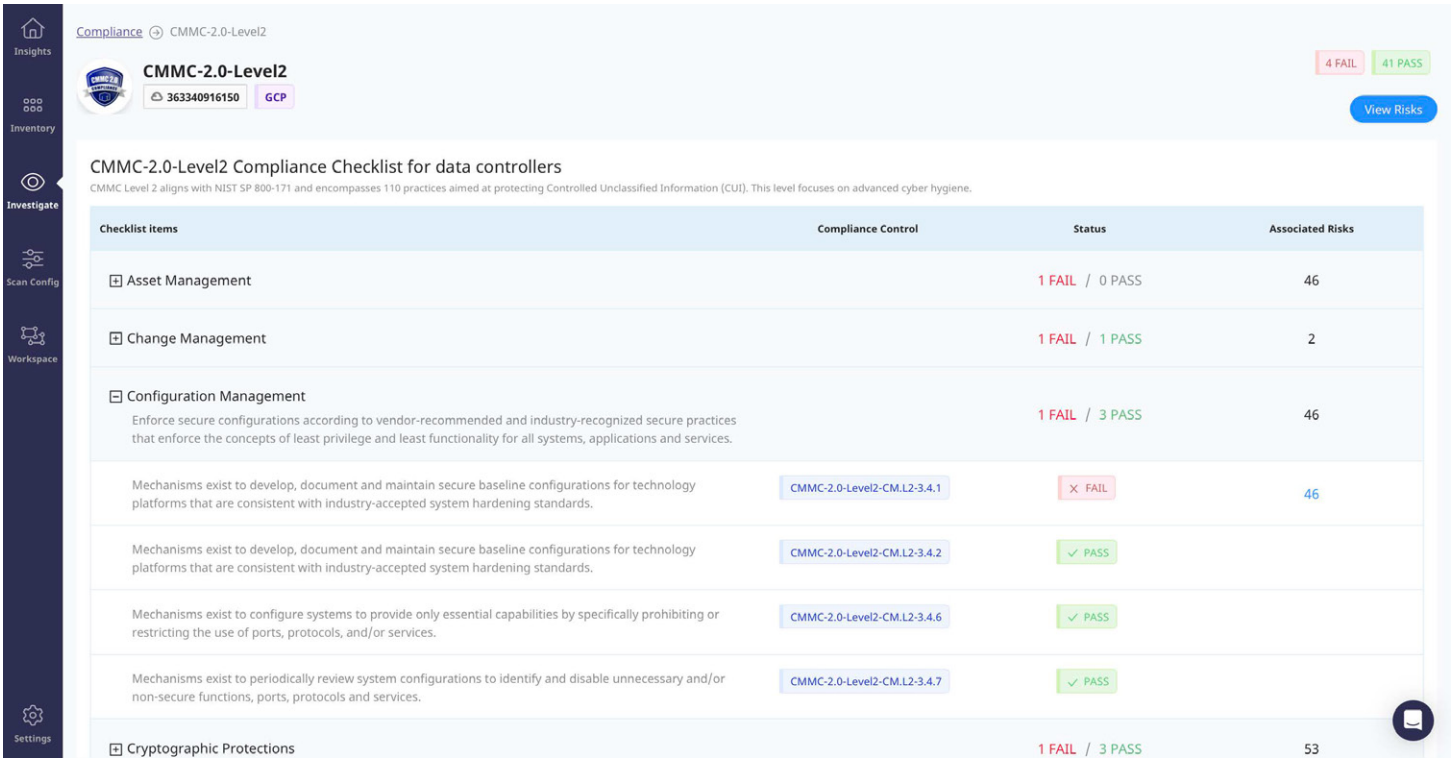


Figure 5: Compliance posture detail for CMMC 2.0

Key benefits

- Safe AI adoption
- Data lake enablement

DSPM for AI

DSPM ensures organizations can safely leverage AI by identifying sensitive data in workflows, preventing exposure that could lead to breaches. It additionally protects data in Microsoft Copilot by applying Microsoft Information Protection (MIP) labels, which are used to enforce protection policies such as encryption and access controls.

It also secures custom LLMs and AI applications on platforms like AWS Bedrock and Azure OpenAI by detecting sensitive data fed into foundational or custom models and RAG workflows.

DSPM provides specialized APIs for LLM security, enabling real-time sensitivity analysis of data flowing into and out of LLMs. These APIs offer full governance and visibility over data usage with seamless integration into customer workflows for effective deployment.

DSPM for Snowflake

The complex data movement, access structures, and extensive sharing typical in Snowflake environments increase the risk of breaches and governance issues. Data and security teams face challenges balancing access with minimizing risks, classifying unstructured data, and identifying hidden sensitive data.

DSPM helps Snowflake customers address issues such as over-privileged access, inefficient or inaccurate data classification, rapid data growth, governance gaps, and inadequate risk tools. Teams can automate continuous data discovery and classification of massive amounts of data, along with precise access management using a customized data access graph.

Native integration with Snowflake Data Cloud lets customers seamlessly secure their data by combining Snowflake Horizon's security capabilities with DSPM.

Scanning architecture

- Safe, efficient scanning

AI-powered and agentless

Using the permissions provided during onboarding, DSPM deploys the AI-powered and agentless cloud functions and VMs within your cloud environment. The spin-up, scale-out, scale-down and tear-down are all managed by the solution. The scanners have read-only access to perform these inspections only when they are deployed within your environment. Data within your environment is accessed using a variety of methods including API-based access and snapshotting within the environment to recreate data stores. Once scanning is complete, the scanner sends only the relevant metadata back to the platform for further processing and then safely terminates. This process, facilitated by scalable cloud-native technologies, ensures that all data scanning activities are confined to internal resources, thereby preserving the privacy and integrity of your data.

In-place scanning

A fundamental advantage of DSPM lies in its ability to perform security scans within the native data environment. That means valuable and sensitive data does not need to be moved or copied outside its original location for security analysis, significantly minimizing potential exposure to threats and vulnerabilities that could arise during data transfer. This provides customers with a highly cost-effective approach compared to other data scanning approaches that require either snapshotting or egressing the data to external vendor locations. By keeping data within its native ecosystem, DSPM also helps organizations reduce their overall attack surface and streamline compliance efforts.

Supported environments

- IaaS, PaaS, SaaS
- On-premises
- LLMs

Supported platforms and technologies

DSPM data discovery capabilities are engineered to operate seamlessly across a diverse range of platforms and services. By supporting an extensive array of data stores, from traditional relational databases to modern NoSQL and key-value stores, DSPM ensures comprehensive visibility into all structured, unstructured, and semi-structured data. This integration extends across major cloud providers and SaaS platforms, including but not limited to AWS, Azure, Google Cloud Platform (GCP), and various enterprise applications like Snowflake, Salesforce, ServiceNow, and Workday, as well as LLMs and copilots.

The common data discovery and classification framework makes it easy to add support for new data store technologies quickly.

Supported technologies include but are not limited to:

S3 Buckets, EBS, RDS, Redshift, DocumentDB, MemoryDB. DynamoDB, Keyspaces, Elasticache, EC2 DBs

Buckets, CloudSQL, MemoryStore, BigQuery, BigTable

Blob Store, File Share, SQL Server, MYSQL Server, PostgreSQL Server, Azure Cache, CosmosDB, Synapse Analytics, MariaDB, NetApp Files

PaaS + SaaS Platforms

Snowflake, Google Drive, OneDrive, Sharepoint, Salesforce

On-Premises

Windows File Share, MySQL, Postgres, MSSQL, MongoDB, Oracle DB, Network File Share

LLM models

Transformative approach

Conclusion

DSPM delivers a transformative solution to modern data security challenges, empowering organizations to eliminate blind spots by pinpointing the location of sensitive and valuable data and tracking who accesses it. This enhanced visibility enables security teams to address threats with full contextual awareness, mitigating human-centric risks and significantly reducing the likelihood of data breaches.

proofpoint.

DISCOVER THE PROOFPOINT PLATFORM →