proofpoint.

SOLUTION BRIEF

Proofpoint Data Security Posture Management

Discover and secure data across SaaS platforms, cloud infrastructure, and on-premises environments

Key Benefits

- **AI classifiers** identify sensitive and business-specific data without manual rules across SaaS, cloud, and on-premises environments
- **Data Risk Map** prioritizes risk using data sensitivity, access, business impact, and movement
- **Business-aware access governance** streamlines direct and delegated remediation and DLP policy creation
- **Built-in AI data security** identifies sensitive data exposed to AI applications and AI training pipelines
- **Compliance dashboards** track posture across 25-plus frameworks with actionable reporting
- **Unified data security** shares intelligence across DSPM, access governance, DLP, and Data Security for AI

The Explosion of Enterprise Data

The rise of AI, database as a service (DBaaS) platforms, and cloud storage has accelerated data sprawl across software as a service (SaaS), cloud, and on-premises environments. As sensitive data spreads across systems and pipelines, teams struggle to see where it all lives. This causes blind spots, increases exposure risk, and complicates compliance.

Uncontrolled Data Access by Humans and AI

Data sprawl is magnified by a lack of control over who—and what—can access sensitive information. Over-privileged users, unauthorized tools, and risky sharing create human-driven risk. AI models, agents, and automated workflows add new, non-human access paths. Without strong governance, misconfigurations, excess permissions, and weak oversight can cause data leaks, misuse, and compliance violations.

55%

of organizations say 21-40% of their data is sensitive.

Source: Proofpoint

68%

of organizations say improper AI use exposed sensitive data.

Source: Proofpoint

Discover, Classify, Govern, and Protect Data

Proofpoint Data Security Posture Management (DSPM) helps teams regain control of sprawling data and reduce risky access by humans and AI. It discovers and classifies sensitive data, shows who and what can access it, and ranks risks. Teams can fix exposures faster and strengthen data security.

Unique Capabilities

As part of Proofpoint Data Security, DSPM with integrated data access governance shares its data classification framework with Proofpoint Enterprise DLP and Proofpoint Data Security for AI. AI classifiers identify sensitive document categories by context and meaning, not just patterns. This improves discovery and classification. It also helps teams govern access, create data loss prevention (DLP) policies, and protect data across cloud, SaaS, on-premises, and AI environments.

DSPM spots excess permissions, risky access, misconfigurations, obsolete data, and attack paths. The Data Risk Map shows where sensitive data lives, how widely it is exposed, and which users, apps, and AI tools can access it. Data access governance workflows support bulk and delegated remediation. DSPM findings can be converted into DLP rules with just a few clicks. These help teams reduce exposure and enforce least privilege.

DSPM enables more secure AI adoption. It finds sensitive data exposed to copilots, large language models (LLMs), and AI apps.

Together, DSPM with data access governance, Enterprise DLP, and Data Security for AI give teams one way to discover, govern, and protect sensitive data through its lifecycle.

Autonomously Classify Business-Critical Documents

DSPM delivers market-leading data classification. It uses regular expressions, natural language processing, and LLMs to improve performance and reduce resource use.

Proofpoint Autonomous Custom Classification (ACC) identifies organization-specific documents without manual rules or training. This helps teams uncover proprietary data, close blind spots, and improve risk detection and policy enforcement.

DSPM can also apply Microsoft Information Protection (MIP) sensitivity labels based on AI classifiers. This helps teams enforce governance policies, support compliance, and protect Microsoft data from unauthorized access or misuse.

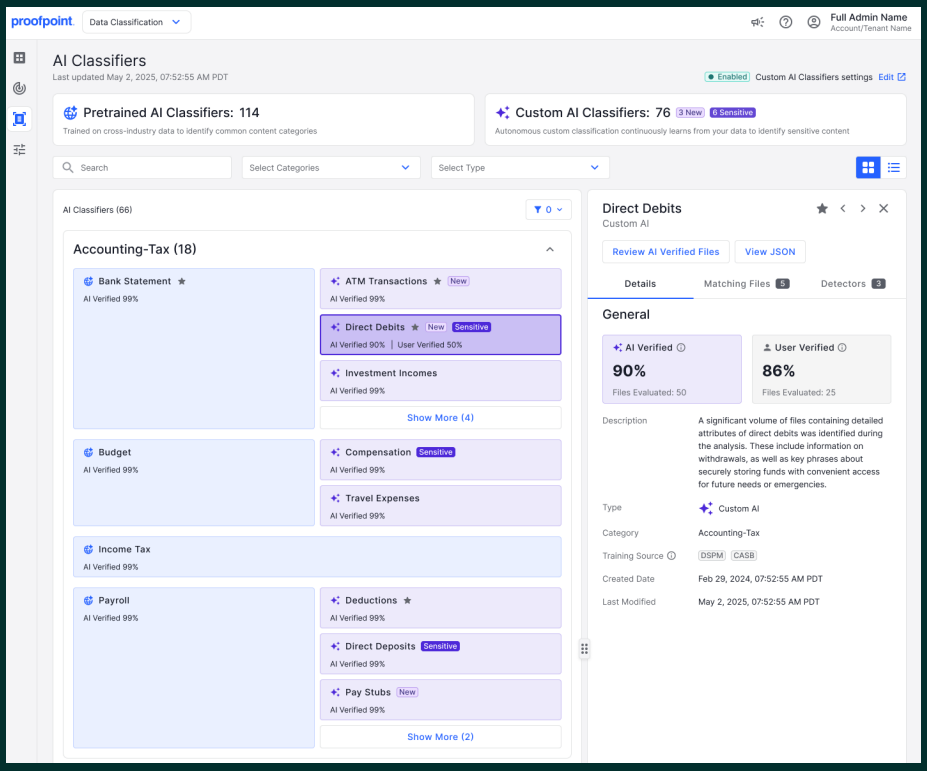

Figure 1. DSPM pretrained and autonomous AI classifiers identify standard and business-specific documents, including contracts, financial records, source code, and employee records.

Map Data Access Risks

The Data Risk Map shows where sensitive data lives in SaaS and on-premises systems. It shows how widely data is shared and which users, apps, or AI tools can access it. It combines AI classification with access and usage insights.

Security teams can find overexposed data, rank risks, validate fixes, and keep access appropriate as AI use grows. Data risk findings consider data sensitivity, access patterns, and exposure. This helps teams focus on data with both high value and high risk while cutting costs and reducing the enterprise risk surface.

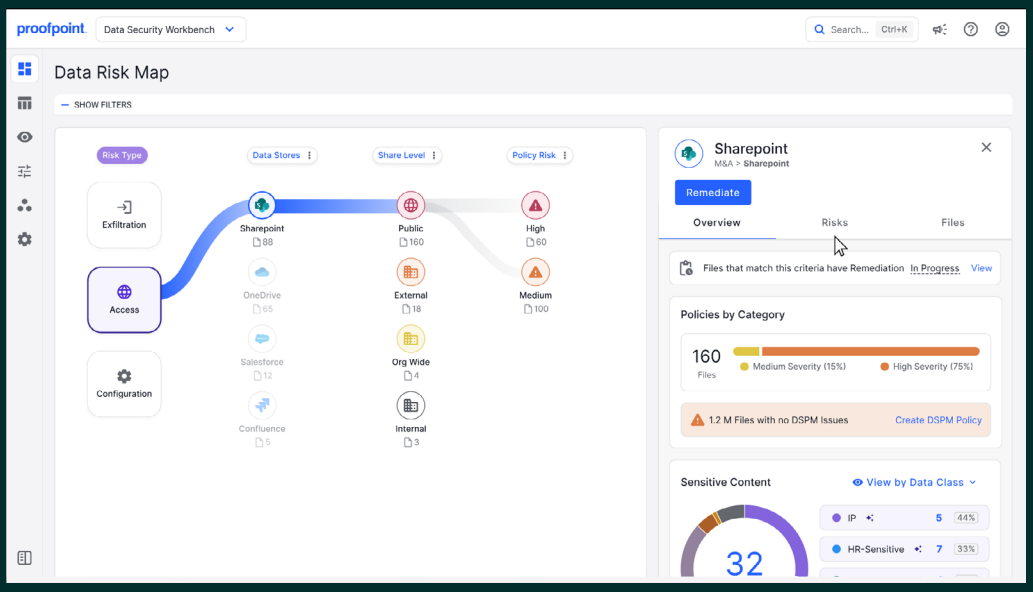

Figure 2. The Data Risk Map shows which repositories contain sensitive data, scope of data sharing, and access by users, applications, and AI tools.

Prioritize Risk Based on Monetary Value of Data

Data security teams must protect many data stores. But not every store has the same value or risk. DSPM uses data valuator technology to estimate breach cost for each data store. This helps teams focus on what matters most. DSPM also includes 200-plus prebuilt access and exposure findings with toxic combination detection. This risk matrix highlights stores with high risk and high financial impact.

Minimize Obsolete Data

In SaaS and on-premises systems, DSPM finds and removes files not recently accessed. AI classifiers help teams keep business-critical data when needed. In infrastructure as a service (IaaS) environments, DSPM finds unneeded data stores. This includes shadow, duplicate, and abandoned data such as stale backups and snapshots.

This cuts storage costs, shrinks the attack surface, and simplifies data management. Teams keep only relevant, active data.

Enforce Least Privilege Access

DSPM supports least privilege access by finding over-permissioned users, unused access, and risky accounts across data stores. This supports stronger data access governance and Zero Trust.

DSPM analyzes identity and access management (IAM) roles, permissions, database grants, and other access controls for human and machine identities. It shows who can access sensitive data in near real time. Teams can remove unneeded permissions and reduce exposure.

DSPM also flags under-protected accounts across SaaS and platform as a service (PaaS) environments. Examples include users with sensitive data access but no multi-factor authentication (MFA), inactive accounts, and apps with excess admin privileges.

Detect Attack Paths in Cloud Environments

DSPM collects information about compute and networking resources, as well as PaaS and SaaS services, across cloud providers. It detects misconfigurations and vulnerabilities in those resources. A graph shows paths an attacker could use to reach sensitive data. Near real-time monitoring helps teams spot changes that raise exposure.

Insights into data sensitivity, access patterns, and risk also help DLP and data detection and response (DDR) tools.

Govern Access Directly or Through Delegation

In SaaS and on-premises systems, DSPM workflows turn exposure insights into action. As AI tools like Microsoft Copilot increase the impact of overshared content, reducing excess access becomes critical. Administrators can revoke public links, external shares, and domain-wide access across Google Workspace and Microsoft 365. This enables enterprise-scale remediation.

Security teams cannot judge the right access level for every file. Data access governance workflows let them assign access reviews to content owners. Automated campaigns, reminders, and tracking make governance easier to sustain.

Integration with Enterprise DLP extends protections beyond data at rest. Sensitive data classified and risks prioritized by DSPM can be mapped to DLP policies. This supports consistent protection and automated remediation across email, endpoint, cloud, and collaboration channels.

In IaaS and PaaS environments, actionable insights and recommendations help teams reduce exposures quickly. Integrations with ticketing, notification, and automation platforms help security operators work with DevOps and platform engineering teams through existing workflows.

Stay Aligned with Compliance Frameworks

DSPM finds privacy and security gaps across 25-plus regulatory compliance frameworks. These include the EU AI Act, GDPR, HIPAA, NIST, CMMC, SOC 2, and others.

Violations are tagged by both framework and control, so analysts can see the compliance impact.

Reporting shows compliance status across the infrastructure, with views by account, resource, and framework. This helps teams fix vulnerabilities, prepare for audits, and maintain compliance.

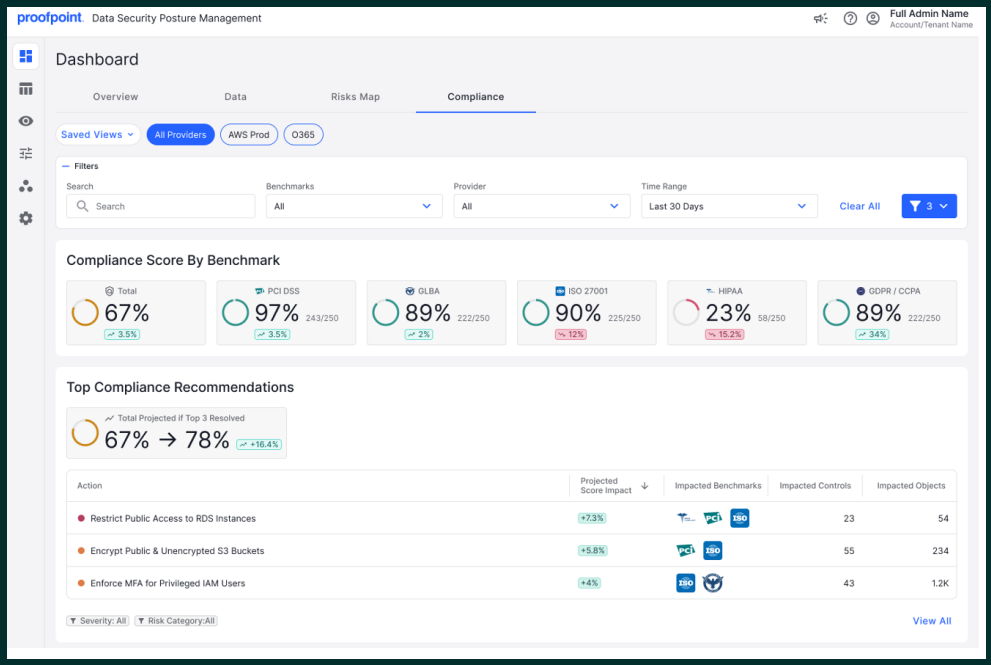

Figure 3. Dashboard highlighting compliance posture.

Reduce AI Data Exposure Risks

DSPM helps organizations scale AI by finding sensitive data exposed to AI apps and workflows.

Proofpoint DSPM feeds exposure insights into the Proofpoint Data Security for AI dashboard. The dashboard gives a central view of data risks across approved and unapproved AI apps. DSPM also monitors AI app misconfigurations and helps teams fix them. This reduces leakage risk, strengthens AI data governance, and supports secure adoption.

DSPM secures custom LLMs and AI apps on platforms like AWS Bedrock and Azure ML. It detects sensitive data fed into foundation models, custom models, and retrieval-augmented generation (RAG) workflows.

DSPM also provides specialized APIs for LLM security. These analyze sensitive data flowing into and out of LLMs in real time. They also provide governance and visibility over data use and integrate with customer workflows.

Supported Platforms and Technologies

DSPM discovers and classifies data across many platforms and services. It supports a wide range of data stores, from relational databases to NoSQL and key-value stores. This gives teams visibility into structured, unstructured, and semi-structured data.

Support spans major cloud and SaaS platforms. Examples include AWS, Azure, Google Cloud Platform (GCP), Snowflake, Salesforce, ServiceNow, Workday, LLMs, and copilots.

The common discovery and classification framework helps Proofpoint add new data store support quickly.

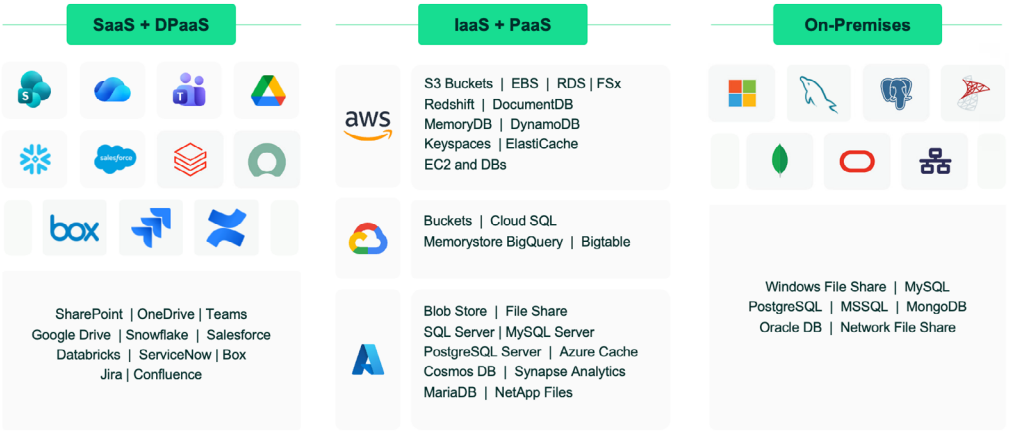

Figure 4. DSPM discovers and classifies data across a wide range of platforms and services.

Conclusion

As organizations adopt AI and manage more data, they need to know where sensitive data lives, who can access it, and how it is used. Proofpoint DSPM reduces exposure by classifying sensitive data, ranking risks, finding excessive access, and enforcing least privilege access across cloud, SaaS, on-premises, and AI environments.

As part of Proofpoint Data Security, Proofpoint DSPM works with Proofpoint Enterprise DLP. Together, they help teams discover, classify, govern, and protect sensitive data. Organizations can strengthen compliance, secure AI adoption, reduce risk, and protect their most valuable information.