Netwoven

Solution Brief

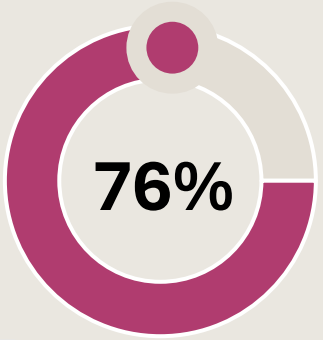
Elevating AI Security with Microsoft Purview DSPM

Table of Content

Overview

Artificial Intelligence (AI) is transforming organizational operations, but its effectiveness relies on the data it uses. As AI adoption accelerates, safeguarding sensitive data in model training, prompt engineering, and AI-driven workflows becomes crucial.

This solution brief outlines Data Security Posture Management (DSPM) for AI and Microsoft Purview's capabilities to enhance data security and compliance, facilitating the adoption of AI tools like Copilots and generative AI apps. DSPM for AI provides visibility, control, and protection over sensitive data in AI environments, enabling responsible and secure AI adoption. It continuously discovers sensitive data, assesses risks, enforces usage policies, and maintains regulatory compliance, ensuring innovation and data protection go hand in hand.



76% of organizations express concern about potential data leakage when using generative AI tools such as ChatGPT, Copilot, or Bard.

Source: Cisco 2024 Data Privacy Benchmark Study

- It provides meaningful analytics and visibility into how AI is being used across the organization.
- DSPM helps identify and protect sensitive data such as PII, financials, IP, or confidential business information that may be exposed in AI prompts, training data, or generated outputs.
- Offers built-in policy frameworks to protect sensitive information and reduce the risk of data leaks through AI interactions.
- Conducts thorough risk evaluations to detect, address, and continuously monitor data exposure risks.
- With proactive detection and real-time policy enforcement, DSPM reduces the likelihood of sensitive data leaving the organization via AI tools, mitigating both security and reputational risks.

Challenges

If an organization adopts AI tools without implementing Data Security Posture Management (DSPM) for AI, it exposes itself to a range of data protection, compliance, and operational risks.

Lack of Visibility into AI Data Usage

Without DSPM, organizations don't know which sensitive data is being used in AI prompts, training sets, or outputs.

Increased Risk of Sensitive Data Exposure

Generative AI tools can unintentionally leak sensitive data through prompt responses or fine-tuned models.

Shadow AI and Unmanaged Tool Usage

Employees may use unauthorized or third-party AI tools (e.g., ChatGPT, Gemini, Claude) without IT oversight.

Overexposure and Misconfiguration

Data intended for internal use may be overexposed to AI tools or made available via misconfigured access controls.

Damage to Trust and Brand Reputation

Misuse of AI, especially involving customer or confidential data, can severely harm customer trust and public perception.

Use Cases

1. Protecting Sensitive Data in AI Prompts and Outputs

- Employees using tools like Microsoft Copilot or ChatGPT may unknowingly input or receive sensitive data.
- DSPM for AI automatically classifies sensitive data in real-time prompts and responses and blocks or warns users based on data protection policies.

2. Securing AI Training and Fine-Tuning Datasets

- AI models may be trained on data containing PII, financial records, or intellectual property.
- DSPM for AI, discovers and labels sensitive data before use in AI training and ensures only authorized, clean data is used for training.

3. Monitoring Third-Party AI Tools (e.g., Gemini, Claude, ChatGPT, Bedrock)

- Employees use external AI platforms without visibility or governance.
- DSPM for AI tracks which AI tools are in use across the organization and monitors what kind of data is being shared with third-party AI.

4. Supporting Responsible AI and Regulatory Compliance

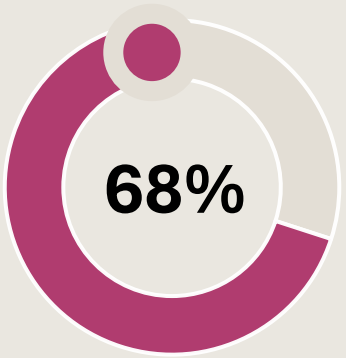
- AI data usage may violate GDPR, HIPAA, AI Act, or other regulatory frameworks.
- DSPM for AI provides compliance reporting for AI data use and ensures sensitive data used in AI adheres to regulatory and internal policies.

5. Detecting AI Misuse by Insider Threats

- Employees or contractors may abuse AI tools to extract or misuse data.
- Monitor insider behavior involving AI data access and trigger alerts for abnormal access patterns or policy violations.
- Integrate with Insider Risk Management for advanced response.

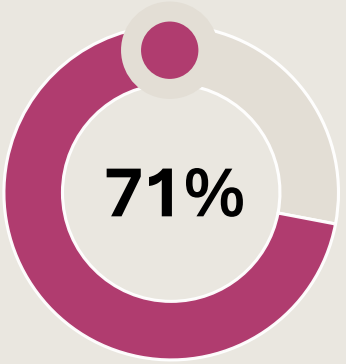
6. Mitigating Prompt Injection and Data Exfiltration Risks

- Malicious or manipulated prompts can exploit AI models to leak data or perform unintended actions.
- DSPM for AI detects and blocks anomalous prompt activity and monitors for signs of prompt injection, exfiltration attempts, or misuse.



68% of enterprises report losing visibility and control over data once it is used in AI/ML pipelines.

Source: Gartner, 2024 Emerging Tech Report

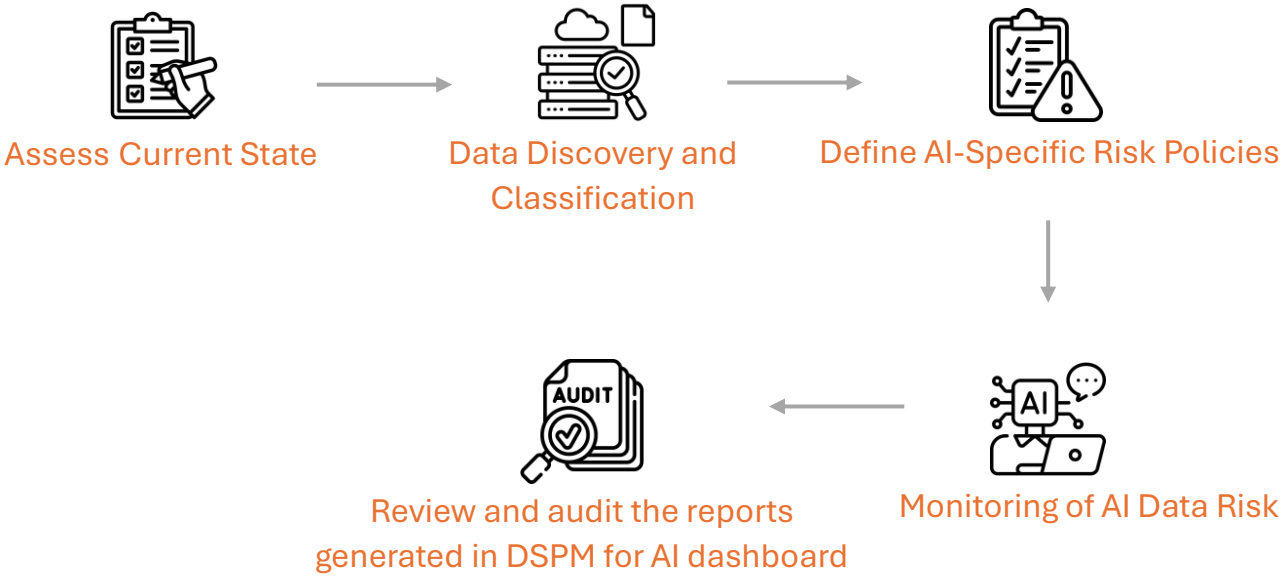


71% of security leaders believe that AI tools increase the risk of accidental or intentional data exposure.

Source: Ponemon Institute & IBM Security, 2023

Netwoven’s Approach

Implementing Microsoft Purview DSPM for AI effectively requires a structured approach to ensure data security, compliance, and responsible AI usage.



Strategy to Implement DSPM for AI

Transitioning to Microsoft Purview DSPM for AI requires a strategic approach to ensure a smooth rollout, effective adoption, and strong data protection.

1. Assess Current State

- Inventory AI tools in use (e.g., Microsoft Copilot, ChatGPT, third-party apps).
- Evaluate existing data protection measures and identify gaps.
- Identify key stakeholders involved in AI tool usage.

2. Data Discovery and Classification

- Use Microsoft Purview to automatically scan data sources across cloud, on-prem, and SaaS platforms.
- Apply built-in and custom sensitive information types (SITs) to tag data used in AI prompts, training, or inference.
- Prioritize classification of data in locations where AI tools (e.g., Copilot, LLMs) are actively used.

3. Define AI-Specific Risk Policies

- Create or extend DLP policies to address AI-specific risks like prompt injection, unintended outputs, and use of PII in LLM training.
- Create policies related to industry specific use cases , and combine it with best practices, and scope the policy to Copilot, third-party AI tools, or prompt input/output content.

4. Monitoring of AI Data Risk

- Make the use of Microsoft Purview DSPM for AI dashboards to monitor high-risk data activities and detect overshared or misused data in AI workloads.

5. Review and Audit The Reports Generated in DSPM for AI dashboard

- These reports provide actionable insights into how sensitive data is being accessed, used, or potentially exposed across AI tools like Microsoft Copilot and third-party AI services.
- Key report elements include the classification status of AI-accessed data, incidents of policy violations, unusual or risky user behaviors, and data overexposure trends. By auditing these reports, security and compliance teams can identify patterns of misuse, gaps in protection policies, and areas that require immediate remediation.

Leveraging DSPM for AI to Drive Organizational Success

- Implementing a proactive framework to identify, classify, monitor, and protect sensitive data being used or accessed by AI systems. Solution like Microsoft Purview's DSPM for AI allows organizations to gain full visibility into where their sensitive data resides, how it flows through AI tools, and whether it is at risk of exposure, misuse, or non-compliance. By applying automated classification, adaptive policy enforcement, and risk-based insights, organizations can ensure that only the right people, tools, and models have access to the right data - at the right time.

- This not only reduces the risk of data breaches and regulatory violations but also helps build trust in AI adoption by aligning with internal governance standards and external regulations like GDPR, HIPAA, or the EU AI Act.

- Ultimately, leveraging DSPM for AI transforms data protection from a compliance burden into a strategic advantage, helping organizations innovate with AI confidently, accelerate digital transformation, and maintain a strong reputation in a data-driven world.

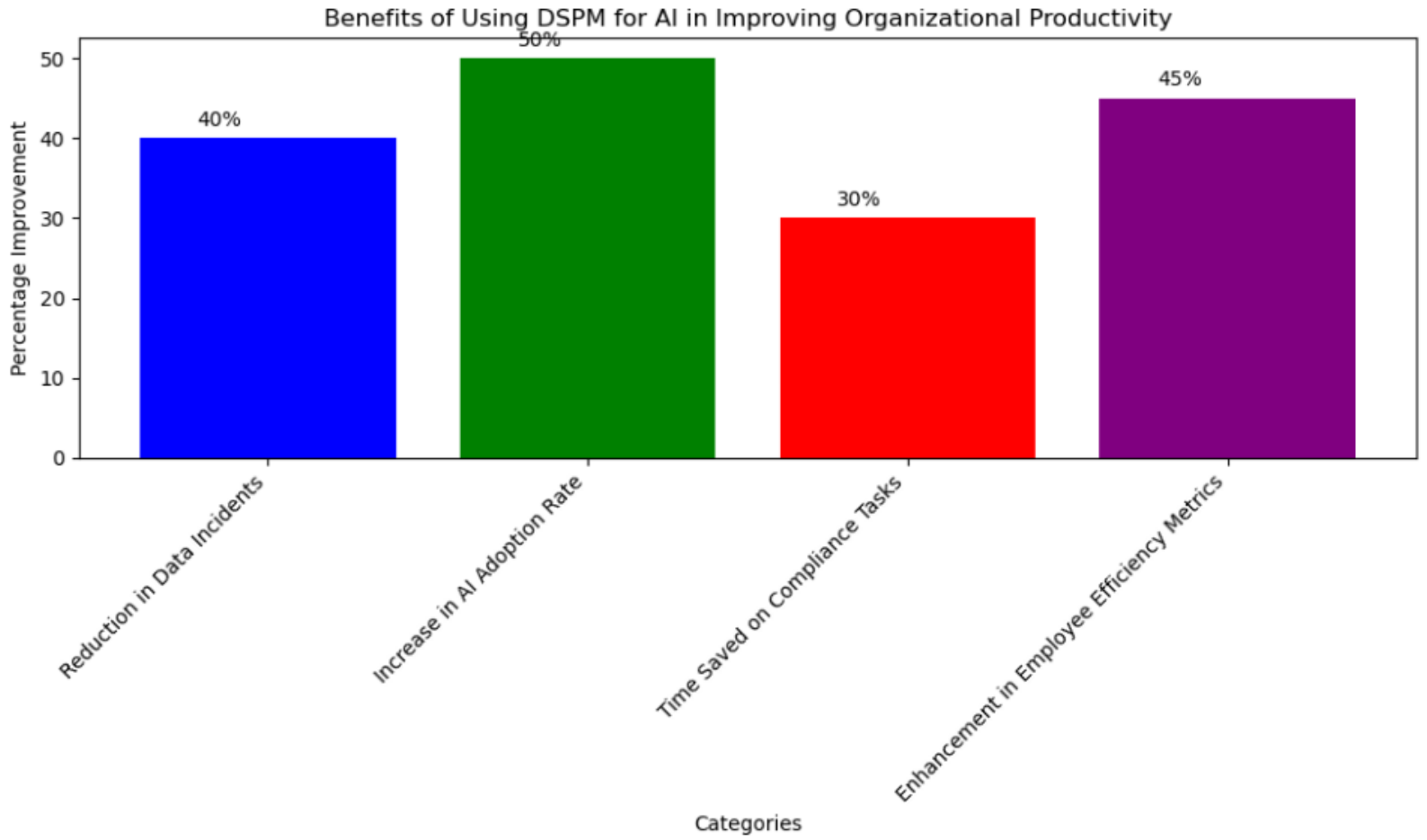
Key Productivity Gains

40% 40% reduction in data incidents due to proactive monitoring and policy enforcement.

50% 50% increase in AI adoption rate as employees feel safer using AI tools.

30% 30% time saved on compliance tasks through automated classification and reporting.

45% 45% improvement in employee efficiency by enabling secure, confident AI usage.



Above illustrative estimates are based on industry trends and expert insights, not directly published by Microsoft or a single authoritative source.

About Netwoven

Netwoven: Your Trusted Microsoft Solutions Partner

Netwoven is a global leader in AI transformation, utilizing Microsoft technologies to address intricate business challenges.
Established in 2001 by senior executives from Microsoft, Oracle, and Intel, Netwoven is headquartered in the San Francisco Bay Area.

Our security practice delivers comprehensive services across all security domains:

- Identity and Access Management
- Endpoint Management
- Secure Software Development
- Microsoft Security Copilot Services
- Data Security, Governance and Compliance
- Security Modernization
- Managed Services
- AI Agents and Security Services

Next Steps

Join our **workshop to explore** the next steps in enhancing AI security with Microsoft Purview DSPM and learn how to implement comprehensive data security measures effectively.

Netwoven Inc.

4000 Pimlico Drive
Suite 114-103 Pleasanton,
CA 94588
Phone: +1 877 638 9683
Email: info@netwoven.com