

SHADOW DATA & SHADOW AI: THE RISKS HIDING IN PLAIN SIGHT

SHADOW RISK READINESS REPORT

Most organisations have no clear picture of where their sensitive data lives or how AI tools are processing it. Uncover what's lurking in your environment and take back control with Symantec DSPM and Cloud Managed DLP.

THE SCALE OF THE PROBLEM



Of employees admit to using AI tools that were not approved by their employer

WalkMe State of AI at Work, 2025



of organisations experienced a data breach linked to Shadow AI with those breaches costing an additional \$670,000 on average.

IBM Cost of a Data Breach 2025



of organisations that suffered an AI – related security incident lacked proper AI access

IBM Newsroom

THE CHALLENGE

YOU CAN'T PROTECT WHAT YOU CAN'T SEE

Sensitive data today is scattered across SaaS apps, cloud storage, endpoints, and collaboration platforms like Slack and Teams. Meanwhile, employees are connecting to unauthorised AI tools uploading files, pasting customer data, and generating outputs with no oversight.

This is Shadow Data and Shadow AI: invisible risk that grows every day your team operates without visibility. According to Gartner (2025), 69% of organisations suspect or have confirmed evidence that employees are using prohibited generative AI

tools. The business impact is already measurable. IBM's Cost of a Data Breach Report (2025) found that 20% of organizations suffered a breach involving shadow AI, with those incidents costing an additional US\$670,000 on average.

Security teams are lean. Budgets are finite. The attack surface keeps growing. Traditional, infrastructure-heavy DLP simply isn't realistic for most teams. There is a faster, smarter path forward.

YOUR FREE REPORT

Symantec DSPM

FIND YOUR SHADOW DATA

*Modern cloud infrastructures are complex. DSPM gives you a real-time map of every sensitive data store across SaaS, IaaS and endpoint devices so you can see, classify and govern data that was previously invisible.

- Full data catalog across cloud, SaaS, and on-premises environments
- Sensitivity scoring and automatic data classification at scale
- Posture dashboards purpose-built for data security teams
- Shared detection engine feeds directly into DLP remediation workflows
- Supports hybrid and multi-cloud environments without re-architecture

Symantec Cloud Managed DLP

CONTROL YOUR SHADOW AI

Employees may be using AI tools you haven't approved. Cloud Managed DLP can safely enable the use of AI apps, monitors and enforces policy across endpoints and SaaS apps, stopping sensitive data from reaching unauthorised AI services before a breach occurs.

- Detect and block uploads to generative AI tools in real time
- Block the use of unsanctioned AI apps
- Pre-built policies and out-of-the-box templates, deployable in days
- No on-premises infrastructure required; cloud console management
- Scale incrementally from visibility to active enforcement

WHY BOTH SOLUTIONS WORK

Unified visibility

DSPM finds where data lives. DLP governs where it goes. Together they deliver complete coverage across cloud, SaaS, and endpoints.

Fast time to value

Cloud-native deployment with pre-built templates means no servers to provision. Achieve meaningful risk insights within days, not months.

Grows with you

Start with monitoring. Incrementally enforce policies. Centrally managed controls mean no re-architecting as your organisation scales.

Compliance-ready

Demonstrate control under GDPR, HIPAA, and industry frameworks

Predictable costs

Per user per year based pricing converts security into a scalable operating expense, not a capital hurdle that stalls critical initiatives.

Enterprise-grade DLP

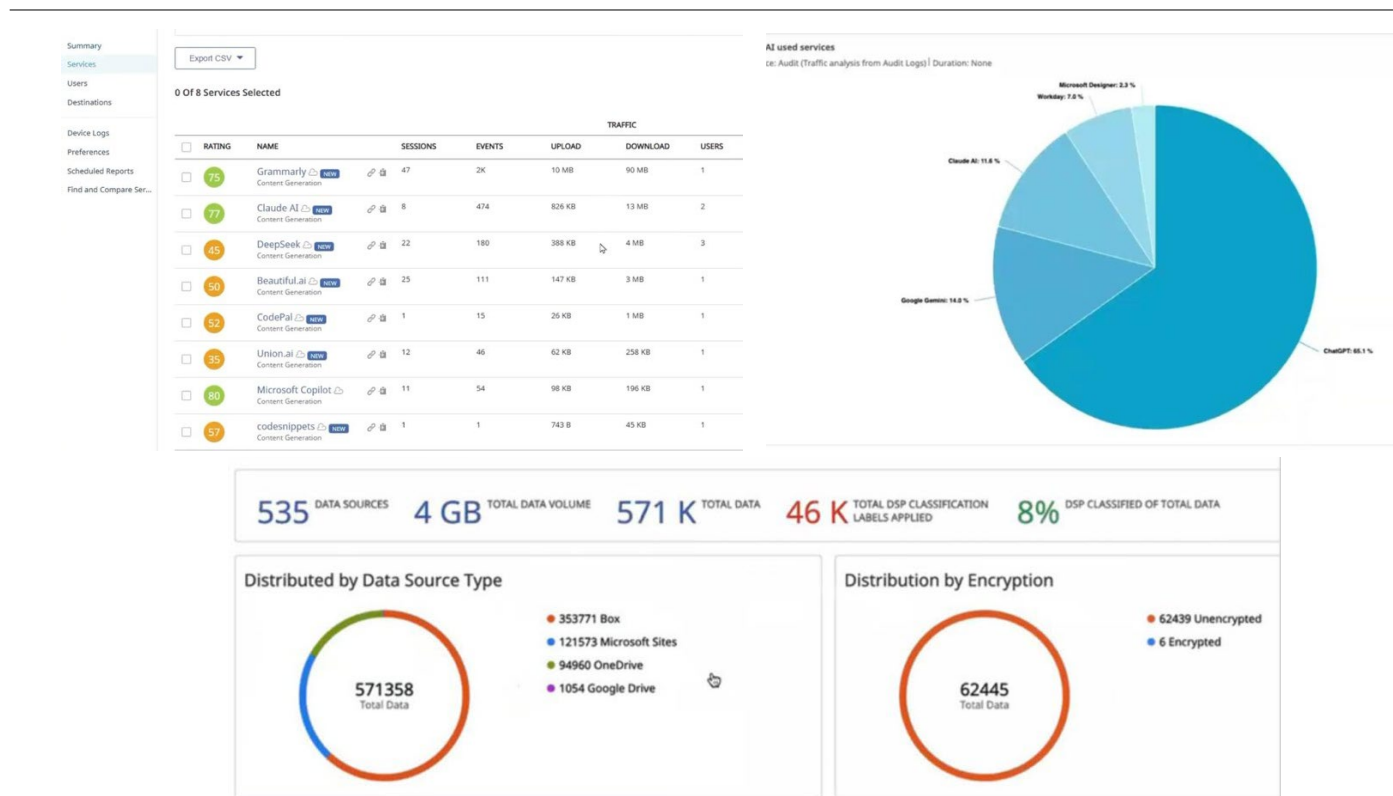
DLP is trusted by 13 of the 15 biggest banks in the world and accessible for organisations of every size and budget.

THE SOLUTION

WHAT'S INCLUDED IN YOUR FREE ASSESSMENT

A personalised assessment of your data exposure across cloud, SaaS, and endpoints — including:

- A no obligation “AI Readiness Data Security Risk Assessment” report and consultation
- AI tool usage snapshot showing which unsanctioned AI tools employees are actively using
- Top data risk findings across your Endpoints, Cloud and SaaS environment
- A prioritised remediation roadmap aligned to your compliance obligations
- A guided walkthrough of findings specific to your organisation



See What's Hiding in Your Environment

Our team will walk you through findings specific to your organisation and show you how quickly you can start reducing risk

REQUEST YOUR FREE SHADOW AI / SHADOW DATA REPORT.