

Top Data & AI Security Priorities for 2026

In 2026, protecting data isn't just part of your AI strategy, it is what makes AI possible.

V I S I B I L I T Y • P R O T E C T I O N • G O V E R N A N C E • A I E N A B L E M E N T

As organizations accelerate the adoption of Microsoft 365 Copilot, AI agents and third-party generative AI applications, security teams face a new challenge: data is being accessed, summarized, shared and transformed faster than ever before.

Traditional data protection strategies are no longer enough.

Organizations need to understand where sensitive data lives, who can access it, how it is being used and how AI changes its exposure.

A modern Data Security strategy must bring together visibility, protection, governance and AI security.

FOUR PRIORITIES ARE DEFINING DATA & AI SECURITY IN 2026:

- 1 Discover and Reduce Data Exposure
- 2 Protect Sensitive Data Everywhere
- 3 Secure AI Without Slowing Innovation
- 4 Move from Data Alerts to Data Security Operations

01 Discover and Reduce Data Exposure

You cannot protect what you cannot see.

Sensitive information is distributed across Microsoft 365, endpoints, cloud applications and increasingly AI interactions. At the same time, excessive permissions, oversharing and unmanaged data can dramatically increase organizational risk when AI gains access to that information.

The objective is no longer simply finding sensitive data.

The objective is understanding which sensitive data represents actual business risk, and taking action before that risk becomes an incident.

ORGANIZATIONS SHOULD ESTABLISH A DATA-CENTRIC SECURITY POSTURE TO:

- ✓ Discover sensitive and business-critical information.
- ✓ Identify overshared and overexposed data.
- ✓ Understand where sensitive information is being accessed and moved.
- ✓ Prioritize the highest-risk data locations and users.
- ✓ Continuously assess and improve their Data Security Posture.

02 Protect Sensitive Data Everywhere

Data protection must follow the information, not the application.

Employees work across email, collaboration platforms, endpoints, SaaS applications, browsers and AI tools. Security controls therefore need to protect sensitive information throughout its lifecycle.

The goal is to move from isolated controls to consistent protection wherever data travels.

ORGANIZATIONS SHOULD IMPLEMENT A LAYERED PROTECTION STRATEGY USING:

IP

Information Protection

Classify and label sensitive information based on business value and regulatory requirements.

DLP

Data Loss Prevention

Detect and prevent inappropriate sharing across Exchange, Teams, SharePoint, OneDrive, endpoints, browsers and cloud applications.

IR

Insider Risk Management

Identify potentially risky user behavior such as unusual downloads, external sharing, data exfiltration or misuse of sensitive information.

03 Secure AI Without Slowing Innovation

AI adoption is changing the Data Security perimeter.

Employees are interacting with Microsoft 365 Copilot, enterprise AI applications, AI agents and public generative AI services, often using organizational data as part of their prompts and workflows.

SECURITY TEAMS MUST ANSWER NEW QUESTIONS:

- ? What AI applications are employees using?
- ? What sensitive information is being shared with them?
- ? What organizational data can Copilot and AI agents access?
- ? Which AI interactions represent real Data Security risk?

ORGANIZATIONS NEED CAPABILITIES THAT ALLOW THEM TO:

- ✓ Discover AI usage across the enterprise.
- ✓ Identify sensitive data being shared with AI applications.
- ✓ Detect risky AI interactions and potential data leakage.
- ✓ Prevent sensitive information from being submitted to unauthorized AI services.
- ✓ Reduce oversharing before deploying Copilot and AI agents.
- ✓ Apply security and compliance controls to enterprise AI.

The objective should not be to block AI.

It should be to enable AI with the right data, the right controls and the right level of trust.

04 Move from Data Alerts to Data Security Operations

More alerts do not automatically create better security.

Security and compliance teams often operate across separate tools, policies and investigations, making it difficult to understand the complete context behind a Data Security incident.

The next evolution of Data Security is moving toward Data Security Operations.

ORGANIZATIONS SHOULD CONNECT SIGNALS ACROSS:

Data + **Users** + **Devices** + **AI** + **Risk**

to understand what happened, what information was affected and what action should be taken.

WITH DATA SECURITY POSTURE MANAGEMENT, INSIDER RISK MANAGEMENT AND AI-ASSISTED DATA SECURITY INVESTIGATIONS, ORGANIZATIONS CAN MOVE TOWARD:

- ✓ Risk-based prioritization.
- ✓ AI-assisted alert triage.
- ✓ Investigation of sensitive data exposure.
- ✓ Identification of compromised or exposed information.
- ✓ Faster remediation of Data Security incidents.
- ✓ Continuous improvement of the organization's Data Security posture.

INSTEAD OF ASKING:

"How many DLP alerts did we receive?"

DATA SECURITY TEAMS SHOULD BE ASKING:

"Which data represents the greatest risk to the organization right now?"

VISIBILITY. PROTECTION. GOVERNANCE. AI ENABLEMENT.

These priorities are interconnected. Organizations that want to successfully adopt AI need more than an AI strategy, they need a Data Security strategy designed for AI.

A MODERN APPROACH WITH MICROSOFT PURVIEW CAN HELP ORGANIZATIONS:

Discover

Understand where sensitive data exists and how it is exposed.

Protect

Apply consistent controls across users, devices, applications and AI.

Investigate

Understand risky behavior and Data Security incidents with deeper context.

Govern

Manage information throughout its lifecycle and support regulatory requirements.

Enable AI

Allow employees and AI agents to safely use organizational data.

FROM DATA VISIBILITY TO AI CONFIDENCE

The organizations that succeed with AI will not be the ones that simply deploy it fastest.

They will be the organizations that understand their data, reduce unnecessary exposure and establish controls that allow people and AI to use information safely.

**Secure the data. Govern the data.
Enable AI.**

contactus@mdsny.com • 646-744-1000 • www.mdsny.com