ANALYST BRIEF
Sponsored by: Cyera

The speed of AI adoption drives the need for immediate access to secure, accurate, and safe data. Democratizing data across the business shares security responsibility with data owners, facilitating faster access to the right data when it is needed.

Democratizing Data: Balancing Security, Risk, and Business Value in the Age of AI

March 2026

Written by: Jennifer Glenn, Research Director, Information and Data Security

Introduction

Enterprise adoption of AI and generative AI technologies is fundamentally reshaping enterprise data strategies. Organizations face significant pressure to make data more accessible to fuel innovation, yet they must simultaneously manage expanding regulatory requirements and escalating security risks.

IDC research shows a widening gap between AI ambition and data security readiness. In IDC's April 2025 *Data Security and Privacy Survey,* only 29% of organizations reported complete alignment between security teams and business leadership on AI objectives, down from 35% in 2024.

One of the biggest contributors to this gap is the visibility of relevant data. This becomes problematic in AI-driven environments where systems require broad and timely access to high-quality data. If that data is poorly classified, inconsistently governed, or insufficiently monitored, the risk of regulatory noncompliance, reputational damage, or operational disruption increases. Some of the biggest challenges organizations are facing with regard to visibility are:

- **Data volume and access risk:** Enterprise data estates continue to expand due to mergers and acquisitions, regulatory retention requirements, and AI experimentation. Legacy data often persists without clear ownership, and overprovisioned access, whether to third parties or internal departments, introduces hidden liabilities. As AI systems draw from larger and more distributed data sets, these unmanaged exposure points can amplify risk.

AT A GLANCE

KEY STATS

According to IDC's *Data Security and Privacy Survey*:

- Only 29% of respondents felt that security teams and business leadership were completely aligned on AI objectives.
- Only 33% felt they had more than 75% of their sensitive data mapped, organized, and monitored.
- 72% of respondents indicated they had more than 75% of their confidential data mapped.

KEY TAKEAWAYS

- Organizations struggle with the ambiguity of classifying and monitoring sensitive data.
- Sharing the responsibility of organizing and controlling sensitive data with business units/data owners via data democratization can offer a balanced approach for securing data for use in AI.

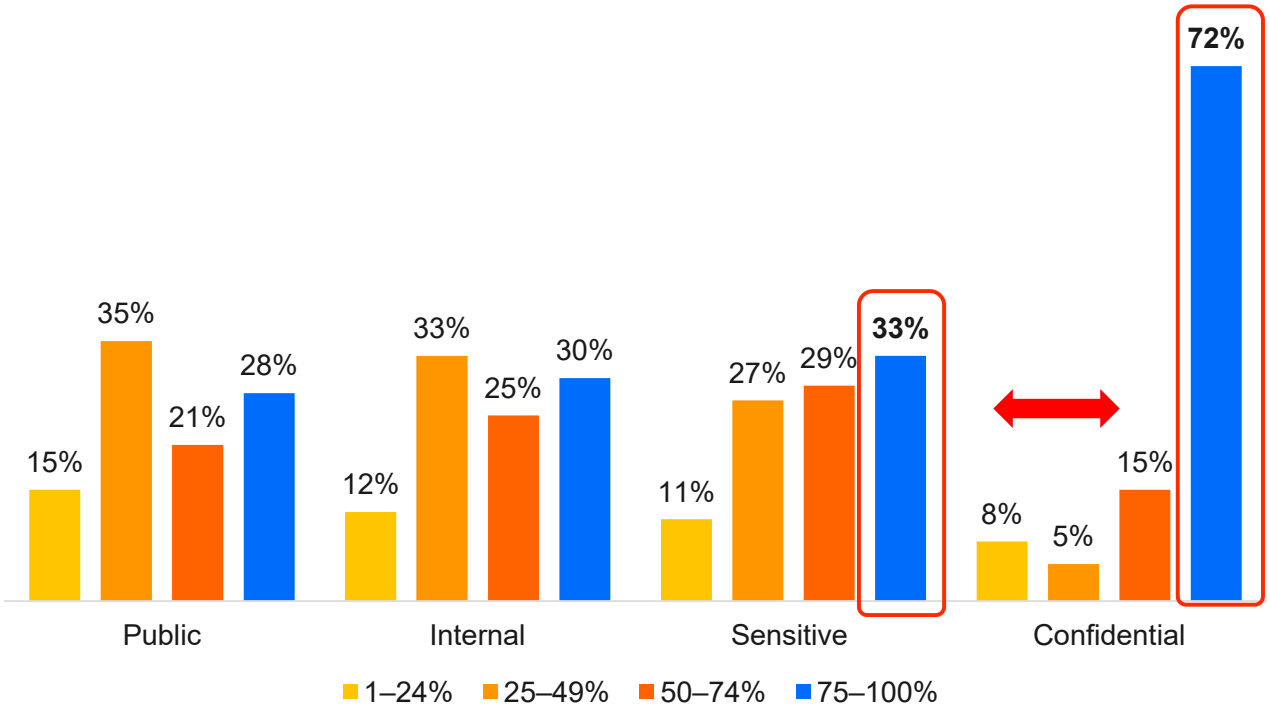
- **Classification challenges:** IDC defines confidential data as information that, if exposed, would have a significant negative impact on business operations, such as company secrets or intellectual property. Sensitive data is defined as information that is subject to regulations and could result in compliance or privacy violations. This includes personally identifiable information and personal health information. It is revealing that in IDC's April 2025 *Data Security and Privacy Survey,* 72% of enterprises reported that three-quarters or more of their confidential data is visible and mapped, yet only 33% could say the same about their sensitive data (see Figure 1). This suggests that organizations may have clearer definitions for confidential information than for more nuanced categories such as employee, customer, or regulated data. Inconsistent definitions across business units complicate governance and increase compliance risk.

- **Tool sprawl and operational complexity:** Security tool sprawl is another obstacle. 16% of C-suite leaders identify managing multiple independent security products as a major challenge. Fragmented tooling environments reduce visibility, increase operational overhead, and complicate the enforcement of consistent policies. As enterprises scale AI initiatives and democratize data access, disjointed control frameworks become increasingly difficult to manage.

FIGURE 1: ***Mapping sensitive data poses a challenge for the enterprise***

Respondents cited more confidential data appropriately mapped and monitored

Q *What percentage of each type of data has visibility within the organization (i.e., is mapped, on a dataflow, organized, and monitored)?*



n = 618

Note: Respondents to the survey indicated that they had more of their confidential data mapped and visible, compared with their sensitive data.

Source: IDC's Data Security and Privacy Survey, April 2025

These findings point to a structural imbalance: Enterprises are leaning into AI, but visibility and governance of their most sensitive information remain incomplete. Data democratization, when paired with unified classification and shared accountability, offers a framework for balancing innovation with risk mitigation.

Considerations for data democratization as a governance model

Data democratization refers to making data broadly accessible across the organization to support informed decision-making and innovation. However, democratization is not synonymous with unrestricted access. Security and business leaders should consider these five priorities to enable AI while minimizing organizational risk:

- **Improve data visibility prior to access expansion:** Mapping and monitoring sensitive data, including where it resides, how it is being used, and who has access to it, must precede large-scale AI deployments. From a priority standpoint, visibility is essential. Without it, there is no way to adequately prepare data for AI initiatives.
- **Unified data classification:** Democratization relies on a common understanding, particularly when it comes to the value of enterprise data. Organizations should establish enterprisewide definitions of sensitive, confidential, customer, and employee data that reduce governance ambiguity.
- **Consolidation and integration of security controls:** Complexity breeds chaos. Multiple dashboards make it hard to visualize the entire data estate, and conflicting policies from multiple tools complicate action. Organizations should seek to minimize the number of data security tools to better align actions with business initiatives.
- **Resource optimization through collaboration:** AI has expanded the scope of data security to multiple teams outside of the department. Compliance, privacy, legal, and HR teams also have a stake in how data is used and treated. In addition, data management teams, data owners, and analysts are also concerned with data security because it impacts the value that data offers. Organizations can address staffing constraints by distributing governance responsibilities and leveraging automation.
- **Shared accountability models:** Shared responsibility of data security is not the same as shared accountability. Data security teams should empower business units to participate in classification, life-cycle management, and access decisions while maintaining centralized oversight.

Benefits of data democratization

When implemented effectively, democratization shifts some responsibility for organizing and controlling sensitive data to the business units and data owners most familiar with its context and value.

Engineering teams, for example, understand which data sets are mission critical, which carry regulatory implications, and how data flows across systems. By involving these stakeholders in classification and life-cycle decisions, organizations can align security controls more closely with operational realities.

This distributed model does not diminish the role of central security teams. Rather, it reinforces governance by embedding it within business processes.

Other benefits of this model include:

- **Accelerated innovation and AI readiness:** Democratized data frameworks enable faster AI development by ensuring that relevant, well-governed data is readily accessible. Removing redundant, obsolete, and trivial data and scrubbing repositories of unnecessary sensitive information reduces risk and friction. This approach supports AI experimentation while maintaining guardrails.
- **Improved risk management:** Business units often have deeper contextual knowledge of the implications of data misuse. By sharing responsibility, organizations can identify risks earlier and make more informed decisions about appropriate controls.
- **Enhanced regulatory compliance:** Audits and regulatory reviews are resource intensive. Democratized visibility allows business units to focus on the compliance requirements most relevant to their data domains, improving preparedness and reducing delays.
- **Cross-functional collaboration and efficiency:** Data democratization encourages collaboration among compliance, legal, privacy, and business teams. A unified framework can also help reduce tool sprawl and improve consistency in policy enforcement, supporting operational efficiency.

Data democratization shifts data security from a centralized reactive function to a shared organizational responsibility.

Conclusion

AI is accelerating the demand for accessible, high-quality data, but it is also exposing foundational weaknesses in how enterprises classify, monitor, and govern their most sensitive information. Data democratization offers a path forward. It shifts data security from a centralized, reactive function to a shared organizational responsibility. Prioritizing visibility, establishing unified classification standards, consolidating controls, and clarifying accountability can help organizations realize value from their AI initiatives without incurring additional risk.

About the analyst

Jennifer Glenn, *Research Director, Information and Data Security*

Jennifer Glenn is research director for the IDC Security and Trust Group and is responsible for the information and data security practice. Ms. Glenn's core coverage includes a broad range of technologies, including messaging security, sensitive data management, encryption, tokenization, rights management, key management, and certificates.

MESSAGE FROM THE SPONSOR

AI didn't just knock on the door — it kicked it in. As organizations race to unlock value from data with GenAI, copilots, and agentic workflows, security teams are facing a familiar tension at an entirely new scale: how do you protect data without slowing the business down?

Organizations can approach the challenge by focusing on key areas that include putting fixes into the hands of data owners, making risk clear to non-security teams so they can focus on what matters most, and empowering business unit owners to manage their own data risk.

Cyera's approach to data security democratization enables organizations to break down silos and drive accountability. It makes data security a team effort, empowering employees from across the business to understand and act on data security risks they are responsible for.

Explore how we're reshaping data security democratization:

Cyera Data Security Democratization

From Discovery to Action: The Security Playbook for Data Democratization at Scale

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
One Beacon Street
Suite 33100
Boston, MA 02108, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com