Analyst Connection, sponsored by:
Cyberhaven

Data Security for the Agentic Enterprise

QUESTIONS POSED BY:

CYBERHAVEN

ANSWERS BY:

Jennifer Glenn

Research Director, Information and Data Security

PUBLISHED:

August 2026

Agentic AI is reshaping enterprise workflows, and trusted data is essential for successful implementations. This Q&A outlines a framework of visibility, lineage, and action to help organizations build a trusted data foundation.

Q1. What do research and market trends reveal about how AI adoption is transforming organizations today?

According to IDC's *Future Enterprise Resiliency and Spending Survey* Wave 8/9 (December 2025, n = 1,897), more than half of organizations already have AI agents running in production, whether within a single business area or across multiple functions. Furthermore, agentic AI is expected to account for roughly 38% of enterprise AI budgets this year, rising to 41% next year.

This shift is not purely financial. Instead, it represents a major change in how work itself is done within the enterprise. Workflows used to run human-to-human. Now they also run human-to-agent and agent-to-agent, often at the same time. This fragments, transforms, and multiplies data at machine speed. Further, when every competitor has access to the same agentic models, the differentiator shifts to the valuable data underneath them. Trusted data is secure, accurate, monitored, and well-governed. Without that foundation, an agent just automates bad decisions faster.

For many organizations, gaps in data hygiene stand in the way of building that foundation. According to IDC's *Data Security and Privacy Survey* (April 2025, n = 618), organizations consider nearly half of their data to be sensitive or confidential, yet less than a third have mapped and monitored more than 75% of it.

Q2. How has the shift in workflows changed risk?

That move from human-to-human work to a mix that also includes human-to-agent and agent-to-agent work is itself what changed the risk. Where workflows used to scale with headcount, they now scale with every agent added to the mix, so the number of connections accessing and using sensitive data grows exponentially. More use means more opportunity for sensitive data to be compromised or exfiltrated.

Furthermore, instead of securing a single, static document or database at a point in time, security teams now have to protect data as part of an ever-evolving process. Policy has to adjust in real time as agents pick up new data, new permissions, or new tasks, rather than being set once and left alone.

Q3. What does data security for the agentic enterprise look like in practice?

In practice, the framework for data security in the agentic enterprise rests on three components: holistic visibility across the environment, a deep understanding of data through lineage, and the ability to act on that understanding when and where it matters. Visibility is only part of the solution. Pairing the context provided by data lineage graphs with real control and action makes the framework work as environments change.

This shifts security from a forensic function to a preventive one by identifying and remediating risk at the moment humans and agents are touching data, before it results in lost data or a compliance or privacy violation.

Q4. How should organizations start implementing actionable data security for agentic deployments?

Organizations should start by closing the visibility gap. According to IDC's *Data Security and Privacy Survey* (April 2025, n = 618), only 46% of organizations have adopted data security posture management, while just 30% have implemented dedicated discovery and classification tools. This is evidence of how far most organizations still have to go before they can see where sensitive data lives or how it is moving across their environment.

Once visibility is established, the next step is to build enough context to understand how AI is interacting with that data, including where, when, and what transformations are occurring as it moves between people, applications, and agents. Context turns the visibility "map" into a clear, actionable picture of risk.

The last step is ensuring that enforcement keeps pace with agent deployment. IDC's *Future Enterprise Resiliency and Spending Survey* Wave 8/9 (December 2025, n = 1,897) found that 44% of organizations plan to significantly increase spending on building customized AI agents in 2026. If the mechanisms enforcing policy do not scale at the same rate, the gap between agents deployed and agents governed only widens. In practice, this means extending data loss prevention and data access governance to treat AI agents as identities in their own right, not just an extension of the human who deployed them; this means the same controls that could quarantine a file, block an exfiltration attempt, or revoke a user's access can just as easily clamp down an agent's permissions, kill an active session, or roll back a change it made in error.

Q5. What should organizations look for in a partner?

Three criteria separate strong data security partners from the rest. The first is architecture. Does one platform cover structured and unstructured data, on-premises systems, cloud, SaaS, endpoints, and AI tools and agents, or does covering that ground take three separate tools stitched together? Unifying data security posture management, data loss prevention, insider risk management, and AI security into a single view makes that breadth usable rather than just comprehensive.

The second criterion is depth of understanding. Data context and agent intent separate partners that can act from those that can only alert. Tracking sensitive data provenance through every transformation to where it ultimately flows turns a simple inventory of files into an accurate picture of risk and improves classification and policy enforcement enough to ease the investigative burden on security teams.

The third criterion is speed and fit. Most organizations already have investments in discovery, classification, DLP, and access governance, so a partner that extends and connects that stack is worth more than one that demands a rip-and-replace. The best partners also make investigation and response fast enough to keep pace with agents: plain-language queries that surface risk instantly, policies that adapt as new data sources and use cases appear, and administration that does not require standing up new infrastructure. To be a partner that can show where data lives, understand what is happening to it, and act on both without slowing agents down is the standard to which every data security vendor should be held in the agentic era.

About the IDC analyst

Jennifer Glenn
Research Director, IDC

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 encompasses a broad range of technologies, including messaging security, sensitive data management, encryption, tokenization, rights management, key management, and certificates.

Message from the sponsor

Cyberhaven is a leader in data security for the agentic enterprise, trusted by the world's most innovative companies to protect their most sensitive data. It traces the full life cycle of your data, adapting protection as context changes. Cyberhaven protects workflows, not just data, by connecting lineage, identity, and behavior to understand how data is created, copied, fragmented, and shared across workflows. Operating in real time where humans and agents act on data, Cyberhaven helps stop risk before it becomes loss. AI changed work. Cyberhaven protects it. Learn more at cyberhaven.com.

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

IDC Research, Inc.
One Beacon Street, Suite 33100, MA 02108, USA
T +1 508 872 8200

blogs.idc.com | LinkedIn @IDC | www.idc.com

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community make fact-based technology decisions and achieve their key business objectives.