An IDC Analyst Brief, sponsored by Logicalis
May 2026

Security in an Age of AI: Why Data Governance Makes the Difference

David Clemente
Research Director
European Security Services, IDC

ANALYST BRIEF
Sponsored by: Logicalis

As organizations get serious about implementing AI agents, they also need to address governance challenges. For security leaders, robust data governance is becoming an essential mechanism that enables organizations to deploy agents quickly, confidently, and securely.

Security in an Age of AI: Why Data Governance Makes the Difference

May 2026

By: David Clemente, Research Director, European Security Services

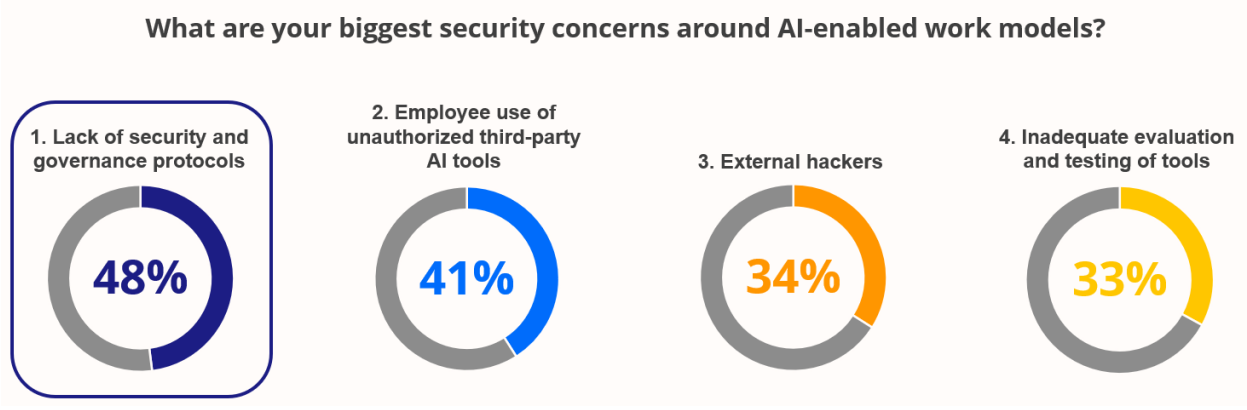
A shift is taking place in 2026. Organizations are moving from AI experimentation to implementation, and doing this in functions across the business. As a result, AI security is quickly becoming less about protecting models and more about governing what AI — specifically, agentic AI — is allowed to do with enterprise data.

That change matters because organizations are entering the agentic era at an industrial scale. IDC projects more than **1 billion AI agents by 2029**, executing around **217 billion actions per day**. In that world, organizations cannot afford to have automated decisions and actions taken with the wrong data, the wrong permissions, or the wrong oversight.

Extending governance to agents

IDC research shows that the top global concern around AI in the enterprise is lack of security and governance (Figure 1 below). Given the speed and variety of ways that AI is being introduced into industries of all kinds, these concerns will limit the return on AI investment until sufficient governance is implemented.

Figure 1 AI-Related Security Concerns



Note: Multiple choice question; total will not equal 100%.

Source: IDC Worldwide Future of Work Survey 2025 (n = 1,440)

For security leaders, the rapid expansion of agents makes data governance an essential part of AI deployment. This includes ensuring that identity, access control, and auditability all have the desired level of sovereignty. Data governance has traditionally focused on organizing data (e.g., catalogues, quality, stewardship) and protecting it (e.g., classification, retention, access control). In an agentic AI world, those fundamentals are still necessary but are no longer sufficient.

Governance must extend to retrieval (what the AI can search and summarize), tool use (what systems it can call), and change authority (what it can create, approve or modify). Successful organizations will treat data governance as an integrated security approach for AI, that unifies identity, data access, and orchestration.

Shining a light on shadow AI

Most organizations are already living with "shadow AI", including employees using unsanctioned tools, browser plug-ins, chatbots, or ad hoc integrations. Shadow AI and unsanctioned AI tools are key vectors of enterprise data leakage, particularly when those tools are connected to enterprise knowledge bases that lack uniform access controls.

The response from security leaders should be to make the secure path the easiest path, by providing approved AI that is easy to adopt, covered by enterprise identity, logging, and data loss prevention, and visible to the organization's security operations. This must all be covered by consistent governance, so the same policies apply whether data sits in a warehouse, a data lake, a ticketing system or a collaboration platform.

Building a strong foundation

Getting the architecture right is the single biggest step in enabling strong and consistent data governance across the organization. A common failure mode in enterprise AI is deploying the wrong architecture and then trying to compensate with process.

Creating a secure architecture for AI requires moving beyond traditional, data-centric models toward flexible systems designed to enable work across complex, fragmented enterprise environments.

Key governance actions to strengthen security and unlock AI value

- **Embed security by design**: Implement Zero Trust principles and ensure AI actions are auditable, explainable, and compliant with regulations such as GDPR, NIS2, and the EU AI Act. This helps to deliver the AI and data sovereignty capabilities that business leaders are increasingly seeking.
- **Extend access control to AI**: Apply context-aware permissions so each agent only accesses the data required for its task, ensuring consistent governance across all systems and data types. IDC research shows that identity security and governance are a top priority for most technology leaders. They know that the risks of getting identity wrong with AI can be significant.
- **Use the right architecture for the task**: Build for single agents when the need is to execute well-defined, isolated tasks, and design for multi-agent systems when workflows are complex, interdependent, and require tight orchestration.

- **Shift from data organization to enablement**: Move beyond traditional data warehouses toward architectures that provide real-time, task-oriented access to data across all formats, supported by a common semantic layer.

The benefits of robust data governance

Enabling AI in the enterprise is not only a technical upgrade but also a shift in strategy. Organizations that succeed will be those that build integrated platforms where security, data access (e.g., via strong identity controls), and orchestration are included from the start, with a governance layer sitting across everything. The benefits of governance include:

- **Trust in AI systems**: With mature oversight and controls, organizations can better explain how AI systems use information and make decisions. This transparency increases confidence and builds trust with customers, employees, and regulators.
- **Effective collaboration**: Clear policies make it easier to share data across teams and systems while maintaining appropriate safeguards. This allows organizations to unlock value from their data without compromising security.
- **Reduced risk of data breaches and misuse**: Strong governance establishes clear policies for how data is stored, accessed, and shared. This lowers the likelihood of breaches, leaks or inappropriate use, which is especially important as AI systems often process large volumes of sensitive data.
- **Better regulatory compliance**: Governance helps organizations meet legal and industry requirements by ensuring proper data handling, retention, and auditability. This reduces the risk of fines, legal liability, and reputational damage.

Conclusion: Secure AI starts with data governance

By applying data governance principles to rapidly evolving AI capabilities, businesses can create an environment that is secure and capable of delivering meaningful, scalable AI-fueled innovation.

The message for security leaders is simple. As agents permeate the enterprise technology stack, data governance becomes the primary security control. At a projected scale of 1 billion agents and 217 billion actions per day, organizations cannot rely on manual approvals, best-effort documentation or after-the-fact security controls.

They need a governance model that offers security by design, robust identity, context-aware access, and auditability in the platforms where AI operates.

Done well, this is not a brake on innovation. It is how organizations unlock AI value at enterprise scale. Agentic AI is becoming a material share of IT spending, and the strategic move now is to treat governance as a critical enabling capability. Build the right architecture, then let teams deploy agents quickly and confidently, without renegotiating security and trust from scratch every time.

About the Analyst

David Clemente: *Research Director*

Dave Clemente is a research director in IDC's European Security practice, with a focus on security services (including managed services and professional services). He is a research professional with more than fifteen years of experience in cybersecurity, including in think tanks (Chatham House and the International Institute for Strategic Studies), professional services, and market analysis. Dave is a regular conference speaker and media contributor and has authored numerous publications on topics including C-suite technology and security priorities, security policy and governance, risk management, and data protection.

MESSAGE FROM THE SPONSOR

As a global security managed services provider, Logicalis sees data governance as the key to making AI secure and scalable. This analyst paper argues that as agentic AI scales, security shifts from protecting models to governing what AI can access and do with enterprise data. Extending governance across identity, permissions, auditability, and tool use reduces shadow AI risk and enables safe AI at scale.

To learn more, please visit www.logicalis.com.

IDC Custom Solutions

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

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com