No AI visibility, no confidence

Blind spots don’t just hide AI threats — they erode confidence in controls

AI PULSE SURVEY — VOL. 4

protiviti®
Global Business Consulting

Table of contents

Executive summary

There's a dual reality playing out in today's cyber landscape: IT leaders see threats enabled by artificial intelligence (AI) rising significantly on the front lines, while views from the C-suite are more moderate, according to Protiviti's latest AI Pulse Survey, which focuses on cybersecurity and resilience. That same disconnect shows up in leadership's visibility into employees' AI tool usage, where we found that many large organisations[1] (**47%**) and medium-sized organisations[2] (**68%**) face unmanaged AI exposure or shadow AI.[3] In essence, boards are funding and governing risk based on an incomplete picture of what's happening across the enterprise.

Traditionally, these discrepancies have been attributed to the lag that organisations often encounter with new technology adoption and the time it takes for risk outcomes to surface, be measured, and reported up to management and the board. But in today's elevated AI-threat landscape, these delays are serious and warrant careful consideration; they can translate into slower prioritisation, underfunded controls and governance decisions made on stale signals.

There's encouraging news; most leaders acknowledge that AI is escalating cyber risk and are confident that their security controls are keeping pace with threats. But that is tempered by the fact that nearly one in three executives lack confidence in their controls, according to the survey.

Why does all this matter? Nation-state actors and other malicious groups are increasingly using AI to accelerate and scale cyberattacks, exploiting enterprise weaknesses in areas such as third-party software, SaaS applications and supply chains.[4] As AI models with enhanced coding, reasoning and autonomous security capabilities are developed, the effort to identify and fix these vulnerabilities before they are exploited by threat actors may prove increasingly challenging to sustain.[5]

These external threats underscore the need for strong cyber risk management — but they also raise an equally important internal question: Do organisations have clear visibility and control over how AI is being used inside their own environments? Without that internal visibility, leaders are operating with blind spots — regardless of their overall cybersecurity maturity, resources or scale.

Implementing a formal AI governance framework does not stop cyberattacks or eliminate external threats. Instead, it addresses a different — but critical — challenge: governing internal AI use with clarity, accountability and consistency. It acts as an assurance accelerator by establishing clear ownership, defining acceptable use standards, and setting monitoring expectations for AI systems and tools in use across the organisation.

Also, the survey found that better AI security confidence often goes hand in hand with formal AI governance, as it provides leadership with measurable oversight rather than relying on assumptions.

[1] In this survey, large organisations are defined as those with more than $5 billion in revenue.
[2] Medium-sized organisations are those with revenues from $100 million to $5 billion.
[3] Shadow AI is the use of AI tools, models or AI-enabled features inside an organisation without formal approval, visibility, or governance controls — often outside IT/security oversight.
[4] Deepfake fraud, for example, is now the fastest-growing social engineering threat to businesses, rising 3000% in North America in a single year, according to Onfido.
[5] In April 2026, Anthropic reported that its Claude Mythos model can identify thousands of potential zero-day vulnerabilities across major operating systems and web browsers, making its full public release too risky.

Notable findings

01

A major blind spot — AI tool use

- Full visibility into AI usage remains the exception, not the norm — especially for mid-sized firms, where **68%** report only partial or no visibility.
- **Among large organisations**, only **53%** *report full visibility* into employee AI tool usage — meaning **47%** face shadow AI.

02

The threat perception gap

- 45% of operational security or IT leaders say AI has increased cyber threats significantly, while **30%** of C-suite/board leaders view the threats as significant.
- When risk feels abstract at the top, organisations are more likely to **underfund detection and response**, delay decisions and overestimate the maturity of AI control testing.

03

Confidence in security controls is not universal

- Nearly **one in three leaders lack strong assurance** that security controls are keeping pace with AI-driven threats.
- Confidence diminishes further as you move from the C-suite to operational teams.

04

Formalised frameworks: an assurance accelerator

- **64%** of **large** organisations have a formal enforced framework versus **30%** for **small** organisations.
- Where governance is formalised, leaders report stronger assurance signals (visibility, training and defensive AI usage).

05

AI threats from third parties

- **32%** of organisations cite *implementing more stringent vendor security standards* as their top action for managing embedded AI risk.
- A close second overall: *proactive AI-specific training for executives and staff*.

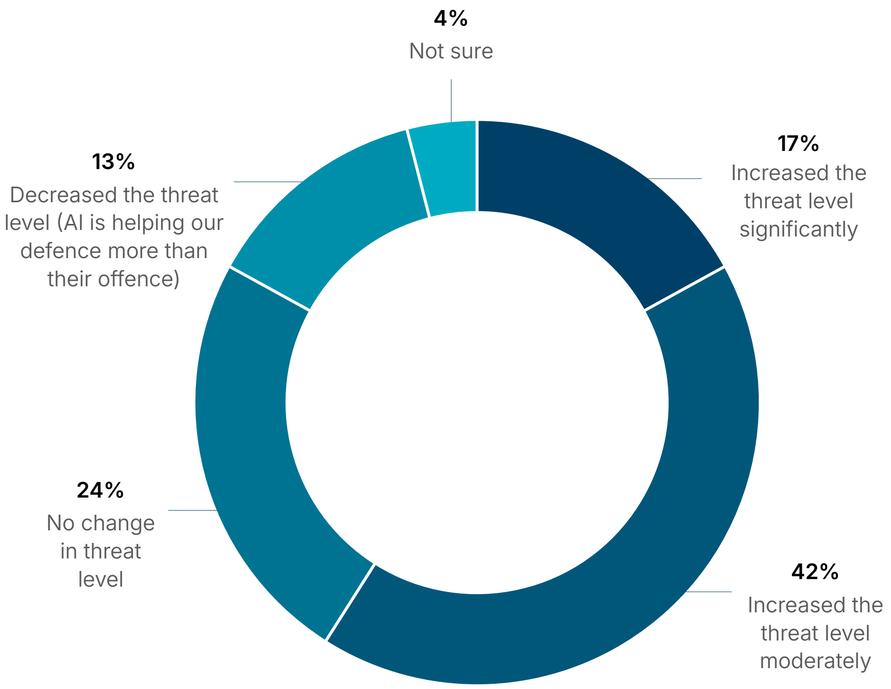
Perception gaps have real consequences

Nearly half of IT leaders believe AI has increased cyber risk significantly, versus 30% of C-suite executives and board members. Confidence in security controls diminishes the further you move away from the C-suite to operational teams.

This misalignment has real implications:

- Delays in decision-making can impede containment and communication, particularly with deepfake and other AI-enabled cyberattacks where every minute counts.
- Overconfidence in cyber controls can translate into undertesting of AI controls and processes, potentially leading to significant business risks as leaders race to adopt AI without fully understanding the dangers.
- Board support and funding are at risk if threats are underappreciated and unmanaged.

Figure 1: **Topline threat-level assessment — overall results**



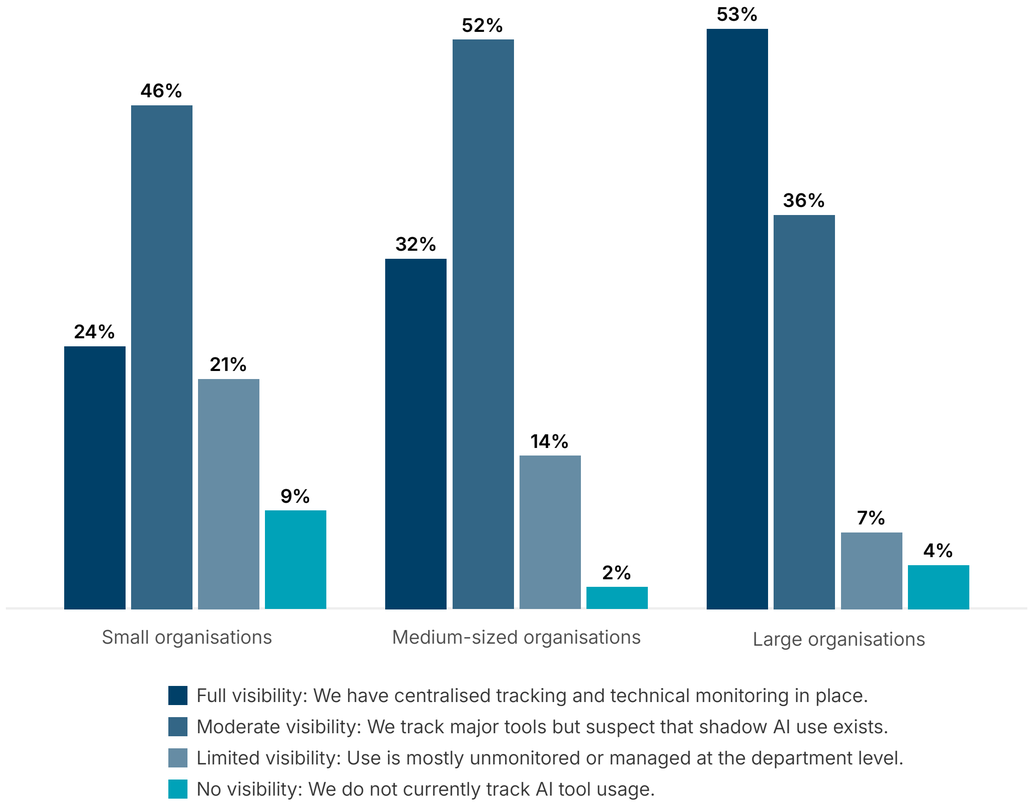
Size doesn’t beat blind spots

Two-thirds of organisations are experiencing challenges with AI systems being deployed or used by employees without proper oversight, leading to control gaps. Most of these are small organisations[6] that have less sophisticated discovery capabilities, weaker vendor supervision and less rigorous approval processes. In these situations, shadow AI thrives and goes unnoticed.

But even among medium-sized and larger firms with more resources, there are blind spots. Redundant tech platforms, loose control and inconsistent compliance, likely due to multiple business units, regions and merger-and-acquisition deals, could be why 47% of large organisations lack full visibility. For medium-sized organisations, that percentage reporting weaker visibility into AI tool usage rises to 68%.

The key takeaway: When leaders don’t see their own blind spots, they miss the shared urgency for detecting threats. Without transparency, unapproved AI tools and extensions can be used freely, consent policies can become inconsistent and data protection may weaken.

Figure 2: **How would you describe your organisation’s visibility into the specific AI tools (both authorised and unauthorised) currently being used by employees?**



[6] In this survey, small organisations are defined as those with less than $100 million in revenue.

4 in 10

organisations — 41% — have a formal AI governance framework. Another 43% indicated they are in the process of implementing a framework.

Why formal frameworks matter

The survey finds that higher formal AI governance framework adoption correlates positively with higher AI tool visibility, regardless of organisation size. From a role perspective, leaders who acknowledged having formal frameworks were more likely to call the AI risk increase "significant."

The results also show that a formal AI governance framework is a good proxy for evidence-based assurance — namely, tool visibility and testing, which is associated with higher confidence. Where frameworks are formalised — and visibility is higher — leaders feel more assured that controls can keep pace.

Table 1: **Frameworks align with higher assurance in controls**

Lens	Formal framework in place	Full AI tool visibility	Less than confident in security controls
Overall	41%	35%	30%
Large organisations	64%	53%	21%
Medium-sized organisations	39%	32%	26%
Small organisations	30%	24%	39%

Third-party embedded AI: Where visibility is won or lost

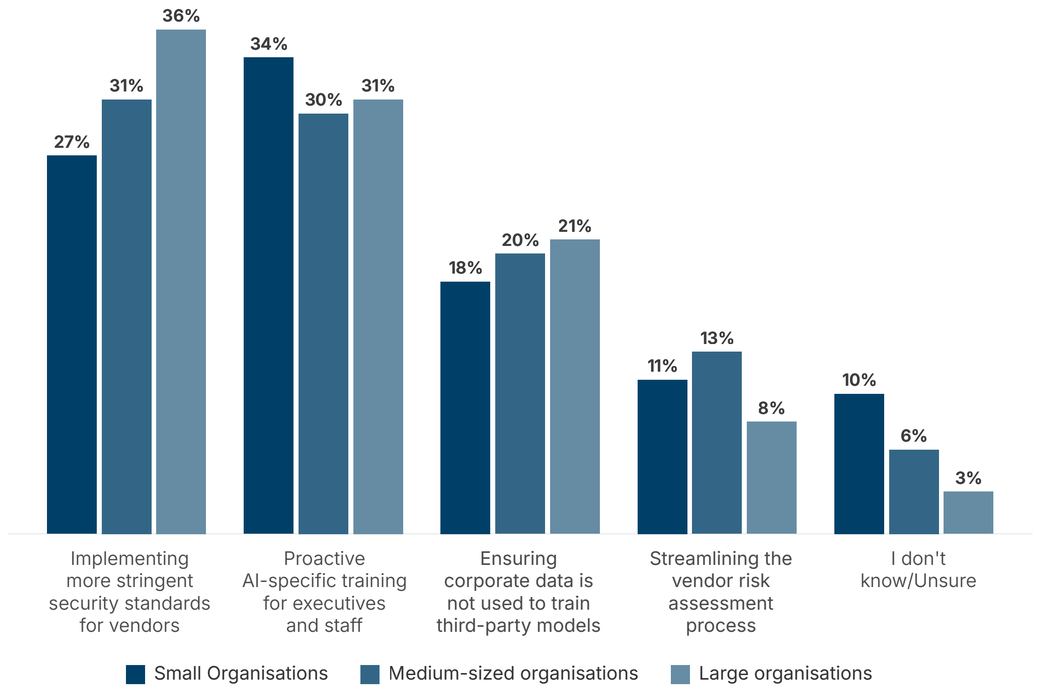
One reason that organisations struggle to track AI usage and where it occurs is the rapid pace at which technology vendors are embedding AI into enterprise tools and platforms. The presence of vendor-controlled AI that isn't subject to oversight or scope limitations is a major blind spot for many organisations.

In the survey, leaders were asked to identify how they are managing embedded AI risk in vendor software; implementing more stringent vendor security standards came in as the top priority, followed by AI-specific training for executives and staff.

According to the survey, as businesses scale, they most commonly rely on strengthened vendor security standards to address AI risks posed by vendors. The second-highest priority for large companies is providing AI-specific training to their executives and staff, underscoring the importance that businesses place on human decision-making for routine approvals and decisions.

The "Do not train on our data" priority reflects growing scrutiny of data governance, retention and secondary use in vendor AI features. Larger firms' rising emphasis here points to maturing contractual controls and auditability expectations.

Figure 3: **What is your organisation's top priority in managing risks posed by embedded AI in third-party vendor software?**



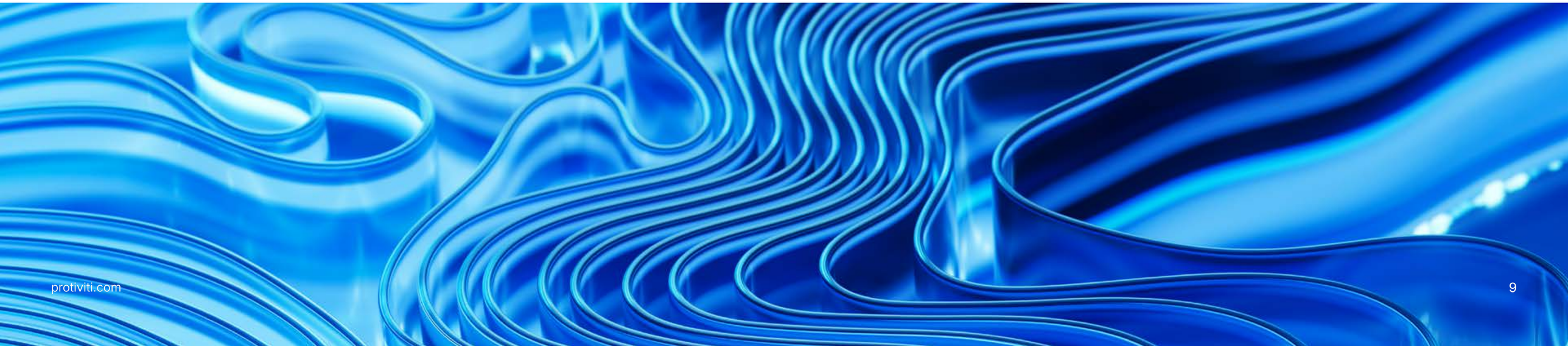
* 1% of large organisations selected "other"

Defensive AI and training: The ultimate confidence builder

AI is extensively employed in the security stacks of nearly a quarter of the organisations we surveyed. Grouped by size, large organisations make up 42% of the most significant users of AI for security, in contrast to 21% of medium-sized companies and 15% of small ones.

In the current elevated threat environment, having AI in the security stack can provide organisations the speed and pattern-recognition advantages that attackers are already deploying. Equally important is comprehensive training beyond just fundamental AI instruction to foster a cultural change and increase cybersecurity confidence among leadership and employees.

The survey results show that organisations that combine defensive AI measures with robust training have better insight into how employees are using AI tools across the enterprise. This improved understanding is connected, as discussed earlier, to a rise in confidence in security capabilities among leaders and for businesses of all sizes.



You can’t defend what you can’t see; invest in enablers

Organisations that feel most confident in managing AI security risks are those that invest most in concrete capabilities that convert intent (we take AI risk seriously) into evidence (we can see, govern and defend it). Here’s a recap of the capabilities or enablers:

- **Formal AI governance framework:** It enables clear acceptable-use rules, ownership, accountability and enforceable guardrails across the enterprise — so AI doesn’t sprawl faster than controls.
- **AI tool monitoring:** You can’t manage what you can’t see. Investing in monitoring capabilities will enable your organisation to detect threats — specifically, shadow AI — early while enhancing compliance, including data protection, and proving controls are working.
- **Organisational readiness and resilience:** This reduces human-driven failures and builds consistency in “how we work” with AI.
- **Using AI to fight AI:** Employing AI in the security stack means faster detection of cyberattacks, better pattern recognition and improved response against AI-accelerated threats.
- **Vendor controls for embedded AI:** This closes a growing blind spot as AI features proliferate inside SaaS and third-party platforms. Where AI is “hidden in the stack,” more stringent vendor security standards and AI-specific training are crucial.

Contacts

Sameer Ansari

Managing Director, Protiviti
sameer.ansari@protiviti.com
Let’s connect on LinkedIn.

Andrew Retrum

Managing Director, Protiviti
andrew.retrum@protiviti.com
Let’s connect on LinkedIn.

Tom Andreesen

Managing Director, Protiviti
thomas.andreesen@protiviti.com
Let’s connect on LinkedIn.

Survey demographics and methodology

This AI Pulse Survey was conducted in February 2026. Nearly 900 participants (n=863) completed our questionnaire, including 150 board members and C-suite executives. However, to gain a deeper understanding of technical, operational and executive perspectives on AI, the report isolated responses from C-suite, board and IT leaders.

Among C-suite participants, CEOs represented the largest share (37%), followed by CTOs (19%) and CIOs (13%), CFOs (11%) and COOs (10%). From a function perspective, IT leaders comprised nearly one-third of respondents (31%), while operations accounted for 21% and finance represented 10%.

Responses were gathered from a diverse range of industries, led by technology (10%), government agencies (8%), retail (8%), manufacturing (7%), and aerospace and defence (6%). Geographically, the survey reflects a broad international footprint, with the United States accounting for 41% of respondents, followed by India (14%), the United Kingdom (12%), Australia (10%) and Canada (9%).

Medium-sized organisations ($100 million to $4.99 billion in annual revenue) accounted for the largest share of respondents, while smaller organisations (under $100 million) represented over a quarter of the total sample. Approximately one-fifth of respondents represented organisations with $5 billion or more in annual revenue.

About Protiviti's AI capabilities

Protiviti helps organisations prioritise, build and deliver AI solutions that create measurable business value. We focus on delivering AI that is innovative, controlled and accountable to your business, ensuring every capability is secure, transparent and aligned to your goals. Our teams build AI solutions that clients can trust so their reputation and results lead the way, supported by strong governance, responsible design and solutions that scale confidently across the enterprise.

We also help organisations manage change and maximise adoption, empowering people to learn, adapt and lead with confidence. Through our AI Studio, proprietary accelerators, technology partners and AI Factory, we provide end-to-end strategy, solution development deployment and ongoing lifecycle oversight — serving as a trusted managed services partner to keep AI safe, effective and continually delivering value.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps clients transform and protect their businesses, and respond to planned and unexpected events. Through a network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned member firms deliver deep expertise and tailored capabilities across technology, artificial intelligence, data, operations, finance, legal, compliance, HR, marketing, digital, risk, and internal audit—enabling organisations to accelerate innovation, navigate risks and safeguard what matters most.

Named to the *Fortune* 100 Best Companies to Work For® list since 2015, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

Face the Future with Confidence®

protiviti®
Global Business Consulting