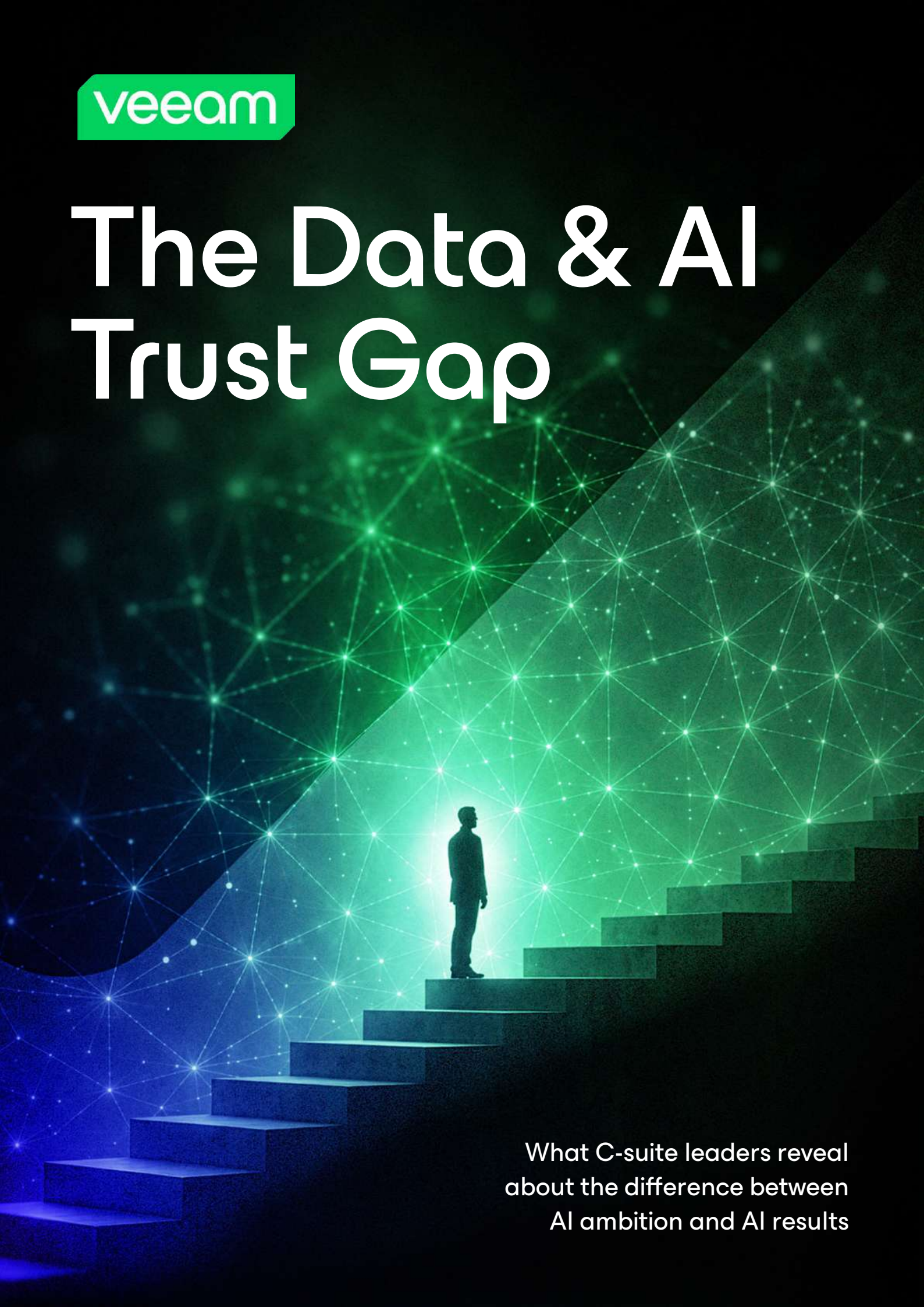
veeam

The Data & AI Trust Gap



What C-suite leaders reveal about the difference between AI ambition and AI results

FOREWORD

Trusted Data, Trusted AI

AI is transforming businesses across all industries. However, to truly realize the potential, organizations must ensure they can trust their data.

Across all organizational sizes, industries, and geographies, businesses are deploying agentic systems that act autonomously. These AI implementations make decisions at speed and operate at a scale no human team can match. The promise is enormous — but so is the risk.

When the data being accessed by an AI cannot be trusted, then the AI doesn't merely underperform; it also runs the risk of compounding errors automatically and at pace. The proliferation of tools used outside security and governance teams' approval processes — or what the industry has come to call shadow AI — is widening that exposure further. 44% of respondents associate shadow AI with increased cyber risk. Currently, only 28% of those who responded to this survey are confident they could detect agents operating outside approved parameters while 47% identify maintaining audit trails for AI decisions as their top compliance concern.

However, there is good news: Regulations are catching up. For example, the EU AI Act is elevating data and AI governance from an internal best practice to a legal and commercial imperative, with more likely to follow.

Veeam CEO Anand Eswaran observes, "The infrastructure to deploy AI exists but the infrastructure to trust it doesn't." It is against this backdrop that Veeam has identified four conditions that, when combined, define what it means to truly trust your data:

- Clear visibility into where data lives and how it flows
- Enforced controls rather than policy alone
- Recovery that is tested and validated
- Executive alignment around ownership and accountability

Crucially, each condition is necessary, and none is sufficient alone.

Of these four conditions, executive alignment is the one most often absent, and the one on which all the others depend. Without leaders who are willing or able to own the problem personally, visibility remains incomplete, controls go unenforced, and recovery plans gather dust. This report examines what that leadership gap looks like in practice, what it is costing organizations, and what closing it requires.

83% of CEOs report pressure to accelerate their AI and data capabilities but

97% say data challenges have slowed AI progress

Contents

Executive Summary

Having surveyed 600 senior leaders worldwide, one finding is consistent: Most organizations don't have an AI adoption problem; they have an AI trust gap.

CEOs are more likely than any other role to believe trusted, compliant data could deliver a significant revenue or efficiency uplift. However, believing the opportunity exists and having the foundations to realize it are very different things.

The strategic data opportunity

48%

of CEOs believe making all data secure and compliant could boost revenues by more than 25%

97%

of CEOs say data challenges have slowed AI progress in the past year

This gap manifests in three ways: **perception, activism, and authority.** CEOs and their technical counterparts do not share the same picture of what AI is deployed or who owns it, which creates a trust deficit that undermines well-intentioned governance efforts. That misalignment feeds an activism gap, where data and AI are discussed episodically rather than proactively at board level, which culminates in an authority gap.

Data leadership: the gaps that need to be closed

16%

of CEOs say they are comfortable leading strategic discussions on data

Accountability for agentic AI remains fragmented, with no single role clearly in charge — despite evidence that when ownership is clearly defined, outcomes improve significantly. Detection confidence is 24% higher when CISOs are responsible for AI agent risk. On the other side, that same confidence is 47% lower when the responsibility is shared. This shared ownership doesn't just slow progress, it actively makes outcomes worse.

The governance issue with AI agents

Who trusts their AI inventory?

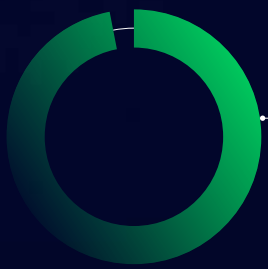
The percentage of each role who says their organization has a complete and reliable AI inventory:

Nobody owns agentic AI risk

The functions that hold primary responsibility for what AI agents do according to respondents:

The organizations that have built the right foundations combine ambition, visibility, and governance. They represent just 7% of those surveyed. Within that 7%, however, 97% of them report significant, formally quantified business outcomes. However, this return remains out of reach until the leadership alignment needed to build it is in place.

Making the connection



97%

of organizations with all three building blocks in place (ambition, visibility, and governance) report significant, formally quantified business outcomes

Data Trust As a Revenue Opportunity

CEOs understand the importance of data, but more must be done across organizations to build trust and break down barriers.

Among C-suite leaders, the strategic value of data is not a matter of debate, and the emergence of agentic AI has only sharpened that conviction. However, the distance between what CEOs believe data can unlock and what their organizations are actually achieving is where the findings from this report become eye-opening.

CEOs are more likely than any other role (48%) to believe that trusted, compliant data could deliver a significant revenue or efficiency uplift; this survey found that 38% of all leaders agree with that perspective. This gap between CEOs and their peers is itself enlightening. It suggests that those closest to the pressure of competitive AI deployment perhaps feel the opportunity most acutely. But feeling the opportunity and having the foundations to realize it are very different things.

The C-suite is not happy with its data

Our organization's data needs to be:

The four conditions of data trust — visibility, enforced controls, tested recovery, and executive alignment — are, by most measures, not yet in place. 79% of C-suite respondents say their organization's data needs to be more up to date, 74% say it needs to be more accurate, and 71% say it needs to be more accessible. In the past 12 months, the challenges cited most as slowing AI progress were inaccurate or inconsistent data (36%), risks from autonomous agent behavior or decision chaining (34%), and data trapped in silos (31%). Data-related issues therefore account for the overwhelming majority of barriers that organizations identify, which is a pattern that points not to isolated technical failures, but to a systemic deficit in the kind of trusted, governed data that safe AI demands.

38%

of all managers think making all data secure and compliant could boost revenues by more than a quarter, but for CEOs this is

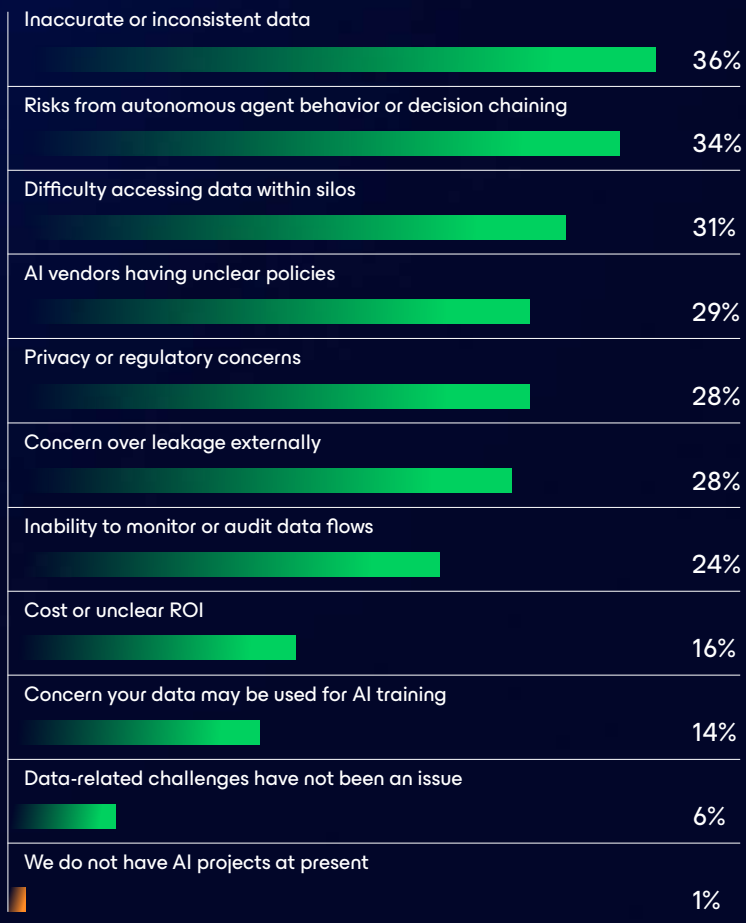
48%

"Data-related issues account for the majority of barriers, which is a pattern that points not to isolated technical failures, but to a deficit in trusted, governed data."

This is due in large part to issues with traceability: 40% report being very confident they could isolate and precisely reverse an agentic AI failure. For organizations already running AI, rapid traceability remains limited. When asked how they could respond within minutes, only 22% felt they could identify which data was used, 29% which systems were accessed, 25% what actions were taken, and 24% what decisions were influenced.

What makes this information particularly consequential is that it exists not despite C-suite awareness, but alongside it. CEOs understand the opportunity that trusted data represents better than anyone else in the room. The challenge then becomes having the organizational readiness to act on it.

Which data-related challenges have slowed your progress in the last 12 months?

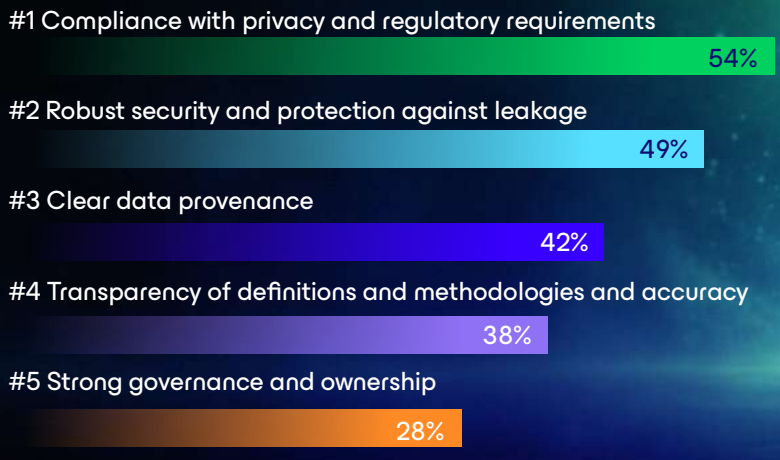


Data Leadership: The Gaps That Need to Be Closed

Compliance and security issues must be addressed to deliver data trust. Leaders should prioritize gaps in perception, activism, and authority.

When asked to identify the most important elements of data trust, the C-suite put defensive priorities above structural ones: Compliance and security ranked ahead of provenance, transparency, and governance. What unites these elements is what they require of the organization: Knowing what data it holds, who is accountable for it, and what standards govern its use. Those are questions that can only be answered — and acted upon — from the top. The research reveals three gaps that are preventing most organizations from getting there.

Compliance is the most important element of data trust



The perception gap: Just over half of CEOs (52%) believe they are engaged and leading by example on data, but of the leaders closest to the data, only 41% of CISOs and 38% of CIOs feel the same.

Part of this disconnect is role based. The CEO and the CISO often have different mental models of where data risk ownership lives. When those don't get reconciled, accountability slips into the gap.

Part of this is a language problem. More than twice as many CEOs as CTOs and CISOs say monitoring and auditing data has slowed their AI progress. The likeliest explanation is definitional: "Auditing" means organizational risk and regulatory exposure to one leader, and a specific set of technical checks to another. When the same words mean different things in the same room, decisions about risk, ownership, and accountability become increasingly difficult to complete. Increasing the frequency, depth, and clarity of C-suite data conversations — and establishing a shared vocabulary around data trust — is the most direct way to close this gap.

"The CEO and the CISO often have different mental models of where data risk ownership lives. When those don't get reconciled, accountability slips into the gap."

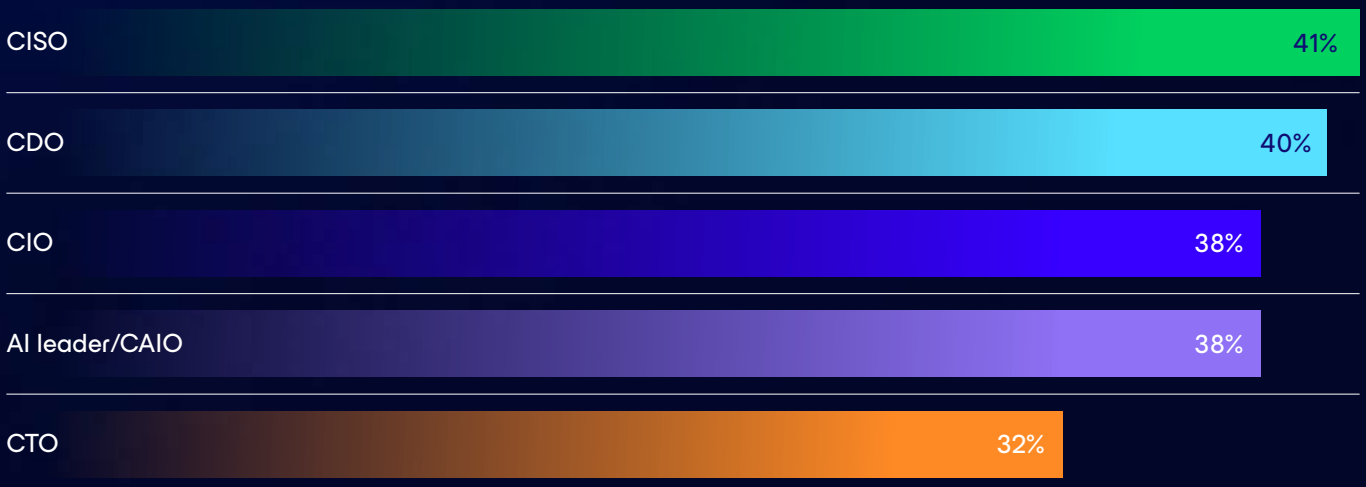
65%

of CEOs believe they have a full AI inventory but only

45%

of data leaders agree

Percentage of senior leaders who say their CEO "leads by example" on data



The activism gap: The second gap is one of activism, and this reflects a broader pattern of reactive rather than proactive data leadership. Senior leaders most commonly discuss data when a strategic opportunity arises (43%) or when a business performance problem needs diagnosing (33%). Just 7% say data discussions are proactively scheduled at board level, and 4% report that data is only discussed following a breach or quality failure. The EU AI Act data underlines this reactive tendency: While 61% of organizations say the Act has influenced their AI investment or strategy, preparedness tells a different story: 65% of CEOs say they are fully prepared for its requirements, yet only 38% of CTOs and 57% of CISOs agree. Even where external compliance pressure exists, it is not reliably translating into proactive, organization-wide governance.

Organizations that discuss data only when something goes wrong are not building the conditions necessary for data trust. Rather, they are managing the consequences of its absence. Proactive data discussions needn't consume indefinite board time. While the foundational conversation will be demanding, subsequent meetings can focus on horizon scanning, compliance updates, and progress against the foundations of data trust. Organizations that make this shift stop managing data crises and start building the conditions that prevent them.

"Organizations that discuss data only when something goes wrong are not building the conditions necessary for data trust. Rather, they are managing the consequences of its absence."

Only

16%

of CEOs say they can lead strategic discussions on data

The authority gap: The third gap is one of authority, and it is perhaps the most consequential of the three. When data discussions do take place, CEOs are willing participants: Only 5% said the conversations were too technical, and none actively avoided them. However, just 16% of CEOs said they were comfortable leading strategic data discussions. This is where the absence of effective data leadership is most acutely felt.

What makes this finding particularly striking is that technical fluency is not what data leaders are asking for. When CISOs, CIOs, CDOs, and CTOs were asked what would most improve their relationship with senior leadership, educating CEOs on data and AI ranked only fourth. What they want above all else is involvement in strategic planning — 47% cited this as their top priority — and for the C-suite to set direction and drive accountability on data from the top down, rather than leaving it to the technical function to manage in isolation.

The good news is that the leadership required is well within reach. Strategic data discussions are not about understanding where encryption fits in the technology stack, but about setting the organization's tolerance for risk, defining its approach to compliance, and making the governance decisions that determine whether data can be trusted. These are precisely the kinds of decisions CEOs are uniquely positioned to make.

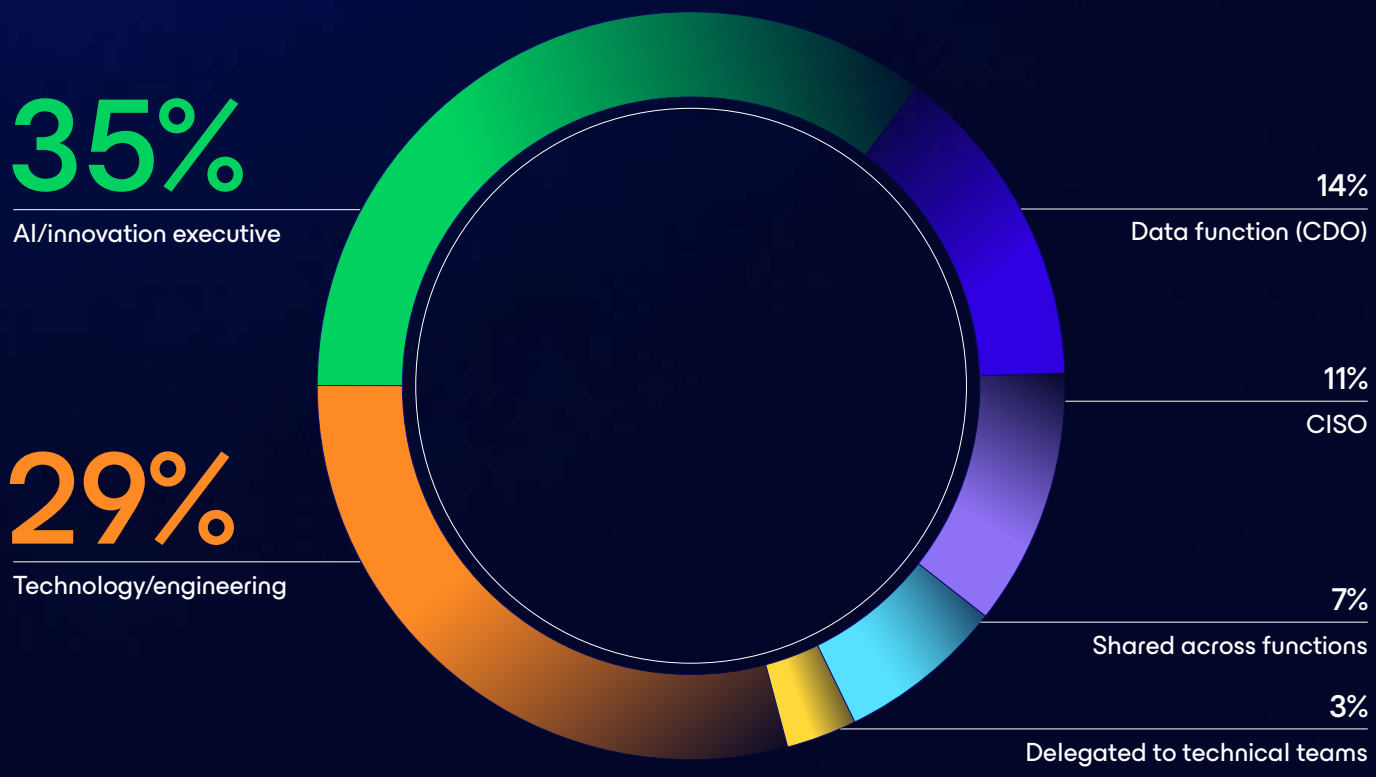
AI Agents and Trust Issues

Fragmented ownership and an inventory confidence gap could limit the benefits of agentic AI. Organizations must reset their governance frameworks to realize its potential.

Agentic AI without governance is agentic AI without trust, and for most organizations, the governance isn't there yet. 88% of organizations are already using or piloting AI agents, but the frameworks needed to oversee them have not kept pace. The result is a growing trust deficit at the heart of how organizations deploy their most powerful technology.

The first sign of that deficit is fragmented ownership. When asked who holds primary responsibility for what AI agents do, no single function commands a clear majority: 35% point to an AI or innovation executive, 29% to technology or engineering teams, 14% to the data function, and just 7% say responsibility is shared across functions in a structured way. When nobody owns the agents, nobody is accountable for what they do.

Ownership of agentic AI risk: Who is responsible?



The second sign is the gap between what leaders believe is deployed and what the reality is. 65% of CEOs are confident their AI inventory is complete and reliable, but only 44% of CISOs and 52% of CIOs agree.

The CEO is likely the one who sets compliance posture and AI strategy. If their picture is wrong, those decisions can be too. As regulations such as the EU AI Act come into force, the cost of that mismatch climbs: Deployers of high-risk AI systems face penalties ranging from €7.5 million to €35 million, or 1% to 7% of global annual turnover, depending on the infringement.[1] The required measures include human oversight, monitoring, record-keeping, and ensuring systems are being used as intended.[2]

"The CEO is likely the one who sets compliance posture and AI strategy. If their picture is wrong, those decisions can be too."

Inventory confidence gap: CEO vs. CISO/CIO

1. Meier, K., & Spichiger, R. (2024, March 15). The EU AI Act: What it means for your business. EY Switzerland.
2. European Union. (2024, June 13). Article 26: Obligations of deployers of high-risk AI systems. In *Regulation (EU) 2024/1689 (Artificial Intelligence Act)*.

The Elusive ROI of AI

Organizations must measure the impact of AI on their business to understand the true picture. This should cover everything from finances to people metrics.

Scaling AI investment requires making it pay off and being able to measure the degree to which it actually does. Most organizations are only doing the first: 85% of respondents claim significant success with data initiatives over the past 12 months, but only about half are seriously measuring ROI, with 45% yet to even try.

This is a significant blind spot. Decisions made on instinct can't be defended and investments made on instinct are rarely repeated. Without measurement, there is no way to know which AI tools are delivering, and which to scale or stop.

ROI measurements typically span three categories: Process improvement like faster decision making (51%), direct financial impacts (48%), and strategic positioning (45%). These metrics reflect an approach to measurement that now recognizes AI's impact across multiple dimensions of the business.

One dimension is consistently underweighted: Only 29% of respondents measure people metrics like staff satisfaction or talent retention when assessing the return on data investments, the lowest of any category. Whether employees are using new tools, whether they understand why, whether the data culture is shifting — none of it is what most organizations are tracking.

Closing this measurement gap matters as much as closing the governance gaps explored elsewhere in this report. The returns you can't measure are the returns you can't defend or repeat.

Given that transformation is not just about technology, but cultural change too, organizations must not ignore the people aspect when measuring ROI.

85%

have had significant success with data initiatives in the past 12 months, but only

45%

failed to formally measure impact

How are companies measuring the ROI of AI?

OPINION

"You Can't Delegate Trust"

Dave Russell

Senior Vice President, Head of Strategy at Veeam Software

Limited visibility and controls create a data trust gap. Leaders should put in place the conditions where trust in data is possible.

Compliance with privacy and regulatory demands needs to align with an organization's risk appetite, which must be set from the company's top leadership. Meeting that standard depends on something more fundamental: data trust. Trust is what allows an organization to use data with confidence — knowing it is secure, governed, and defensible under scrutiny. Robust security requires the ability to see and control data in ways that reinforce the right behaviors, access, and usage across the business.

Data provenance requires clear rules around what data can be trusted based on where it originated and how it has changed. Transparency of definitions requires IT teams to establish consistent standards so everyone speaks the same data language. Strong governance requires clear accountability for data. Not so there is someone to blame, but rather to ensure that trust can be demonstrated consistently, decisions can be made quickly, and risk is managed as intended.

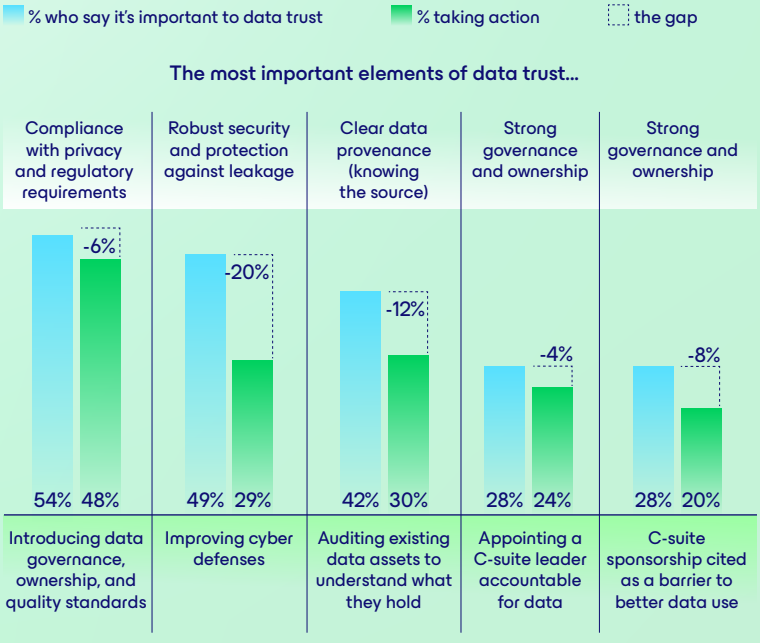
This research reveals a significant gap between what leaders say trust requires and what organizations are currently able to do to deliver it. Only 30% of organizations are auditing their existing data assets to understand what they hold, leaving the remaining 70% without the visibility needed to demonstrate clear data provenance. Just 24% have appointed a C-suite leader accountable for data, and 1 in 5 cite a lack of C-suite sponsorship as a major barrier to better data use.

What these findings reveal is a trust gap driven by limited data visibility and controls. Leaders may understand what trust requires, but without a reliable and current understanding of the data environment — and without the operational mechanisms to enforce governance — organizations struggle to act on that understanding effectively. This matters because the return on closing that gap is quantifiable: 25% of respondents believe complete data trust could unlock a 25–50% improvement in revenue or efficiency, while a further 13% think it could deliver more than 50%.

Leaders can ensure that the right governance and security infrastructure is in place, but they cannot delegate the conditions and solutions that make trust possible. Creating the conditions where trust is measurable, repeatable, and provable is what separates organizations that understand what data trust requires from those that can actually deliver it.

The data trust vs. action deficit

The elements that are most important to data trust according to leaders, compared to the associated actions taken by organizations:



...versus what actions their organizations are actually taking.

Five Things to Know About Shadow AI

The data visibility and governance challenges outlined in this report are most visible in the proliferation of shadow AI. These are AI tools used by employees outside the approval, oversight, or governance processes of security and technology teams. It is widespread, growing, and a direct challenge to data trust.

01 | Nearly all organizations have a shadow AI problem

95% of organizations know their employees are using unapproved tools, while 93% of senior leaders recognize it as a problem. It persists anyway, widening the data visibility gap.

02 | Training is the first line of defense

More than half of organizations (57%) are responding with general AI training and awareness campaigns to address data leakage, cybersecurity exposure, and reputational damage from AI misuse.

03 | Technical measures have limits

Data access controls (47%) and network monitoring (45%) can restrict unapproved tool use on company devices, but employees can — and do — simply switch to personal devices to sidestep them entirely.

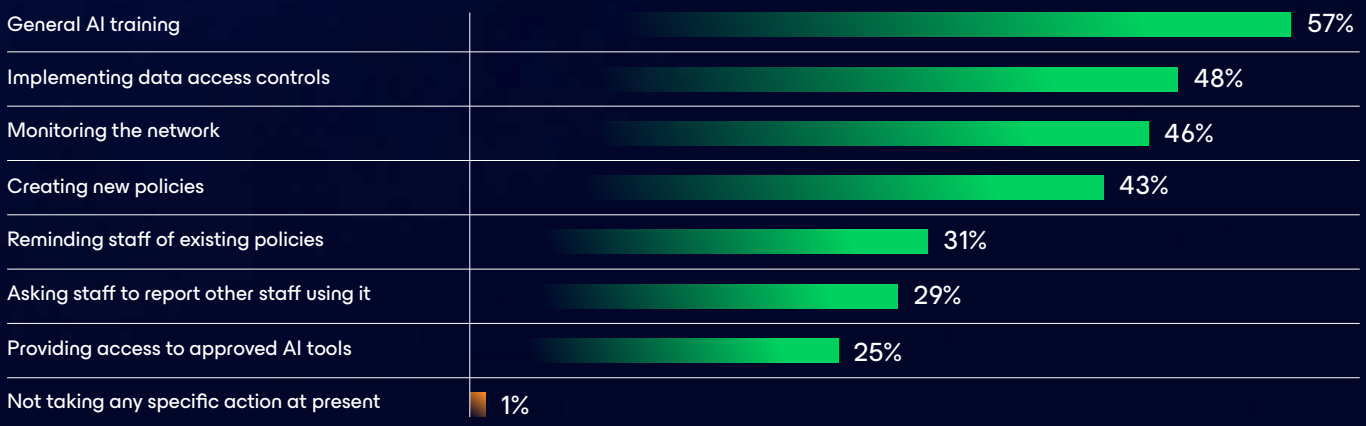
04 | Approved alternatives are not widely available

Only 25% of organizations provide all employees with access to approved AI tools. When sanctioned alternatives are unavailable, unauthorized ones fill the gap, making restriction a less effective strategy than provision.

05 | Policies exist but enforcement does not

Organizations have shadow AI policies; what they lack is the follow-through to make them meaningful. Without consistent enforcement and regular training, awareness alone will not close the gap.

What are managers doing to curb shadow AI?

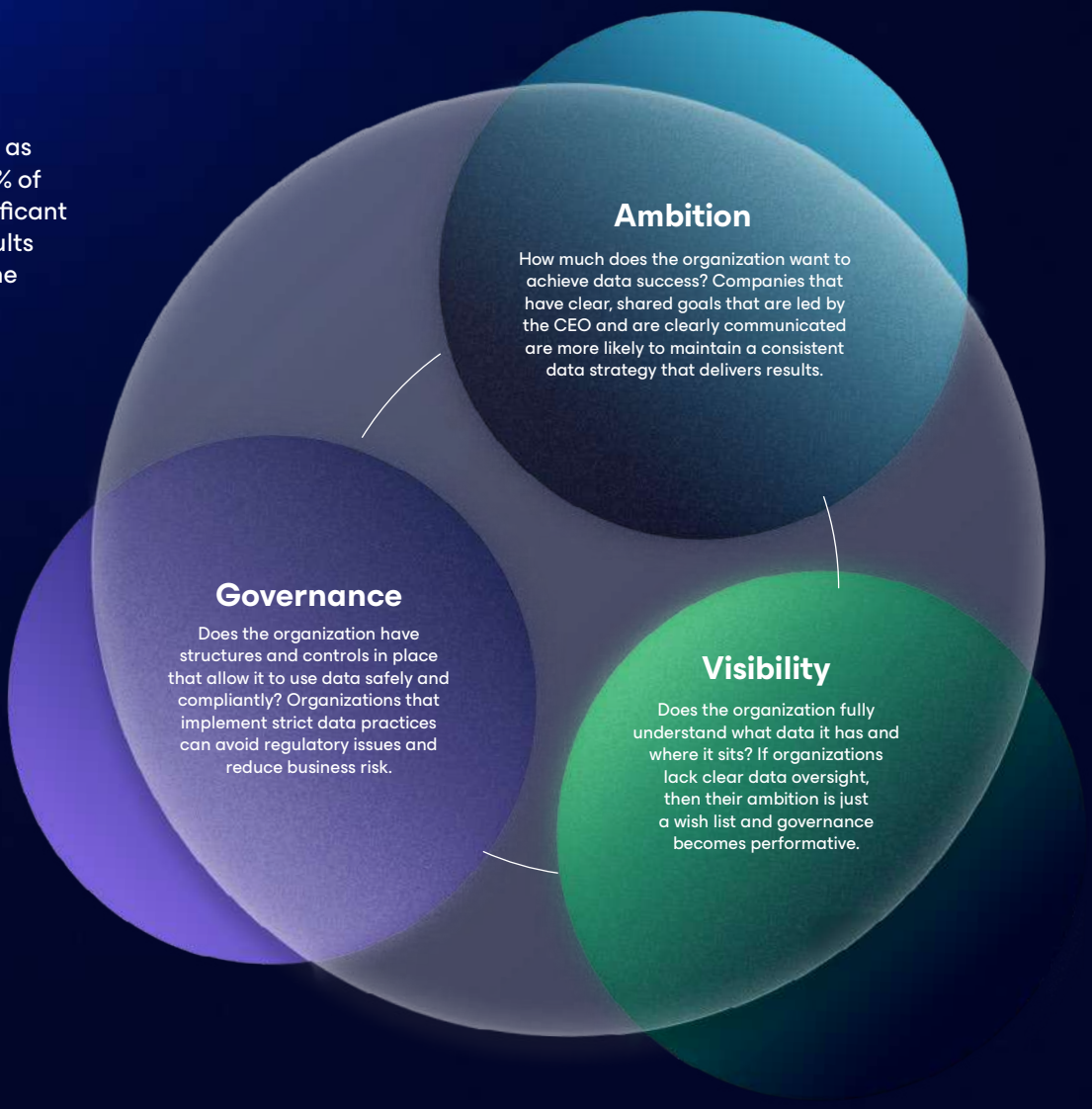


The Building Blocks of AI Readiness

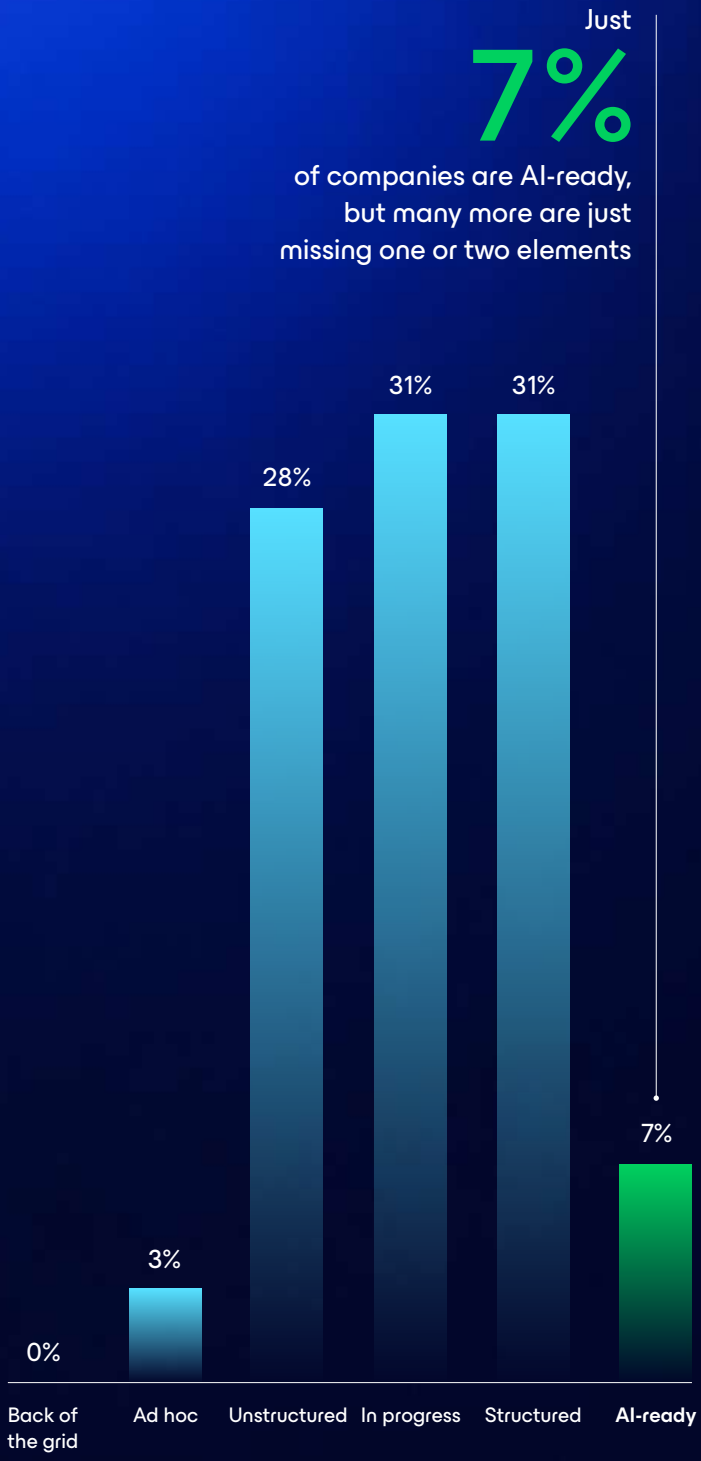
AI readiness is built on ambition, governance, and visibility. When these foundations are in place, organizations see concrete results from their investment.

The payoff for treating data as a strategic asset is clear: 47% of organizations reported significant and quantified business results from a data initiative over the past 12 months. Of those with quantified success, 56% saw it in revenue growth. Singapore-based respondents led on revenue (75%). U.S. organizations led on product design and innovation (45%), against 29% in Germany.

From this, we see data success is not driven by individual expertise. AI readiness is driven by a holistic approach that is led from the top, underpinned by three building blocks: ambition, governance, and visibility.



State of AI-readiness



97%

of organizations that qualify as "AI-ready" report specific, significant business outcomes in the last year that were formally quantified

Organizations with all three blocks are already delivering results: 97% of "AI-ready" organizations report significant, formally quantified outcomes from the past year. While the qualifying group is small at only 7%, the gap isn't as wide as it looks, with 60% having at least two of the three blocks in place.

For organizations not yet AI-ready, the first step is to carry out a comprehensive audit of what data exists, who owns it, and where the gaps are. Closing those gaps is the essential action currently separating the 7% from the rest.

"For organizations not yet AI-ready, the first step is to carry out a comprehensive audit of what data exists, who owns it, and where the gaps are."

CONCLUDING OPINION

From AI Ambitions to AI Results

Data presents huge opportunities for organizations, but it depends on trust. Leaders who build the right foundations will chart a path to enduring success.

The data opportunity explored in this report is real — but it is not evenly distributed. It flows to the organizations that have done the harder, less visible work: Building a reliable picture of what data they hold, establishing clear ownership, and creating the governance structures that allow data to move safely and at scale. The research is unambiguous on this point. Among organizations that have all three building blocks in place, 97% are delivering significant, formally quantified business outcomes. The gap between them and the majority is not a question of investment or technology; it's a question of trust. Trust, as this report has shown, requires leadership to make a measurable impact.

While the significance of data has long been acknowledged, organizations still need the leadership conditions in place to act on what they already know. The revenue upside, the competitive differentiation, the AI returns; all of it is contingent on executive alignment around ownership and accountability, a critical condition of data trust.

AI is already operating inside most organizations. As regulatory pressure continues to intensify, and the distance between AI ambition and reality grows wider, those without the right foundations will find the cost of waiting is measurable financially, operationally, and reputationally. The organizations closing that gap are not doing anything extraordinary. They are simply ensuring that someone at the top has decided the opportunity is worth owning.

For organizations ready to take that step, Veeam exists as a strategic partner that understands the infrastructure achieving data trust at scale requires and is designed to make it possible.

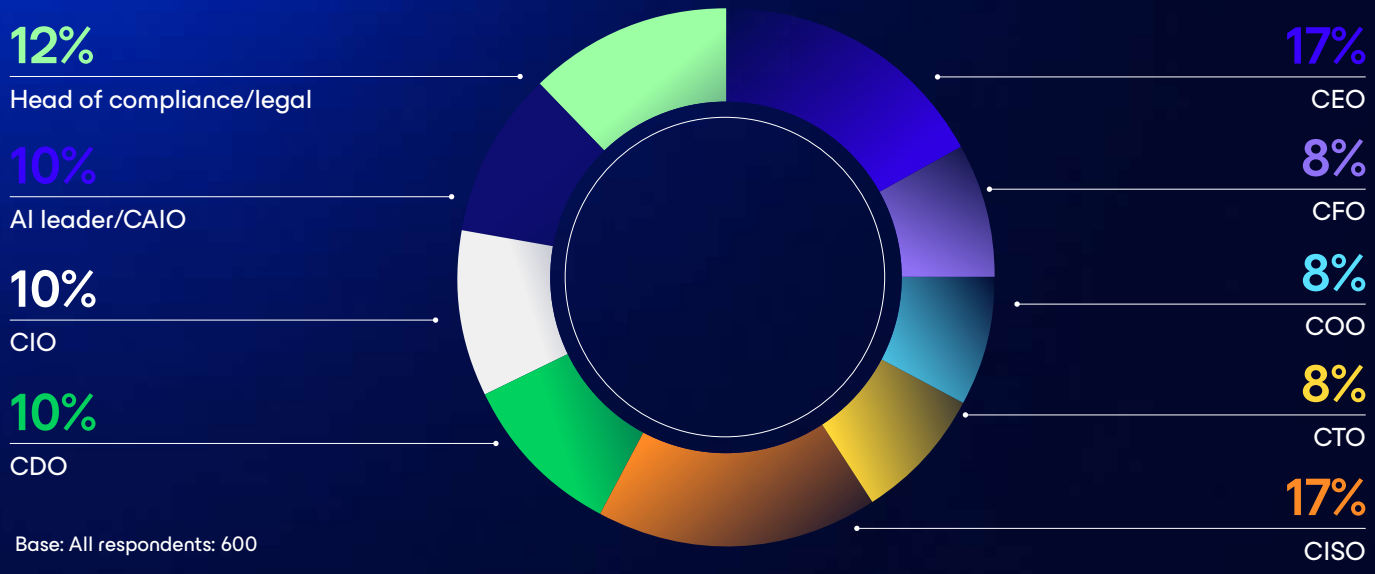
About the Survey

The research, undertaken between March 16–April 6, 2026, is based on a global survey of 600 senior executives across industries including financial services, healthcare, manufacturing, retail, and technology. Respondents included CEOs, CIOs, CISOs, CDOs, and other senior leaders responsible for data, AI, technology, and compliance, spanning organizations across North America, Europe, and Asia Pacific.

To find out how Veeam can help your organization unlock the promise of data and AI, visit www.veeam.com

Job titles surveyed

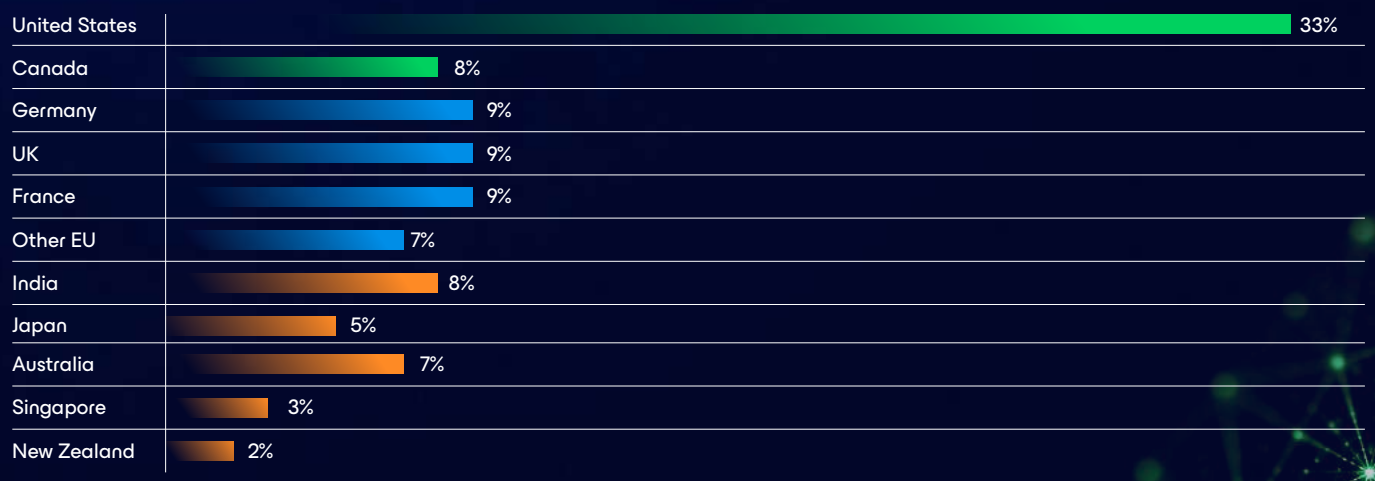
Percentage breakdown of respondents by job title



Base: All respondents: 600

Where they're located

Percentage breakdown of respondents across geographies



Base: All respondents: 600

Veeam is the Data and AI Trust Company, specializing in helping organizations ensure their data and AI are fully understood, secured, and resilient to enable the acceleration of safe AI at scale. As the market leader in both data resilience and data security posture management, Veeam is built for the convergence of identity, data, security, and AI risk.

Veeam delivers deep contextual intelligence across every data asset, identity, and AI model. The company governs access for both humans and AI agents, automates privacy, compliance, and remediation processes, and protects and recovers organizations from modern threats — including ransomware, disasters, AI errors, and ensuring the restoration of clean, trusted data. Veeam empowers organizations to move beyond simply protecting data, enabling them to activate and unlock its full potential.

Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 82% of the Fortune 500, who trust Veeam to keep their businesses running. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.