VansonBourne

Building Cloud Trust:

How trust and security are shaping the next phase of cloud growth



Introduction

Cloud has become the defining architecture of modern enterprise IT. What began as a question of feasibility has evolved into one of optimization. As organizations modernize, the cloud now underpins not only infrastructure decisions but also how innovation, agility, and resilience are designed into business operations. Trust has become the cornerstone of this evolution, shaping how organizations select partners, manage risk, and balance opportunity with control.

This report examines how enterprises are establishing that trust, through investment, governance, and collaboration. It explores the growing confidence in public cloud environments, the barriers that continue to test adoption, and the expanding role of AI in strengthening both protection and performance. Together, these insights highlight how the cloud has matured from an enabling technology to a strategic platform. One that demands robust security, accountability, and shared responsibility to sustain confidence at scale.

Key findings:



59%

of applications run in the cloud today, rising to 75% within the next year, signaling a decisive shift towards the cloud



56%

responded the public cloud was best positioned to deliver security as opposed to 37% that chose on-premises and 7% that responded neither model



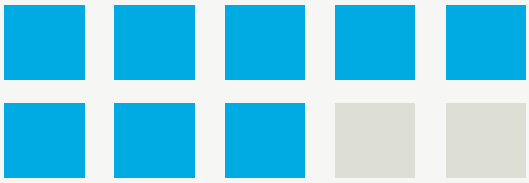
51%

responded the public cloud was best positioned to meet regulations vs 41% that responded on-premises



81%

agree that their primary cloud provider's native security and compliance capabilities exceed what their team could deliver independently



Around eight in ten organizations report at least one data breach in the past year, both in on-premises infrastructure (78%) or in the public cloud (79%) showing that risk stems from operational factors rather than the environment itself



identify AI security and risk management frameworks as their top priority for reducing cyber risk over the next three years, underscoring the need for strong oversight as AI adoption grows



plan to deploy AI agents within Security Operations Centers (SOCs) in the coming year, marking a shift toward more automated and adaptive approaches to threat detection and response



agree that native security features are among the most important criteria when selecting third-party AI solutions, reaffirming that trust and protection remain central to AI innovation

Laying the foundations of cloud trust

Organizations are preparing for continued cloud expansion

The role of cloud computing in enterprise IT strategies is no longer a question of "if," but "how fast." Organizations who currently use a mix of on-premises and cloud environments are making decisive moves to modernize, with their spending aligned toward a cloud-first future.

Today, organizations estimate that an average of 59% of applications run in the cloud. In 12 months, that is predicted to increase to 75% on average. This projected 16-point swing in a single year indicates that the public cloud is becoming increasingly central to how organizations pursue efficiency, competitiveness, and improved customer experiences.

59%

Today, organizations estimate that an average of 59% of applications run in the cloud

75%

In 12 months, that is predicted to increase to 75% on average

As organizations modernize their application portfolios, the shift to the cloud extends beyond where applications run to where they are built. Almost all respondents (99%) already develop applications in the public cloud today, compared to 94% still building on-premises. In 12 months' time, cloud usage for app development is expected to remain near-universal (95%), while on-premises drops to 75%. This indicates that the public cloud is steadily becoming the primary environment for application development, as on-premises use becomes more targeted.

What's changing now is not just where applications are built, but how central the cloud has become to driving modernization and growth.

Environments organizations use to build applications today and in next 12 months

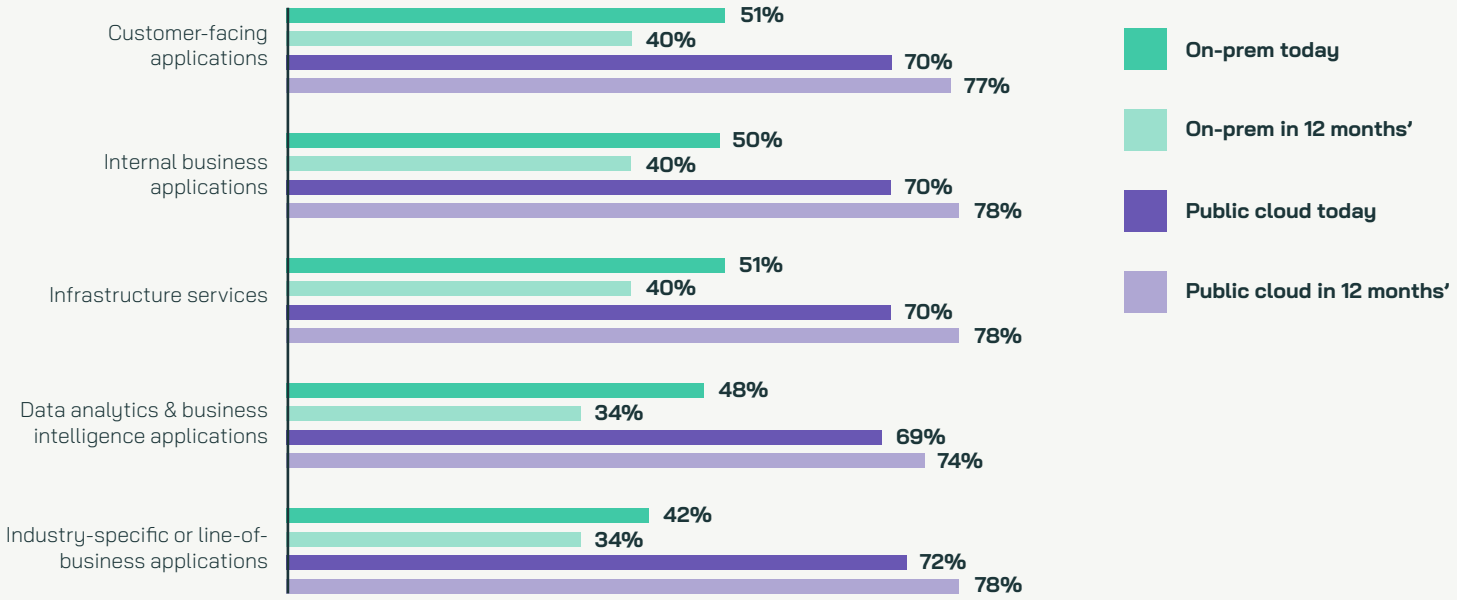


Figure 1: Which environments does your organization use to build the following applications? (Base sizes in chart) *Base size for answer option "Data analytics and business intelligence applications": today = 1,412; in 12 months = 1,409

Cloud development has moved beyond selective use cases to become the foundation of modernization, extending into core business systems, infrastructure, and data platforms. This marks a shift toward building with the cloud as the default, where innovation, scalability, and resilience are embedded from the start.

Industry spotlight

Across every industry, cloud has become the primary environment for building applications. Even in highly regulated industries such as government, financial services, and energy, most organizations now build more in the cloud than on-premises.

Financial services is one of the leading industries when it comes to overall cloud maturity, with around three-quarters of institutions now building both customer-facing (77%) and internal business applications (77%) in the cloud, reflecting the industry's drive for agility, security, and compliance at scale.

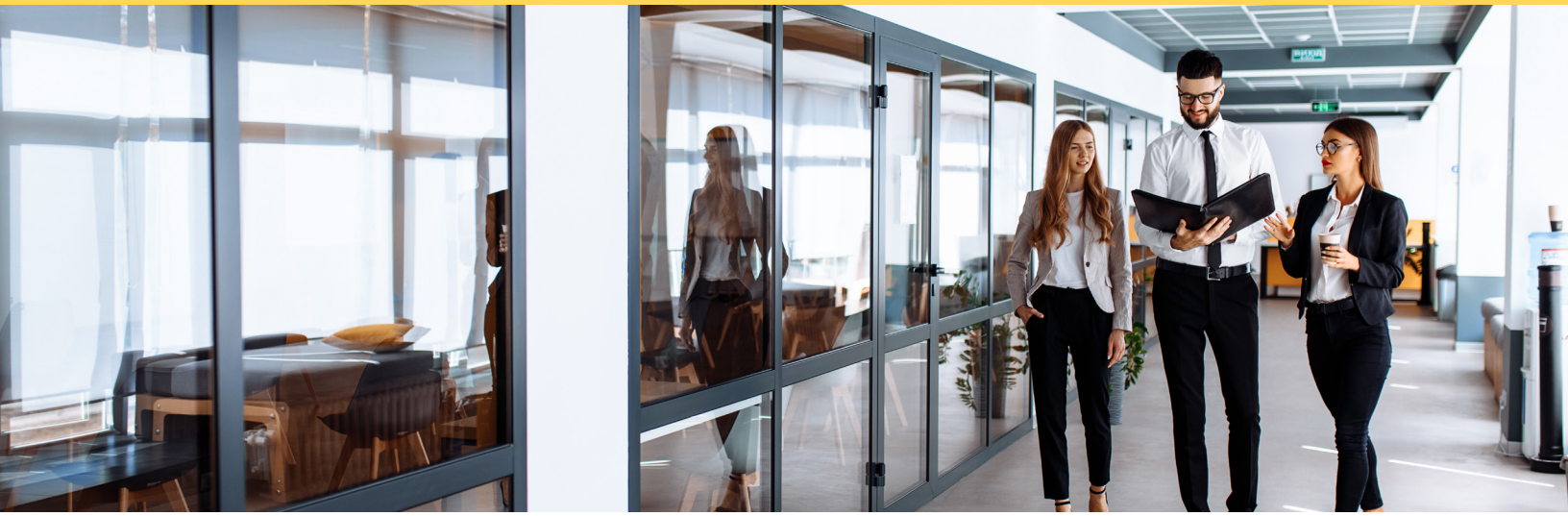
Media and entertainment is another stand out industry, with 80% building customer-facing applications and 78% building industry-specific applications in the cloud, underlining how cloud is integral to their operating models.

Telecommunications and manufacturing follow closely, using the cloud to modernize infrastructure and accelerate innovation in data-heavy environments. Retail and consumer goods organizations show strong momentum across the board, with around two-thirds to three-quarters of workloads now built in the cloud, as they lean on elasticity and analytics to improve customer engagement and supply-chain visibility.

In healthcare and education, adoption is similarly widespread but more measured (still above 70% for most workloads) driven by a balance between digital modernization and privacy mandates.

Regional spotlight

While cloud use for application building is strong across all regions, organizations in Asia Pacific (APJ) are the most likely to report doing so. Across nearly all major application types surveyed, APJ organizations are ahead by a few percentage points. For example, 74% of APJ organizations build internal business applications in the cloud, compared with 71% in Europe and 62% in the Americas. Similarly, 72% in APJ build customer-facing applications in the cloud, versus 70% in the Americas and 68% in Europe. Data analytics and business intelligence applications is the only category where APJ are not ahead, and even then, only by a single percentage point (Europe 70%, APJ 69%, Americas 68%). This greater use of cloud environments in Asia Pacific reflects strong confidence in the cloud's ability to deliver scalability, reliability, and performance. In fact, 57% of organizations in the region see the public cloud as best positioned to meet these needs, compared with 55% in the Americas and 54% in Europe. This confidence likely underpins a broader commitment to use cloud as a platform for innovation and growth, enabling faster development and delivery of new digital services.



Cloud provider environments organizations are using to build applications

Surveyed organizations are consistently building their businesses on cloud offerings from leading providers with Amazon Web Services (AWS), Google Cloud Platform, IBM Cloud, and Microsoft Azure among the most widely used. Responses suggest 17 to 21 point lead for using AWS to build customer-facing applications, internal business applications, infrastructure services, and industry or line-of-business specific applications.

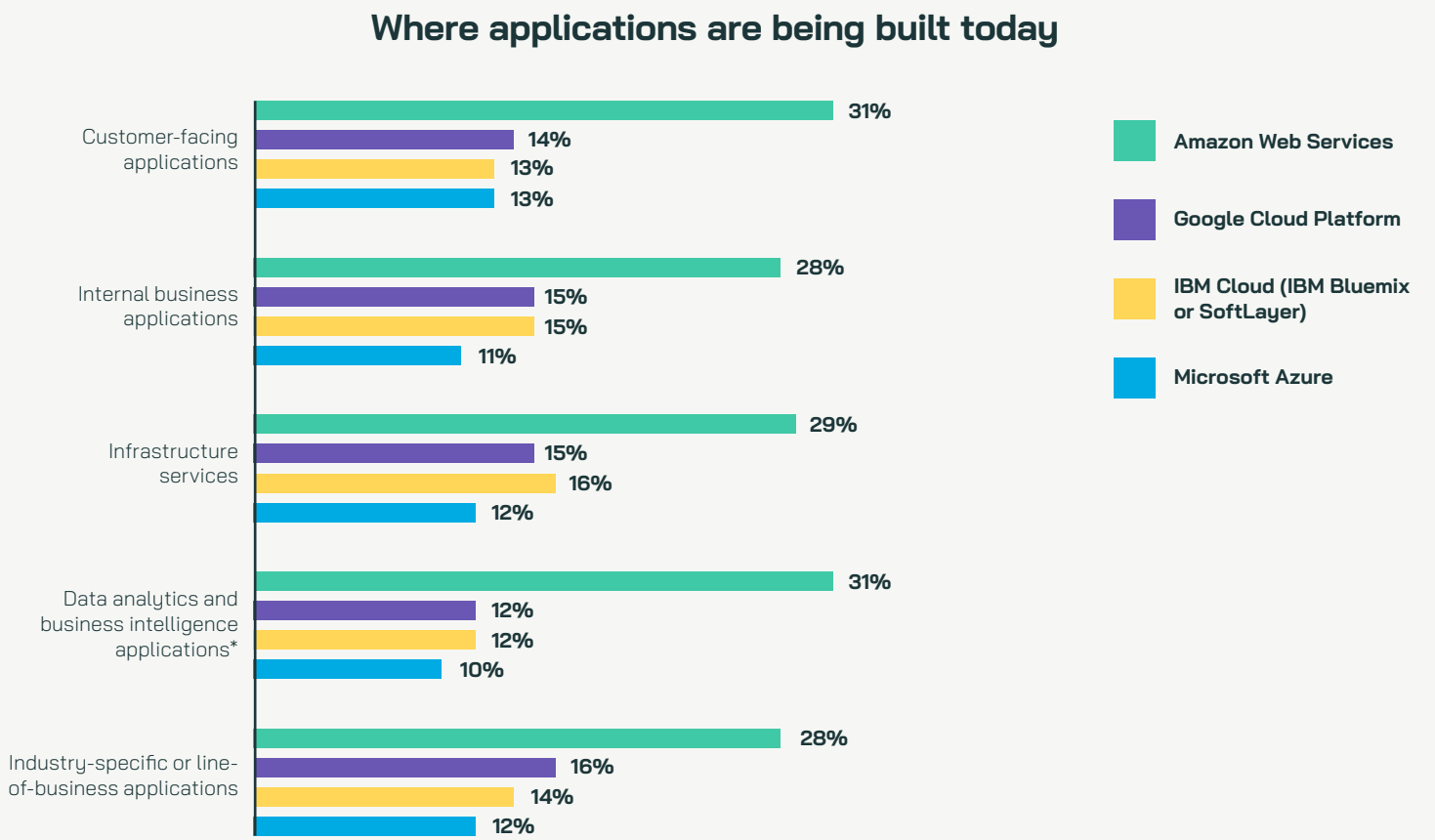


Figure 2: Which environments does your organization use to build the following applications? (Today = 2,798) *Base size for answer option "Data analytics and business intelligence applications": today = 1,412

Budgets support innovation/transformation

Organizations are not only planning for change, they are funding it. The vast majority report that their budgets are on the rise, with 93% expecting an increase in overall IT spending. This willingness to commit resources reinforces that cloud adoption is more than an aspiration: businesses are investing to gain the scalability, speed, and agility needed to compete through faster innovation and expanded market opportunities.

Nearly all respondents (97%) agree that their organization will increase spending on professional services from cloud providers in the next 12 months. This signals growing recognition that specialist expertise is critical to accelerate adoption and manage complexity at scale. Technically focused respondents are especially emphatic, with 52% of both IT and security professionals strongly agreeing, underscoring reliance on providers' depth of knowledge to maintain performance and security. Decision-maker respondents are somewhat less likely to strongly agree (IT: 41%; security: 39%), suggesting leaders may underestimate how much expert support is required to deliver on cloud ambitions.

Critically, much of this investment is directed toward cybersecurity. Organizations aren't just buying tools. They're buying providers' expertise, such as playbooks, managed services, and response management that can harden posture at scale as AI accelerates attacker speed and sophistication of attacks.

This emphasis reflects the trust organizations place in cloud providers' ability to combine technology with proven operational know-how. They are looking for partners who can optimize costs, accelerate migration, and maintain compliance while actively strengthening security. Fittingly, 90% expect to increase their cybersecurity budgets in the next 12 months.

Trusting the cloud's ability to deliver

As organizations deepen their reliance on cloud services, confidence in both public cloud and on-premises environments remains consistently high when each is assessed independently. When asked about their own ability to meet critical business and IT requirements on-premises, organizations express strong confidence. The same is true when they evaluate public cloud providers, reflecting widespread trust in the cloud's maturity and capability.

Respondents who are 'very confident' in cloud providers and on-premises environments to address the following requirements

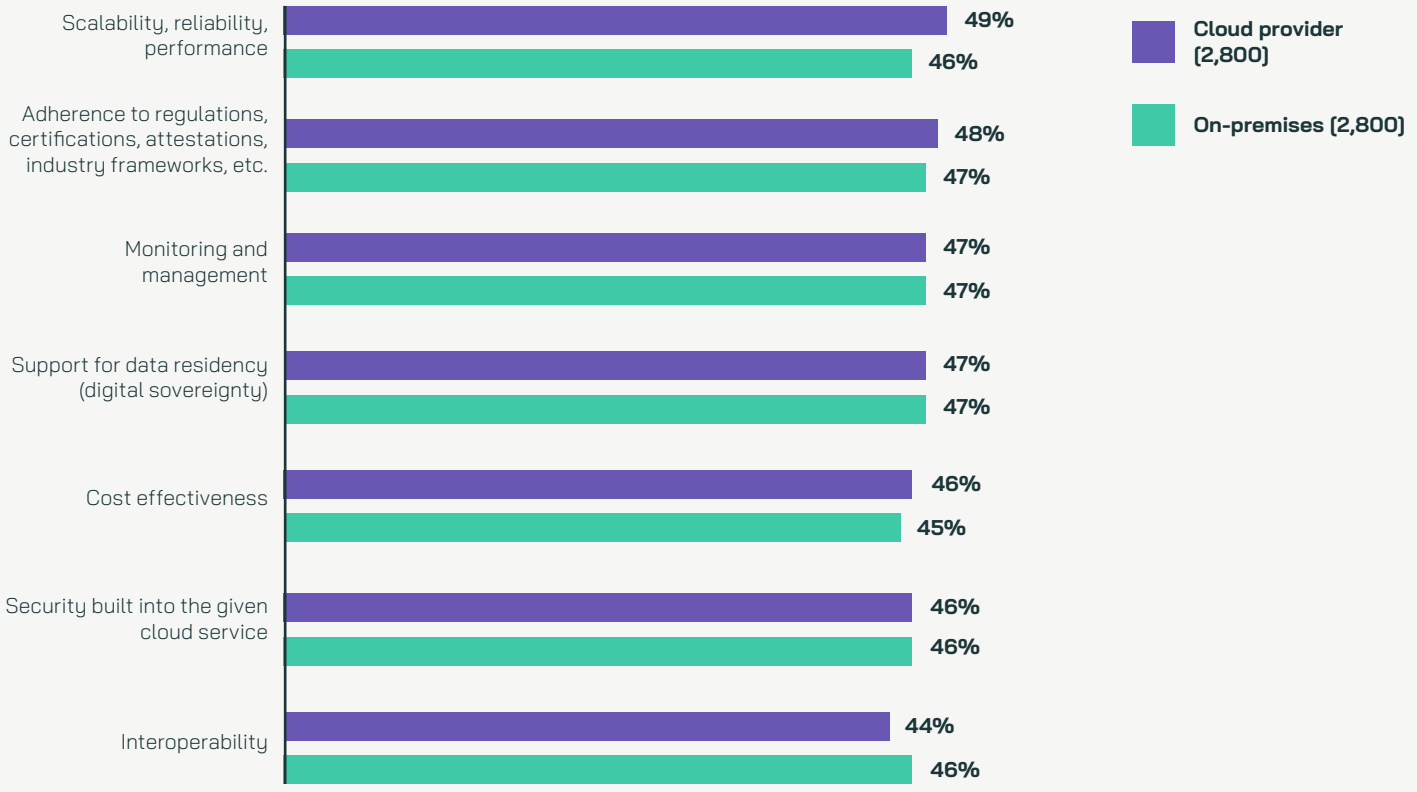


Figure 3. How confident are you in your cloud provider's ability to address the following requirements, and how confident are you in your organization's ability to address its on-premises environment? Only showing those who are 'Very confident' (2,800)

However, when respondents directly compare the two environments, public cloud providers emerge as stronger across every requirement tested—demonstrating that while on-premises infrastructure remains dependable, the cloud is increasingly viewed as the more capable foundation for future performance.

IT environment (on-premises vs. cloud service provider) best positioned to address the following requirements

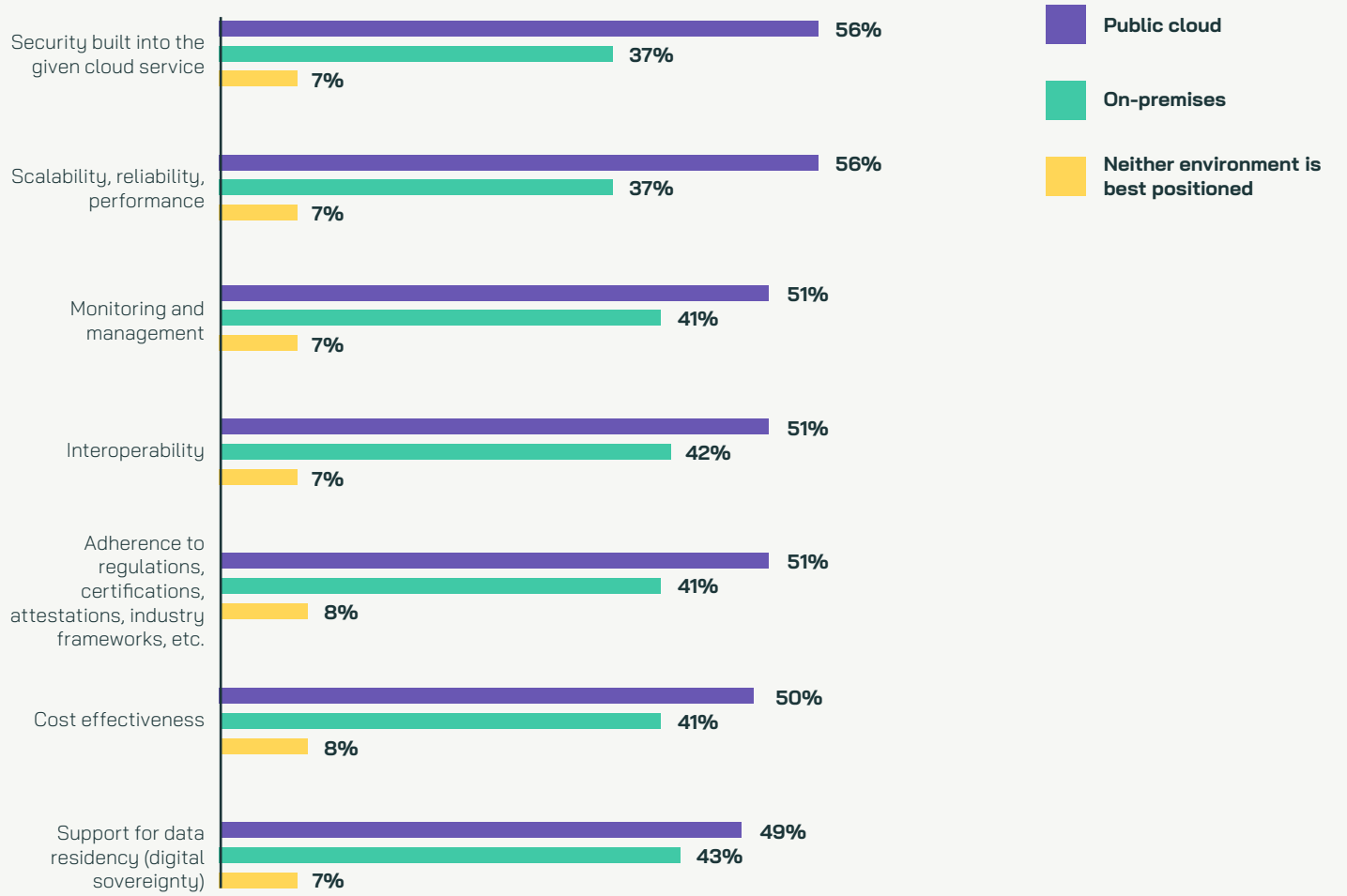


Figure 4. Which IT environment (on-premises vs. cloud service provider) do you feel is best positioned to address the following requirements? (2,800)

Decision-makers show the strongest confidence in public cloud environments, particularly for security built into the service (security DMs: 59% / IT DMs: 56%) and scalability, reliability, and performance (security DMs: 59% / IT DMs: 58%) reflecting belief in the cloud's role as a platform for growth and resilience. Technically focused security respondents are the most likely to believe cloud is best placed to support digital sovereignty (51%) and adherence to regulations, certifications, attestations, industry frameworks (54%), reflecting their strong focus on security assurance and control, and highlighting the trust they place in the cloud to meet rigorous compliance standards.

Further to this, around eight in ten respondents (81%) agree that their primary provider's native security and compliance capabilities exceed what their own teams could deliver independently . This perspective reflects the trust placed in the maturity of today's cloud environments. Organizations increasingly recognize that leading cloud providers combine robust availability and scale with the highest standards of security, digital sovereignty, and compliance. Decision-makers increasingly regard the cloud as a trusted environment for delivering their innovations.

Elements that build cloud trust

Confidence in the cloud does not exist in a vacuum. It is built on the way organizations assess and validate their cloud providers: Trust in the cloud is rooted in proof, not promises.

Factors that influence how organizations assess and trust a public cloud provider's security

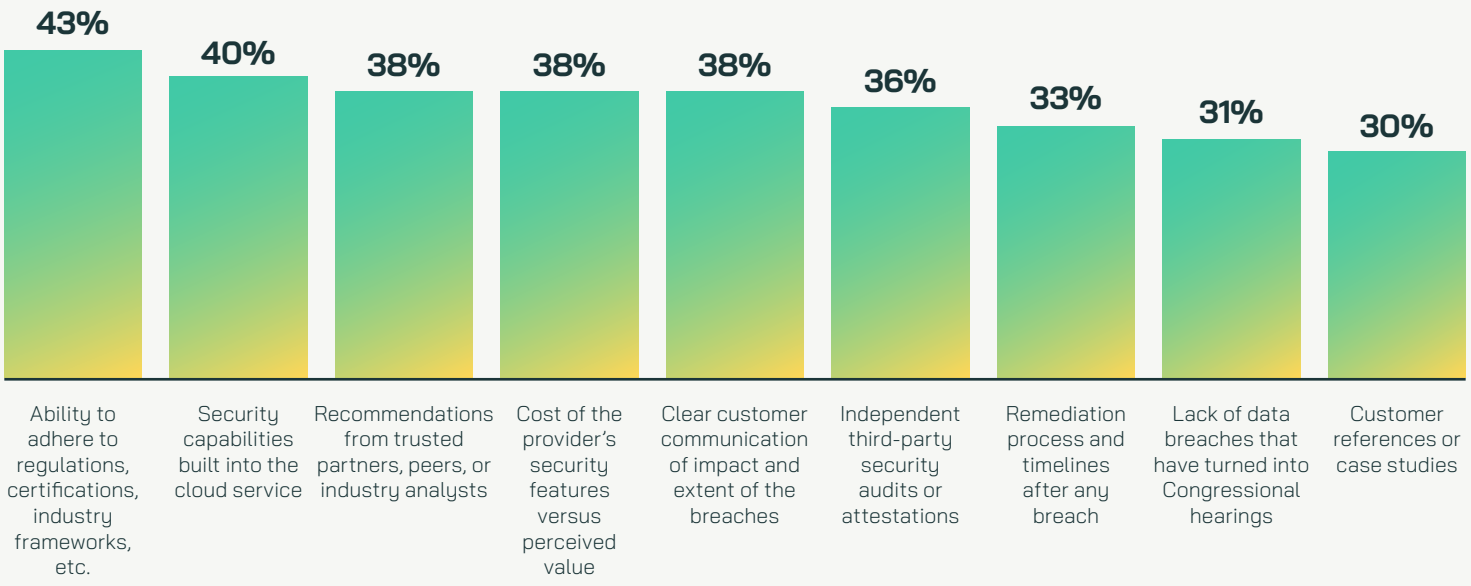


Figure 5. Which of the following factors influence how your organization assesses and trusts a public cloud provider's security? (2,800)

Organizations weigh a combination of structural assurances and behavioral signals when deciding who to trust. In other words, trust is earned not just through technical capability, but through conduct, how cloud providers demonstrate accountability, consistency, and openness when challenges arise.

Decision-makers tend to build trust in cloud providers through formal assurance and governance factors, placing greater weight on regulatory adherence (ITDMs 43%; Security DMs 44%), third-party audits (ITDMs 40%; Security DMs 36%), and clear communication during incidents (ITDMs 40%; Security DMs 41%).

In contrast, respondents in practitioner roles (especially security focused ones) base trust more on first-hand operational experience, prioritizing remediation process and timelines (security practitioners: 36%). The distinction highlights how leaders value certified confidence, while practitioners look for demonstrated resilience in practice.

Those with a cleaner security track record, such as fewer reported breaches, faster response, and clear evidence of remediation, hold a measurable advantage over providers whose breaches have escalated to public or governmental scrutiny, underscoring how closely trust and performance are linked.

Industry spotlight

While the foundations of cloud trust are consistent across industries, the factors that carry the most weight vary depending on each industry's priorities and risk landscape. Across every vertical, except automotive and manufacturing, the ability to adhere to regulations, certifications and industry frameworks is among the top influences of trust, with results ranging from 40% to 47%.

Automotive and manufacturing organizations are more focused on independent third-party security audits or attestations (45%), valuing externally verified proof of security over provider-issued assurances. This priority is also shared with information technology & services organizations (44%), and education & nonprofit (43%). This perhaps reflects a reliance on complex supply chains and sensitive intellectual property, where external validation provides assurance that partners and providers uphold consistent, verifiable security standards.

Retail and consumer packaged goods (51%) and automotive and manufacturing (44%) place greater weight on security capabilities that are built into the cloud service, perhaps reflecting their reliance on large volumes of customer and operational data that demand continuous protection. Media, leisure, and entertainment (42%) also highlight built-in security as a key driver, likely tied to the high value and sensitivity of digital content.

In contrast, financial services organizations focus more on the cost of the provider's security features versus perceived value (43%) and clear customer communication of any impacts and extent of breaches (44%), underscoring the importance of transparency and measurable return on investment in a regulated environment.

Across all industries, organizations place greatest trust in providers that show, not tell, proving their reliability and openness through transparent communication and accountable action over time.

The foundations of cloud trust, in decision-makers' own words

Decision-makers describe what would give them absolute confidence that their data is safer in the cloud than on-premises.

"Comprehensive encryption, strict access controls, regular third-party security audits, and transparent incident response processes."

"The cloud should offer end-to-end encryption for both data at rest and in transit, while also providing the ability to securely manage and control encryption keys."

"Confidence would also stem from knowing the cloud provider has a proven history of effectively managing security incidents and protecting their clients' data."

Overall, trust in the cloud is multi-layered. It depends on both structural assurances (like certifications, audits, and cloud native security) and situational experience (such as how transparently providers communicate and support customers during security incidents). Responses highlight that robust security capabilities, independent validation, and clear security incident procedures must be in place before they send their data into the cloud over processing and storing on-premises. The growth in cloud spending expected over the next 12 months shows that cloud providers are delivering on these must-haves.

Where trust is tested: impact of security and compliance

Barriers slowing cloud adoption

Even with growing confidence in the cloud's ability to deliver, some factors slow adoption.

Factors holding organizations back from further public cloud adoption

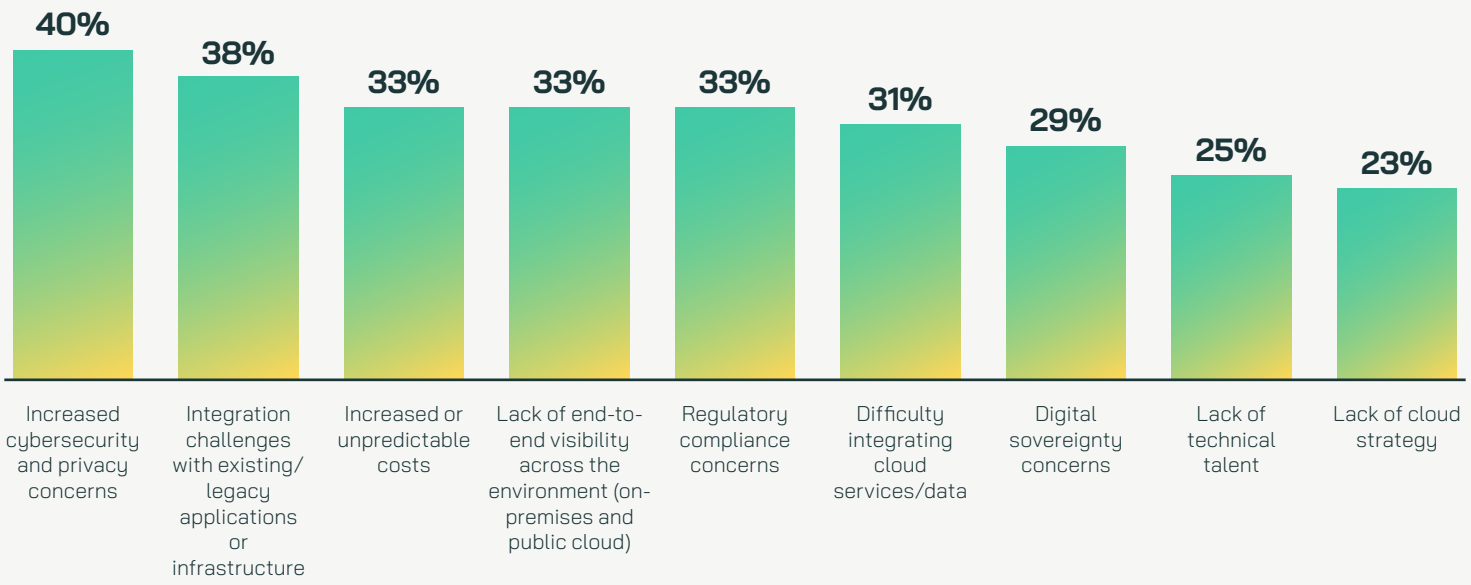


Figure 6. Which of the following, if any, is holding your organization back from further public cloud adoption? (2,800)

The most common issues center on security and integration, balancing the need to protect sensitive data with the complexity of connecting modern cloud systems to legacy infrastructure. Concerns around regulation, end-to-end visibility across the environment (on-premises and public cloud), and cost add further layers of complexity, while skills shortages and the absence of a clear strategy make transformation harder to scale. These barriers are not signs of hesitation but reminders that successful cloud adoption depends on strong foundations: visibility, control, and the ability to manage complexity with confidence.

For decision-makers, concerns are led by cybersecurity and privacy (ITDMs: 41%; Security DMs: 44%). In contrast, technical respondents are more focused on visibility and control, with roughly a third citing lack of end-to-end visibility (IT practitioners: 34%; Security practitioners: 35%). This highlights how leaders remain focused on managing external risk, while technical teams prioritize operational control and transparency as cloud environments grow more complex.

Even with high levels of trust, adoption is tempered by practical realities. Addressing these pain points will be critical for cloud providers to sustain confidence and accelerate growth. Especially when so many organizations agree (97%) that they will be increasing spending on professional services from cloud providers in the next 12 months.

Industry spotlight

Across industries, the obstacles to cloud adoption take different shapes. In financial services, cybersecurity and privacy concerns do not seem to be as much of a concern as for all other industries. This likely reflects years of investment meeting security and compliance frameworks, in tandem with the industry's early adoption of cloud computing, which have built stronger confidence in cloud providers' capabilities for managing risk. Instead, financial services organizations are more worried about integration with existing/legacy applications or infrastructure (38%) and integrating cloud services/data (37%).

Increased cybersecurity and privacy concerns are holding organizations back from further cloud adoption

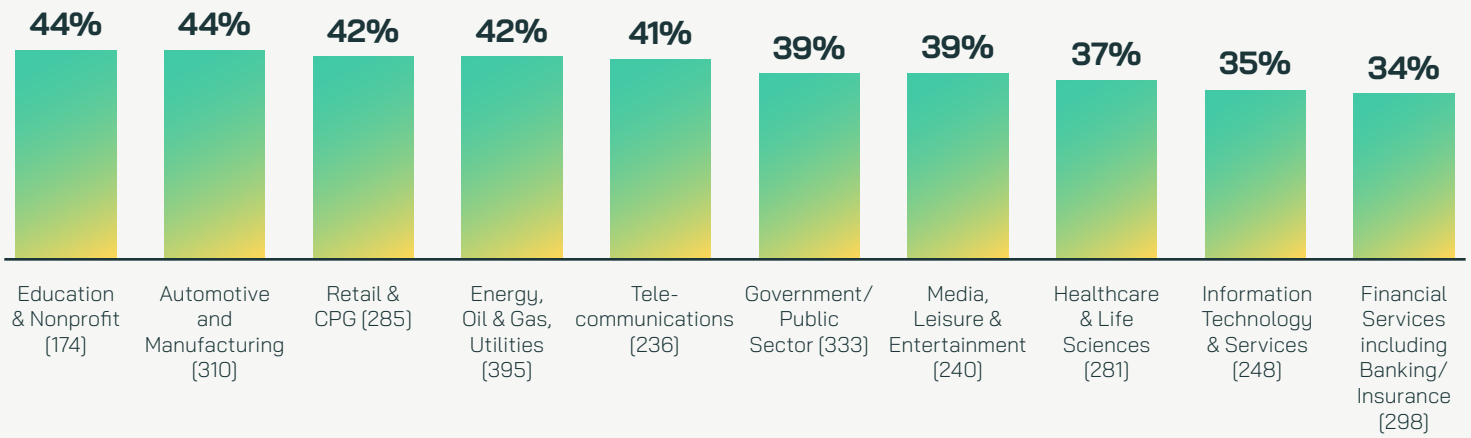


Figure 7. Which of the following, if any, is holding your organization back from further public cloud adoption? Split by industry and only showing responses to increased cybersecurity and privacy concerns (base in chart)

By contrast, automotive and manufacturing and retail and CPG organizations are more likely to cite integration challenges and cost unpredictability, highlighting the difficulty of connecting complex operational systems with newer digital infrastructure. Meanwhile, education and nonprofit respondents show heightened concern over security and visibility, suggesting that limited resources may amplify risk perception.

Regional spotlight

While barriers to cloud adoption are broadly consistent across regions, some subtle differences mirror the patterns seen earlier in application build environments. Asia Pacific organizations (previously highlighted as the most cloud-active) are slightly more likely to cite cybersecurity and privacy concerns (42%), indicating that as adoption scales, ensuring secure growth and maintaining strong data protection standards remain key priorities. European organizations are comparatively more concerned with regulatory compliance (35%), reflecting stricter governance requirements and a stronger emphasis on transparency. Meanwhile, organizations in the Americas are less likely to report regulatory and visibility challenges but continue to face integration (39%) and cost pressures (35%), pointing to a focus on optimizing existing cloud investments rather than expanding coverage.

Breaches are a universal reality across cloud and on-premises

Cyberattacks are not confined to one environment; they are a universal reality. Around eight in ten organizations report suffering at least one data breach in the past year, whether in their on-premises infrastructure (78%) or in the public cloud (79%).

This parity underscores that the public cloud is not inherently riskier and can, in fact, offer stronger baseline protection when implemented and managed effectively.

Public cloud providers operate under a shared responsibility model. Providers are responsible for securing the infrastructure of the cloud itself. Customers only need to handle security of the assets they put in the cloud, creating less ground to cover. For security of the cloud, public cloud providers implement higher levels of access controls than most organizations take for their offices. Some precautions for securing the physical perimeter include high security fences, video surveillance, intrusion detection systems, multi-factor access control, and human guards – all of which is overseen and monitored by 24x7 Security Operations Centers. Data leaving a datacenter is encrypted at the network level as it travels between infrastructure locations.

Looking deeper, most incidents trace back to operational weaknesses. The most common triggers include vulnerability exploitation (24% cloud / 20% on-premises) and compromised credentials (20% cloud / 19% on-premises), alongside physical theft (19% cloud / 14% on-premises) and misconfiguration (16% cloud / 11% on-premises). Human factors (whether insider error or malicious intent) play a consistent role across both settings, underscoring that breaches are often the result of operational complexity and mistakes, as much as external attacks.

Primary cause of the most impactful data breach across on-premises and public cloud environments

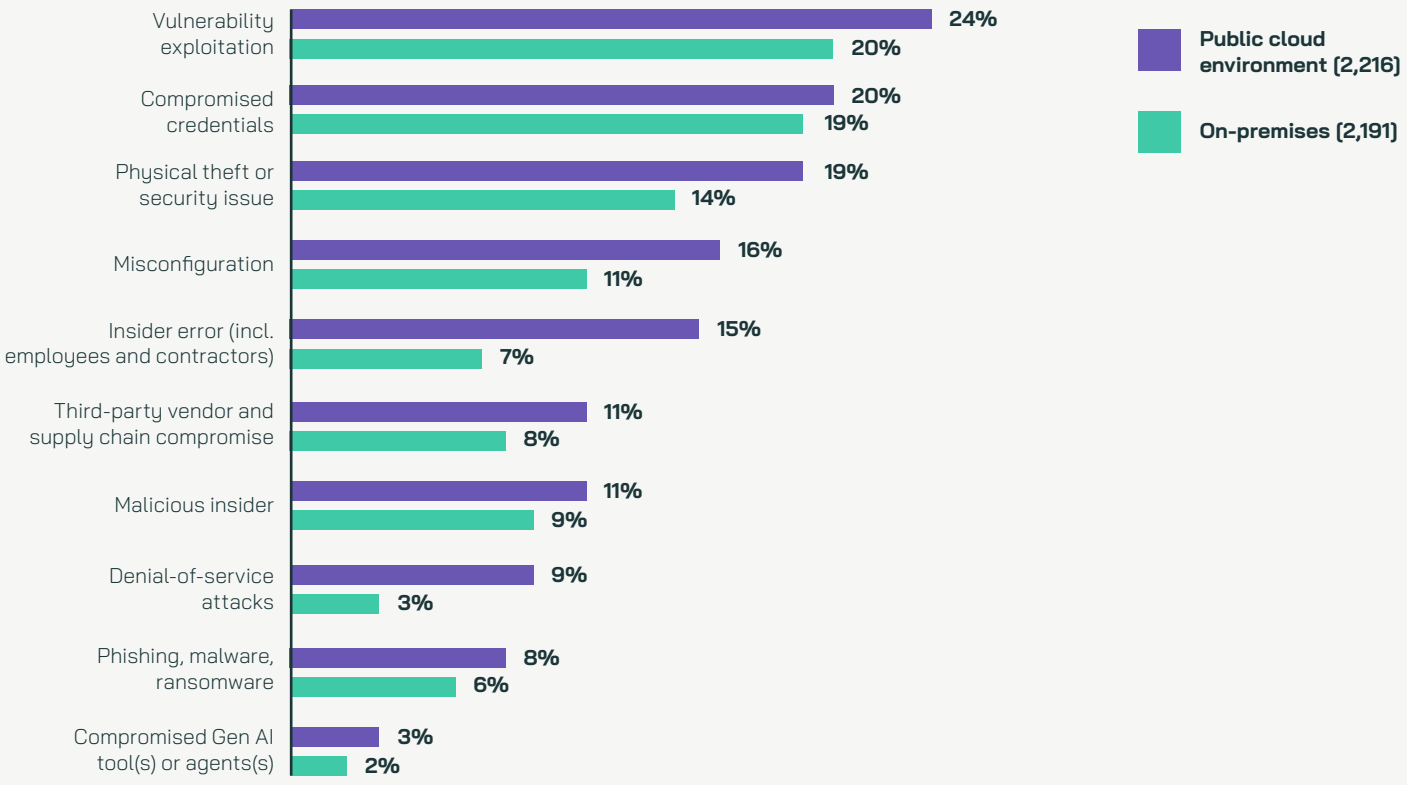


Figure 8. What was the primary cause of the most impactful data breach your organization experienced with regards to its on-premises and/ or public cloud environments? Only showing the environments respondents' organizations experienced a breach in over the last 12 months (base in chart)

The consequences of an attack highlight the organizational impacts. Around a third report operational downtime (35% on-premises / 31% cloud), brand or reputational damage (31% / 31%), and loss of sensitive data (31% / 30%). Many also face increased cybersecurity or insurance costs (36% / 35%), legal or regulatory action (31% / 29%), and customer loss (31% / 28%). In other words, it is not the environment that determines the damage, but the effectiveness of the defenses in place.

It is therefore no surprise that nine in ten organizations (91%) say they would trust a cloud provider less if it had a history of breaches or regulatory fines. Security performance and trust are inseparable: for organizations, confidence depends on knowing their cloud provider can demonstrate resilience, transparency, and accountability when it matters most.

For organizations, this parity between cloud and on-premises reframes the question. It is less about where data sits, and more about the confidence they have in how it is protected.



Reinforcing cloud trust through AI

The growing role of AI in cloud security

Building on that foundation of trust, many now see AI as the next ally in strengthening defenses. With cloud adoption expanding and security budgets on the rise, leaders expect AI-driven tools to play a larger role in helping them detect risks earlier, automate response, and reinforce protection across complex environments.

Respondents highlight just how central AI is becoming to future security strategies. When asked about priorities for reducing cyber risk over the next three years, respondents report AI-driven analysis and detection (23%) as one of the top areas of focus, with an even greater share (39%) highlighting the need for AI security and risk management frameworks. This shows that organizations not only see AI as a powerful tool but also recognize the need for strong guardrails and oversight.

Most important priority for reducing cyber risk over the next three years

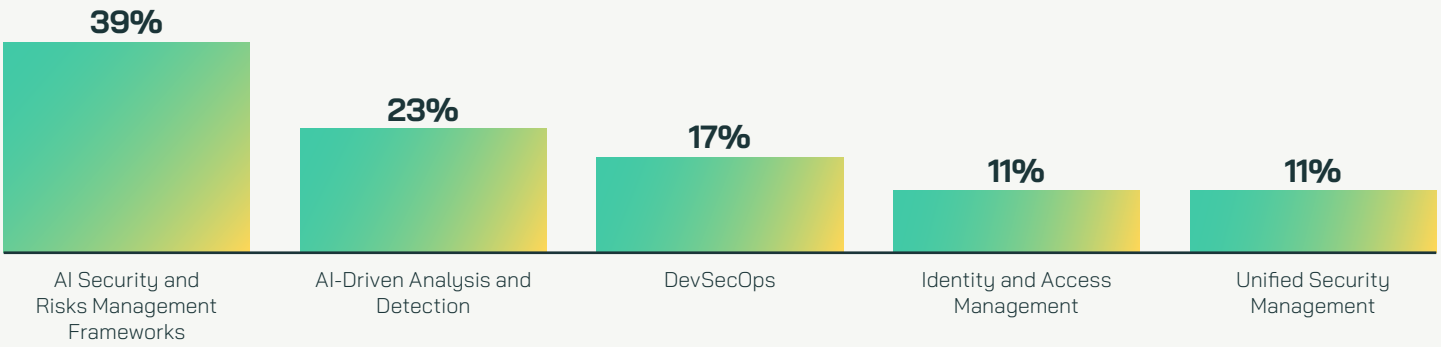


Figure 9. Which of the following, if any, do you believe will be the most important priority for reducing cyber risk over the next three years? (2,800)

Security focused respondents (both decision-makers and technically focused) are the most likely to prioritize AI security and risk management frameworks (44% respectively). This reflects their emphasis on secure and governed AI adoption. IT decision makers take a broader view, balancing AI security and risk management frameworks (33%) with a focus on AI-driven analysis and detection (29%), while IT practitioners teams lean toward DevSecOps (20%) and unified security management (14%), highlighting their role in embedding security into development and operations. These differences highlight how AI is reshaping security priorities, with leaders focused on governance and frameworks while technical teams work to operationalize protection through integrated tools and processes.

Industry spotlight

Priorities for reducing cyber risk differ markedly by industry, reflecting each industry's regulatory pressures, risk exposure, and digital maturity. Government and public sector organizations (50%) are the most likely to prioritize AI security and risk management frameworks, reflecting their focus on governance and responsible AI use. Healthcare and life sciences (47%) follow closely, highlighting the need to protect sensitive data and meet regulatory standards.

Government and public sector organizations place less emphasis on AI-Driven Analysis and Detection (17%). By contrast, telecommunications (28%), IT and services (30%), and media and entertainment (31%) place greater emphasis on AI-driven analysis and detection to strengthen real-time threat monitoring across complex, data-intensive environments, an approach aligned with their high operational connectivity and exposure to dynamic cyber threats.

Education and nonprofit organizations (28%) stand out for their focus on DevSecOps, embedding security earlier in the development process, an indication of resource constraints and a preference for prevention over response. Meanwhile, healthcare (15%) and automotive and manufacturing (15%) show slightly higher interest in unified security management, suggesting a drive to consolidate tools and improve visibility across distributed systems and supply chains.

Overall, while AI security frameworks dominate, each industry's priorities mirror its risk reality: highly regulated industries focus on governance and compliance, while digital-first industries prioritize automation, speed, and continuous monitoring.

Regional spotlight

Regional priorities for reducing cyber risk over the next three years reflect each market's broader stage of cloud and digital maturity. Asia Pacific organizations, previously shown to have higher levels of cloud usage for application building, are the most likely to prioritize AI security and risk management frameworks (46%), compared with 36% in the Americas and 32% in Europe, highlighting a proactive focus on governing AI use securely as adoption accelerates. European organizations place greater emphasis on AI-driven analysis and detection (26%) and unified security management (14%), underscoring their stronger focus on compliance and visibility. Meanwhile, organizations in the Americas take a more balanced approach, spreading priorities across AI security (36%) and AI-driven detection (24%) to strengthen both oversight and operational defenses.



The increasing use of AI agents for security tasks

Further to this, planned AI agent adoption reinforces this momentum.

Current and planned use of AI agents for security tasks

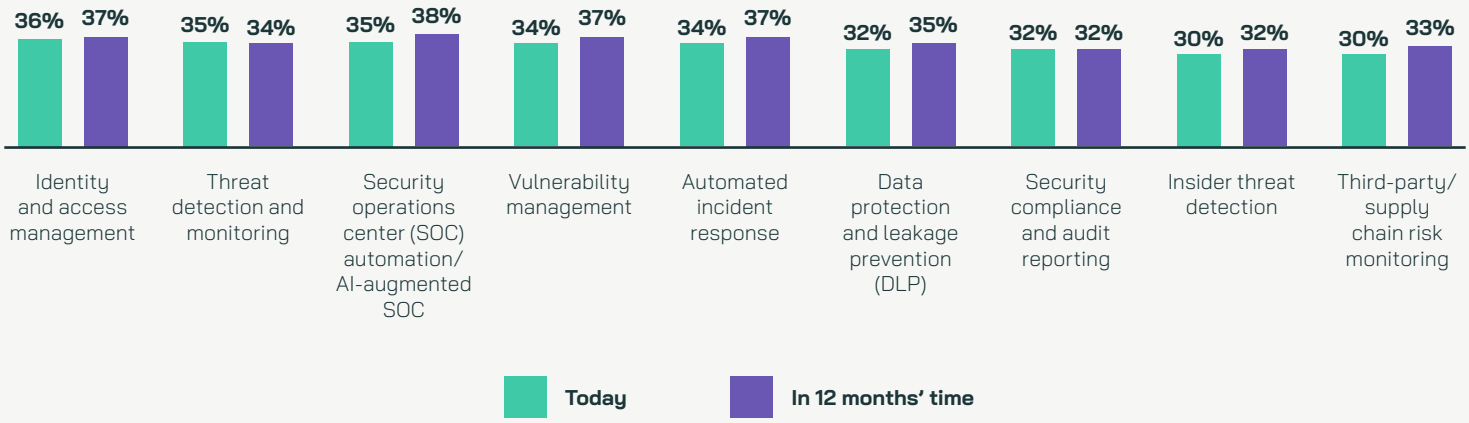


Figure 10. Which of the following security tasks, if any, does your organization plan to use AI agents for today, and which does it expect to use them for in the next 12 months? (2,800)

The growing focus on AI-augmented SOC operations reflects a shift toward faster, more proactive security models. As threat volumes rise and attack surfaces expand, organizations recognize that traditional manual monitoring can no longer keep pace. Automating incident response and integrating AI agents into SOC workflows allow teams to detect anomalies sooner, contain breaches faster, and reduce fatigue from routine tasks, all essential as cloud environments scale in size and complexity.

Crucially, organizations are making clear that security must be built into AI from the start. Nearly all respondents (98%) agree that built-in security features are one of the most important factors when selecting third-party AI solutions. As one respondent explains in their own words: "AI-based threat detection which recognizes and removes threats before they have a chance to do harm" would provide them with the confidence needed to trust the cloud with their data compared to an on-premises environment.

Others highlight the importance of coupling advanced AI with human expertise and proven processes, signaling that trust depends on both technology and accountability.

While the majority (88%) favored a more cautious approach, just over 12% disagree that AI security and risk concerns are a significant barrier to migrating more workloads and/or data to the cloud (with decision-makers more likely than practitioners to respond this way). This may indicate early adopters who have already set guardrails to pave the way for AI adoption. Many AI security concepts and risk assessment frameworks are built on foundational security principles, so highly regulated industries have foundations in place.

AI is not without its own risks and respondents stress the importance of controls and oversight, with one noting that absolute confidence would come from "seeing clear rules for how AI can be securely trained, monitored, and kept in line with compliance requirements." This tension underscores the dual role AI plays: as both a driver of resilience and a new vector of risk.

Organizations are eager to bring AI into their cloud security strategies, but on their terms. AI is viewed as indispensable for advancing protection, yet confidence in its use will hinge on cloud providers' ability to pair innovation with safeguards, governance, and transparency.

Conclusion

The direction of travel is clear: cloud is now the standard foundation for enterprise transformation, and its success relies on maintaining trust. Confidence in the public cloud is no longer defined only by technical capability, it depends equally on transparency, reliability, and responsible conduct. As the pace of digitalization accelerates and AI reshapes the security landscape, the challenge for both providers and customers is to sustain that confidence through continuous improvement and collaboration.

For organizations, the focus is shifting from whether to trust the cloud to how that trust is verified and reinforced. For providers, expectations are rising from service delivery to partnership, one measured by openness, consistency, and resilience in the face of change. The result is a more mature equilibrium, where cloud trust is not assumed but earned, and where that trust becomes the essential foundation for future innovation and growth.

Methodology

AWS commissioned independent market research specialist Vanson Bourne to undertake the research upon which this written report is based.

A total of 2,800 decision-makers and practitioners in technology and security roles were interviewed in September and October 2025. All respondents must be responsible for / have influence over decision making regarding cloud environments / technology / security in their organization. In addition, their organization must already be using a mix of on-premises data centers and cloud environments.

To qualify for the research, respondents must work in organizations with 500 or more employees (1,000 or more in the US) across a variety of industries: Healthcare and Life Sciences, Government/ Public Sector, Financial Services, Automotive and Manufacturing, Retail and CPG, Telecommunications, Information Technology and Services, Media, Leisure and Entertainment, Education and Nonprofit, and Energy, Oil & Gas, and Utilities.

Respondents represent a number of countries across the Americas, Europe and APJ:

Region	Country	Number of respondents
Americas	US	400
	Canada	200
	Mexico	200
Europe	UK	200
	Germany	200
	France	200
	Nordics	200
APJ	China	200
	Japan	200
	South Korea	200
	Singapore	200
	Australia	200
	India	200

The interviews were conducted online and were undertaken using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate. Unless otherwise indicated, the results discussed are based on the total sample.



About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information, visit www.vansonbourne.com