cloud security alliance®

tenable

Survey Report

The State of Cloud and AI Security 2025

Acknowledgments

Lead Author

Hillary Baron

Contributors

Marina Bregkou
Josh Buker
Ryan Gifford
Alex Kaluza
John Yeoh

Graphic Design

Claire Lehnert
Stephen Lumpe

About the Sponsor

Tenable® is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation, and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight, and action across the attack surface, equipping modern organizations to protect against attacks, from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for approximately 44,000 customers around the globe. Learn more at tenable.com.

www.tenable.com

Table of Contents

Executive Summary

Hybrid and multi-cloud architectures have become the standard for most organizations, with 82% operating hybrid environments and 63% using multiple cloud providers. At the same time, AI adoption is accelerating, with over half of organizations deploying AI for business needs—and 34% of those with AI workloads already experiencing breaches. Yet security strategies have not kept pace, leaving teams reactive and fragmented.

This survey reveals six critical insights:

1. Hybrid and Multi-Cloud Dominate:
Flexible infrastructure demands unified security visibility and policy enforcement—still lacking for most.

2. Identity Risks Lead But Remain Under-Managed:
Identity is now the top risk and breach cause, but many organizations rely on basic controls and metrics, missing deeper governance gaps.

3. Expertise Gap Stalls Progress:
Limited cloud security expertise undermines leadership alignment, strategy, and investment.

4. Measuring Breaches, Not Prevention:
KPIs remain reactive, focused on incidents instead of risk reduction and resilience.

5. AI Adoption Outpaces Security Readiness:
Organizations prioritize compliance and novel AI risks over proven cloud and identity controls.

6. Leadership Must Reset Strategy:
Outdated assumptions and underinvestment leave security teams without the structural support to mature.

To address these gaps, organizations should:

- Build integrated visibility and controls across hybrid and multi-cloud infrastructures
- Mature identity governance for human and non-human identities
- Focus KPIs on prevention and resilience
- Improve leadership's understanding of the true operational needs
- Treat compliance as a baseline for AI security, not the endpoint

Security maturity depends on strategic alignment and risk-driven planning. Organizations that move beyond point solutions and reactive operations will be better equipped to secure evolving cloud and AI environments.

Key Findings

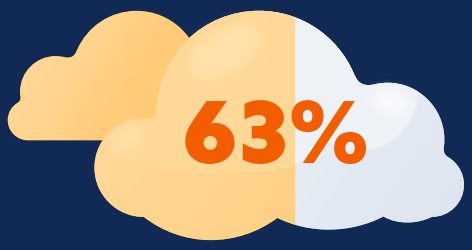
Cloud and AI are no longer emerging trends—they're embedded in the way organizations operate, with hybrid and multi-cloud architectures providing flexibility and AI moving quickly from pilot projects to business-critical workloads. Yet while adoption has surged, security strategies have struggled to keep up. The findings reveal a clear gap between awareness and execution: while most organizations recognize where their risks lie, many remain reactive, fragmented, and misaligned.

Key Finding 1:

Hybrid and Multi-Cloud Dominate

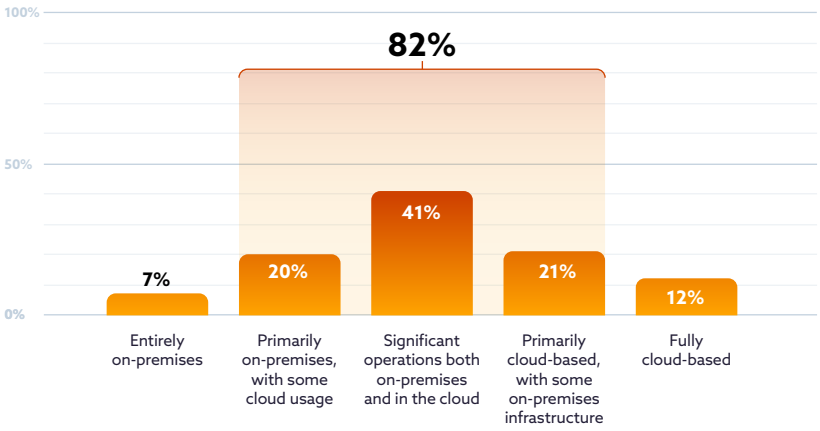
Hybrid and multi-cloud architectures aren't emerging trends—they're already the norm for most organizations, and here to stay. Rather than migrating everything to a single provider or abandoning on-prem entirely, organizations are deliberately choosing a mix of environments to meet their operational, financial, and regulatory needs. These models offer the flexibility to run workloads where they make the most sense—whether that's in the cloud, across multiple providers, or still on-premises.

Sixty-three percent of organizations report using more than one cloud provider, with multi-cloud users operating an average of between 2 and 3 cloud environments



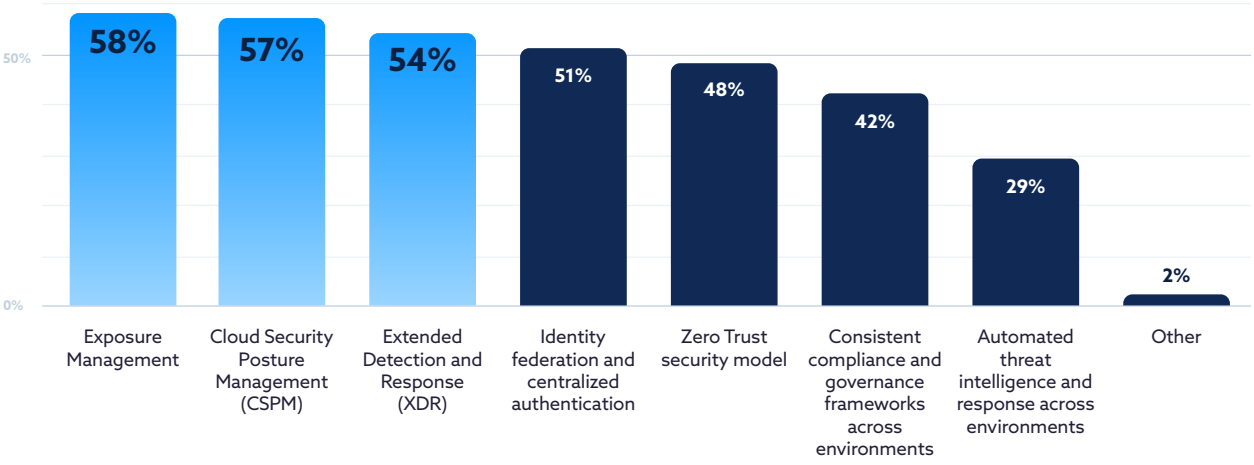
Sixty-three percent of organizations report using more than one cloud provider, with multi-cloud users operating an average of between 2 and 3 (2.7) cloud environments. At the same time, **82% of organizations maintain hybrid infrastructure of some kind**, either split evenly between on-prem and cloud or leaning more heavily on one type of environment.

What best describes your organization's IT/ cloud infrastructure?



To secure this fragmented infrastructure, organizations are leaning into tools designed to span cloud and on-prem. **Unified security monitoring and risk prioritization (58%)**, **cloud security posture management (CSPM) (57%)**, and **extended detection and response (XDR) (54%)** are the most commonly used controls across hybrid environments. This signals a shift away from siloed or provider-native tooling toward broader visibility and control mechanisms that can keep pace with the complexity of hybrid infrastructure.

What security measures is your organization taking to understand and act on exposure and related risk across your hybrid environments?



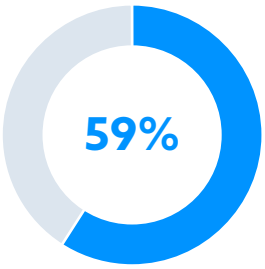
The move toward hybrid and multi-cloud is likely driven by a combination of cost optimization, regulatory demands, and performance requirements. In some cases, organizations are even moving workloads back on-prem to better manage expenses or gain more direct control, as noted in a previous Cloud Security Alliance (CSA) survey report. Regardless of the motivation, this model demands security strategies capable of providing consistent policy enforcement, identity management, and risk monitoring across a landscape that is anything but uniform.

Key Finding 2:

Identity Has Become the Cloud's Weakest (and Organizations' Most Watched) Link

Identity-related issues now top the list of cloud security concerns—outpacing long-standing risks like misconfigurations, insider threats, and workload vulnerabilities in perception, breach impact, and strategic focus. While this signals meaningful progress in awareness, there is a critical gap between understanding identity as a key threat and measures taken to effectively secure it. Governance, measurement, and operational coordination all lag behind reported intent.

Top security risk to organization's cloud infrastructure

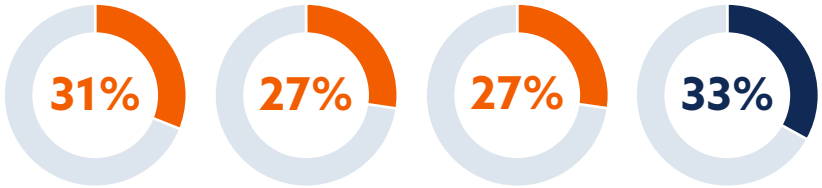


Insecure identities and risky permissions

Fifty-nine percent of organizations identified insecure identities and risky permissions as the top security risk to their cloud infrastructure. This concern is borne out in breach data as well. Among those who experienced a cloud-related breach, three of the top four causes were identity-related: **excessive permissions (31%)**, **inconsistent access controls (27%)**, and **weak identity hygiene (27%)**.

Which of the following factors do you think contributed the most to your organization's breach?

Identity-Related



Excessive permissions (e.g., overprivileged accounts or roles)

Inconsistent access controls across cloud environments

Weak identity hygiene (e.g., no MFA, inactive access keys)

Misconfigured cloud services or infrastructure

These issues are interconnected but distinct. Excessive permissions—like standing admin access or broad role assignments—can escalate even minor compromises into major breaches. Inconsistent access controls across environments create uneven protections and blind spots that attackers can exploit. Weak identity hygiene—defined as poor processes for identifying and remediating risky behaviors like unrotated keys, unused credentials, or orphaned accounts—leads to long-lived vulnerabilities that often go undetected until after an incident occurs.

Together, these patterns point to a layered, systemic problem: it's not just a few misconfigured accounts but a fundamental breakdown in how identity is governed across teams and systems. These are not merely technical lapses, they're operational challenges rooted in a lack of shared ownership, oversight, and accountability across cloud and identity access management (IAM) functions.

Even as organizations report that they recognize these risks and are prioritizing Zero Trust, security maturity still lags. When asked about top challenges, **28% of respondents cited misalignment between cloud and IAM teams**, and **21% reported difficulty enforcing least privilege**. This indicates that many organizations know where the problem is, but still lack the structure or workflows to address it at scale.

Top challenges securing organization's cloud infrastructure

28% Lack of alignment between cloud security and IAM teams

21% Difficulty enforcing least privilege

To close the gap, organizations are prioritizing Zero Trust architectures and are **implementing least privilege for identities was the most selected cloud security priority for the next 12 months (44%)**. Yet measurement practices remain early-stage. **Forty-two percent of organizations track multifactor authentication (MFA) or single sign-on (SSO) adoption rates**—the most common IAM KPI—but this only shows whether controls are in place, not whether they're effective. Few organizations monitor deeper indicators of identity risk like privilege misuse, access anomalies, or non-human identity abuse.

44%

Of organizations consider implementing least privilege for identities a top priority

42%

Of organizations track multifactor authentication (MFA) or single sign-on (SSO) adoption rates

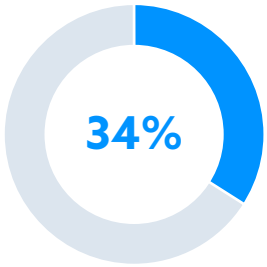
The data paints a picture of identity as both a well-recognized threat and a still-maturing discipline in secure management. Organizations are moving in the right direction, but meaningful progress will require more than policy declarations. They'll need to restructure IAM programs and supporting systems such as identity providers, improve coordination with cloud teams, and shift from binary adoption metrics to more dynamic indicators of identity risk and resilience.

Key Finding 3:

The Expertise Gap Creates a Leadership Alignment Challenge

The lack of cloud security expertise isn't just a staffing or hands-on implementation problem, it's a strategic obstacle that shapes how organizations plan, budget, and prioritize security at every level. As security teams struggle to operationalize cloud protections with limited expertise, that gap begins to shape decisions affecting leadership alignment, resource allocation, and organizational risk posture.

Top challenges to securing organization's cloud infrastructure



Lack of expertise

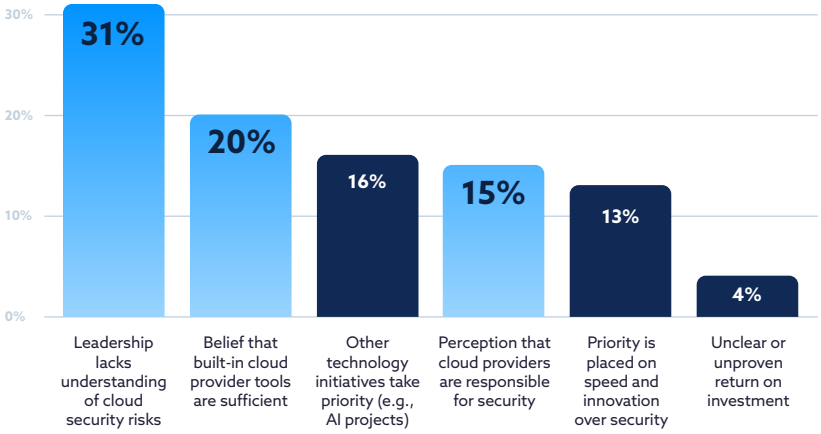
Thirty-four percent of respondents identified lack of expertise as the top challenge to securing cloud infrastructure—more than any other issue. But the impact of that gap doesn't stop at the hands-on level. It creates a ripple effect that undermines planning and execution. When asked about barriers to implementing new cloud security capabilities, respondents pointed to **unclear strategy (39%)**, **insufficient budget (35%)**, and **resources being diverted to other priorities (31%)**—all symptoms of leadership struggling to set direction, assess tradeoffs, or fully grasp the risks at stake.

What are the top 3 barriers to implementing new cloud security capabilities for your organization?

39%	Unclear strategy or plan for cloud security	**29%**	Integration with legacy systems	**17%**	Vendor lock-in or internal loyalty to vendors
35%	Insufficient budget	**26%**	Lack of processes or documentation	**16%**	Available tools and solutions do not meet organization's needs
31%	Resources diverted to other priorities	**23%**	Lack of support from senior management	**11%**	Friction with DevOps team
30%	Expertise constraints	**20%**	Time constraints	**1%**	Other

This disconnect is further underscored by how leadership views cloud security. Nearly **a third of respondents (31%) said their executive leadership lacks sufficient understanding of cloud security risks**. Others noted that leaders believe **built-in cloud provider tools are "good enough" (20%)**, or assume that the **cloud provider is primarily responsible for securing the environment (15%)**—a clear misunderstanding of the shared responsibility model. These perceptions suggest that many executive teams still operate under legacy security assumptions, making it difficult for security teams to gain support for the tools, staffing, or time needed to secure today's complex hybrid and multi-cloud environments.

If your organization lacks support from senior management, what is the primary reason for their limited support of new cloud security efforts?



Rather than treat expertise solely as a hiring or training issue, organizations can reframe the problem as a broader operational challenge—one that can be addressed through a combination of internal enablement, external partnerships, and platform choices that reduce cognitive load. There's also a clear opportunity to use these platforms and tools not only to improve security posture but to help educate leadership along the way. By aligning executive understanding with security realities, organizations can shift from reactive, point-solution thinking to more strategic, integrated security programs.

Key Finding 4:

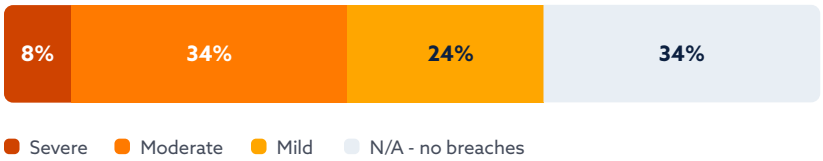
Fighting Fires Instead of Preventing Them–Measuring Breaches, Not Prevention

Cloud security remains caught in a reactive loop. While breaches remain a persistent and significant challenge, organizations are measuring performance based on what's already gone wrong, rather than how effectively risk is being reduced or prevented. The result is a metrics culture that reinforces crisis response over long-term resilience.

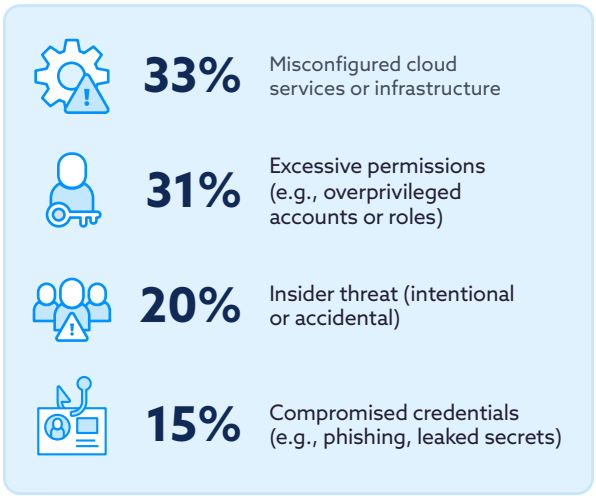
The most commonly tracked cloud security KPI is **security incident frequency and severity (43%)**, a metric that only becomes relevant after an incident occurs. In IAM, the top metric is **MFA/SSO adoption rates (42%)**, which tracks whether basic controls are in place, not whether they're effective or being misused. Together, these figures suggest that organizations remain focused on surface-level indicators rather than more strategic, forward-looking measures of performance.

This rearview mirror mindset is also reflected in breach data. Organizations reported an average of 2.17 cloud-related breaches over the past 18 months, yet **only 8% categorized any of those as "severe"**. While some incidents may truly be low-impact, the discrepancy suggests many are being perceived as less severe—potentially because they didn't trigger mandatory reporting thresholds, significant media coverage, or obvious operational impact.

On average, rate the level of severity of the cloud-related breach(es) your organization has experienced.



Which of the following factors do you think contributed the most to your organization's breach?



The data reveals a disconnect between breach frequency and how incidents are internally evaluated, one that complicates efforts to measure and communicate true security performance. That disconnect becomes even more troubling when considered alongside the root causes of these breaches, many of which are preventable. **Thirty-three percent cited misconfigured cloud services**, while **31% pointed to excessive permissions**, **20% to insider threats**, and **15% to compromised credentials**—issues that could be mitigated through stronger configuration management, access governance, and proactive detection.

All of this points to a dangerous measurement blind spot. Breach rates remain high, yet few incidents are classified as severe, and the KPIs most organizations track remain rooted in reaction rather than prevention. Measurement remains tied to post-incident response rather than forward-looking risk reduction.

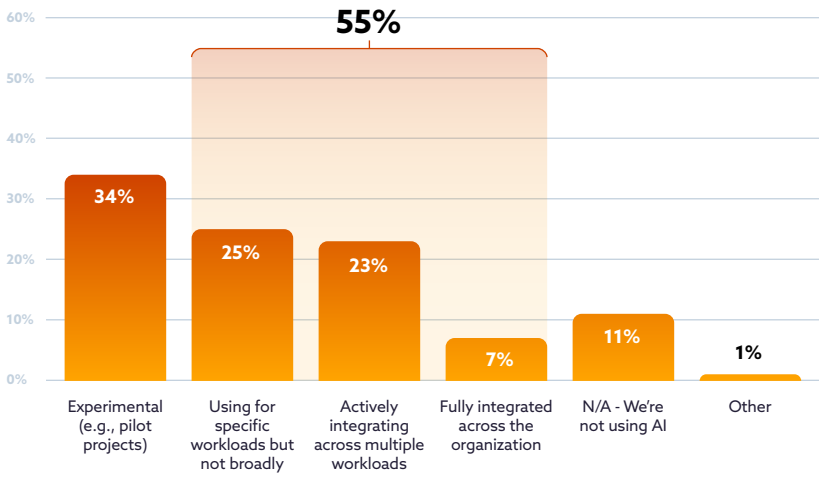
This approach fails in two critical ways: it doesn't demonstrate the value of proactive investment to leadership, and it obscures the full scope of risk by assuming incidents are always visible, reportable, and correctly classified. In environments with limited detection capabilities—or where performance is judged by the absence of "severe" incidents—critical events could be missed or minimized. Breaking that cycle requires more than new measurements or tools—it demands a redefinition of success, one centered on risk reduction rather than damage control.

Key Finding 5:

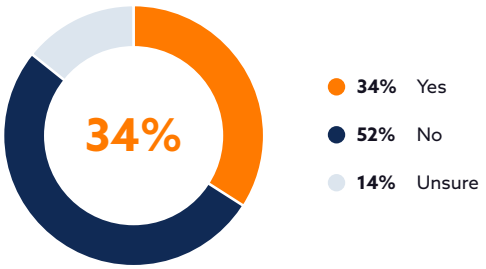
AI Adoption Accelerates While Security Targets the Wrong Risks

AI adoption is outpacing the readiness of many security teams. While 34% of organizations describe their AI use as "experimental", even more have already moved beyond that stage. **A combined 55% are using AI for active business needs**—25% for specific workloads, 23% actively integrating across multiple systems, and 7% fully integrated across the organization. These are not theoretical pilots; they represent operational deployments with real business impact. Yet as AI moves into production, security efforts aren't always keeping pace. The result: **more than a third of organizations with AI workloads (34%) have already experienced an AI-related breach**, raising urgent questions about AI security readiness and risk management.

To what extent is your organization developing AI applications in the cloud?



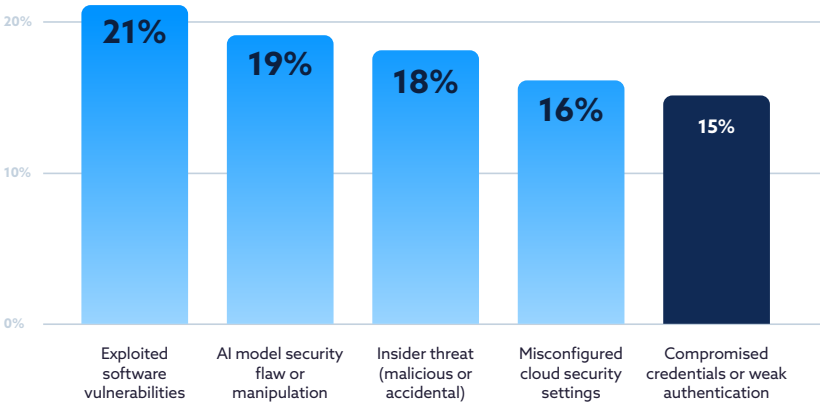
Did any of the cloud data breaches your organization experienced involve an AI workload?



The occurrence of AI-related breaches points to a deeper issue: while AI is being operationalized, security practices haven't fully caught up.

Organizations are moving fast to deploy AI, but their understanding of where the risks lie—and how to mitigate them—still appears immature. That disconnect becomes even more apparent when comparing what's actually causing breaches to what security teams are most concerned about. The most common causes of AI-related breaches include familiar threats: **exploited software vulnerabilities (21%)**, **AI model flaws (19%)**, **insider threats (18%)**, and **misconfigured cloud settings (16%)**. Yet when asked which breach types they're most concerned about, organizations gravitated toward unfamiliar or "AI-native" risks—such as **model manipulation (18%)** and **the use of unauthorized AI models (15%)**—while **concerns about insider threats (9%)** and compromised credentials (7%) ranked much lower. This misalignment suggests that many security programs are still treating AI as fundamentally novel, rather than applying proven cloud and identity security principles to these new systems.

What was the primary cause of the data breach involving an AI workload?



Which type of cloud data breaches involving AI workloads is your organization most concerned about?

18% AI model security flaw or manipulation

15% Use of unauthorized AI models in development

13% Misconfigured cloud security settings

11% Prefer not to disclose

10% Unclear or unknown cause

9% Insider threat (malicious or accidental)

8% Third-party vendor or supply chain attack

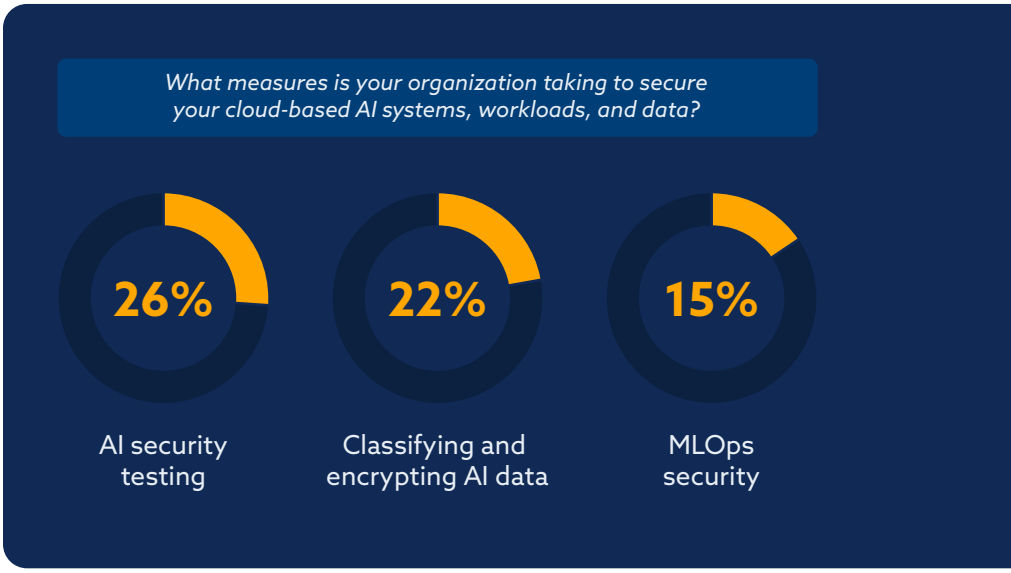
7% Compromised credentials or weak authentication

5% Exploited software vulnerabilities

2% Ineffective decommissioning of pre-production AI assets

Security controls further illustrate this imbalance. More than **half of organizations (51%) rely on compliance frameworks** like NIST AI RMF or the EU AI Act to guide their AI security efforts. Regulatory alignment is essential and offers a necessary foundation, but frameworks alone aren't built to keep pace with the speed and complexity of AI adoption.

A strong security program should proactively address the organization's specific risk profile. Yet the low adoption of core technical safeguards suggests that many organizations stop at compliance. Only **26% conduct AI-specific security testing** such as red teaming, just **22% classify and encrypt AI data**, and only **15% have implemented MLOps security practices**. This compliance-heavy but technically shallow posture can leave AI workloads exposed.



Without deeper technical investment and risk-informed strategies, organizations are in danger of overlooking foundational security practices that already exist in other domains, like identity governance, workload hardening, and data protection. And this accounts only for sanctioned use; with shadow AI on the rise, the unmonitored portion of the AI landscape may pose even greater risk.

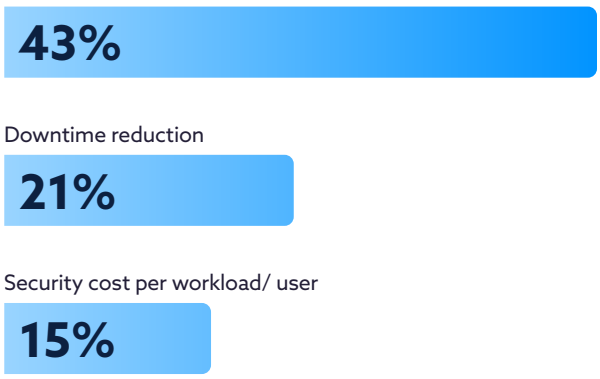
Key Finding 6:

Time for a Security Strategy Reset

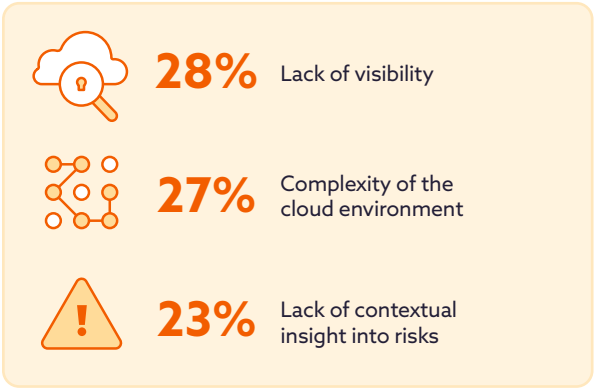
Many security teams know what needs to be done, but their leadership is still operating under outdated assumptions. As cloud and AI deployments expand across hybrid and multi-cloud environments, security complexity is increasing. Yet at the executive level, misconceptions about responsibility and risk are stalling progress and preventing organizations from scaling their security strategies effectively.

As noted previously, many executives still overestimate the security coverage provided by cloud providers or built-in tools, and this misunderstanding shapes how success is measured. Although cloud providers continue to enhance their native security offerings, these are typically limited to their own platforms and do not extend to multi-cloud or hybrid scenarios, leaving gaps in visibility and control. Most organizations still rely on reactive KPIs like **incident frequency and severity (43%)**, while few track more proactive metrics like **downtime reduction (21%)** or **security cost per workload (15%)**. Compounding this challenge, there are still relatively few solutions that unify visibility and risk assessment across hybrid environments, making it even harder for teams to measure and manage risk holistically. The result is a persistent strategic blind spot. Without clear understanding or meaningful performance indicators, security teams lack the direction and resources to prioritize long-term maturity.

How do you demonstrate the KPIs of your cloud security technology investments?



Top challenges securing organization's cloud infrastructure



The implications are significant. Organizations have complex environments—82% of organizations operate hybrid environments and 63% have a multi-cloud environment—and they struggle with them. Some of the top challenges beyond the ones discussed earlier include **lack of visibility (28%)**, **complexity of the cloud environment (27%)**, and **lack of contextual insights into risks (23%)**, all of which are needed to understand and prioritize risk. But instead of investing in foundational efforts like unified visibility or simplifying their tool landscape, just 20% prioritize unified risk assessment, and only 13% are focused on tool consolidation.

This leaves security teams managing fragmented solutions without the structural support to reduce risk holistically or scale their efforts effectively.

To break this cycle, organizations need more than technical fixes—they need a strategic reset. Leadership must move beyond assumptions that security is "baked in" and instead invest in platforms and processes that provide integrated visibility, reduce complexity, and enable forward-looking risk management. This shift is especially urgent as AI adoption accelerates, introducing new risks that require both foundational security maturity and the agility to respond to emerging threats. Until that reset occurs, even the most capable security teams will remain locked in reactive operations, without the strategic alignment required to scale, adapt, and mature.

Conclusion

Most organizations already operate in hybrid and multi-cloud environments, and over half are using AI for business-critical workloads. While infrastructure and innovation have evolved rapidly, security strategy has not kept pace. Across the board, organizations are struggling with fragmented security tooling, immature identity governance, and measurement practices that remain reactive rather than proactive. To strengthen cloud and AI security programs, organizations must shift from reactive responses to proactive, risk-informed strategies. That means:

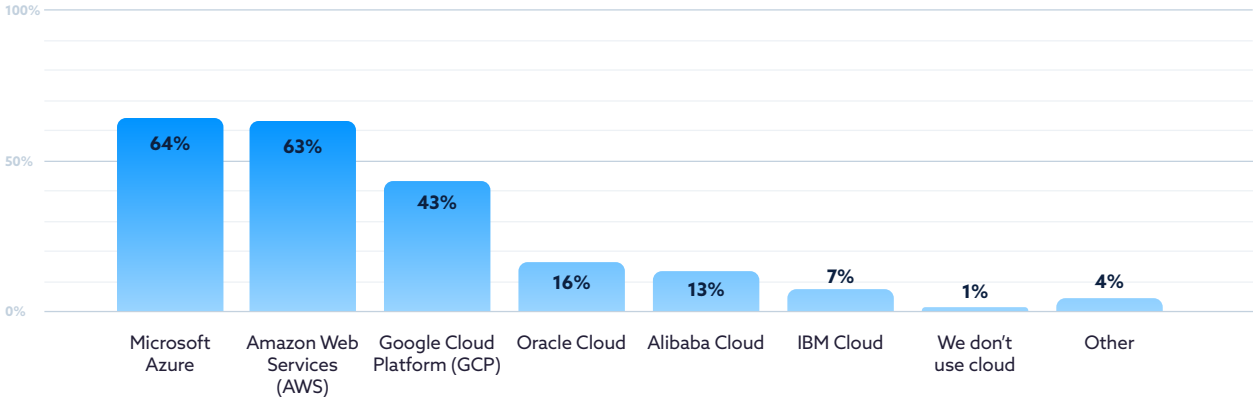
- Prioritizing unified visibility and consistent policy enforcement across hybrid and multi-cloud environments
- Investing in identity governance, including controls for least privilege and non-human identities
- Expanding KPIs to reflect prevention and resilience—not just incident response
- Aligning leadership understanding with operational realities to support smarter planning and resource allocation
- Moving beyond compliance as the ceiling of AI security, using it instead as a starting point for deeper technical safeguards

Security maturity won't come from tools alone—it requires a coordinated effort across teams, leadership, and strategy. The organizations that succeed will be those that build the structures to understand, prioritize, and reduce risk before incidents occur.

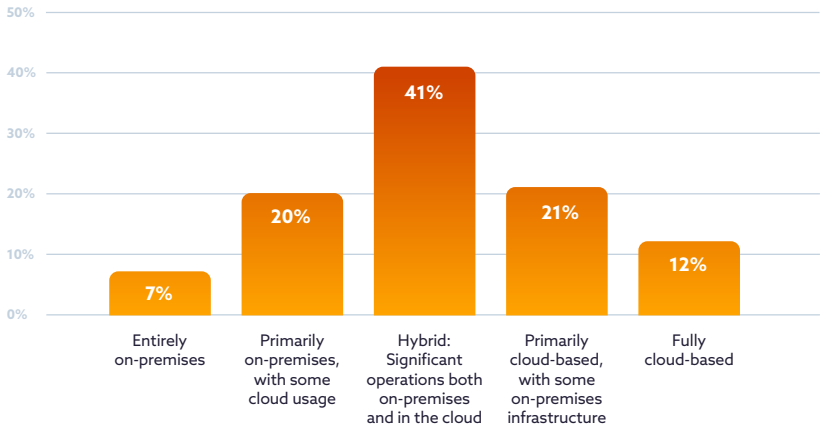
Full Survey Results

Cloud Infrastructure

Which of the following cloud providers does your organization use?

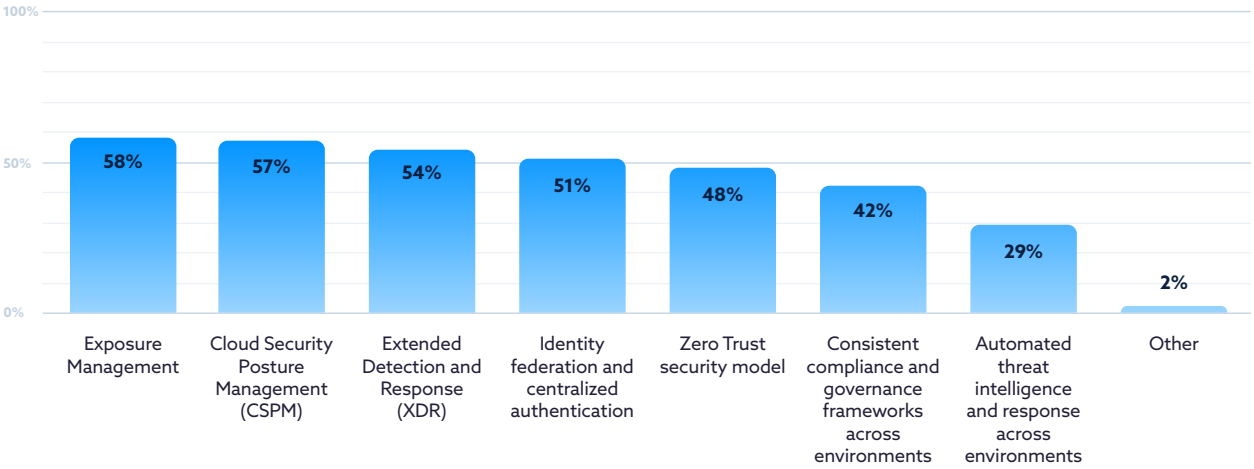


What best describes your organization's IT/ cloud infrastructure?



Cloud Security

What security measures is your organization taking to understand and act on exposure and related risk across your hybrid environments?



What security measures is your organization using to understand and act on exposure and related risks in your cloud environment?

63% API security

59% Compliance and governance frameworks for cloud environments

58% Cloud Security Posture Management (CPSM)

57% Zero Trust security model

53% Identity federation and centralized authentication

42% Extended Detection and Response (XDR)

41% Infrastructure-as-Code (IaC) security scanning

34% Automated threat intelligence and response

27% Unified cloud risk monitoring and prioritization

19% Cloud Infrastructure Entitlement Management (CIEM)

6% Other

Risks, Challenges, and Barriers

What do you consider the 3 greatest security risks to your organization's cloud infrastructure?

59% Insecure human/service identities and risky permissions

47% Cloud misconfigurations

31% 3rd-party risks/supply-chain attacks

31% Human error

22% Publicly exposed cloud resources

21% Workload vulnerabilities or runtime threats

20% Insecure APIs or other interfaces

19% Ransomware attacks

15% Network misonfigurations

11% Noncompliance with standards

11% Deficient documentation or processes

1% Other

What are the top 3 challenges to securing your organization's cloud infrastructure?

34% Lack of expertise

28% Lack of alignment between cloud security and IAM teams

28% Lack of visibility

27% Complexity of the cloud environment

23% Lack of contextual insight into risks

23% Time constraints

22% Lack of documentation and processes

21% Difficulty enforcing least privilege

19% Lack of automation or proper tooling

17% Difficulty with identity lifecycle management

16% Friction with DevOps

12% Lack of granular controls

7% Lack of temporary access (Just in Time) controls

2% Other

What are the top 3 barriers to implementing new cloud security capabilities for your organization?

39% Unclear strategy or plan for cloud security

35% Insufficient budget

31% Resources diverted to other priorities

30% Expertise constraints

29% Integration with legacy systems

26% Lack of processes or documentation

23% Lack of support from senior management

20% Time constraints

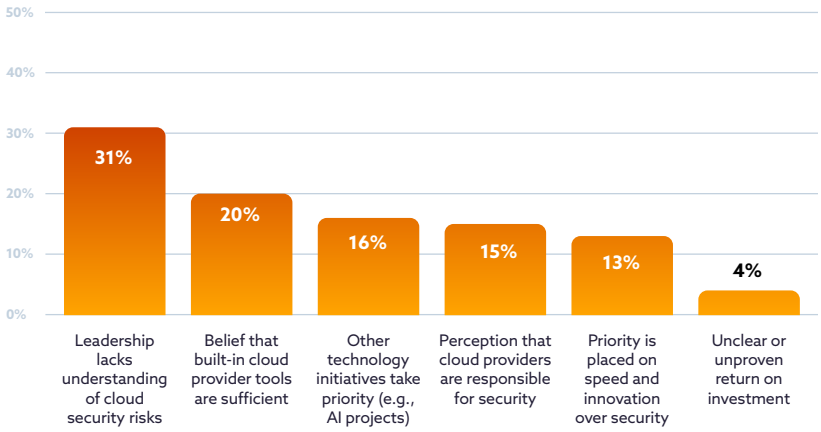
17% Vendor lock-in or internal loyalty to vendors

16% Available tools and solutions do not meet organization's needs

11% Friction with DevOps team

1% Other

If your organization lacks support from senior management, what is the primary reason for their limited support of new cloud security efforts?



Priorities and KPIs

What are your top 3 cloud infrastructure security priorities over the next 12 months?

44% Implement zero trust and least privilege for identities

36% Detect and remediate cloud misconfigurations

26% Maintain compliance (e.g., NIST, SOC2, ISO, PCI-DSS, CIS)

24% Implement temporary elevated access (JIT) for DevOps and others (i.e. remove standing privileges)

21% Evaluate and mitigate attack surface of cloud infrastructure

20% Unify risk assessment for hybrid environments (i.e. across cloud, on-prem, OT)

20% Implement cloud detection and response (CDR)

17% Budget optimization

17% Manage workload vulnerabilities

15% Improve resiliency and disaster recovery

15% Data analytics and AI security integration

15% Implement Infrastructure-as-Code (IaC) scanning

13% Tool consolidation

2% Preparing for quantum threat

How do you demonstrate the KPIs of your cloud security technology investments?

43% Security incident frequency and severity

36% Mean Time to Remediate (MTTR)

33% Compliance and audit scores

32% Mean Time to Detect (MTTD)

25% Mean Time to Identify (MTTI)

21% Downtime reduction

18% False positive rate

17% Mean Time to Contain (MTTC)

17% Mean Time to Restore Normality (MTTRN)

15% Security cost per workload/user

14% Time to Value (TTV)

14% Anecdotal reports on the performance of the technology

6% We don't measure the performance of our technology investments

1% Other

How do you demonstrate the KPIs of your IAM security technology investments?

42% Multi-factor Authentication (MFA)/ single sign-on (SSO) adoption rates

28% Security incident frequency and severity

24% Compliance and audit scores

22% Mean Time to Detect (MTTD)

22% Mean Time to Identify (MTTI)

21% Mean Time to Remediate (MTTR)

21% Frequency of access anomalies

16% Frequency of privilege access abuse

16% Security cost per workload/user

14% False positive rate

13% Mean Time to Contain (MTTC)

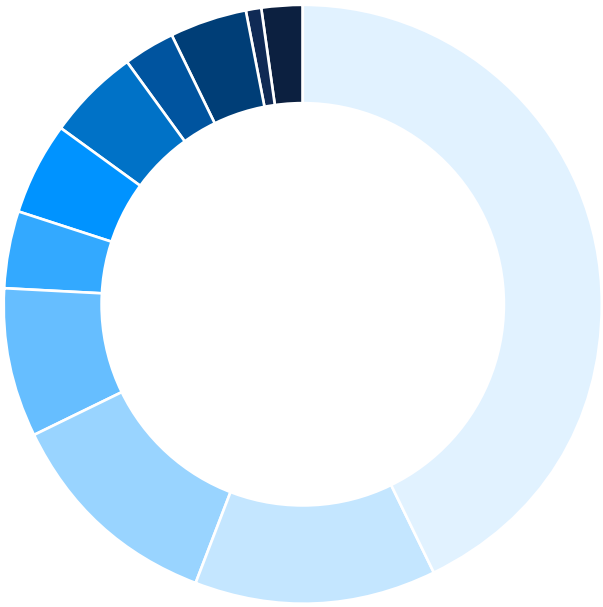
13% Time to Value (TTV)

12% Mean Time to Restore Normality (MTTRN)

9% Anecdotal reports on the performance of the technology

9% We don't measure the performance of our technology investments

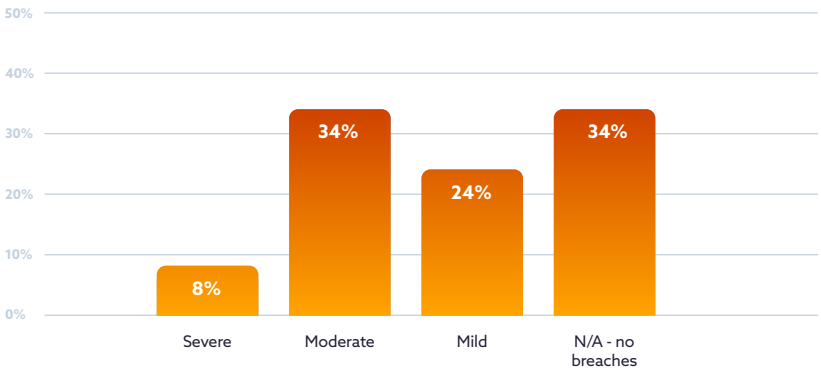
Cloud Breaches



How many cloud-related breaches has your organization experienced in the past 18 months?

42%	0	5%	6
13%	1	3%	7
12%	2	4%	8
8%	3	1%	9
4%	4	2%	10
5%	5		

On average, rate the level of severity of the cloud-related breach(es) your organization has experienced.

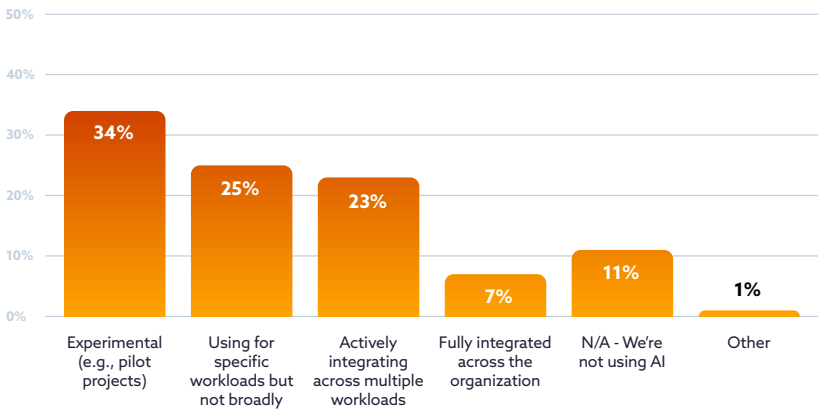


Which of the following factors do you think contributed the most to your organization's breach?

33%	Misconfigured cloud services or infrastructure	**20%**	Insider threat (intentional or accidental)	**15%**	Compromised credentials (e.g., phishing, leaked secrets)
31%	Excessive permissions (e.g., overprivileged accounts or roles)	**20%**	Insecure APIs or other interfaces	**15%**	Insufficient expertise or lack of personnel
27%	Inconsistent access controls across cloud environments	**18%**	Third-party/vendor compromise	**9%**	Exploited vulnerabilities
27%	Weak identity hygiene (e.g., no MFA, inactive access keys)	**17%**	Unintended public exposure (e.g. open S3 buckets, misconfigured databases)	**25%**	N/A - No breaches

AI Security

To what extent is your organization developing AI applications in the cloud?

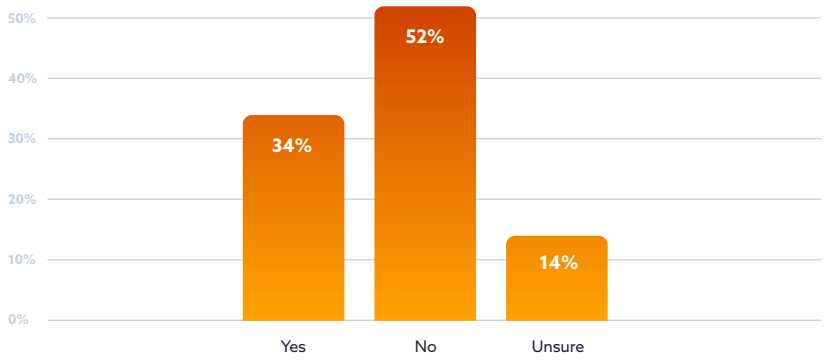


What measures is your organization taking to secure your cloud-based AI systems, workloads, and data?

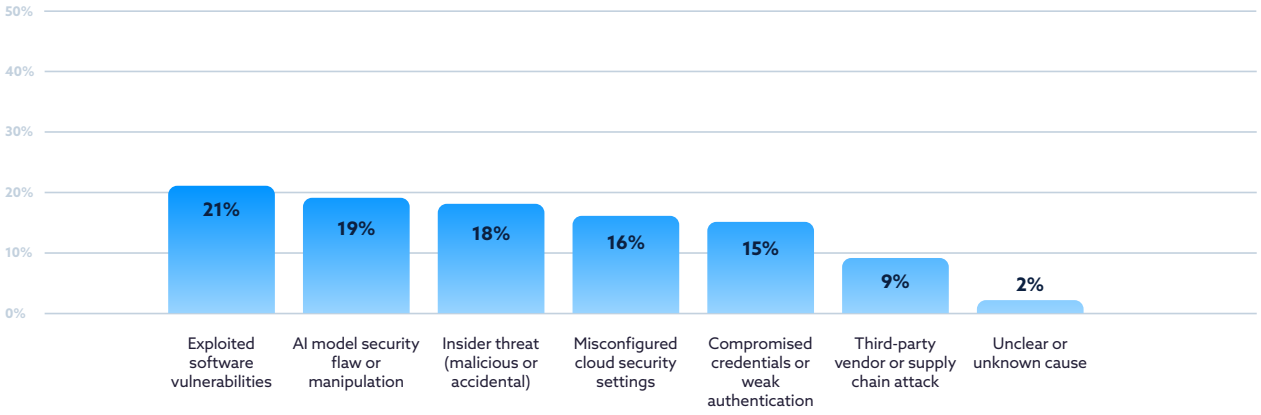
51%	Enforcing compliance with AI/Cloud security frameworks	**30%**	Zero trust and network segmentation of AI workloads	**22%**	Classifying and encrypting AI data
46%	Adopting industry best practices	**30%**	Threat detection and incident response for AI-related activity	**15%**	MLOps security
35%	Regular security audits of AI model integration protections	**26%**	AI security testing	**5%**	None of these apply
34%	AI-specific identity and access controls	**23%**	AI supply chain security	**1%**	Other

AI Breaches

Did any of the cloud data breaches your organization experienced involve an AI workload?



What was the primary cause of the data breach involving an AI workload?



Which type of cloud data breaches involving AI workloads is your organization most concerned about?

18% AI model security flaw or manipulation

15% Use of unauthorized AI models in development

13% Misconfigured cloud security settings

11% Prefer not to disclose

10% Unclear or unknown cause

9% Insider threat (malicious or accidental)

8% Third-party vendor or supply chain attack

7% Compromised credentials or weak authentication

5% Exploited software vulnerabilities

2% Ineffective decommissioning of pre-production AI assets

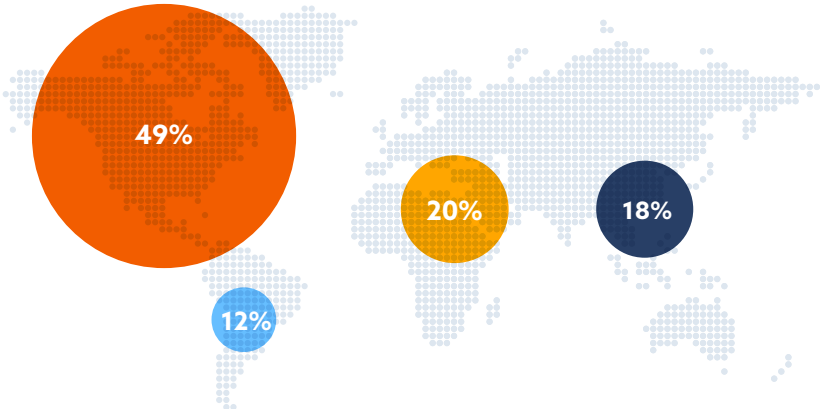
3% Other

Demographics

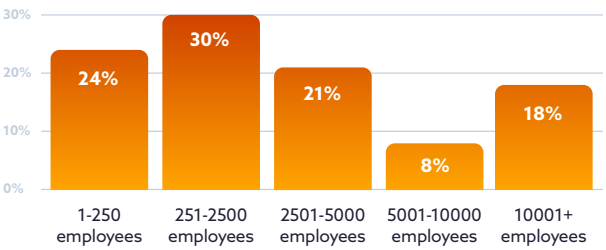
This global survey gathered insights from 1,025 IT and security professionals across a diverse range of organizations, industries, sizes, and geographic regions. The demographic breakdown provides important context for understanding the findings, highlighting the varied experiences and challenges faced by organizations in different sectors and operational scales.

What region of the world are you located in?

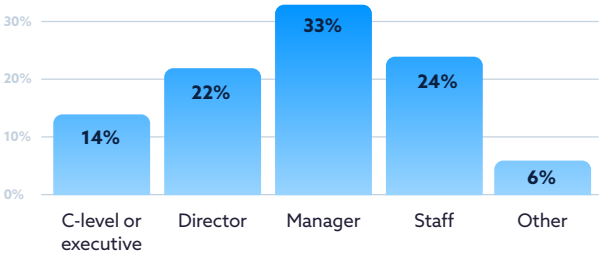
- North America
- Latin/ South America
- Europe, Middle East, Africa (EMEA)
- Asia Pacific (APAC)



Organization size



Which best describes your job level?



Which of the following best describes the principal industry of your organization?

23%	Telecommunications, Technology, Internet & Electronics	**3%**	Insurance	**2%**	Retail & Consumer Durables
17%	Finance & Financial Services	**3%**	Automotive	**2%**	Transportation & Delivery
7%	Education	**2%**	Airlines & Aerospace (including Defense)	**1%**	Agriculture
6%	Government	**2%**	Utilities, Energy, and Extraction	**1%**	Health & Fitness
5%	Business Support & Logistics	**2%**	Advertising & Marketing	**1%**	Real Estate
5%	Manufacturing	**2%**	Entertainment & Leisure	**4%**	Prefer not to answer
4%	Healthcare & Pharmaceuticals	**2%**	Food & Beverages		
3%	Construction, Machinery, and Homes	**2%**	Nonprofit		

Survey Methodology and Creation

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to widely promote best practices and ensure cybersecurity in cloud computing and IT technologies. CSA also educates various stakeholders within these industries about security concerns in all other forms of computing. CSA's membership is a broad coalition of industry practitioners, corporations, and professional associations. One of CSA's primary goals is to conduct surveys that assess information security trends. These surveys provide information on organizations' current maturity, opinions, interests, and intentions regarding information security and technology.

Tenable commissioned CSA to develop a survey and report to better understand the industry's knowledge, attitudes, and opinions regarding cloud and AI security trends. Tenable financed the project and co-developed the questionnaire with CSA research analysts. The survey was conducted online by CSA in May 2025 and received 1,025 responses from IT and security professionals from organizations of various sizes and locations. CSA research analysts performed the data analysis and interpretation for this report.

Goals of the Study

This survey was designed to better understand how security teams are navigating this complexity—addressing everything from identity and infrastructure protection to leadership alignment and the emerging role of AI in cloud workloads. The goal is to uncover how organizations are adapting their strategies, prioritizing risk, and measuring progress in a rapidly shifting threat landscape.

Core objectives:

- Understand how organizations are responding to evolving security challenges across cloud, multi-cloud, and hybrid environments
- Explore how infrastructure, workloads, identities, and data are being secured in cloud-native and hybrid setups
- Identify the top risks, barriers, and priorities shaping modern cloud security strategies
- Examine how organizations track and communicate cloud-related security KPIs to business leadership
- Assess the state of AI adoption in the cloud and how AI systems, workloads, and data are being secured