tenable | Report

2024 Cloud Security Outlook

Navigating barriers and setting priorities

A global survey of cloud security professionals

Table of contents

Introduction and key findings

Cloud deployments are well understood to be an organization's greatest area of risk exposure. Effectively securing the cloud requires looking across every aspect of potential exposure including vulnerabilities, configurations and identities. Even cloud-native organizations grapple with the difficulty of detecting and remediating risk in their cloud — and, increasingly, multi-cloud — environments.

To gain control over cloud security gaps, organizations must be able to discern the most critical risks and set priorities. To do so at scale requires integrated, comprehensive risk analysis across all parts of the cloud infrastructure and automation of both the detection of risk and its remediation.

Tenable's survey sought to unveil the barriers and priorities organizations face in achieving effective cloud security in 2024. Gauging the pulse of the industry provides valuable insights into the strategies organizations are employing to tackle the evolving complexities of cloud security amid diverse technological landscapes and financial constraints.

1 The vast majority suffered cloud breaches; 58% reported actual harm from exposed sensitive data

Some 95% of cloud security professionals reported cloud-related breaches, with 92% reporting that their sensitive data was exposed and 58% of those acknowledging that the sensitive data exposure caused harm.* To address this exposure reality, the C-suite should empower and equip security leaders to enforce policies that protect sensitive data across their organization's cloud environments.

2 The top risks to cloud infrastructure are insecure identities and misconfigurations

Among security risks to their cloud infrastructure, respondents ranked insecure human/service identities and permissions, and cloud misconfigurations, at the top (39%). The biggest challenges to securing identities and permissions included lack of visibility (53%) and difficulty in managing entitlements in a multi-cloud environment (50%). Of the organizations that suffered cloud-related breaches, a striking 99% cited identities and permissions risk as the cause. Pivotal to overcoming these issues is a cohesive security approach inclusive of identity risk analysis that helps facilitate security recommendations.

3 Insufficient expertise in cloud infrastructure security plagues 95% of organizations

95% of respondents were affected by a lack of expertise in cloud infrastructure protection. Still, topping organizations' security priorities over the next 12 months are the implementation of zero trust/least privilege, detecting and remediating cloud misconfigurations, and applying Just-in-Time access — initiatives that require deep if not expert insight. These findings underscore the need for automation and intuitive tools to bridge the expertise gap and expedite productivity for existing teams. The survey also found that organizations are interested in assessing the value of their cloud security efforts and investments; specifically, the majority seek to measure mean time to investigation and remediation.

* "Harm" is defined by the National Institute of Standards and Technology at the U.S. Department of Commerce (NIST) Cybersecurity Framework as "any adverse effects that would be experienced by an individual (i.e., that may be socially, physically, or financially damaging) or an organization if the confidentiality of PII were breached."

Survey Report Findings

Cloud-related breaches in the past 18 months

A staggering 95% of respondents acknowledged experiencing a cloud-related breach within the past 18 months, with an average of 3.6 breaches per respondent. This high incidence underscores the pervasive nature of cloud security challenges. Indeed, IBM's Cost of a Data Breach 2023 report found that 82% of breaches involved data stored in the cloud.

Overall, the 95% finding highlights the critical need for robust cloud security measures and a proactive approach to address the full scope of vulnerabilities that potentially exist in the rapidly evolving threat landscape. Breaches have a quantitative cost — a reality that justifies the budget for investing in effective risk management tooling.

European organizations had a significantly higher incidence — or perhaps awareness — of cloud-related breaches. Only 2% reported not having any breaches, in contrast with 12% of their North American counterparts. Of the 98% of European respondents reporting cloud-related breaches, 61% attributed excessive permissions to be the main cause.

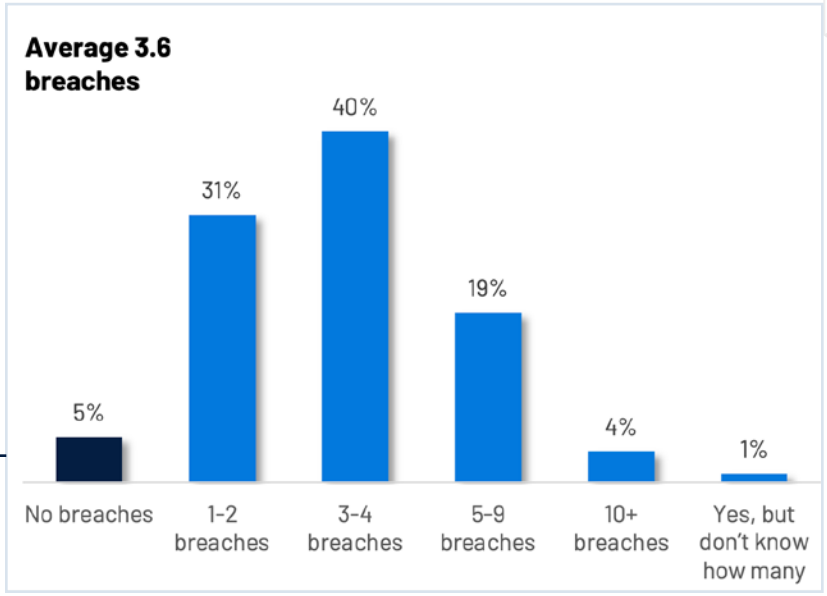


Figure 1: Cloud-related Breaches in the Past 18 Months

Figure 2: No Cloud-related Breaches in the Past 18 Months, by Region

* Base: 600

Acknowledgement of situations in which sensitive data was exposed

92% of survey respondents acknowledged situations in which sensitive data was exposed at their organizations. Of those, 58% reported that the incidents resulted in harm, defined by the NIST Cybersecurity Framework as any adverse effects that would be experienced by an individual or an organization if confidentiality were breached.

The findings further indicate that sensitive data exposure harmed organizations in some industries more than others. For example, the IT (73%) and Retail (72%) sectors reported harm in greater numbers than the Manufacturing (57%), Banking (53%) and Public sectors (38%).

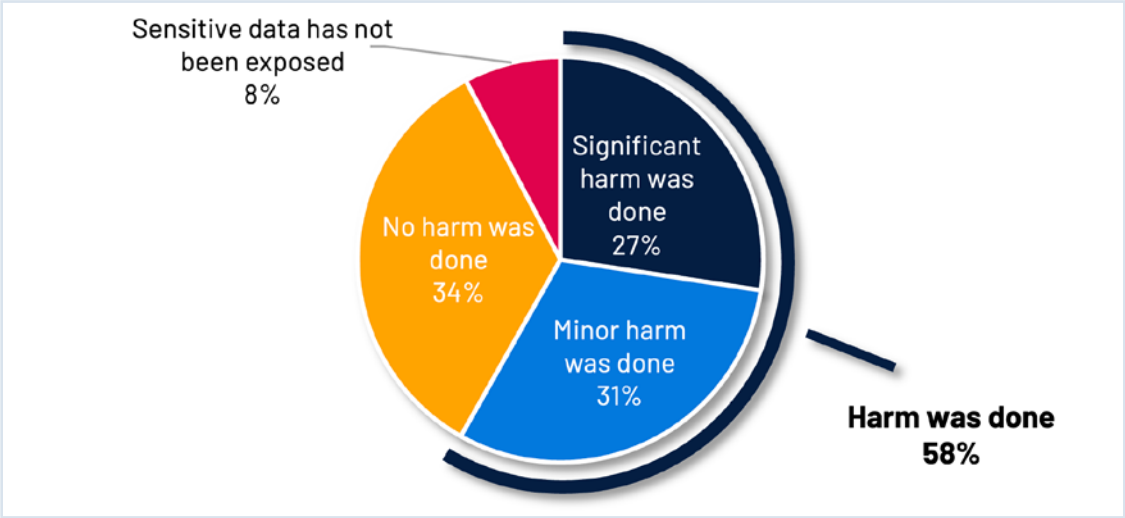


Figure 3: Acknowledgement of Situations in Which Sensitive Data Was Exposed

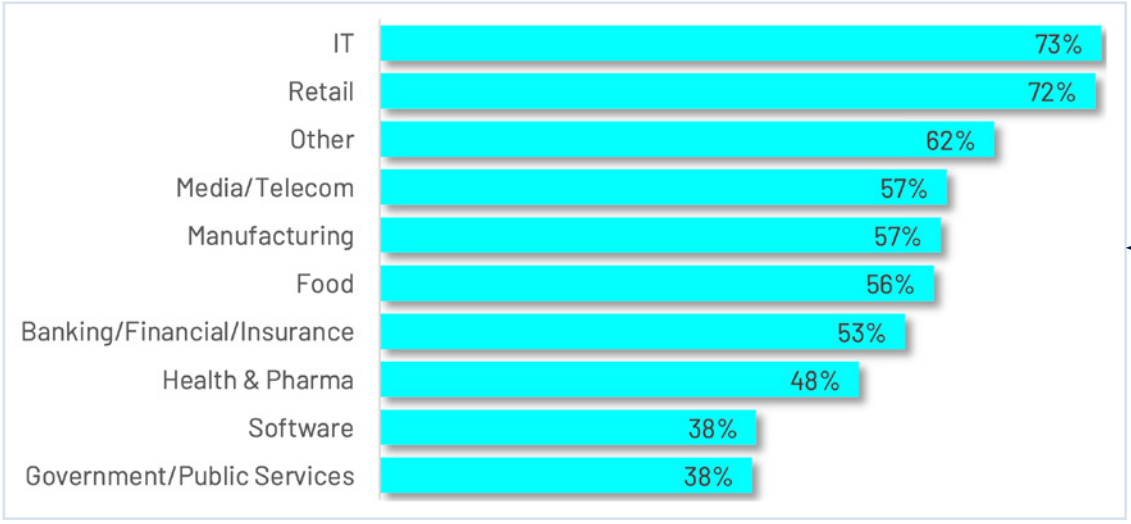


Figure 4: "Harm was done", by Industry

* Base: 569

Top security risks to cloud infrastructure

The number one security risk reported for cloud infrastructure was a tie between insecure human/service identities and risky permissions (39%), and cloud misconfigurations (39%).

While cloud misconfigurations have long been a top concern among cloud security professionals, the data points to identity security as being equally concerning.

It is worth noting that, out of a total of nine, respondents ranked six risk factors fairly evenly. This even distribution underscores an integrated approach to cloud security as essential to navigating the complex and interconnected landscape of cloud security risks.

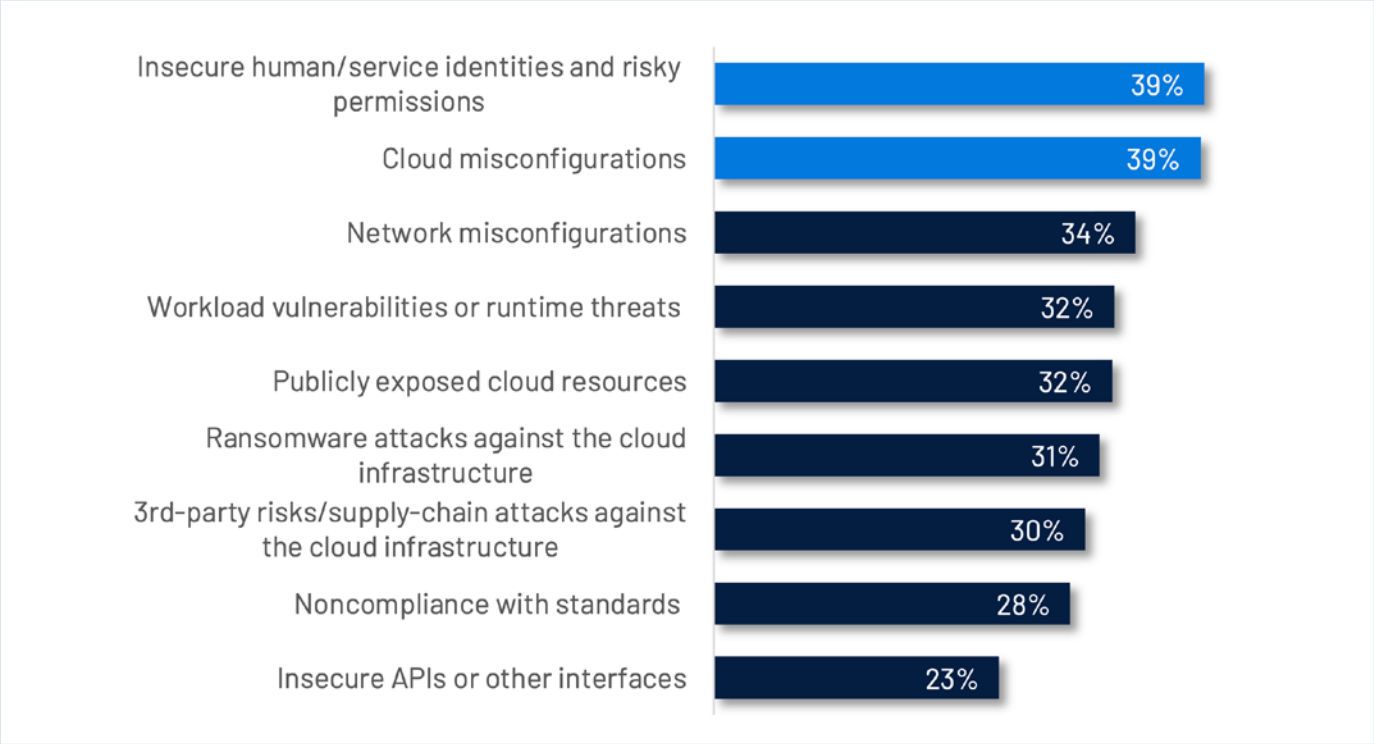


Figure 5: Top Security Risks to Cloud Infrastructure

* Base: 600. Question allowed more than one answer and as a result, percentages will add up to more than 100%

Top risk factors contributing to cloud-related breaches 1/2

To understand the cause, we asked those who experienced cloud-related breaches to identify their top contributing identity/access risks and factors. Nearly all (99%) confirmed that their breaches were related to identities and permissions. This finding underscores the critical role of access governance in cloud security.

Among the 95% of organizations affected by cloud breaches, respondents identified the top three identity/access risk factors as:

- Excessive permissions (56%)
- Lack of visibility into risk related to identities and/or assigned permissions (53%)
- Standing risky privileges for cloud administrators, developers and/or DevOps (49%)

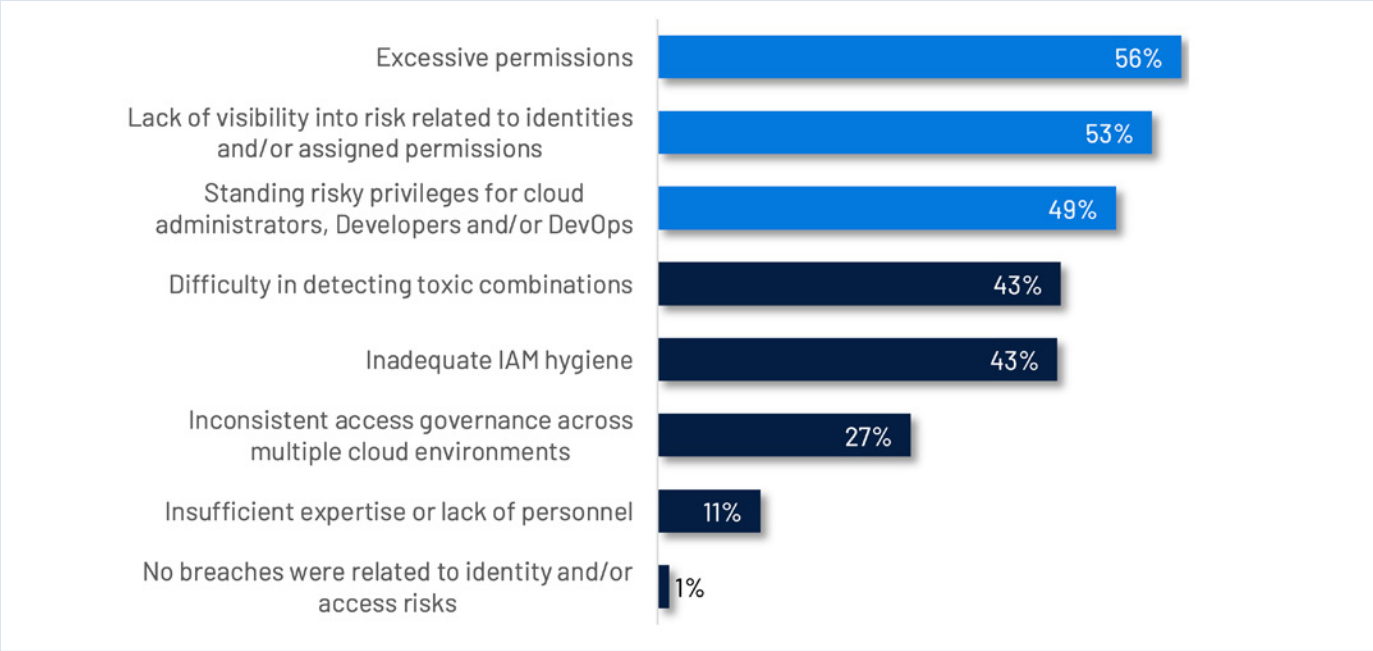


Figure 6: Top Contributing Identity/Access Risks and Factors for Cloud-Related Breaches

* Base: 569. Question allowed more than one answer and as a result, percentages will add up to more than 100%

Top risk factors contributing to cloud-related breaches 2/2

The findings revealed some regional disparities regarding the causes assigned to cloud-related breaches.

In Europe, organizations were significantly more inclined, by a disparity of 13%, to attribute their cloud-related breaches to excessive permissions (61%) than North American organizations (48%). European respondents were also much more inclined, by a disparity of 16%, to pin difficulty in detecting toxic combinations (49%) on their cloud-related breaches than were their North American counterparts (32%).

The third largest geographical disparity regarding cloud-related breach causes was insufficient expertise. 14% more NA organizations cited insufficient expertise as the cause than did EU organizations.

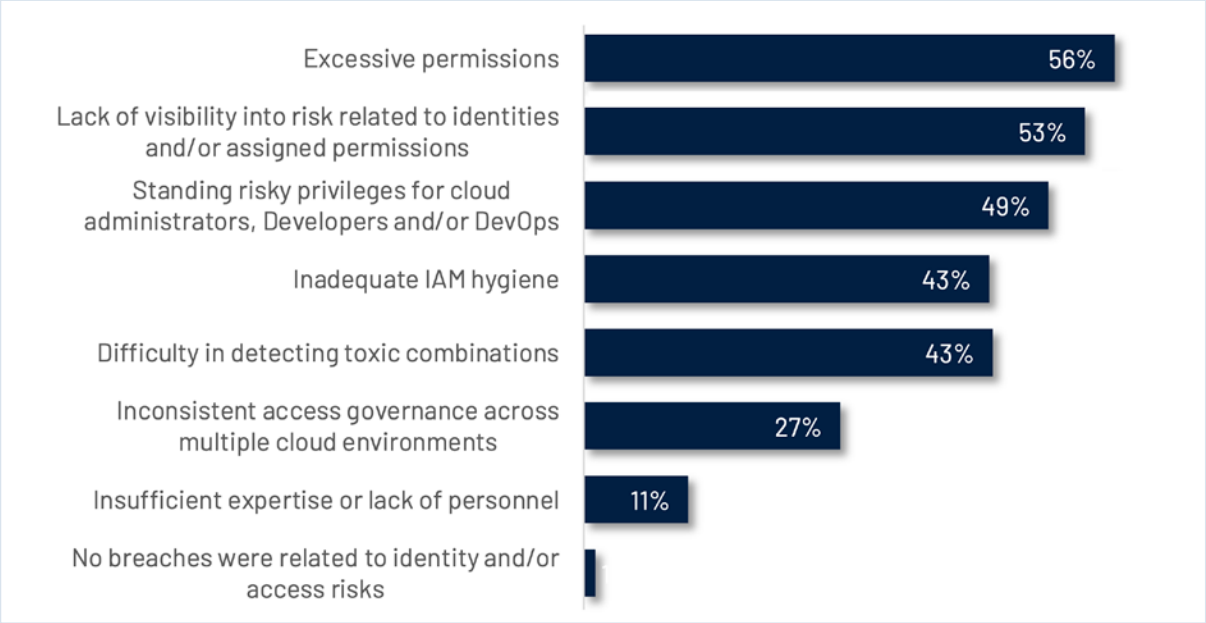


Figure 7: Top Contributing Identity/Access Risks and Factors for Cloud-Related Breaches

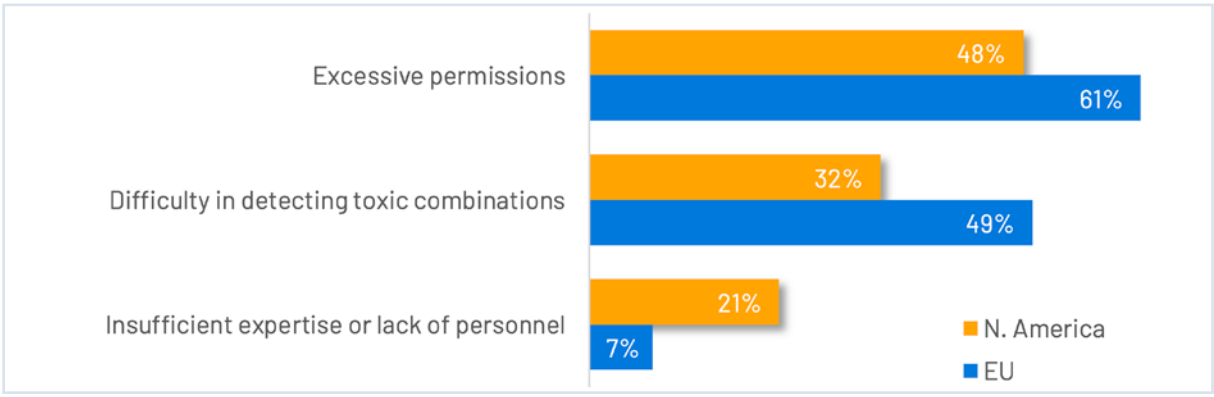


Figure 8: Identity/Access Risks and Factors for Cloud-Related Breaches with Greatest Disparity by Region

* Base: 569. Question allowed more than one answer and as a result, percentages will add up to more than 100%

Top challenges to securing identities and governing permissions in cloud infrastructure

The top challenges to securing identities and governing permissions in cloud infrastructure were:

- Lack of visibility into cloud identities, entitlements and resources (53%)
- Difficulty in managing entitlements in a multi-cloud environment (50%)
- Lack of IAM security prioritization by cloud and security practitioners (49%)

A close fourth challenge to securing identities and the permissions that give them access to resources is the fear of Developer/DevOps' teams that security "will break something" (43%).

These challenges directly correlate with the recognition of insecure identities as a top security risk (Fig. 5), emphasizing the intricate nature of managing identity and entitlements in the cloud — and across multiple clouds. The findings underscore the importance of strategic measures to enhance visibility and have teams focus on IAM security. They also call for building trust and effective communication between security and development teams.

Figure 9: Top Challenges to Securing Identities and Governing Permissions in Cloud Infrastructure

* Base: 569. Question allowed more than one answer and as a result, percentages will add up to more than 100%

Top barriers to implementing new cloud security capabilities

The primary barriers to implementing new cloud security capabilities included a lack of ability to remediate (51%), a lack of support or budget from senior management (50%) and unclear ownership of cloud security responsibilities (44%). Notably, even with knowledge of how to remediate, 27% of respondents expressed hesitancy to act, driven by developer and/or DevOps' fears that security actions may break something. This reported DevOps fear was somewhat higher in North America (36%) than in the EU (23%).

Also of note is the substantial degree of uncertainty around who is responsible for cloud security. This finding highlights the need for organizations to identify and better leverage the responsibility for cloud security that is shared within their organizations. Such initiatives are core to advancing cloud security maturity — and require cloud security tooling designed for high usability, visibility and collaboration between security and development/DevOps teams.

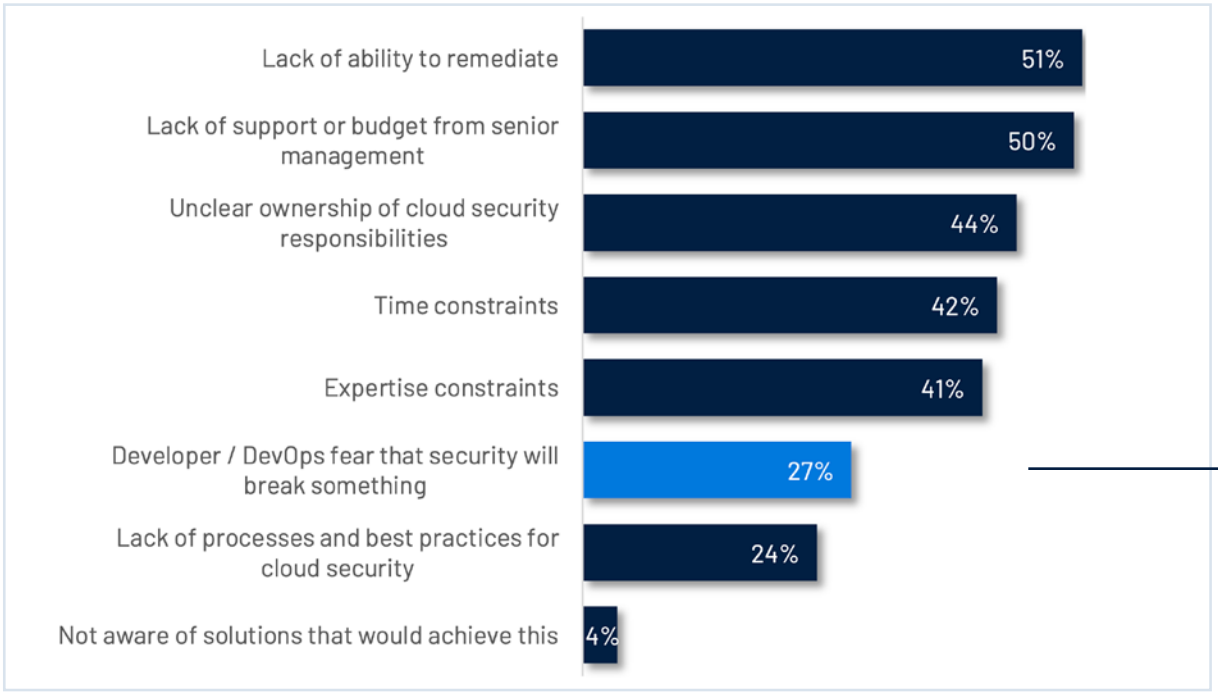


Figure 10: Top Barriers to Implementing New Cloud Security Capabilities – Global

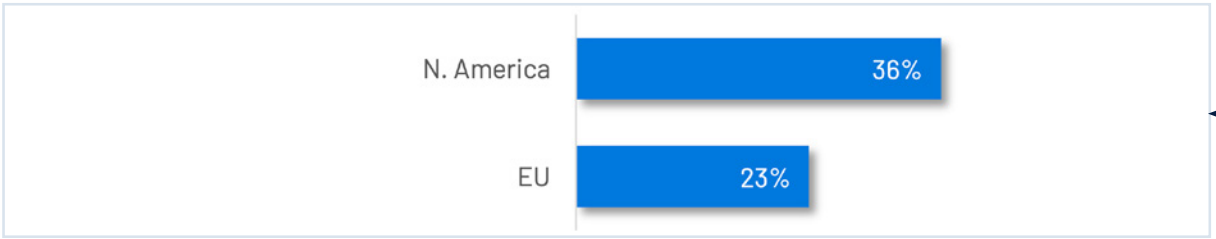


Figure 11: "Developer/DevOps fear that security will break something", by Region

* Base: 600. Question allowed more than one answer and as a result, percentages will add up to more than 100%

Impact of lack of expertise on cloud infrastructure security

Respondents were asked if a lack of expertise in the areas of cloud infrastructure, cloud IAM and/or cloud security affected their organization's efforts to protect their cloud infrastructure.

95% acknowledged being affected by a lack of expertise — and 67% of them said the lack puts them at risk.

This substantial response underscores the seriousness of the expertise shortage in cloud security. It highlights the crucial role of technology in closing the skilled personnel gap, with a pressing need for tooling that not only serves as a force multiplier by helping existing teams be more productive, but also fills the void created by a lack of human expertise.

A critical need exists for solutions that help organizations implement security best practices and align with the demand for comprehensive platforms for effectively navigating the intricate landscape of cloud security.

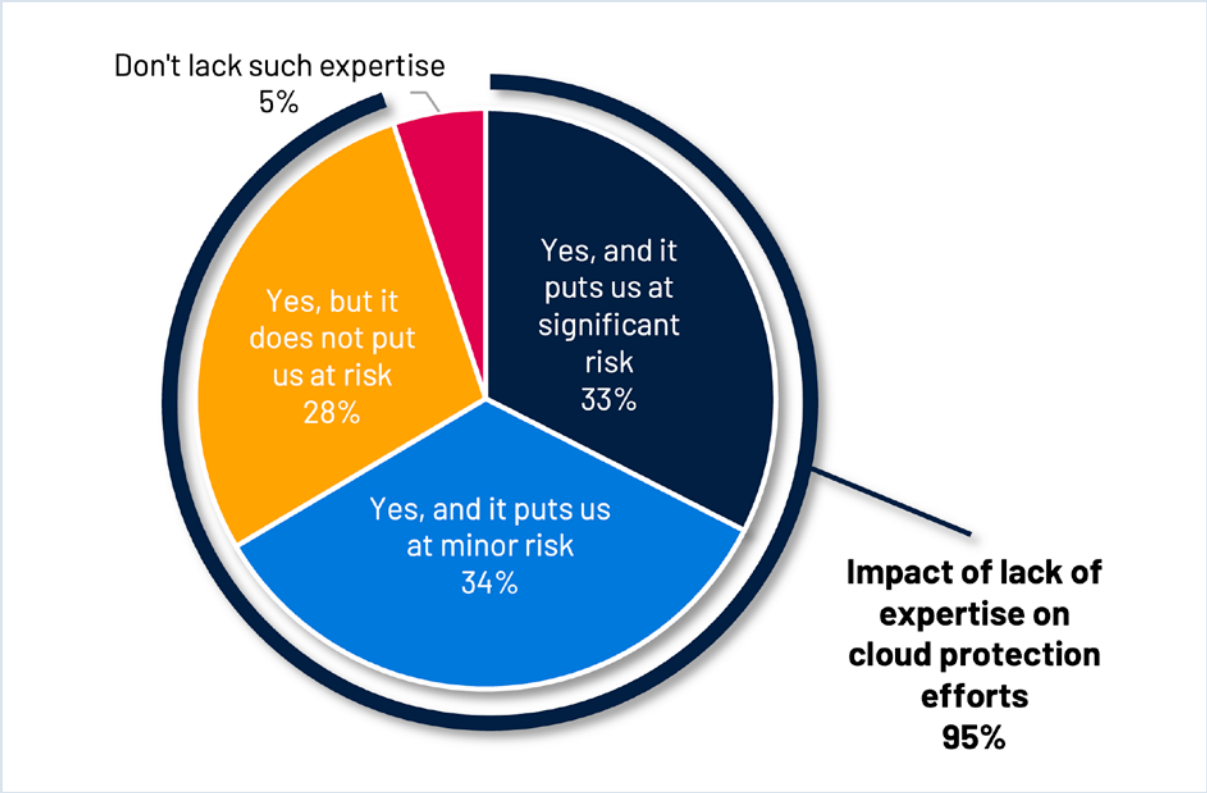


Figure 12: Impact of Lack of Expertise on Cloud Infrastructure Protection Efforts

* Base: 600

Top cloud infrastructure security priorities for the next 12 months

The primary security priorities for cloud infrastructure in the 12 months ahead included implementing zero trust and least privilege for identities (38%), detecting and remediating cloud misconfigurations (38%), and implementing temporary elevated access (often called Just-In-Time access) for DevOps and related roles (33%).

Most striking is the near-same level of importance assigned to most of the areas of cloud infrastructure security.

Put simply: Everything is a priority.

The findings reveal the intricate challenges faced by cloud security professionals who need to address a wide variety of concerns, post-haste. This emphasizes the importance of adopting a comprehensive strategy that incorporates tools that address a range of security areas to ensure a robust security posture based on effective and dynamic prioritization of the most important risks.

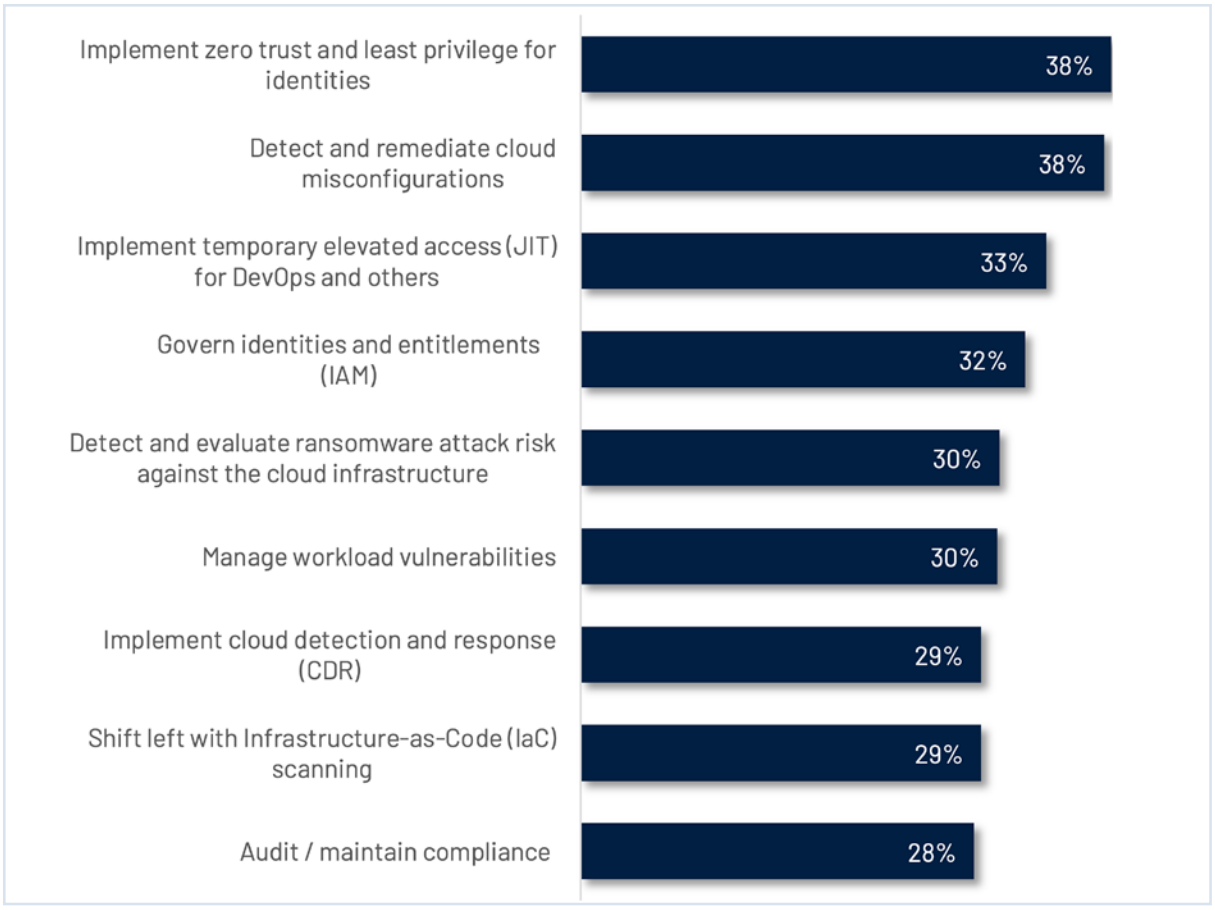


Figure 13: Top Cloud Infrastructure Security Priorities for the Next 12 Months

* Base: 600. Question allowed more than one answer and as a result, percentages will add up to more than 100%

KPIs used for cloud security technology investments

The top key performance indicators (KPIs) that organizations are using to show return on their cloud security technology investments are time to investigate/neutralize a possible threat (56%), time to remediate a finding (56%) and time to detect risk (46%).

These KPIs reveal a micro-level, day-to-day approach to assessing the success of security efforts and practices. The fact that a remediation-related KPI tops the list points to the importance of remediation processes in a cloud security strategy and tooling. KPIs also help convey to executive leadership the concrete value of cloud security investments in closing the expertise gap highlighted in the findings.

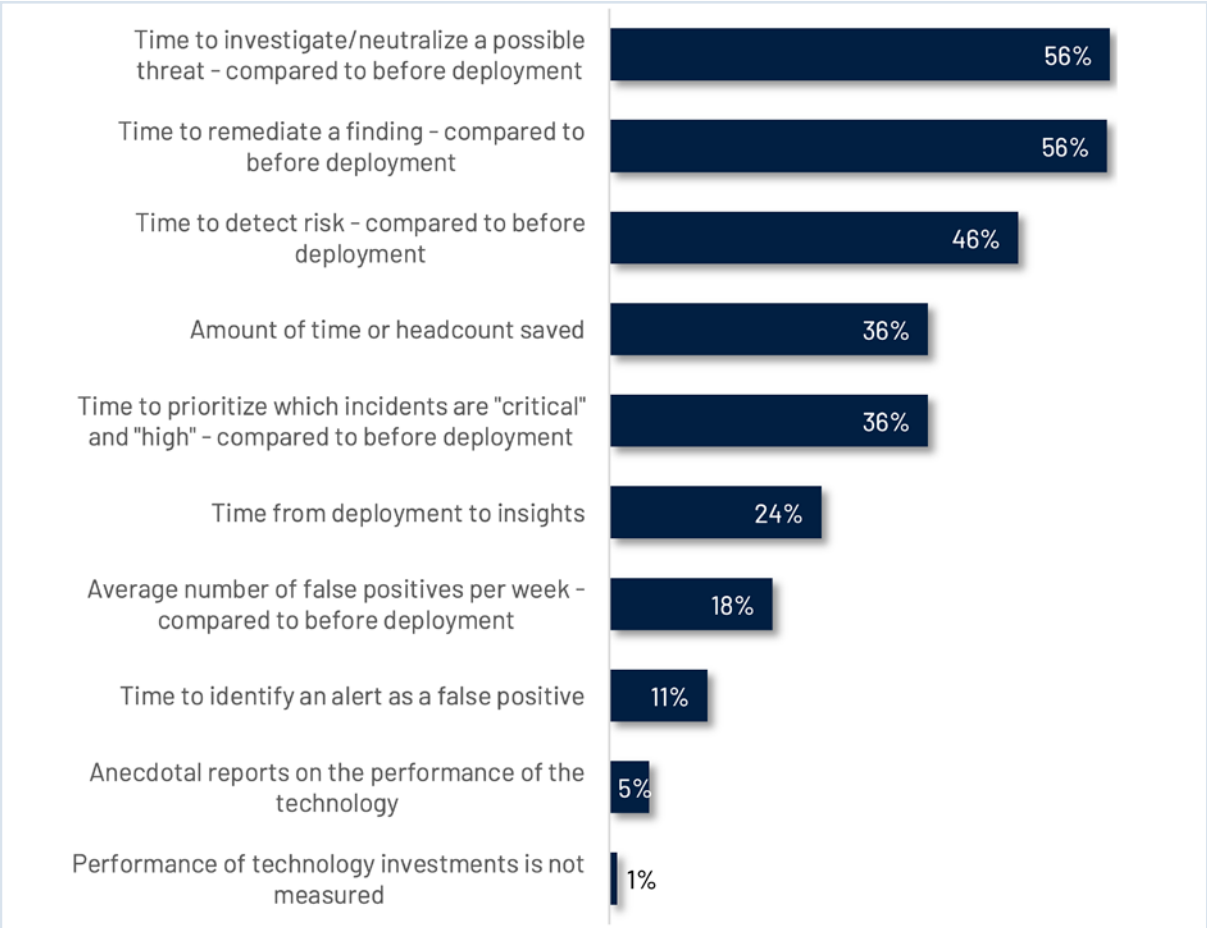


Figure 14: KPIs Used for Cloud Security Technology Investments

* Base: 600. Question allowed more than one answer and as a result, percentages will add up to more than 100%

KPIs used for IAM security technology investments

The top key performance indicators (KPIs) that organizations are using to show the return on their IAM security technology investments were:

- Time to investigate/neutralize a possible threat — compared to before deployment (60%)
- Time to prioritize which identity risks are “critical” and “high” — compared to before deployment (56%)
- Improved ability to convey KPIs to different audiences — high level outcomes to executives, specific data/trends to tech (55%)

Notably, 3% of respondents reported not measuring the performance of their technology investments at all.

These KPIs reveal a continuous approach to assessing the success of IAM risk reduction efforts. The fact that threat investigation and risk prioritization KPIs top the list points to the importance of IAM risk insights and prioritization in a cloud security strategy. Organizations are also seeking to improve their reporting capabilities around IAM security.

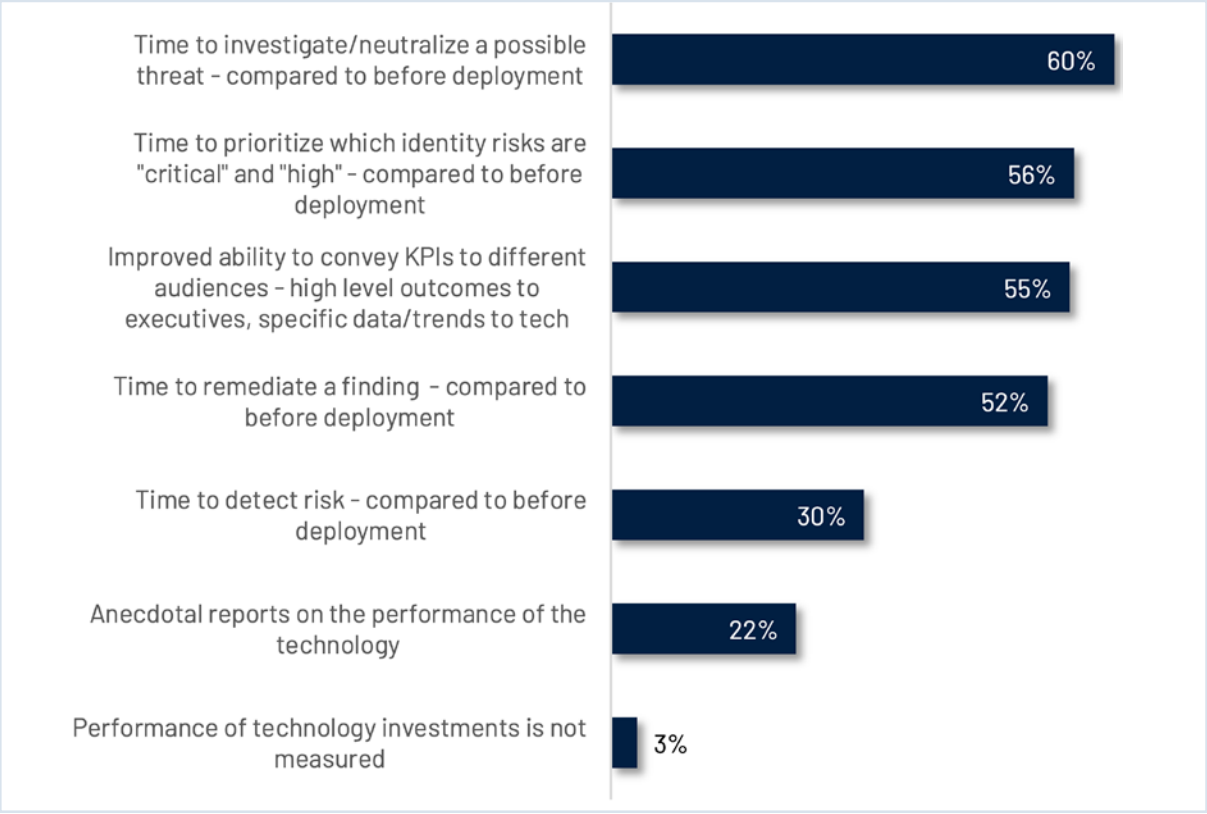


Figure 15: KPIs Used for IAM Security Technology Investments

* Base: 600. Question allowed more than one answer and as a result, percentages will add up to more than 100%

Demographics

Industry, country, annual revenue, department and job seniority

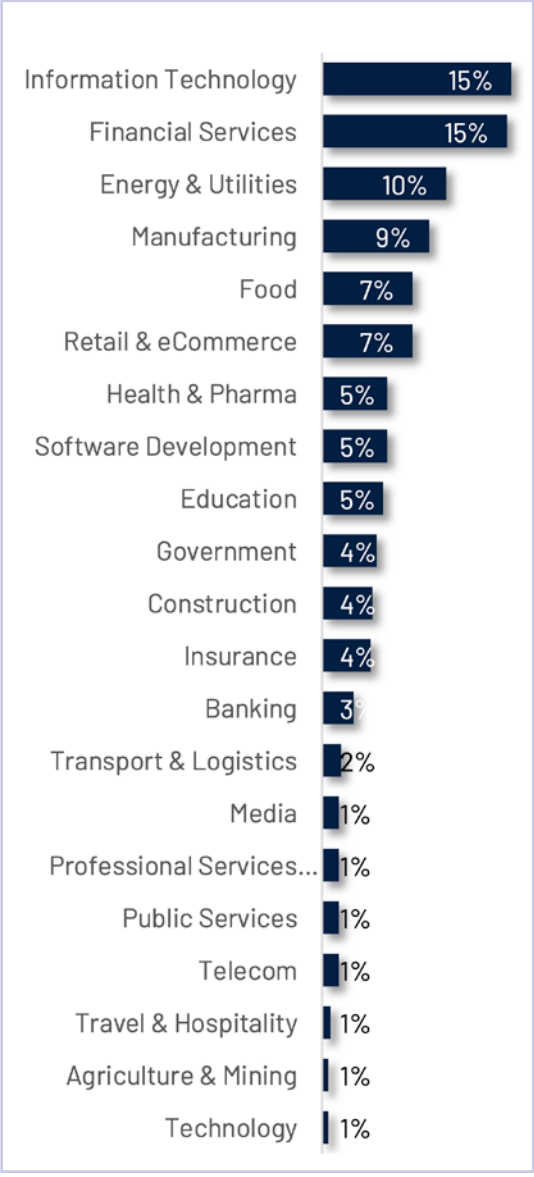


Figure 16: Industry

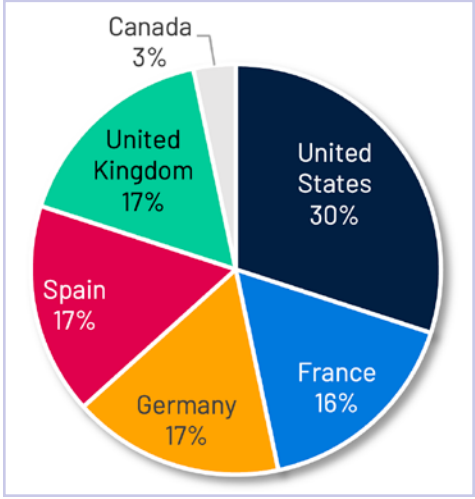


Figure 17: Country

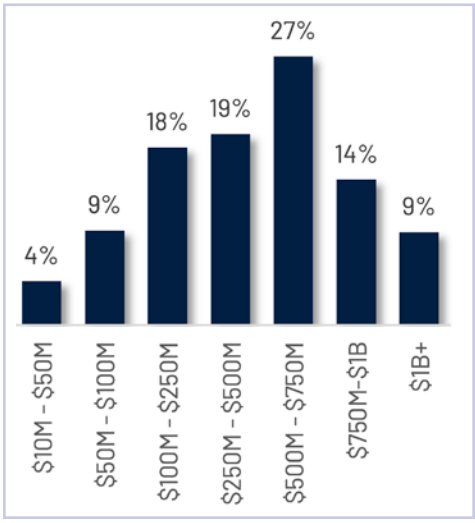


Figure 18: Annual Revenue

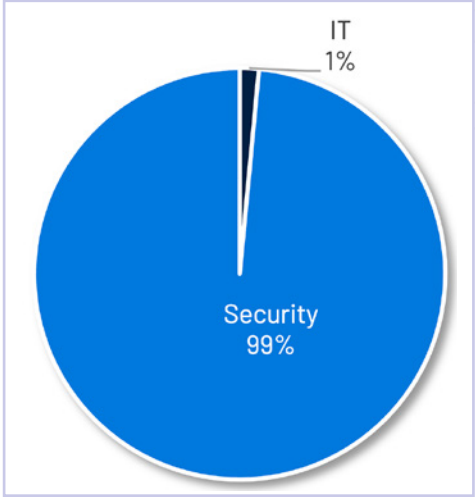


Figure 19: Department

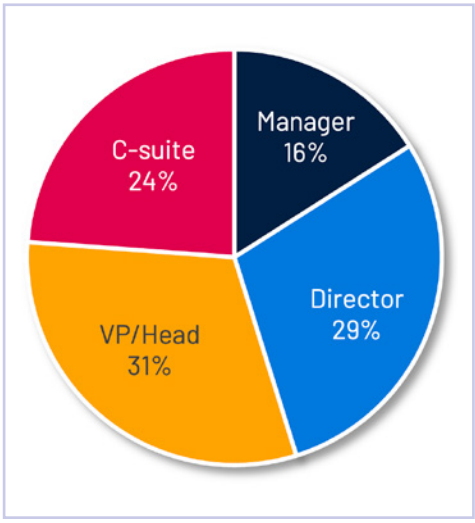


Figure 20: Job Seniority

Job responsibilities and roles involving cloud entitlements security

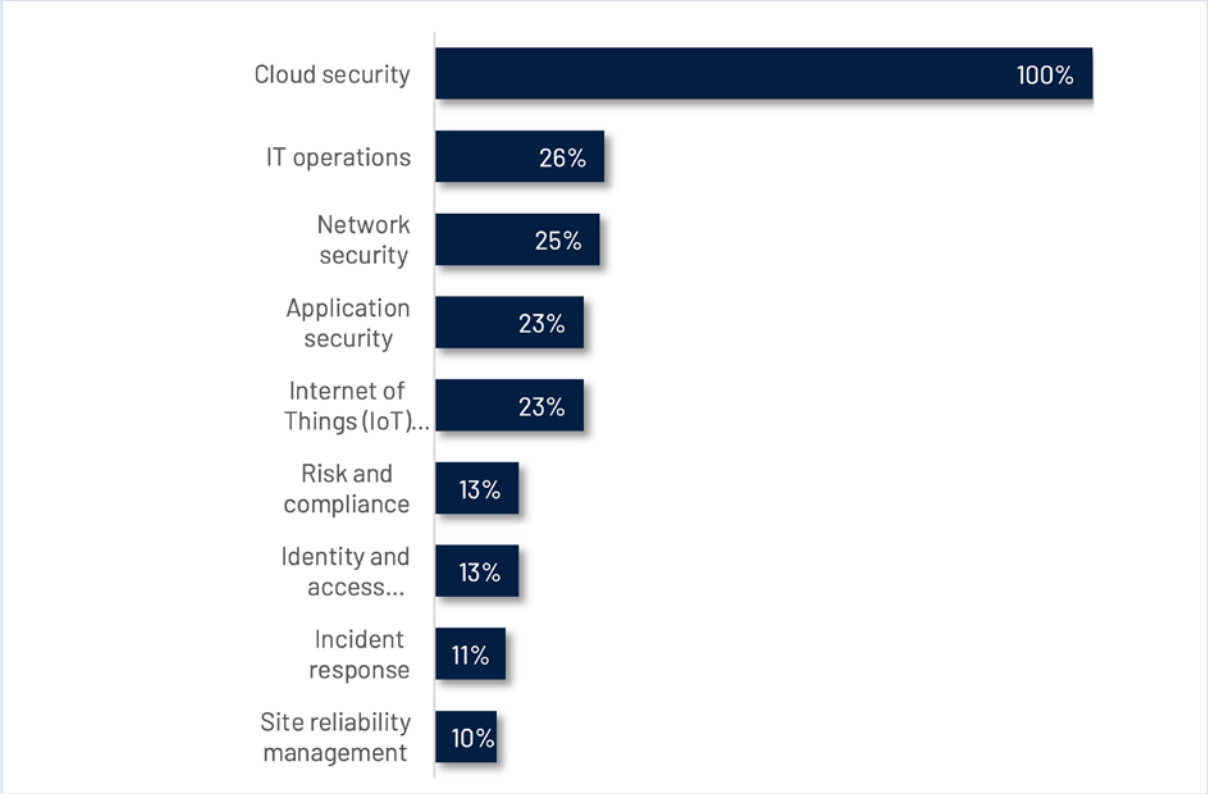
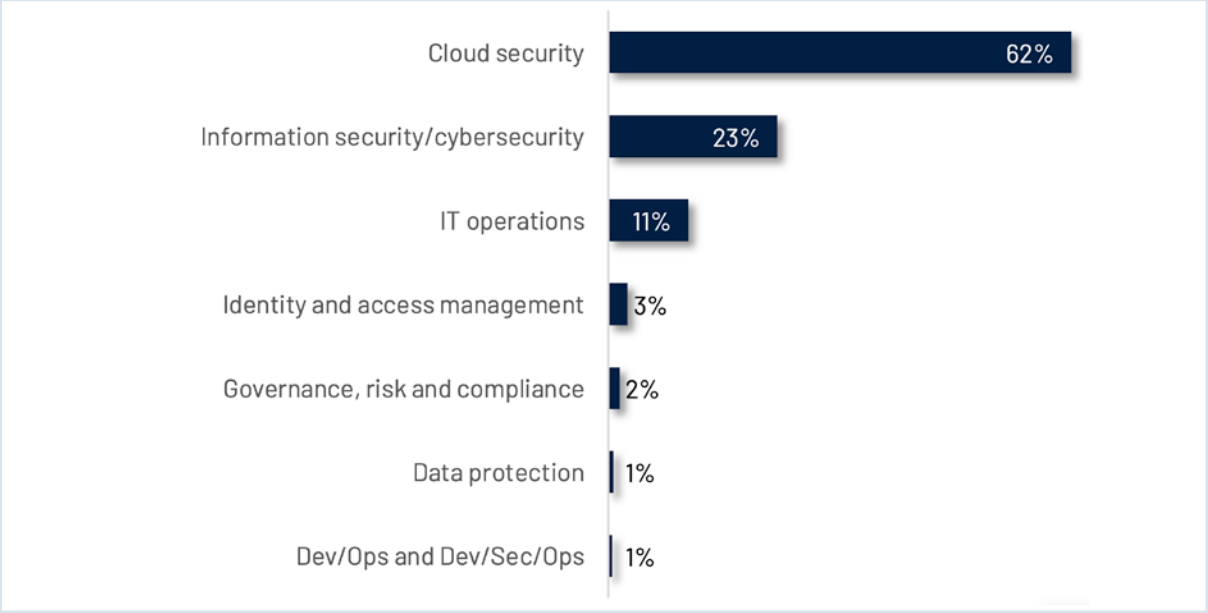


Figure 21: Job Responsibilities



22: Roles Involving Cloud Entitlements Security

* Base: 600. Question allowed more than one answer and as a result, percentages will add up to more than 100%

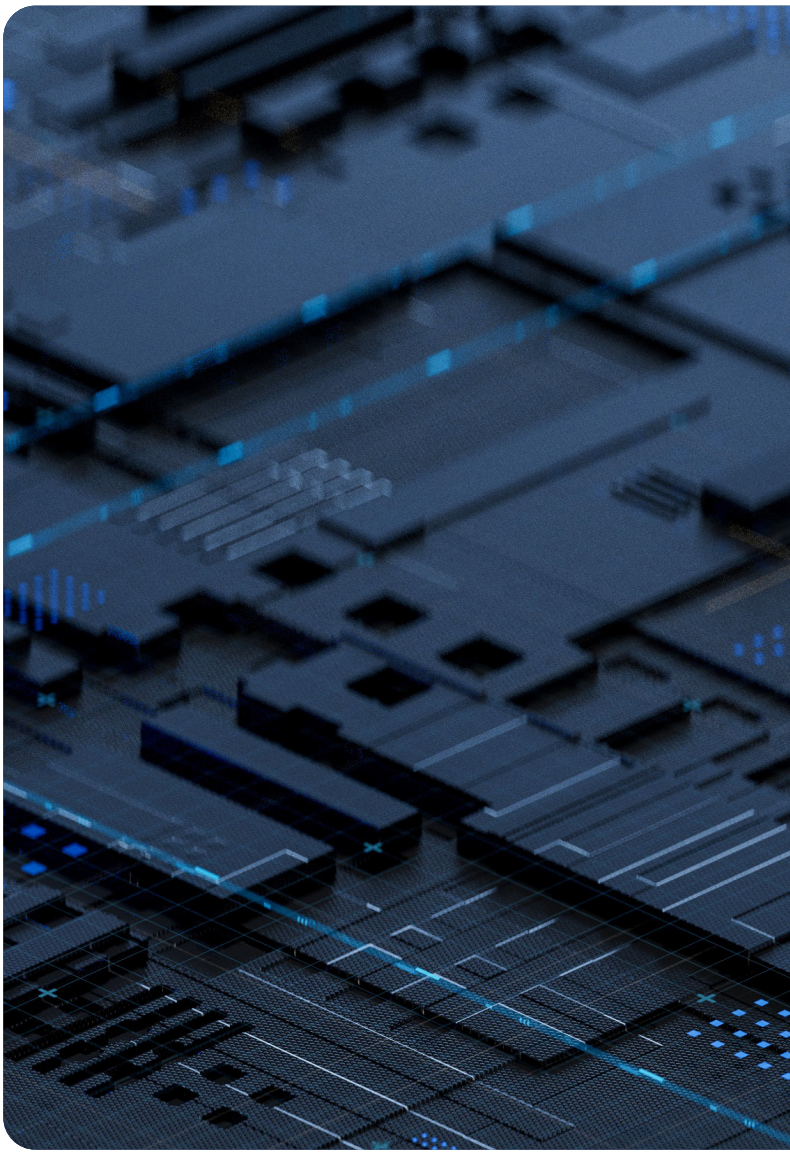
Methodology

In collaboration with Global Surveyz, an independent survey company, Tenable surveyed 600 full-time employees — 200 from North America (United States, Canada) and 400 from Europe (France, Germany, Spain, United Kingdom) — focusing on those responsible for cloud security.

Half the participants came from organizations with annual revenue of $10 million - $500 million, and half with over $500 million. The respondent base included a mix of senior roles, including managers, directors, VPs and SVPs.

The survey provides a snapshot of current challenges and priorities in cloud security for large enterprises.

Not all totals will equal 100% due to rounding or the allowing of multiple answers.



About Tenable Cloud Security

Tenable Cloud Security is the actionable cloud security platform (CNAPP), rapidly exposing and closing priority security gaps caused by misconfigurations, risky entitlements, and vulnerabilities. These weaknesses are the epicenter of cloud risk. Tenable is a world leader at isolating and eradicating these exposures at scale across infrastructure, workloads, identities, data and AI services.

To learn more, visit tenable.com/cloud-security

About Tenable

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 www.tenable.com.

Contact Us

Please email us at sales@tenable.com or visit tenable.com/contact.

112624