Cybersecurity
INSIDERS

THE STATE OF CLOUD SECURITY

Key Findings From the MixMode Survey

MixMode®

INTRODUCTION

The rapid adoption of cloud computing opens up new opportunities while simultaneously intensifying security challenges for organizations. Faced with a quickly changing threat landscape, many security teams are scrambling to protect and defend complex, multi-cloud environments — a task made even more challenging by a severe cybersecurity skills shortage.

This cloud security survey of 588 security professionals reveals major gaps in organizations' abilities to secure cloud platforms and workloads. Despite multi-cloud adoption reaching mainstream levels, key capabilities for cloud security such as real-time threat detection and response, comprehensive visibility, workload protection, and data security remain limited. This report identifies these top challenges, assesses the effectiveness of current tools and controls, and outlines what's needed for enterprises to achieve robust cloud security postures.

The research further reveals that organizations continue to rely on legacy security solutions like SIEM for cloud security, leaving them:

- Uncertain about their ability to secure cloud environments effectively
- Vulnerable to data breaches that could expose sensitive information
- Relying on staff with limited cloud security expertise
- Unprepared to monitor the high volume of activity in modern cloud environments

Key findings include:

- **Cloud Security Concerns:** An alarming 75% of respondents are extremely or very concerned about cloud security.
- **Lack of Real-Time Detection:** A majority of respondents are not utilizing real-time threat detection capabilities across their cloud infrastructure.
- **Complexity of Multi-Cloud Environments:** Multi-cloud (38%) and hybrid (40%) strategies add complexity, demanding innovative security management.
- **Reliance on Traditional Solutions:** Traditional solutions are still being used, despite preferences for native cloud security controls, exposing organizations to inefficiencies and threats.
- **Need for Unified Solutions:** The use of multiple security point solutions underscores a need for unified, AI-driven approaches for robust security across platforms.

We would like to express our sincere gratitude to MixMode for their invaluable contribution to this research project. We hope this report is a valuable guide for our cybersecurity community readers, assisting you in navigating the complexities of cloud security through innovative and effective strategies.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

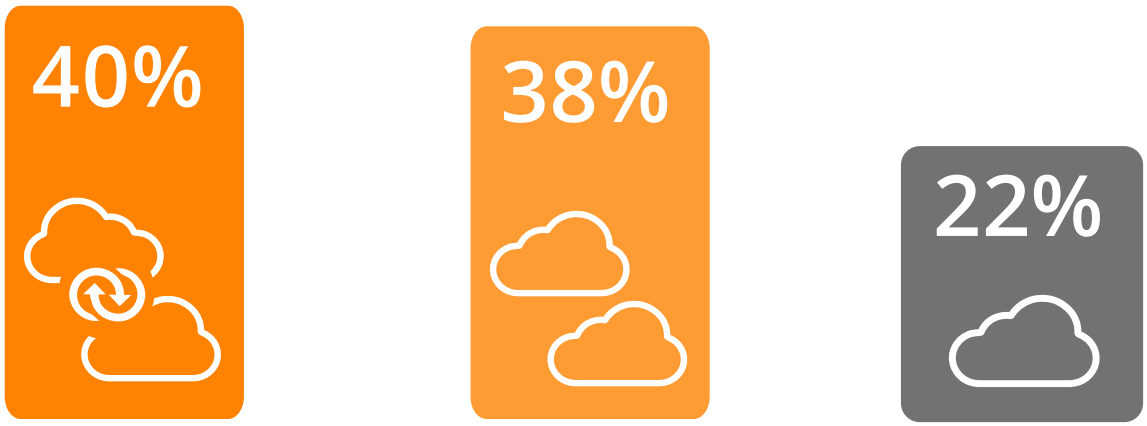
CLOUD DEPLOYMENT STRATEGIES

Most organizations are embracing multi-cloud (38%) or hybrid (40%) strategies to serve diverse business needs. A multi-cloud strategy allows businesses to utilize services from various cloud providers, optimizing costs and features, while a hybrid strategy combines private and public cloud services for increased flexibility and security. However, these approaches also add layers of complexity and management, and open organizations up to broader attack vectors, making cloud security more challenging.

The growing emphasis on agility in cloud management has led organizations to align cloud resources more closely with business goals. However, the resulting complexity necessitates a more robust and sophisticated approach to ensuring security across platforms.

What is your primary cloud deployment strategy?

78% of organizations are using a multi-cloud or hybrid environment



HYBRID
(e.g., integration between private and public clouds)

MULTI-CLOUD
(e.g., multiple providers without integration)

SINGLE CLOUD

CLOUD SECURITY CONCERNS

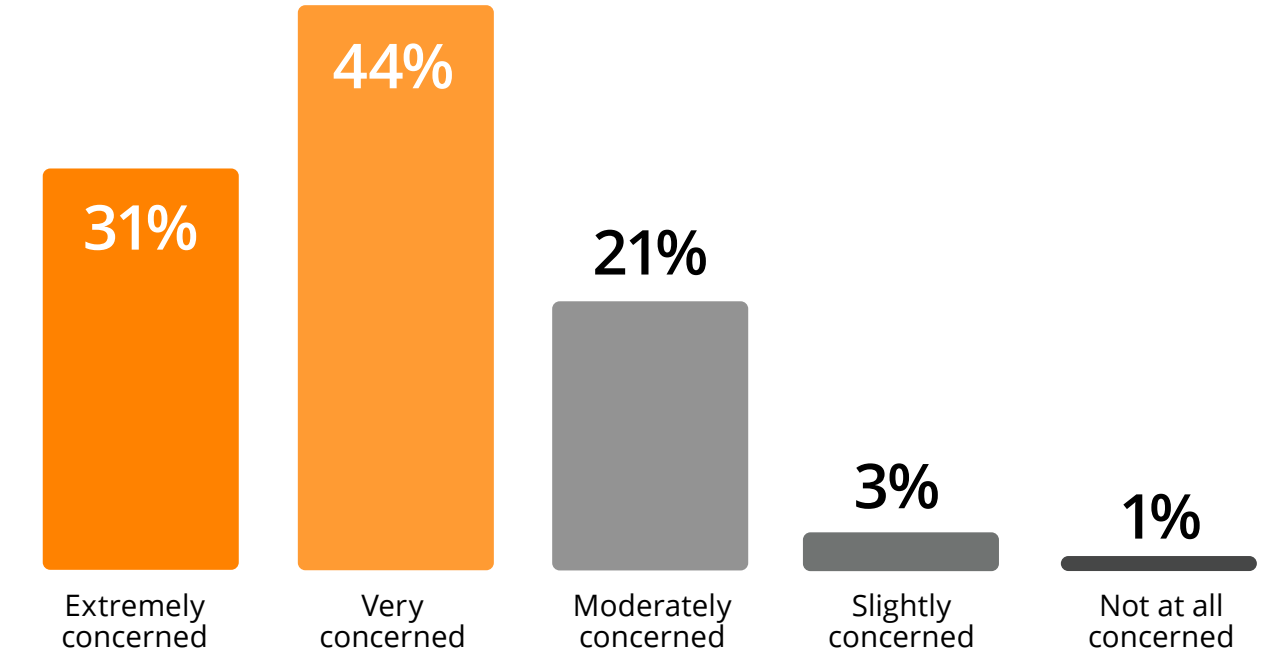
The evolution of cloud security has been turbulent, often manifesting in bursts of revolutionary changes, and continues to be a major concern for cybersecurity professionals. Despite cloud environments maturing significantly over the last decade, 75% of survey respondents are either extremely or very concerned about cloud security.

This highlights the urgent need for a shift in the way we are securing cloud infrastructure. We will explore the specific cloud security concerns and recommended approaches to addressing them in the following pages.

How concerned are you about the security of public clouds?

75%

of organizations are very or extremely concerned about cloud security

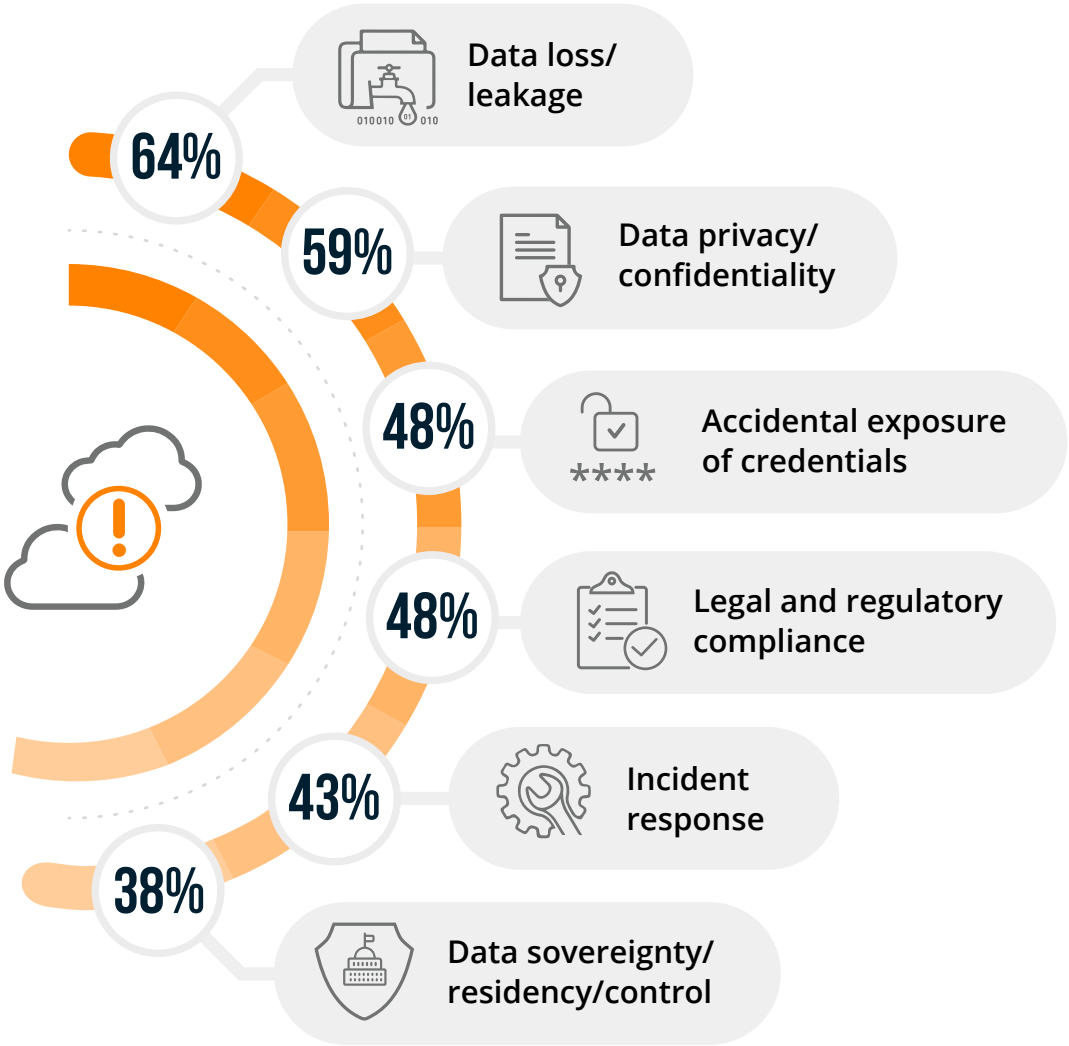


TOP CLOUD SECURITY CONCERNS

Despite the growing maturity level of cloud operations, an alarming majority of security professionals remain concerned about the security of cloud environments. The most pressing concerns include data loss and leakage (64%), data privacy (59%), and the accidental exposure of credentials (48%).

This underscores the urgent need for advanced cloud security solutions that can keep pace with increasingly complex and multifaceted cloud environments, and adapt to rapidly evolving threat landscapes.

What are your biggest cloud security concerns?



Visibility and transparency 35% | Availability of services, systems, and data 34% | Business continuity 33% | Disaster recovery 29% | Lack of forensic data 27% | Fraud (e.g., theft of SSN records) 26% | Liability 24% | Performance 23% | Having to adopt new security tools 18% | Not sure/other 5%

LACK OF CONFIDENCE IN CLOUD SECURITY ABILITIES

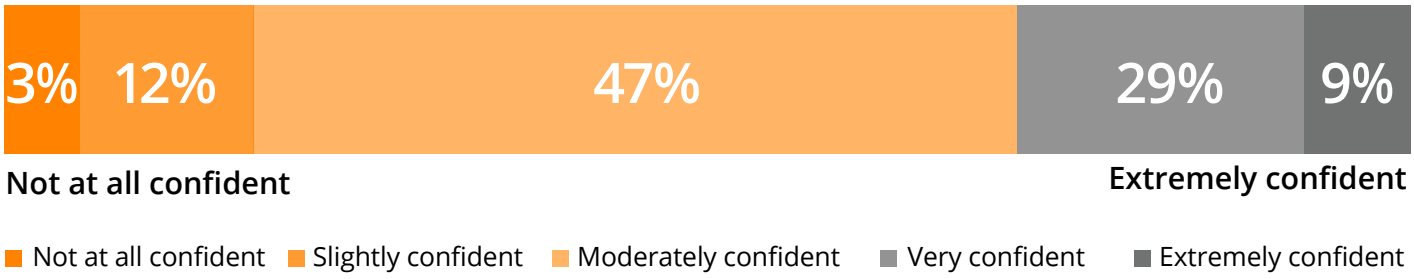
With multi-cloud complexity on the rise, it is not surprising that 62% of cybersecurity professionals are, at best, only moderately confident in their organization's ability to secure their cloud environment.

The survey results highlight the importance of a more innovative approach to cloud security. Utilizing intelligent systems that can continuously adapt to an organization's unique infrastructure, without the need for manual input, is a vital strategy to navigate complex multi-cloud strategies and deliver robust security in the face of evolving threats.

How confident are you in your organization's cloud security posture?

62%

of respondents are not very confident in their organization's ability to protect their cloud environment



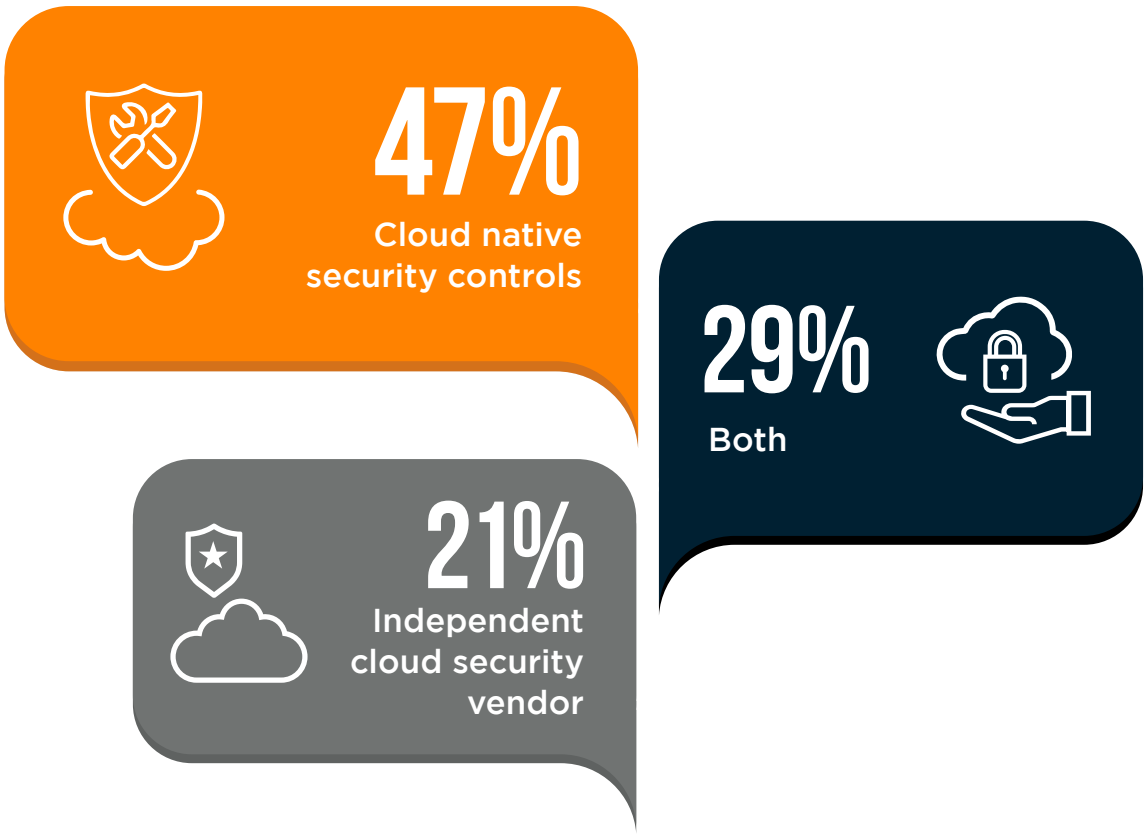
CLOUD NATIVE SECURITY PREFERENCE

Forty-seven percent of survey respondents favor native cloud security controls, compared to 21% who prefer solutions from independent security vendors. A third of respondents (29%) prefer a blend of both.

The choice between native cloud security controls and third-party tools is a strategic decision that hinges on several key factors. Native controls offer seamless integration within specific cloud environments but may lack the flexibility and comprehensive protection needed across diverse or multi-cloud settings. Third-party tools can provide more advanced, customizable security features capable of responding to evolving threats but may require careful selection for compatibility and cost-effectiveness.

Ultimately, this choice reflects an organization's unique needs, risk profile, and goals, and demands a balanced approach that recognizes both the complexity of modern cloud infrastructure and the evolving landscape of cybersecurity threats.

Do you prefer cloud native security controls or using an independent security vendor for your cloud security needs?

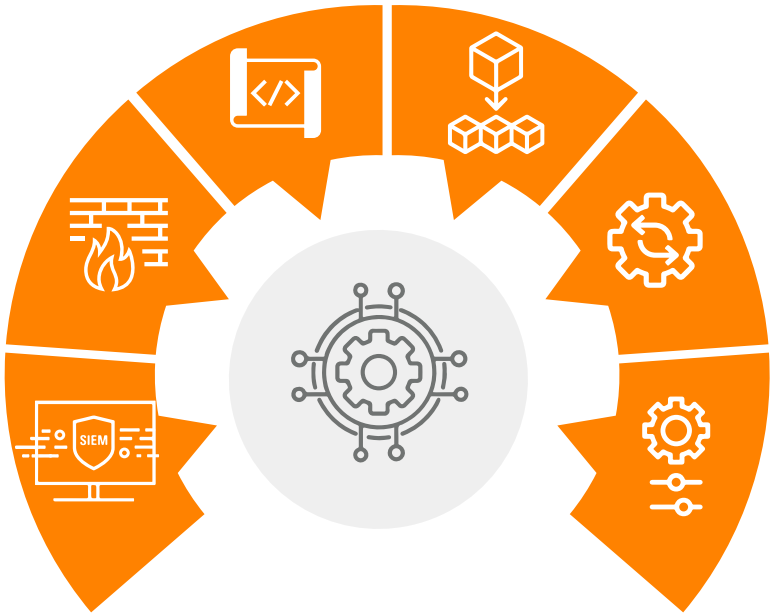


Other 3%

RELIANCE ON TRADITIONAL SECURITY TOOLS

While most organizations prefer cloud-native security controls, 70% still rely on legacy solutions like SIEM, which struggle to scale in complex cloud environments. This reliance on outdated methods risks exposing organizations to threats and inefficiencies, especially in multi-cloud settings.

Which of the following automation and orchestration tools are you leveraging to aid in security controls implementation or processes?



39% Infrastructure-as-a-code (and security-as-a-code) in templates

37% Microservices (serverless and containers)

66% Web application firewalls

35% Security orchestration, automation, and response (SOAR) tools

70% Security Information Event Management (SIEM)

33% Configuration orchestration tools

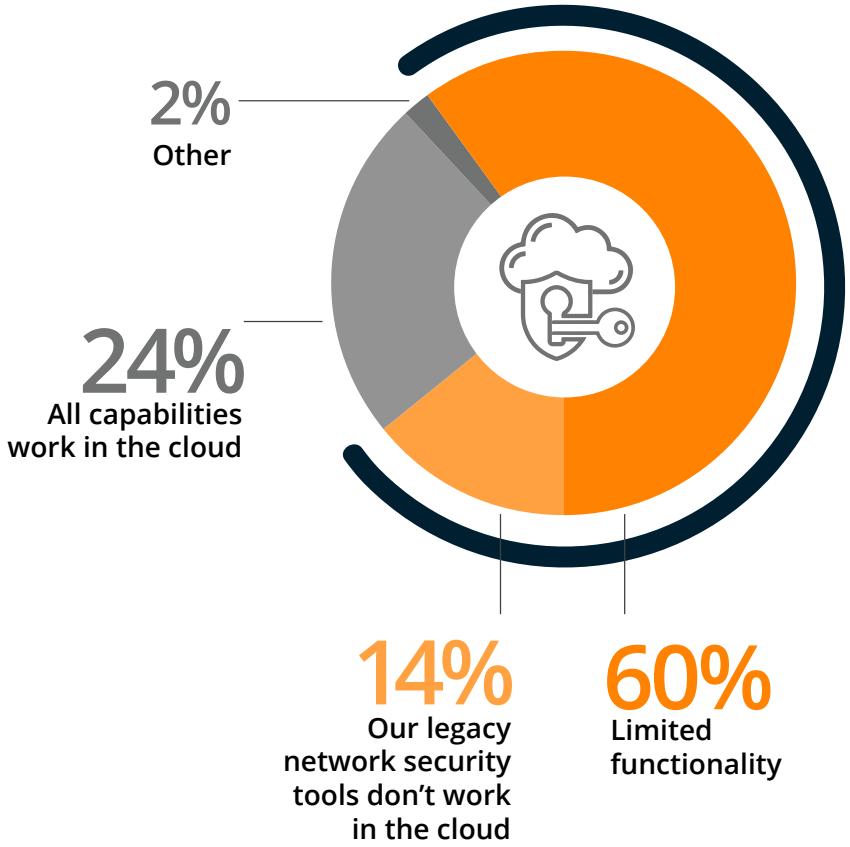
Microsegmentation 31% | Plugins for Continuous Integration (CI) / Continuous Delivery (CD) tools (e.g. Jenkins or TeamCity) 30% | cloud infrastructure entitlement management (CIEM) 12% | Other 2%

LEGACY TOOLS FALL SHORT IN CLOUD ENVIRONMENTS

Cloud computing is complex and highly dynamic, posing distinct security challenges that most legacy tools struggle to meet. A significant 74% of organizations acknowledge that their legacy security solutions are either entirely ineffective or offer only limited functionality in their cloud environments.

Dependence on these legacy tools, unable to scale with the complexity of the cloud, leaves organizations grappling with significant shortcomings as they seek to protect their cloud environment.

Which statement best describes how your legacy network security tools/ appliances work in cloud environments?



74%

confirm that their legacy security solutions either don't work at all or have limited functionality in cloud environments

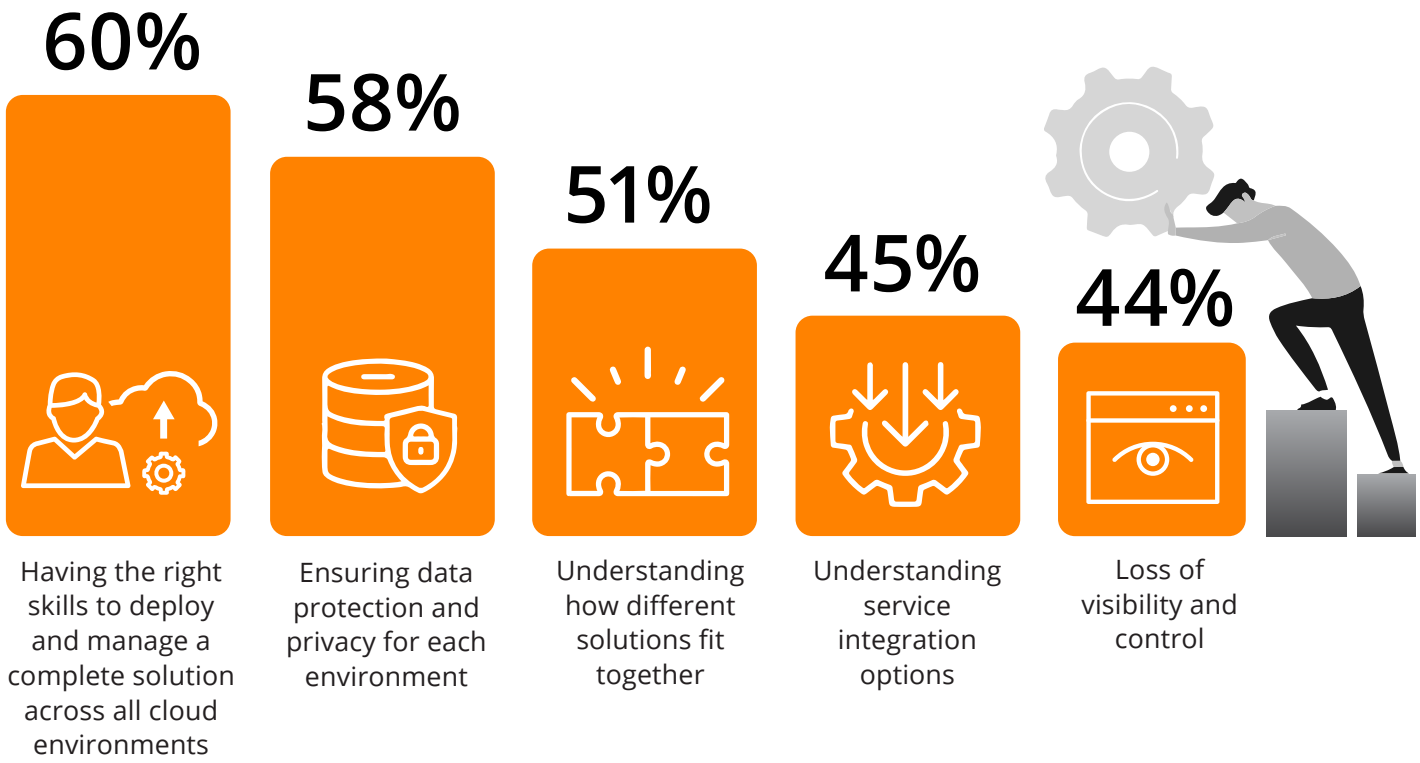
MULTI-CLOUD SECURITY CHALLENGES

The difficulties of safeguarding cloud workloads expand drastically with the addition of a multi-cloud environment. This is clearly shown by the four primary issues that organizations struggle with — all of which relate to having the right personnel and in-depth understanding of the separate cloud platforms.

Specifically, the survey findings show that 60% of respondents struggle with having the right skills to deploy and manage a complete solution across all cloud environments, while 58% face challenges in ensuring data protection and privacy for each environment.

Navigating these challenges requires an innovative approach leveraging generative AI, offering real-time threat detection that adapts to the organization's unique multi-cloud infrastructure without needing pre-set rules or constant human intervention. Such a system can help organizations overcome skill barriers, ensuring robust and efficient security in complex multi-cloud environments.

What are your biggest challenges securing multi-cloud environments?



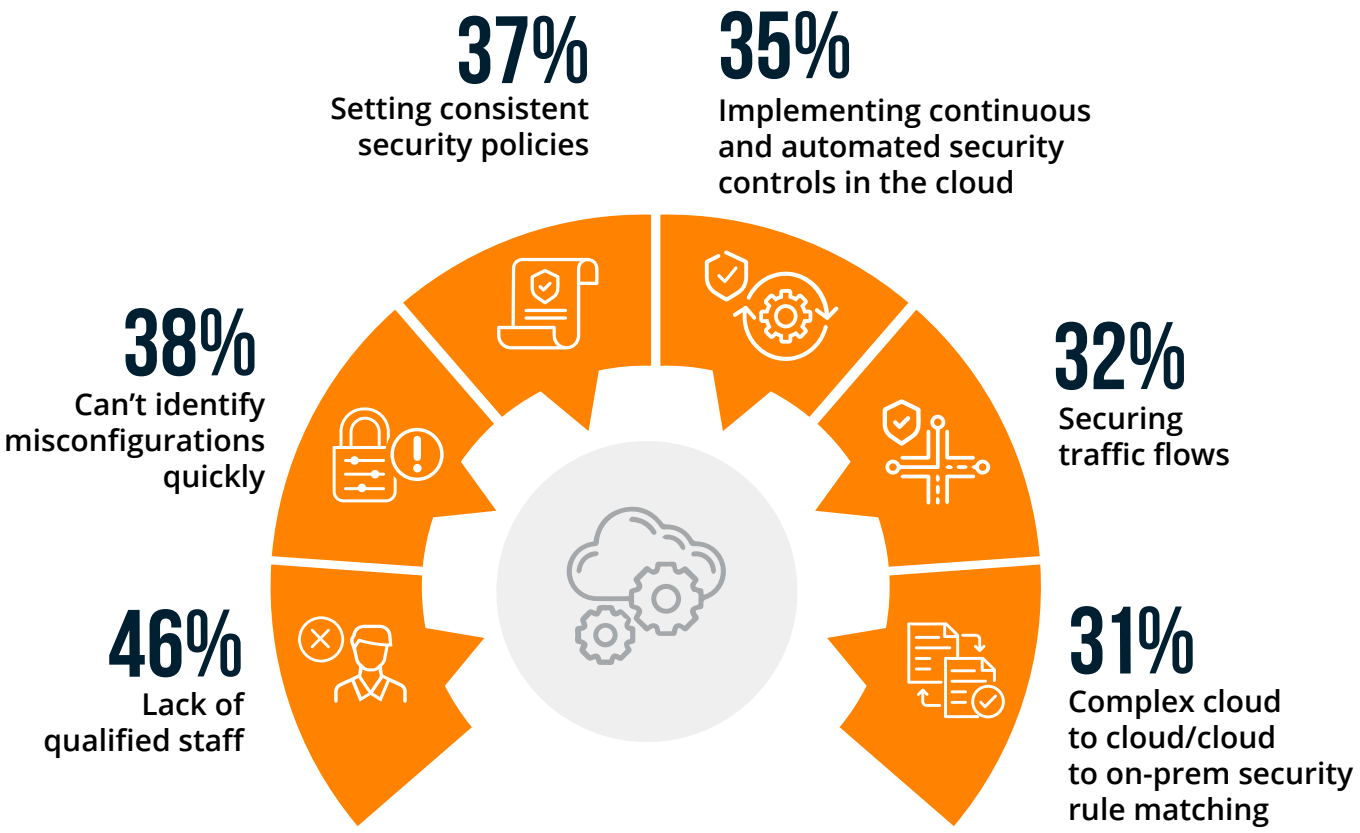
Providing seamless access to users based on their credentials 40% | Selecting the right set of services 39% | Managing the costs of different solutions 39% | Keeping up with the rate of change 39% | Other 2%

CLOUD SECURITY HEADACHES

IT professionals face substantial operational challenges when it comes to safeguarding cloud workloads. The primary concern remains the shortage of qualified cybersecurity staff, with 46% of organizations grappling with the talent and skills gap in managing cloud security. With the scarcity of cybersecurity professionals in the job market failing to meet the high demand, organizations find that automating security controls and tasks is their most viable route to establishing a more robust security posture.

By implementing security solutions that can learn and adapt to an organization's unique infrastructure without the need for constant human oversight, organizations can create an adaptive baseline that minimizes false positives. Such an AI-driven approach aligns well with the dynamic nature of cloud environments and helps organizations overcome the challenges of policy setting, compliance, and human error. It provides a robust yet flexible path to ensure continuous compliance and security in the face of a rapidly changing threat landscape, reducing the pressure on already scarce cybersecurity personnel.

What are your biggest operational, day-to-day headaches trying to protect cloud workloads?



Security can't keep up with the pace of changes to new / existing applications 30% | Justifying more security spending 30% | No automatic discovery / visibility / control to infrastructure security 29% | Lack of integration with on-prem security technologies 28% | No flexibility 27% | None 27%

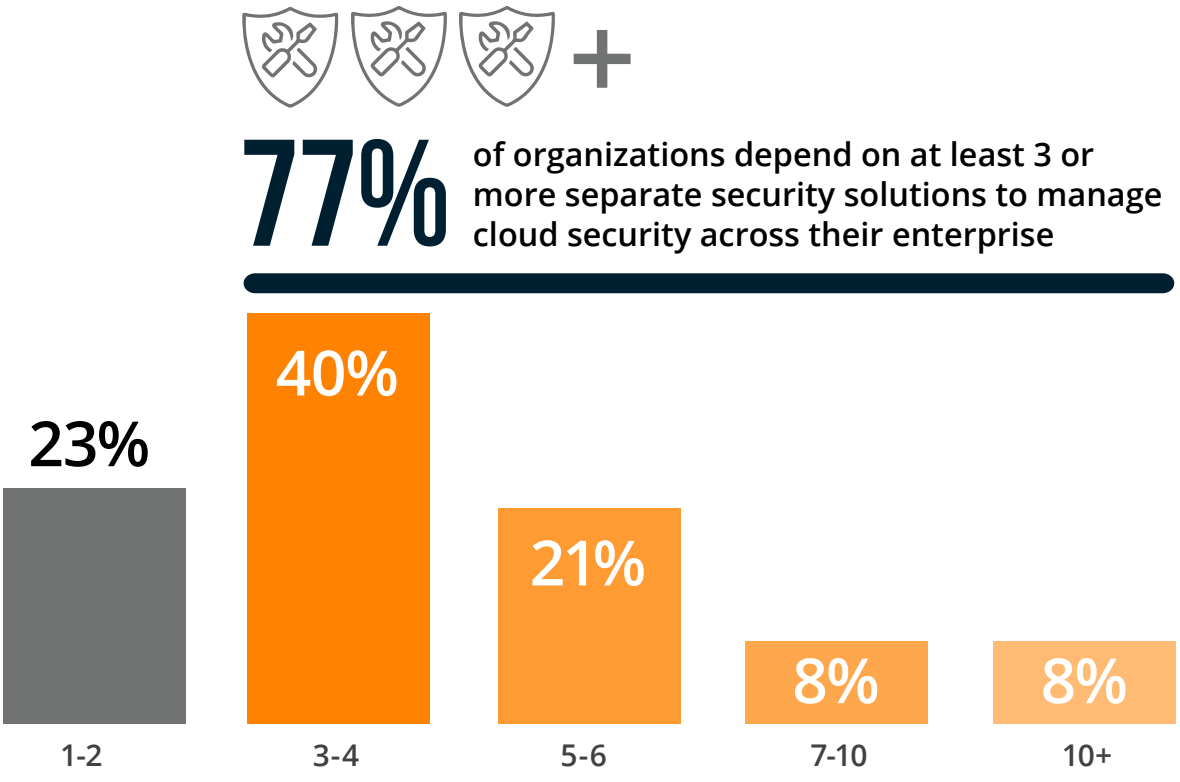
SECURITY SOLUTION OVERLOAD

The number of separate security solutions needed to configure policies across an organization's cloud footprint is a significant factor affecting both security effectiveness and operational efficiency.

Most respondents in our survey (77%) depend on at least 3 separate security solutions to manage cloud security across their enterprise; 37% even use 5 solutions or more. This plethora of security solutions introduces heightened complexity, presenting cyber adversaries with exploitable gaps to target.

Facing the challenge of managing multiple security solutions, organizations could benefit from a unified approach that leverages generative AI for real-time threat detection. By creating a continuously evolving baseline that adapts to an organization's unique needs, this strategy minimizes fragmentation and cost. The ability to predict known and zero-day attacks, combined with a reduction in false positives, offers a streamlined and efficient solution for robust security in a complex, multi-cloud environment.

How many separate security solutions do your users have to access to configure the policies that secure your enterprise's entire cloud footprint?



THE ROLE OF CLOUD ARCHITECTURE

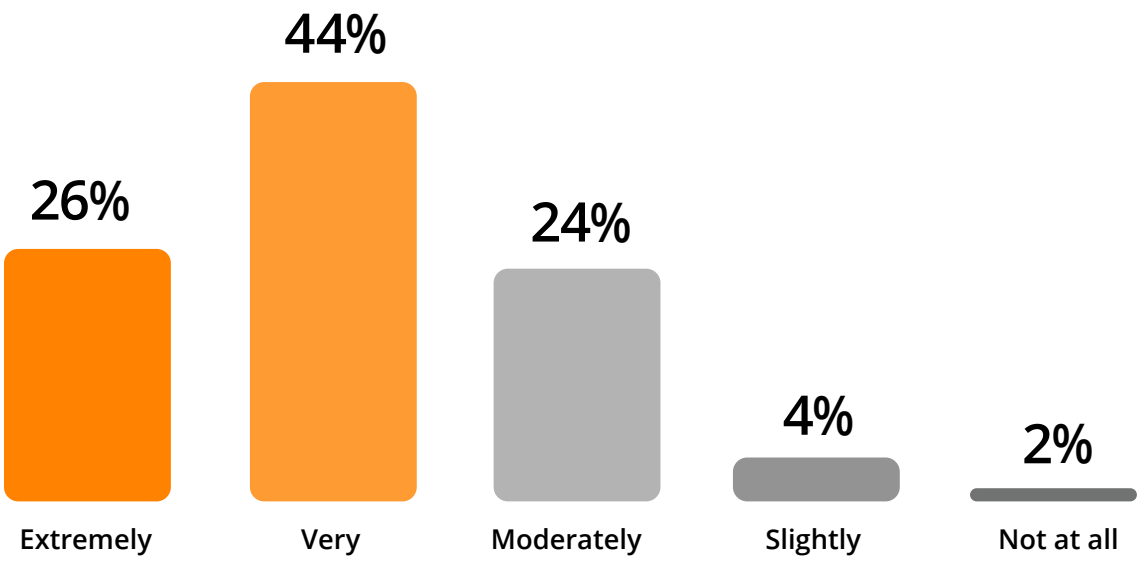
The survey highlights the significant role that architecture plays in cloud security solution scalability, performance, and uptime, with 70% of respondents seeing it as having a major impact. The choice of architecture can greatly influence the efficiency and effectiveness of a security platform.

This finding underscores the need for adaptable, self-learning AI-powered and cloud-native solutions. These solutions need to be able to adjust to an organization's unique infrastructure, and provide flexibility and robust detection and response to the complex demands of scalability, performance, and uptime across various cloud environments.

How much does architecture affect cloud security solution scalability, performance, and uptime? For example, comparing solutions built in the public cloud vs. security vendors' private data centers.

70%

of respondents claim architecture very to extremely much impacts cloud security solutions scalability, performance and uptime



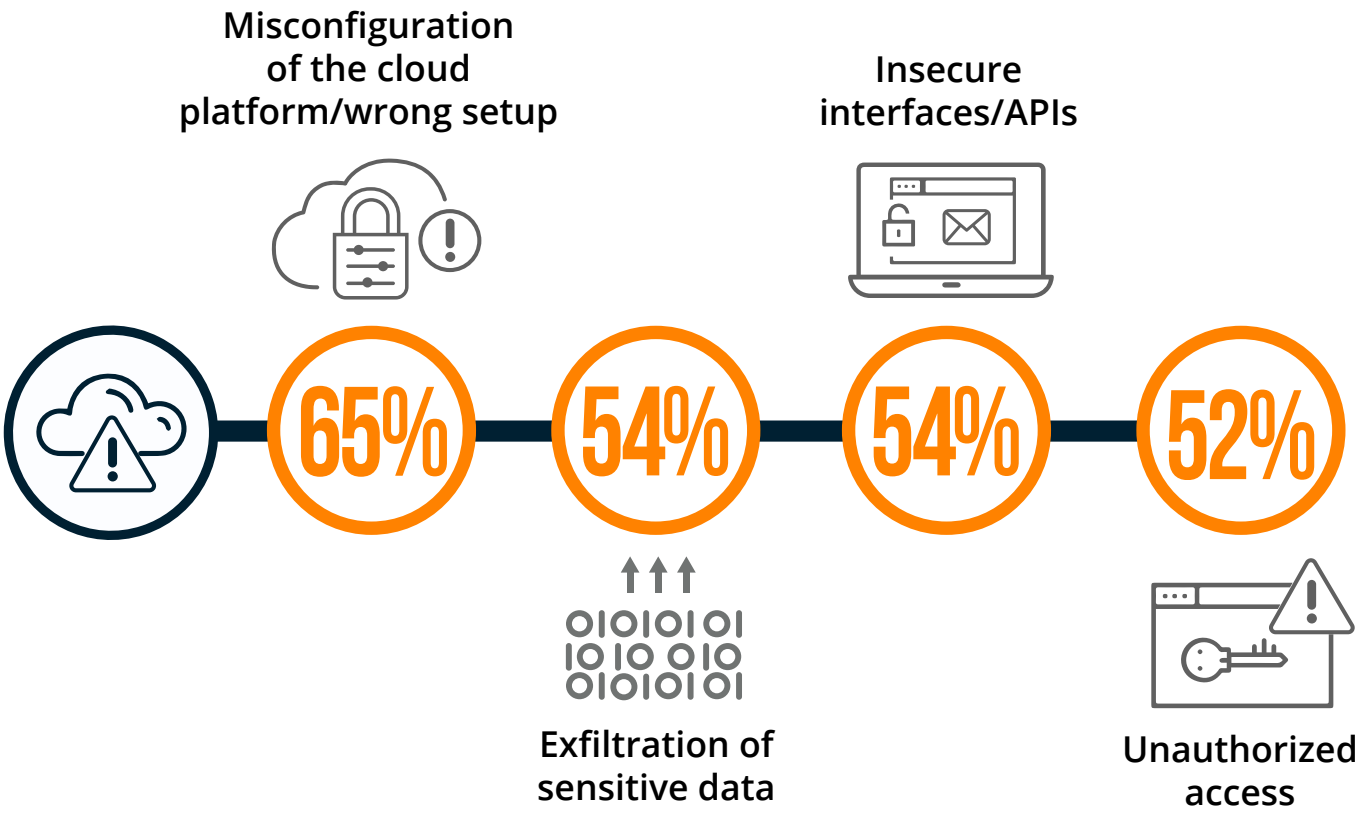
TOP CLOUD THREATS

The survey findings draw attention to the critical vulnerabilities present in cloud security, with misconfiguration of the cloud platform topping the list at 65%. This is followed closely by threats linked to exfiltration of sensitive data, insecure interfaces/APIs (both at 54%), and unauthorized access (52%).

These statistics demonstrate the multifaceted challenges faced by organizations in securing cloud environments. Misconfiguration, in particular, can create a cascade of vulnerabilities leading to data breaches and unauthorized access. Addressing these complex threats requires a sophisticated approach to threat detection and response.

Utilizing self-learning algorithms that predict and counter known and novel attacks, including zero-day threats, provides an efficient way to secure cloud environments without adding complexity.

What do you see as the biggest security threats in public clouds?



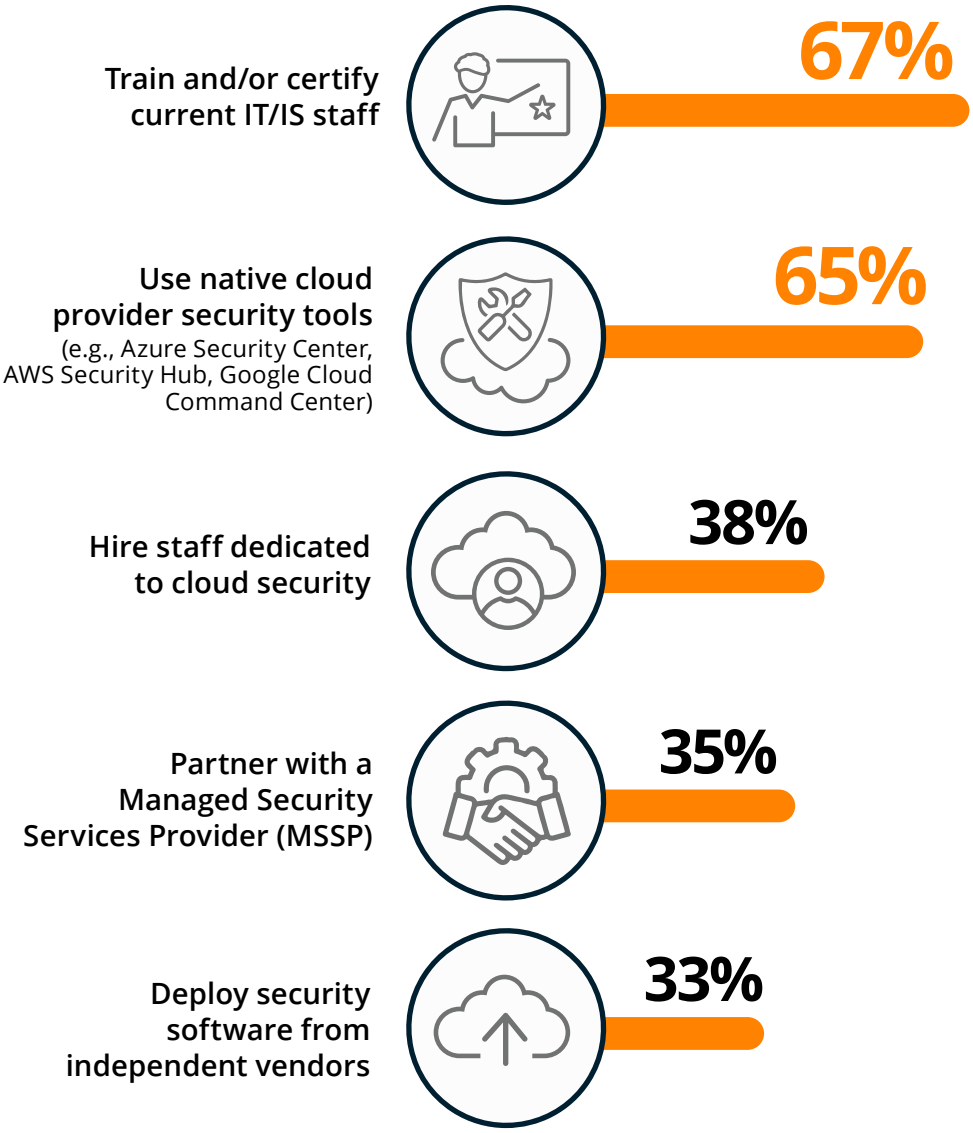
Hijacking of accounts, services, or traffic 45% | External sharing of data 43% | Malicious insiders 40% | Malware / Ransomware 39% | Foreign state-sponsored cyber attacks 34% | Denial of service attacks 32% | Cloud cryptojacking 23% | Theft of service 20% | Lost mobile devices 13% | Don't know / other 6%

CHANGING SECURITY NEEDS

How do organizations respond to changing security needs? The most popular approach among survey participants is to invest in training and certification for their existing IT and information security staff (67%). This helps to bridge the skills gap and empowers employees to better handle the unique security challenges that arise in the cloud environment.

This is closely followed by using native cloud provider security tools (65%). Hiring cloud security staff only follows at a distant third spot (38%).

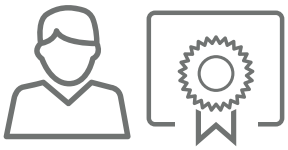
When moving to the cloud, how do you handle your changing security needs?

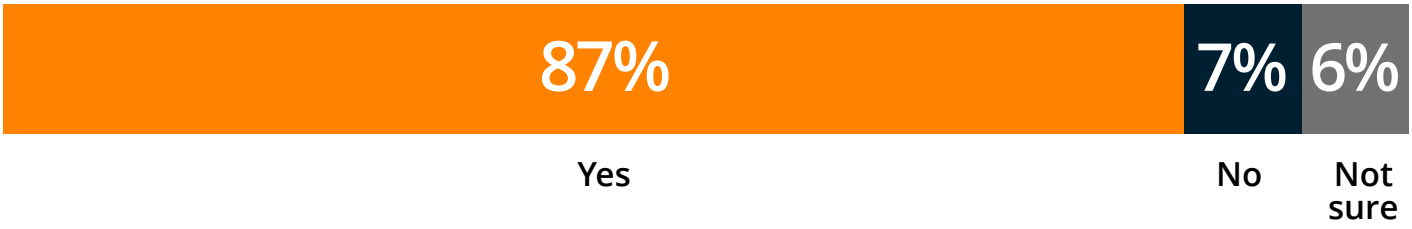


CLOUD SECURITY TRAINING

The survey results highlight the strong demand for cloud security training and certifications as one of the most promising paths to addressing the cybersecurity skills gap. A large majority of respondents confirm that they or their team would benefit from cloud security training and certifications (87%), indicating that there is a significant need for cybersecurity skill development.

Do you think you or your team need cloud security training and/or certification(s) to be better equipped to operate in cloud environments?





TALENT GAP CONCERN

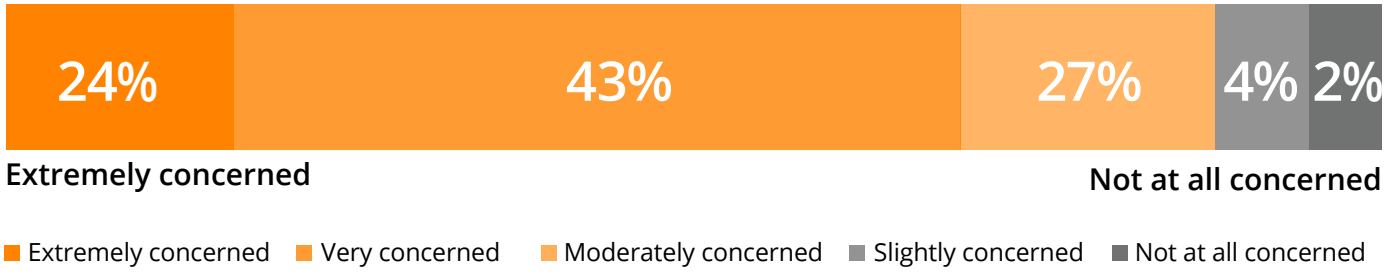
Addressing the cybersecurity skills gap is vital to ensure robust cloud security and provide robust defenses against evolving threats. An alarming 94% of professionals in our survey are moderately to extremely concerned about the industry-wide shortage of qualified cybersecurity professionals.

The talent shortage calls for innovative security solutions that minimize human reliance. Utilizing dynamic learning algorithms, these types of platforms offer advanced threat detection without human input. This fills the gap left by the scarcity of qualified cybersecurity professionals, while efficiently defending against modern cyber threats.

Do you think you or your team need cloud security training and/or certification(s) to be better equipped to operate in cloud environments?

94%

of respondents are moderately to extremely concerned about the skills shortage of qualified cybersecurity professionals



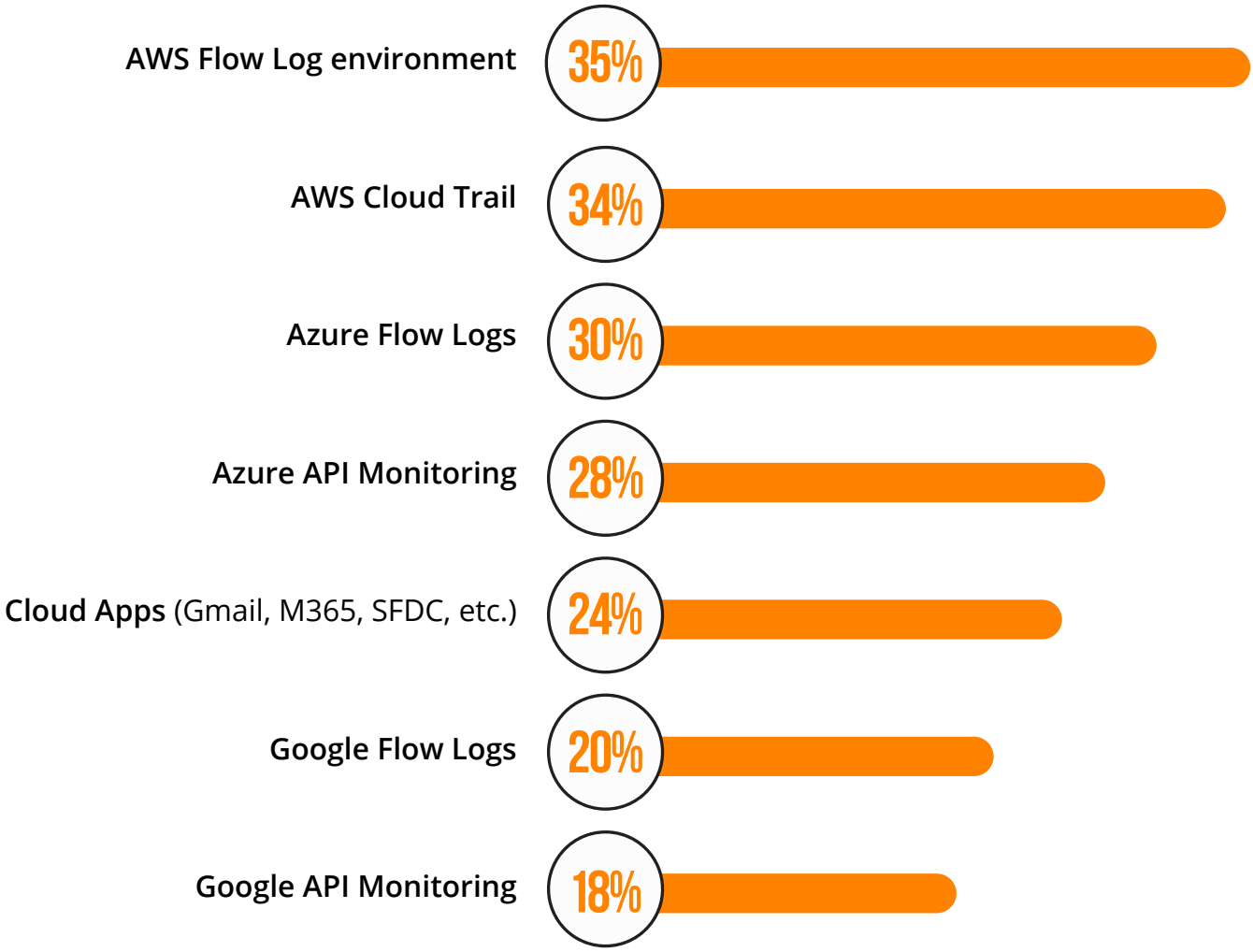
Is your organization or team experiencing a shortage in cybersecurity talent?

LACK OF REAL-TIME THREAT DETECTION

While up to 35% of respondents confirm they're performing real-time threat detection and response within their cloud environment, most respondents in our survey are not. Relying on traditional security technology for real-time cloud monitoring can be prohibitively expensive, leading to a false sense of security with legacy tools or cloud provider security offerings.

This data highlights utilization of real-time detection across multiple services, reflecting an awareness of the need for continuous vigilance. However, the varied cloud landscape points to a challenge in managing multiple platforms, indicating a demand for a unified solution. Such a solution, driven by self-adaptive AI, would allow for seamless visibility across different cloud environments, ensuring that real-time threat detection is not only comprehensive but also efficient and precise.

Are you doing real-time threat detection on your cloud environment?



No 8%

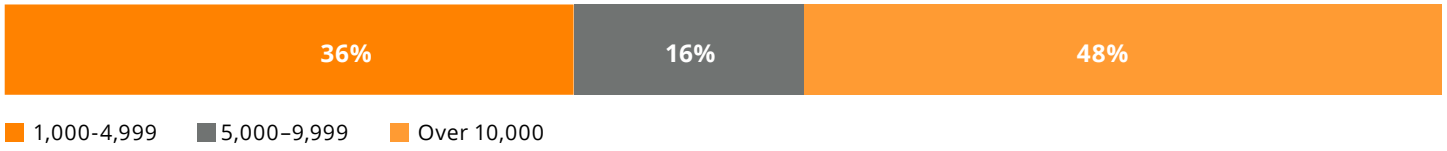
METHODOLOGY & DEMOGRAPHICS

The 2023 Cloud Security Report is based on an extensive survey of 588 cybersecurity professionals conducted in August 2023, to uncover how cloud user organizations are adopting the cloud, how they see cloud security evolving, and what best practices IT cybersecurity leaders are prioritizing in their move to the cloud. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

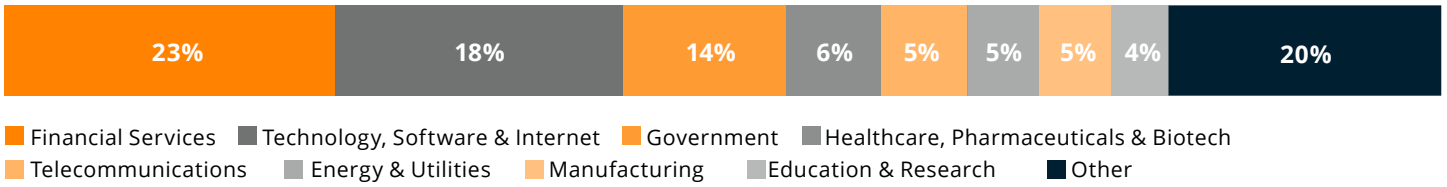
CAREER LEVEL

DEPARTMENT

COMPANY SIZE



INDUSTRY



MixMode is the leader in delivering generative AI cybersecurity solutions for real-time threat detection and response at scale. MixMode offers a patented, self-supervised learning Platform designed to detect known and unknown threats in real-time across cloud, hybrid, or on-prem environments. Large enterprises with big data environments, including global entities in financial services, fortune 1K commercial enterprises, critical infrastructure, and government sectors, trust MixMode to protect their most critical assets. Backed by PSG and Entrada Ventures, the company is headquartered in Santa Barbara, CA.

MixMode Cloud Detection and Response

MixMode's Cloud Detection and Response Solution provides real-time protection for your entire cloud infrastructure, capable of ingesting and analyzing large volumes of diverse cloud data from multiple sources, including cloud, on-prem and hybrid environments.

MixMode continuously monitors your environment and correlates cloud traffic with log data, SIEM logs, and network data to deliver comprehensive visibility and real-time threat detection that ensures the defense of cloud applications and infrastructure against both known and unknown threats.

The MixMode Platform:

- Proactively identifies and resolves threats sooner, including active, novel attacks that other platforms miss.
- Reduces false positives and automates manual processes to focus on what matters.
- Streamlines visibility while up-leveling existing investments.
- Ingests and analyzes large volumes of data in real-time without increasing spend.

MixMode's cloud-native adaptability makes it easy to install and run across AWS, Azure, GCP, and many other cloud platforms in only minutes.

Contact us to learn more:

www.mixmode.ai | +1 (858) 225-2352 | info@mixmode.ai

Cybersecurity
INSIDERS

Cybersecurity Insiders brings together 600,000+ IT security professionals and world-class technology vendors to facilitate smart problem-solving and collaboration in tackling today's most critical cybersecurity challenges.

Our approach focuses on creating and curating unique content that educates and informs cybersecurity professionals about the latest cybersecurity trends, solutions, and best practices. From comprehensive research studies and unbiased product reviews to practical e-guides, engaging webinars, and educational articles - we are committed to providing resources that provide evidence-based answers to today's complex cybersecurity challenges.

Contact us today to learn how Cybersecurity Insiders can help you stand out in a crowded market and boost demand, brand visibility, and thought leadership presence.

Email us at info@cybersecurity-insiders.com or visit cybersecurity-insiders.com