Cybersecurity
INSIDERS

2023 REPORT

CLOUD SECURITY

TREND MICRO™

Introduction

As more organizations adopt cloud computing (including multi-cloud), they face various cybersecurity challenges, including lack of control, limited visibility, and an ongoing skills gap - all hindering faster and more effective adoption of cloud technologies.

The 2023 Cloud Security Report is a comprehensive study based on an extensive survey conducted among 351 cybersecurity professionals in the European Union (EU). By analyzing the latest trends in cloud adoption, identifying prevalent security challenges, and highlighting best practices, this report provides insights for organizations seeking to fortify their cloud environments.

Key findings from the report shed light on the current landscape:

- Many organizations are migrating their workloads to the cloud, with 39% of respondents having already moved over half of their workloads. Moreover, 62% of organizations plan to achieve this milestone within 12-18 months.
- The complexity of multi-cloud environments introduces considerable challenges when securing cloud workloads. Key concerns include the need for proficient employee skills to deploy and manage comprehensive solutions across diverse cloud environments (61%), ensuring data protection and privacy for each environment (59%), and addressing the loss of visibility and control (47%).
- Misconfigurations (32%), malware/ransomware (16%), compromised accounts (16%), and vulnerabilities in the underlying app infrastructure (12%) are the most concerning vectors for data leakage in the cloud.
- The primary drivers for considering cloud-based security solutions include enhanced scalability (54%), accelerated time to deployment (52%), and reduced effort in managing patches and upgrades (51%). Cost savings (41%) and meeting cloud compliance expectations (37%) also influence cloud security adoption.
- When evaluating cloud security solutions, cost emerges as the most important criterion, with 62% of respondents prioritizing it. Other factors include manageability (55%), product features/functionality (52%), product performance and effectiveness (51%), integrations with other security solutions (49%), support (46%), and vendor experience and reputation (44%).

We thank Trend Micro for supporting this important industry research project. We hope you'll find this report informative and helpful as you continue your efforts to secure your organization's cloud journey against evolving threats.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

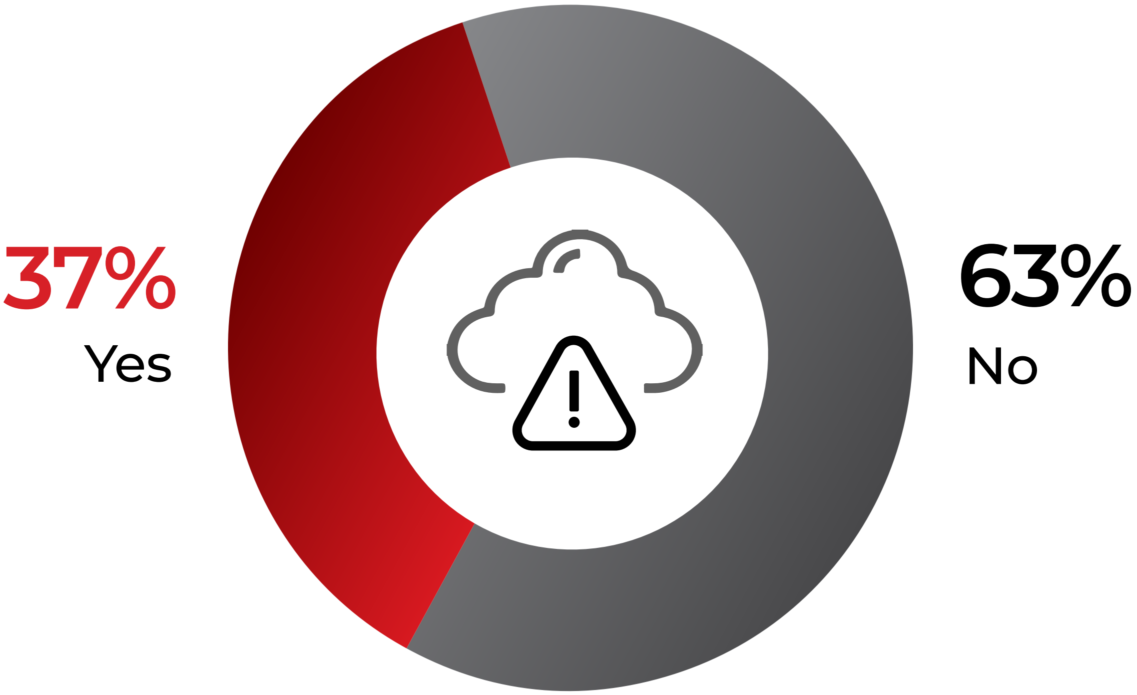
Cybersecurity
INSIDERS

Cloud Security Incidents

Security incidents happen frequently: 37% of organizations experienced a public cloud-related security incident in the last 12 months. Misconfiguration was the leading cause, followed by account compromise and exploited vulnerabilities.

This finding suggests that organizations should prioritize enhancing their cloud security measures and improving incident detection and reporting. Continuous monitoring and regular security audits can help organizations better understand their security posture and reduce the risk of cloud-related security incidents.

Did your organization experience a public cloud related security incident in the last 12 months?



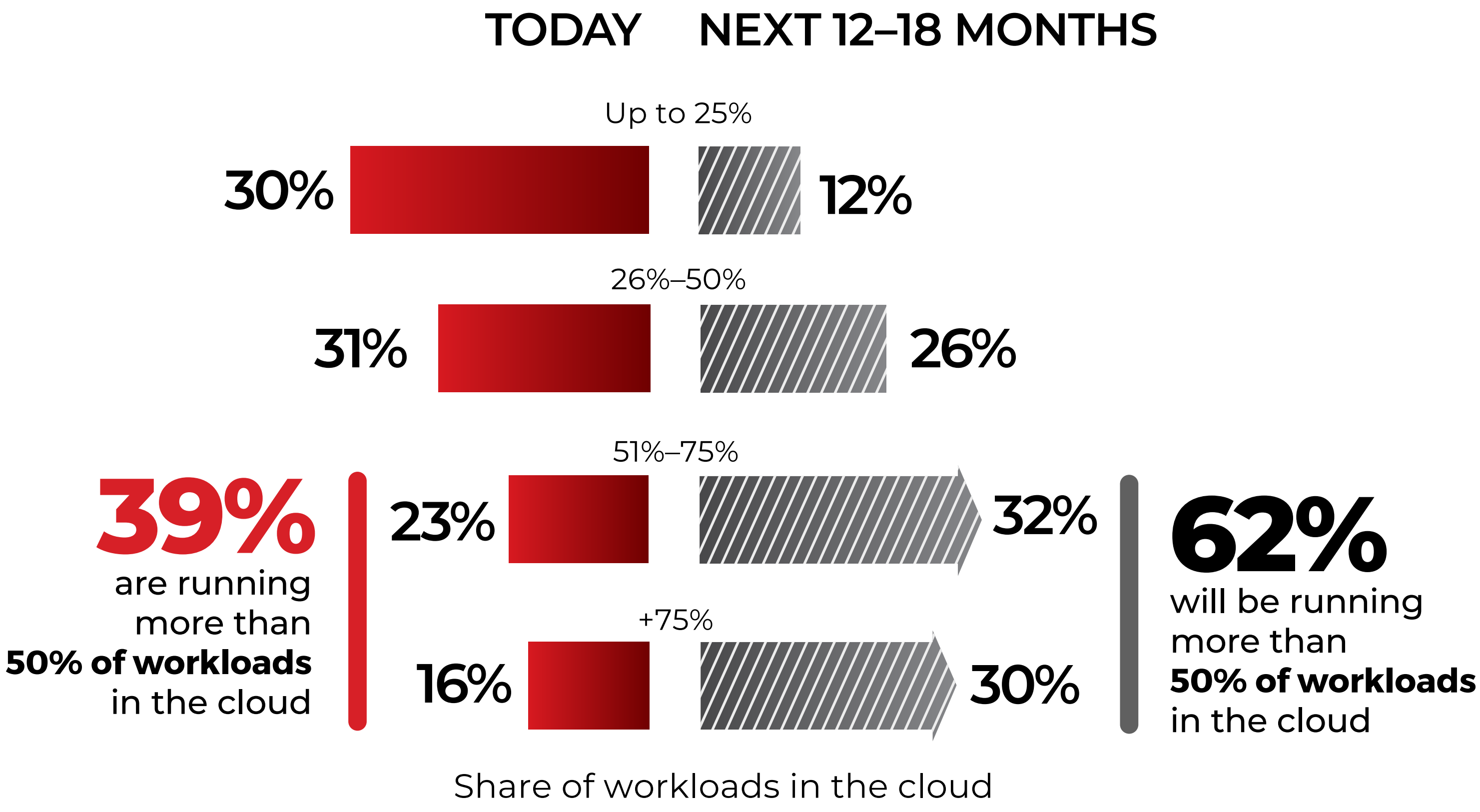
Shifting Workloads In The Cloud

Organizations are increasingly transitioning their workloads to the cloud. 39% of respondents have migrated over half of their workloads, and 62% plan to achieve this milestone within the next 12-18 months.

In light of these findings, it is crucial for organizations to prioritize cloud security and develop a robust migration strategy. This includes assessing the current IT infrastructure, identifying potential vulnerabilities, and implementing appropriate security measures.

What percentage of your workloads are in the cloud today?

What percentage of your workloads will be in the cloud in the next 12–18 months?

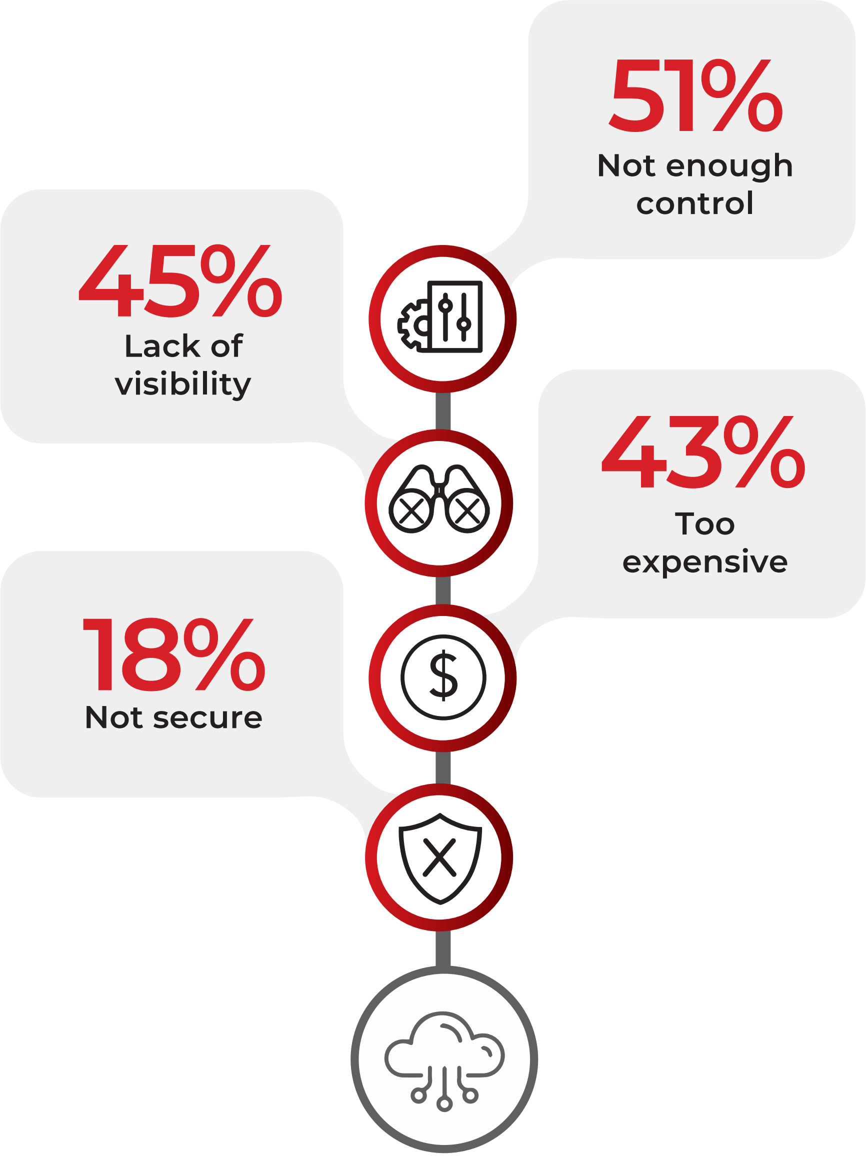


Cloud Adoption Surprises

As cloud adoption continues to gain momentum, security professionals may encounter unexpected challenges that could impede its progress. The top three cloud-related concerns highlighted in this survey are lack of control (51%), limited visibility (45%), and higher costs than anticipated (43%).

Organizations should seek out cloud service providers that offer granular control, comprehensive visibility into the cloud environment, and transparent pricing structures to overcome these obstacles. Engaging in thorough planning and research and investing in employee training will help mitigate these concerns and ensure a smoother transition to the cloud.

What surprises did you uncover that may slow/stop cloud adoption?

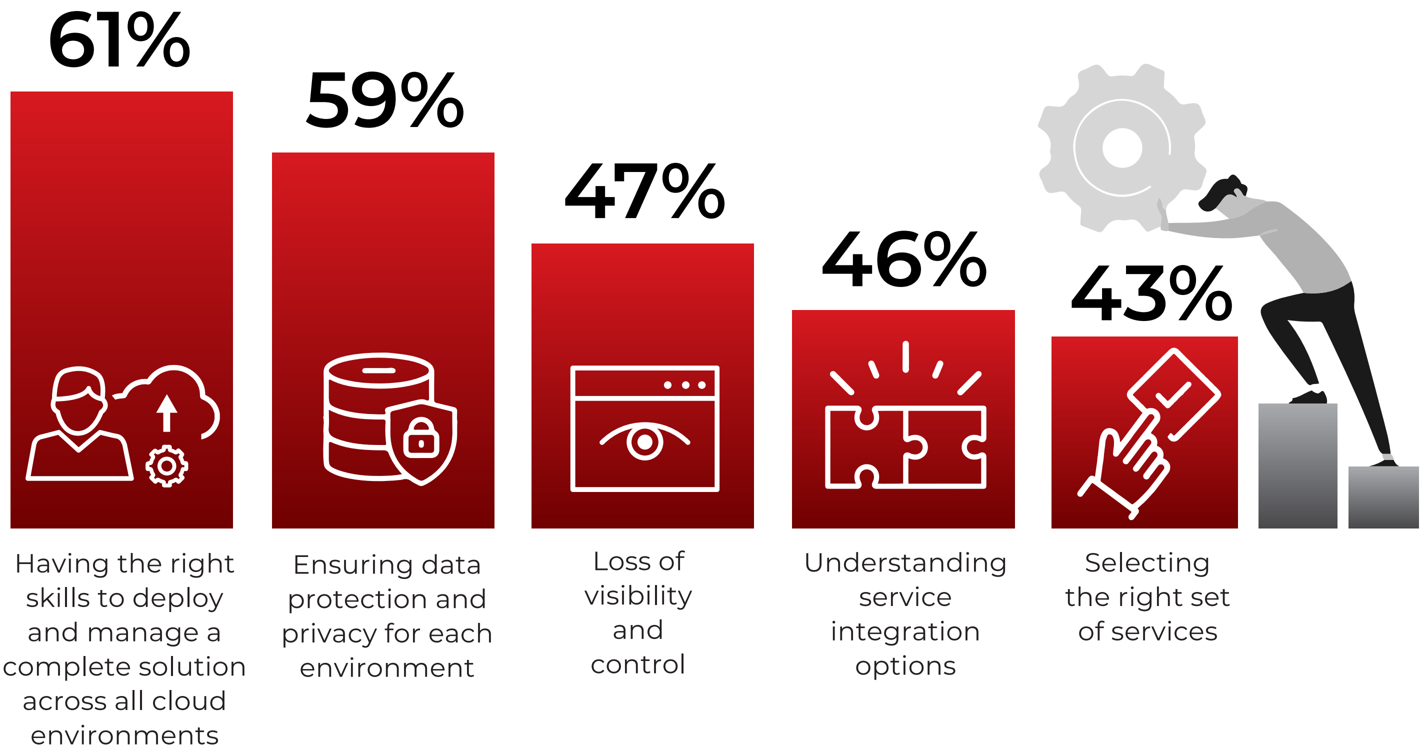


Multi-Cloud Security Challenges

The complexity of multi-cloud environments brings significant challenges in securing cloud workloads, including having the right employee skills to deploy and manage a complete solution across diverse cloud environments (61%), ensuring data protection and privacy for each environment (59%), and addressing the loss of visibility and control (47%).

To address these challenges, organizations should invest in continuous training and development for their IT professionals, fostering a culture of knowledge sharing and staying informed about best practices in multi-cloud security.

What are your biggest challenges securing multi-cloud environments?



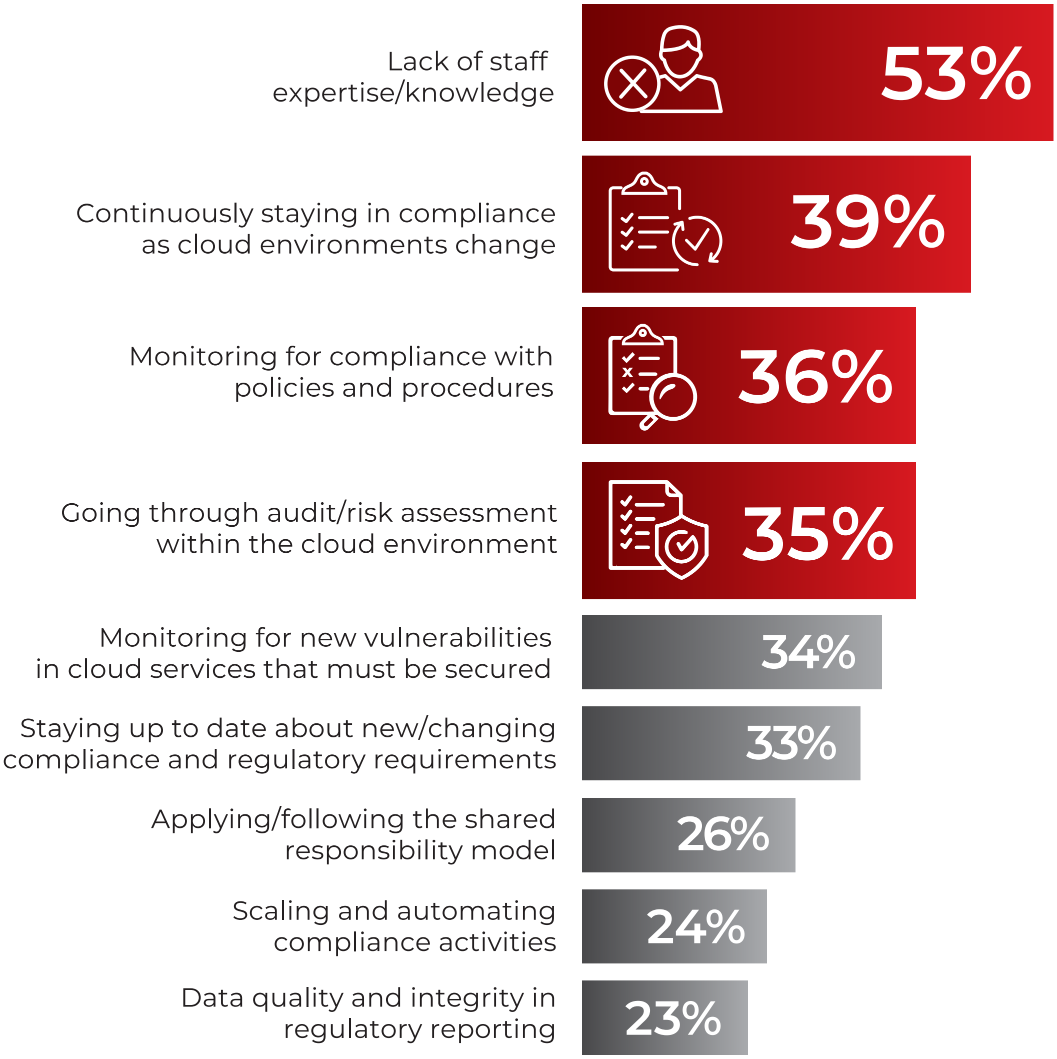
Additional responses include:
Understanding how different solutions fit together 42% | Keeping up with the rate of change 40% | Managing the costs of different solutions 39% | Providing seamless access to users based on their credentials 38%

Cloud Compliance Challenges

The most significant challenges organizations face in maintaining cloud compliance are the lack of staff expertise and knowledge (53%), continuously staying in compliance as cloud environments change (39%), and monitoring for compliance with policies and procedures (36%).

The ongoing struggle to find qualified personnel who can effectively manage and ensure compliance in cloud environments has persisted as the top challenge for several years. Additionally, organizations grapple with adapting to the dynamic nature of cloud environments and keeping track of regulatory requirements. To solve these cloud security compliance challenges, organizations should continue to invest in staff training and certification, develop robust compliance monitoring processes, and stay informed about regulatory changes and emerging threats in the cloud environment.

Which part of the cloud compliance process is the most challenging?



Data Leakage Risk

The survey reveals that the most concerning data leakage vectors in the cloud are misconfigurations (32%), malware/ransomware (16%), compromised accounts (16%), and vulnerabilities in the underlying app infrastructure (12%).

To tackle these challenges, organizations can deploy a mix of technology solutions, such as data loss prevention tools and multi-factor authentication, and invest in staff training and awareness programs to strengthen security practices and minimize human-related risks.

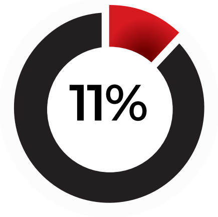
What is the data leakage vector that you find most concerning for your organization?

32% Misconfigurations

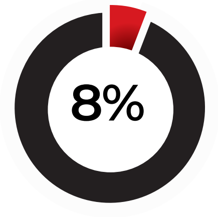
16% Malware/ Ransomware

16% Compromised accounts

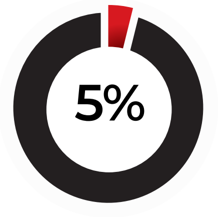
12% Vulnerabilities in underlying app infrastructure



Unsanctioned cloud apps



Unmanaged devices



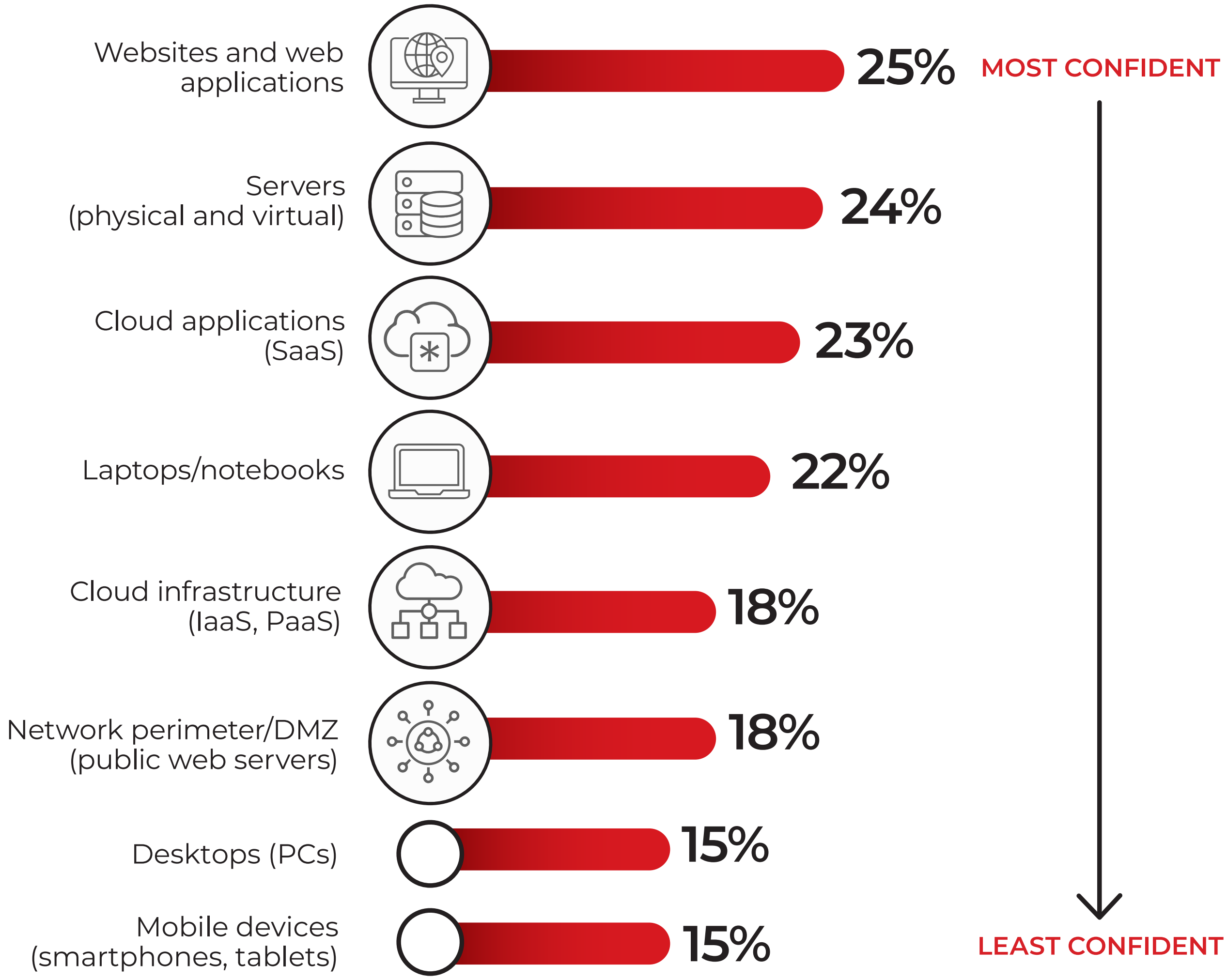
Unsecured WiFi

Confidence in Security

Securing your cloud environment is crucial for protecting critical assets and data. However, cybersecurity professionals' confidence in their ability to secure the various components of the cloud ecosystems varies. The survey reveals cybersecurity professionals express the highest confidence in securing websites and web applications (25%), servers (physical and virtual) (24%), and cloud applications (SaaS) (23%). Conversely, they report less confidence in securing cloud infrastructure (IaaS, PaaS) (18%) and endpoints such as desktops (PCs) (15%) and mobile devices (smartphones, tablets) (15%).

Organizations should prioritize staff training in cloud security best practices and invest in advanced security tools, such as unified endpoint management, to address these security concerns.

Of the following components, which are you most/least confident in being able to secure in the cloud?



Additional responses include:
Datastores (file servers, databases, SANs) 14% | Application programming interfaces (APIs) 13% | Containers 12% | Internet of Things (IoT) 5%

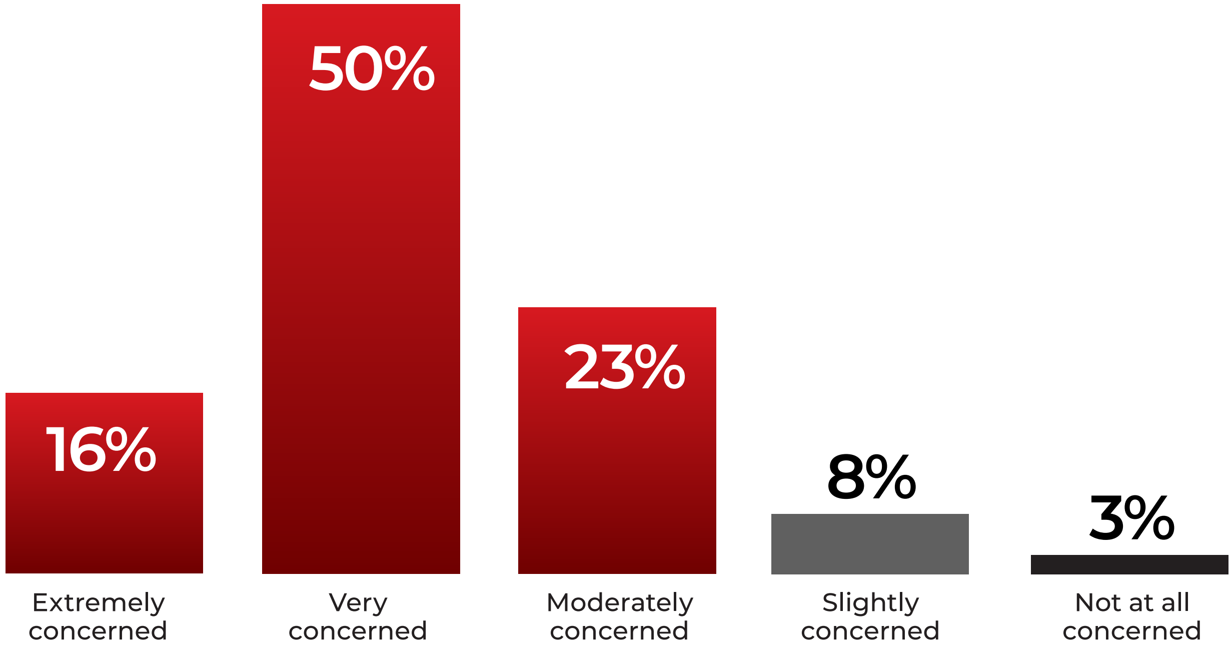
Talent Gap Concern

Addressing the cybersecurity skills gap is vital to ensure robust cloud security and provide strong defenses against evolving threats. An alarming 89% of professionals in our survey are moderately to extremely concerned about the industry-wide shortage of qualified cybersecurity professionals. While there is no silver bullet to solve this issue quickly, organizations should invest in continuous staff training and certification programs, and consider partnering with educational institutions for talent development.

How concerned are you about the industry-wide skills shortage of qualified cybersecurity professionals?

89%

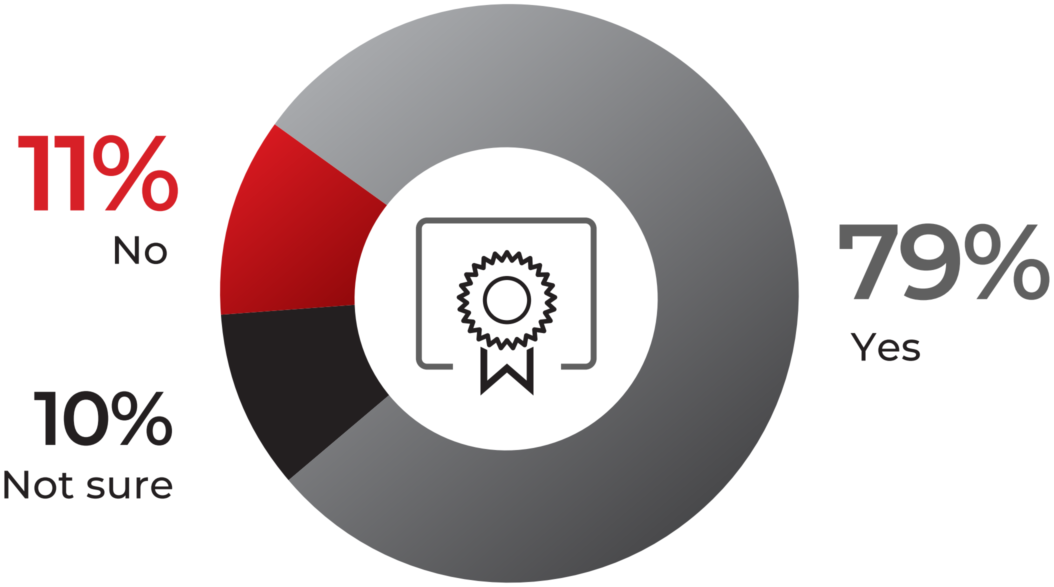
of organizations are moderately to extremely concerned about the industry-wide skills shortage of qualified cybersecurity professionals



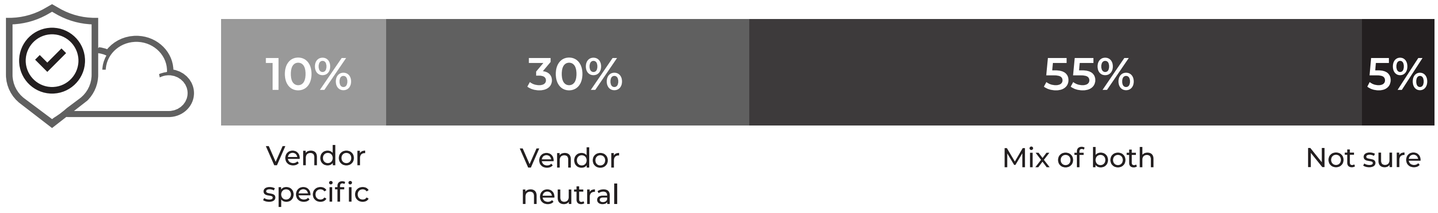
Cloud Security Training

The demand for cloud security training and certification is evident, with 79% of cybersecurity professionals believing that they or their team need such education to operate better in cloud environments. Regarding certifications, a majority (55%) prefer a mix of vendor-specific and vendor-neutral options, while 30% lean towards vendor-neutral certifications. Organizations should invest in tailored training programs to address this need, considering a balanced approach that includes vendor-specific and vendor-neutral certifications for a comprehensive skill set.

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



When considering cloud security certification for yourself and/or your team, do you consider vendor-specific certifications or vendor-neutral certifications?

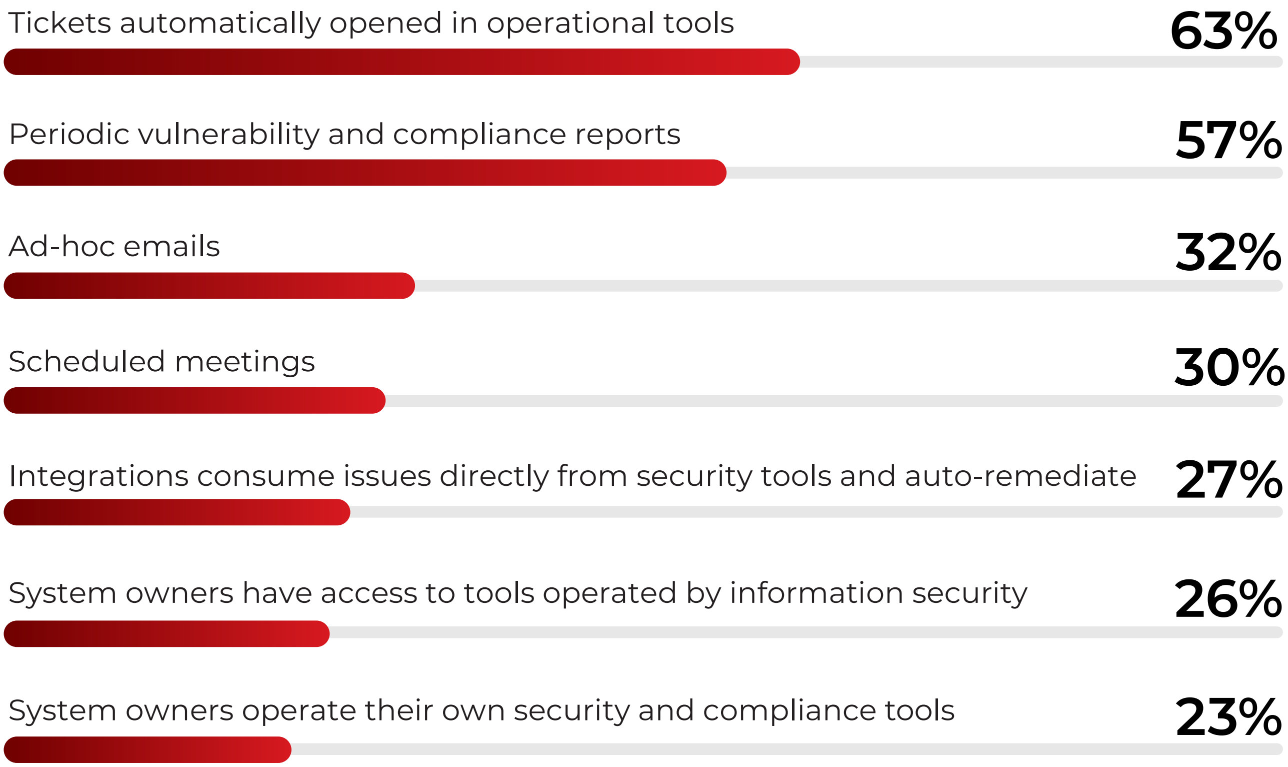


Remediation Management

Efficient remediation management is crucial for addressing cloud security and compliance issues quickly and comprehensively. The primary method used by 63% of cybersecurity professionals involves automatically opening tickets in operational tools, followed by 57% who rely on periodic vulnerability and compliance reports. Less popular methods include ad-hoc emails (32%), scheduled meetings (30%), and direct integrations with security tools for auto-remediation (27%).

To improve remediation management, organizations should streamline processes by adopting automation and integrating security tools with operational tools, ensuring efficient and timely issue resolution.

What is the primary method for managing remediation of security and compliance issues with system owners?

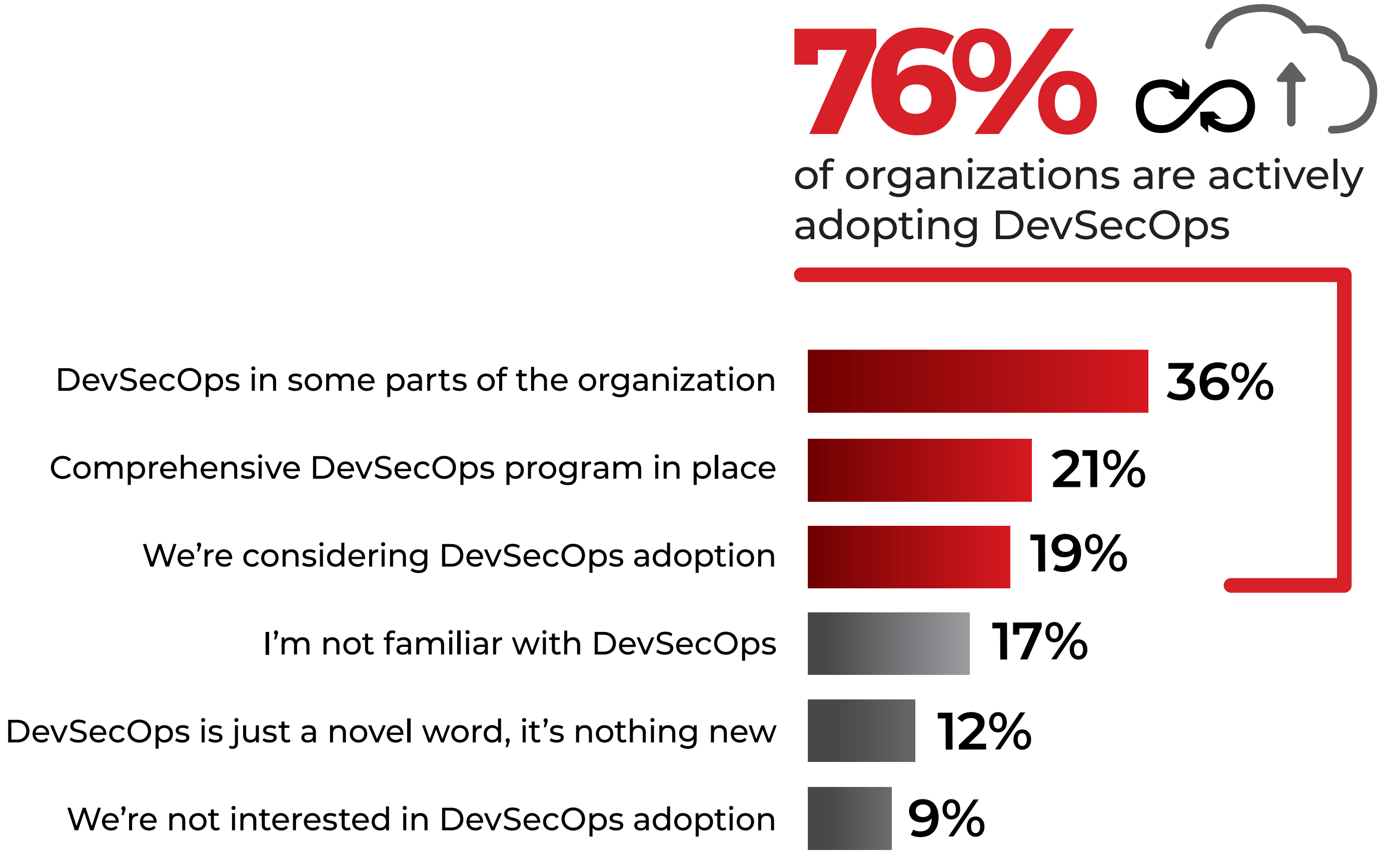


DevSecOps Adoption

DevSecOps is rapidly being adopted by organizations, with 76% of organizations confirming some degree of active adoption. A third of organizations have implemented DevSecOps in some areas (36%), while 21% already have a comprehensive DevSecOps program. Interestingly, 19% are considering DevSecOps adoption and 17% are unfamiliar with the concept.

To enhance cloud security, organizations should explore DevSecOps solutions to facilitate seamless integration of security practices into the development process.

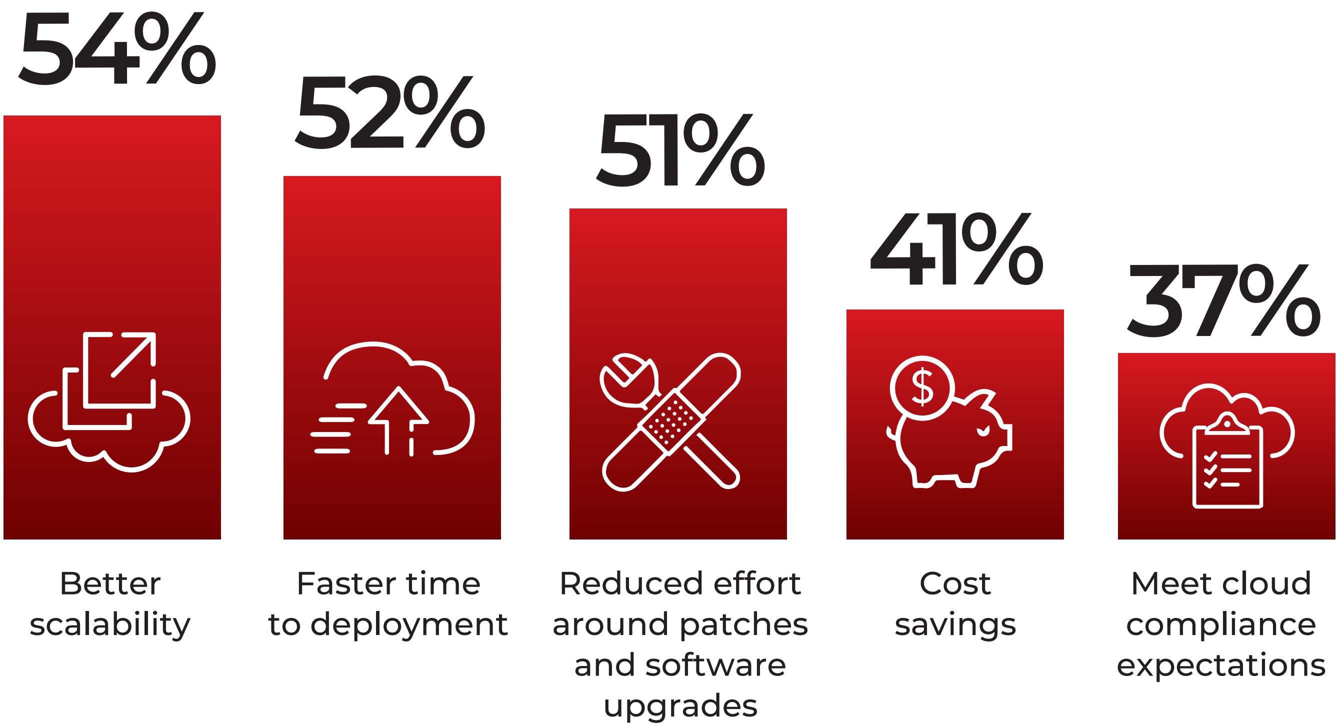
What is your organization's current position on DevSecOps? (select all that apply)



Drivers for Cloud-Based Security

What are the primary drivers for adopting cloud-based security solutions? The survey reveals that better scalability (54%), faster time to deployment (52%), and reduced effort around patches and upgrades (51%) are the top reasons for considering cloud-based security. Additionally, cost savings (41%) and meeting cloud compliance expectations (37%) also play significant roles. To tackle these concerns, organizations can leverage Trend Micro's Cloud One platform for a comprehensive, scalable, and cost-effective cloud security solution that meets compliance standards.

What are the main drivers for considering cloud-based security solutions?

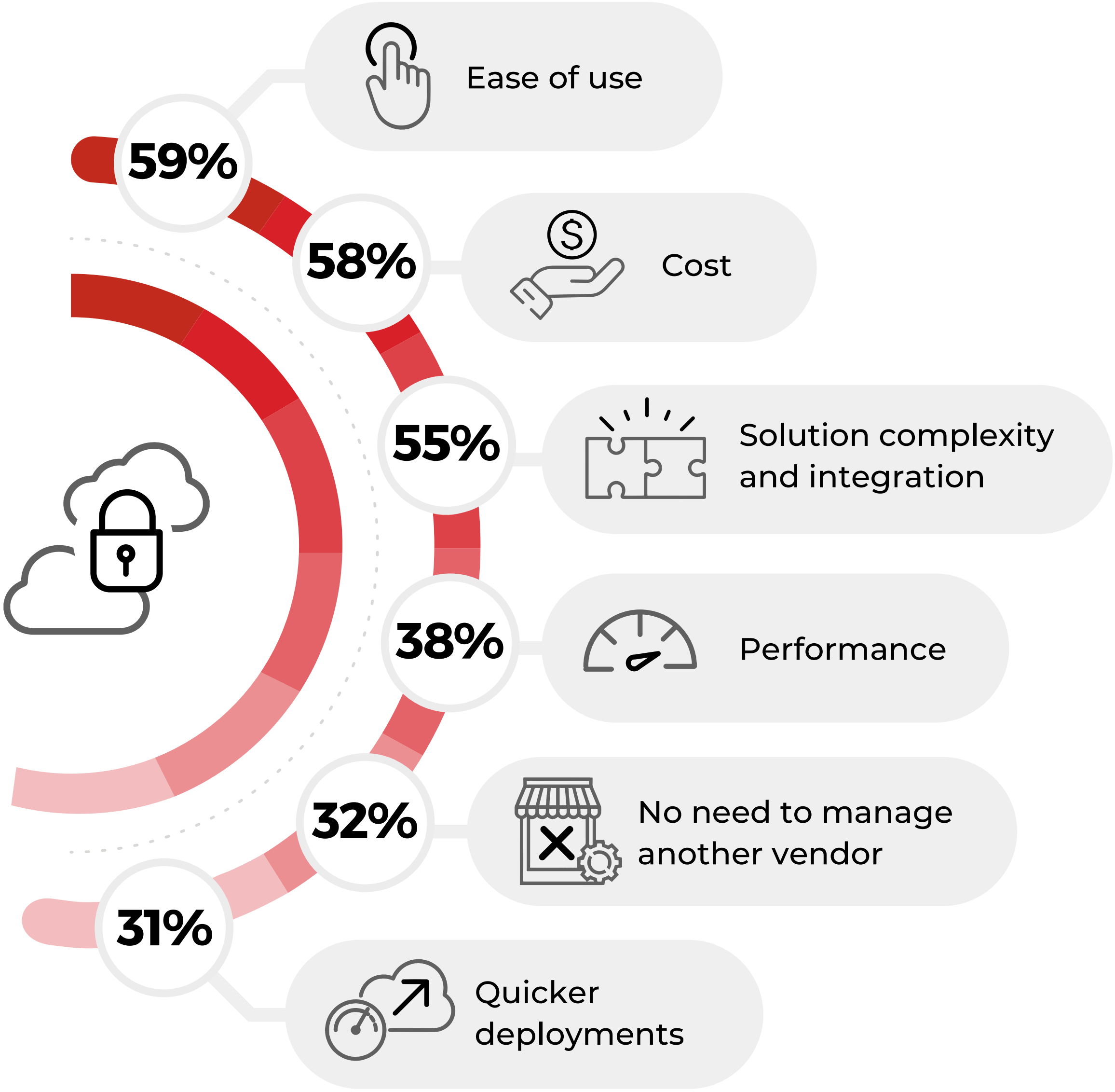


Additional responses include:
Easier policy management 35% | Better uptime 34% | Better visibility into user activity and system behavior 33% | Need for secure app access from any location 32% | Our data/workloads reside in the cloud (or are moving to the cloud) 32% | Better performance 31% | Reduction of appliance footprint in branch offices 25% | Other 1%

Cloud Native or 3rd Party?

We asked cybersecurity professionals about their top criteria when deciding between cloud-native and third-party, independent cloud security solutions. Ease of use emerged as the most important factor (59%), followed closely by cost (58%) and solution complexity and integration (55%). Performance (38%), not having to manage another vendor (32%), and quicker deployments (31%) were also considered important decision factors.

What criteria are most important to you when deciding between cloud native versus independent cloud security solutions?



Cloud Security Solution Preferences

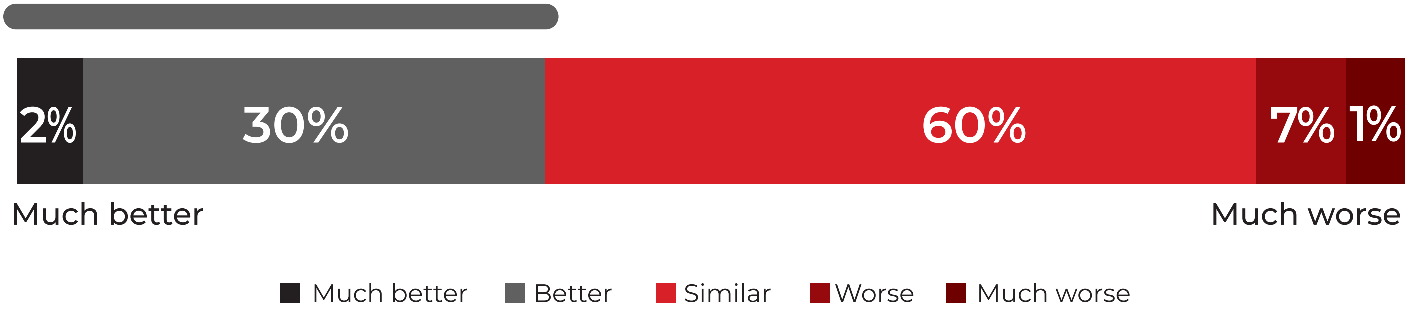
When asked how third-party security solutions compare to native cloud security platforms provided by the cloud operator, more than half of cybersecurity professionals think both perform similarly (60%). A third of professionals (32%) think dedicated third-party security solutions perform better.

These findings suggest that there is a general belief among cybersecurity professionals that third-party security vendors can either provide similar or, in some cases, better cloud security compared to cloud vendors. This emphasizes the importance of evaluating security options and choosing the most effective solution for an organization's specific needs and requirements.

How do you think cloud security from a 3rd-party security vendor compares with cloud security from a cloud vendor?

32%

think that cloud security from an independent security vendor is better than cloud-native security from a cloud provider

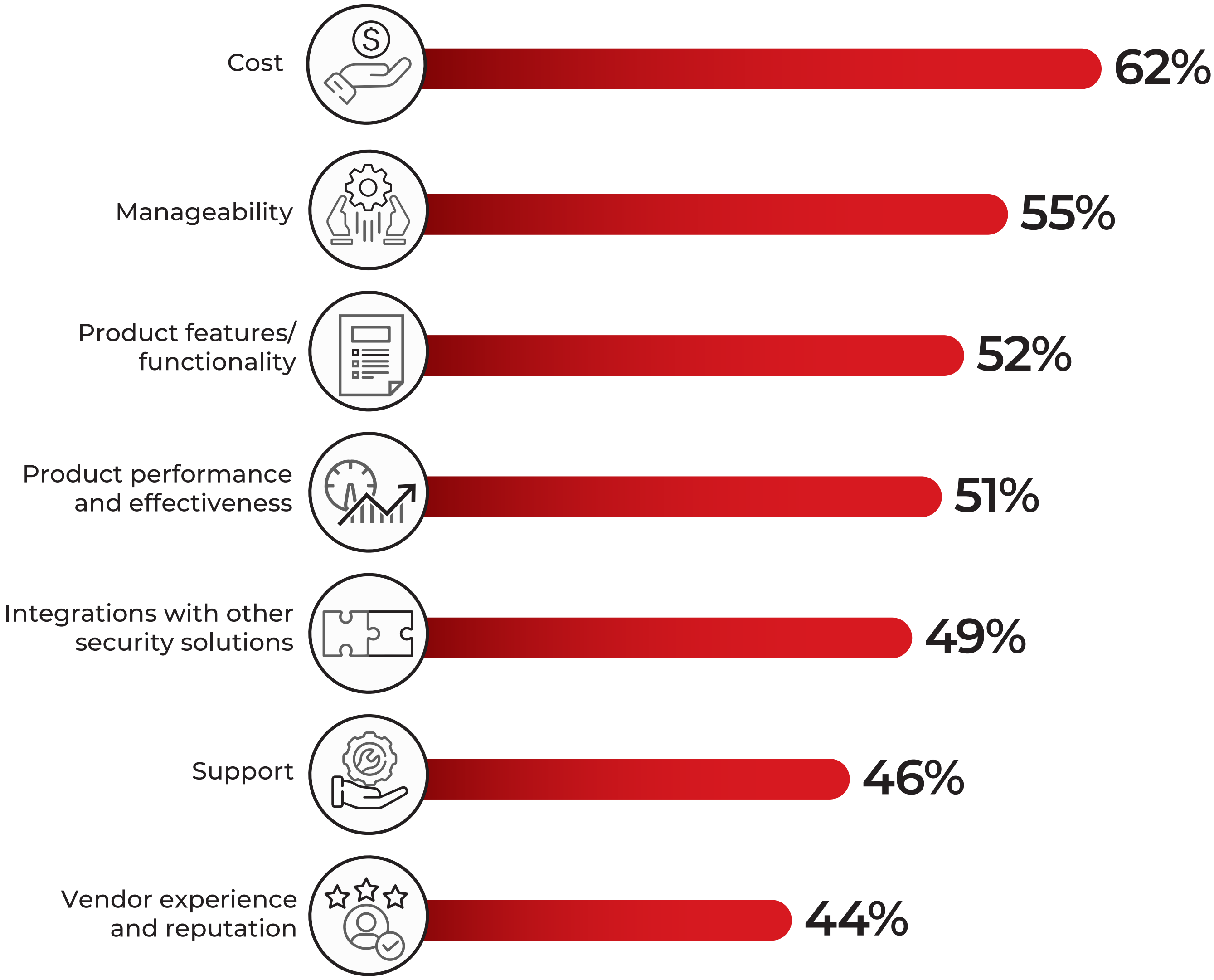


Cloud Security Evaluation

We asked cybersecurity professionals about their most important criteria when evaluating cloud security solutions. Cost tops the list (62%), followed by manageability (55%), product features/functionality (52%), product performance and effectiveness (51%), integrations with other security solutions (49%), support (46%), and vendor experience and reputation (44%). This distribution highlights the emphasis on balancing costs, usability, and efficacy in cloud security solutions.

A surprising finding is the lower importance of vendor experience and reputation compared to other factors, indicating that organizations may prioritize functionality over the reputation of established brands in the cloud security market.

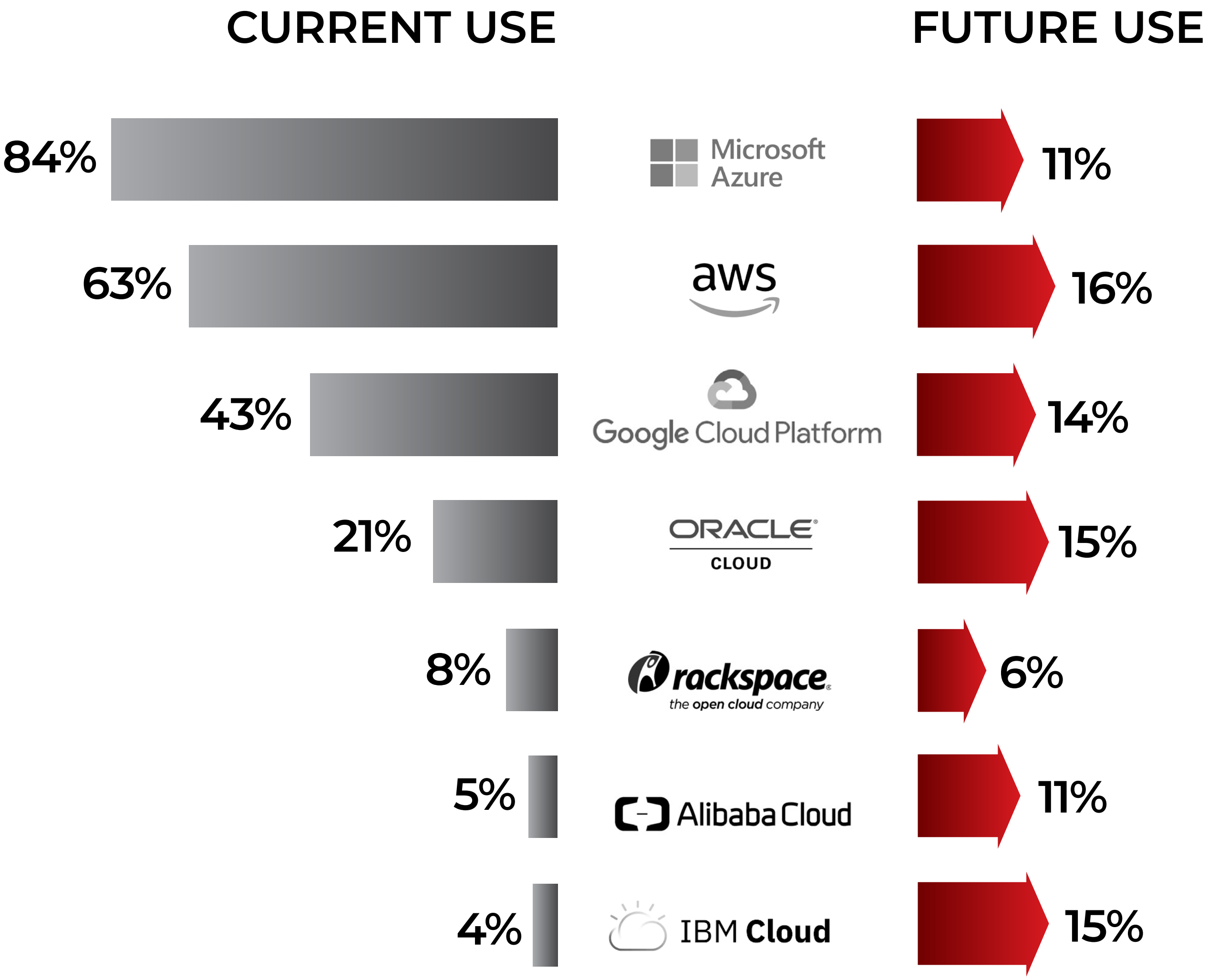
What criteria do you consider most important when evaluating a cloud security solution?



Preferred Cloud Providers

Which cloud providers are organizations prioritizing? The big name providers, such as Microsoft Azure (84%) and Amazon Web Services (63%), continue to dominate the market. However, future cloud adoption is highest for AWS (+16), Google Cloud Platform (+14%), and Oracle Cloud (+15%).

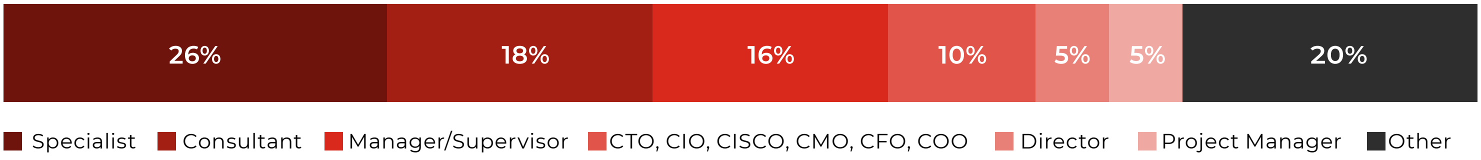
What cloud IaaS provider(s) do you currently use or plan to use in the future?



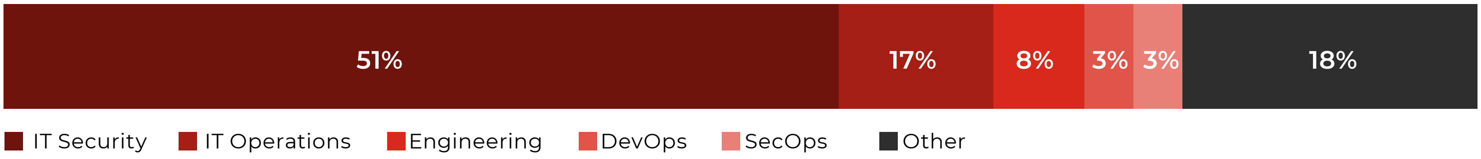
Methodology & Demographics

The 2023 Cloud Security Report is based on an extensive survey of 351 cybersecurity professionals in the EU conducted in March 2023. The study explored how cloud user organizations adopt the cloud, their perceptions of cloud security evolution, and the best practices IT cybersecurity leaders prioritize in their cloud transition. The respondents encompass technical executives and IT security practitioners, providing a balanced representation of organizations of diverse sizes across a wide range of industries.

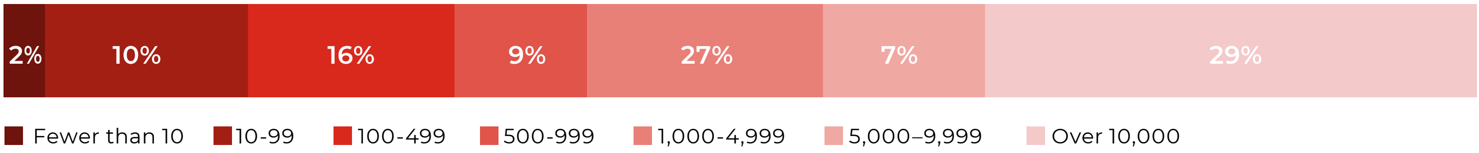
CAREER LEVEL



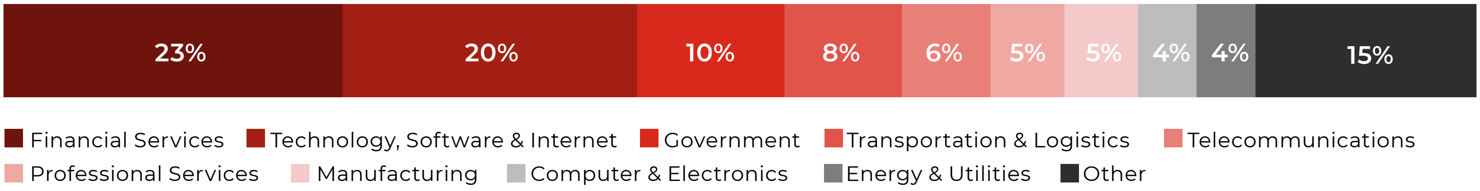
DEPARTMENT



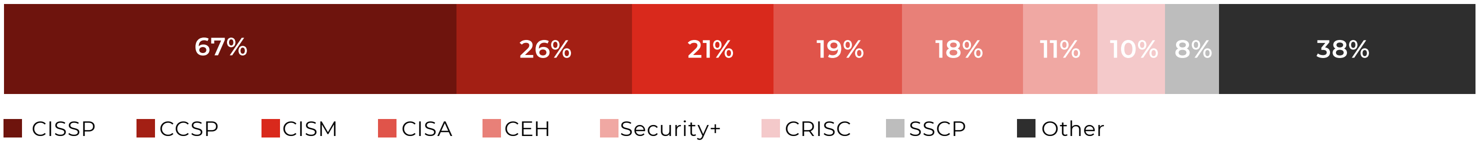
COMPANY SIZE



INDUSTRY



SECURITY CERTIFICATIONS HELD



TREND MICRO™

At Trend Micro, everything we do is about making the world a safer place for exchanging digital information. We believe cyber risks are business risks, and we empower organizations with complete visibility of their digital assets to understand how well they are protected and where to prioritize their investments to lower their risk.

We secure the world by anticipating global changes in modern infrastructures, evolutions in threats, shifts in user behaviors, and advancement in application development. We help customers transform cybersecurity from siloed technologies to a unified security platform that accelerates digital transformation, hybrid workforce collaboration, SOC modernization, vendor consolidations, and operationalization of Zero Trust strategy while integrating with their existing investments and partner ecosystems.

As a global cybersecurity leader, our platform, threat intelligence, and services are deployed by over 500,000 enterprise customers across 175 countries and recognized by third-party reviewers and industry analysts.

www.TrendMicro.com

Cybersecurity
INSIDERS

Cybersecurity Insiders is a 600,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

We provide cybersecurity marketers with unique marketing opportunities to reach this qualified audience and deliver fact-based, third-party validation thought leadership content, demand-generation programs, and brand visibility in the cybersecurity market.

For more information please visit
www.cybersecurity-insiders.com