Technology and Cloud Security Maturity

cloud security alliance®

Acknowledgments

Lead Authors:

Hillary Baron

Contributors:

Josh Buker
Sean Heide
Alex Kaluza
Shamun Mahmud
John Yeoh

Designers:

Claire Lehnert
Stephen Lumpe

Special Thanks:

CSA Bangalore Research Working Group

CSA Bangalore Chapter

Pooja Agrawalla
Madhukeshwar Bhat
Preeti Bheesikar
Satyavathi Divadari
Savitha Gowda
Akash Gupta
Akshata Mongha
Manjesh Pai
Krishna Pandey
Sailaja Vadlamudi
Shirish Verma
Vandana Verma
Sujatha Yakasari

Micro Focus

Harley Adams
Ramses Gallego
Brent Jenkins
Joe Leung
Spiros Liolis
Carole Murphy
Niel Pandya
Stan Wisseman

Table of Contents

Acknowledgements 3
Survey Creation and Methodology 5
    Goals of the Study 5
Introduction 6
    Key Finding 1: Organizations utilizing multi-cloud despite challenges 6
    Key Finding 2: Maturity of privacy-by-design lags 7
    Key Finding 3: Use of Zero Trust, AI/Machine Learning and Serverless expanding in the next two years 7
    Key Finding 4: Use of SDP, ASM, and CSPM expected to increase in the next two years 8
    Key Finding 5: Organizations not planning for key technologies Blockchain, Quantum-safe security, 5G 8
Cloud Strategy 9
Multi-Cloud Users Only 10
Security Strategy 12
Current and Future Use of Cloud Security and Related Technologies 14
Demographics 18
About the Sponsor 20

Survey Creation and Methodology

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to widely promote best practices for ensuring cyber security in cloud computing and IT technologies. CSA is also tasked with educating 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 help gauge the maturity of information security technology at various points in the industry, as well as the rate of adoption of security best practices.

Micro Focus commissioned CSA and CSA's Bangalore Chapter to develop a survey to add to the industry's knowledge about current technology and cloud security maturity and to prepare this report of the survey's findings. Micro Focus financed the project and co-developed the initiative by participating with CSA in developing survey questions addressing hybrid cloud security. The survey was conducted online by CSA from Oct to Nov 2021 and received 256 responses from IT and security professionals from a variety of organization sizes and locations. The data analysis was performed by CSA's research team.

Goals of the study

The goal of this survey is to better understand the maturity levels of organizations for the cloud and technology both currently and in the near future. Key areas of interest include:

- Current cloud use and strategy
- Top drivers for using multi-cloud environments
- Current and future cloud security strategies and solutions
- Predicted changes in the use of cloud and related technologies

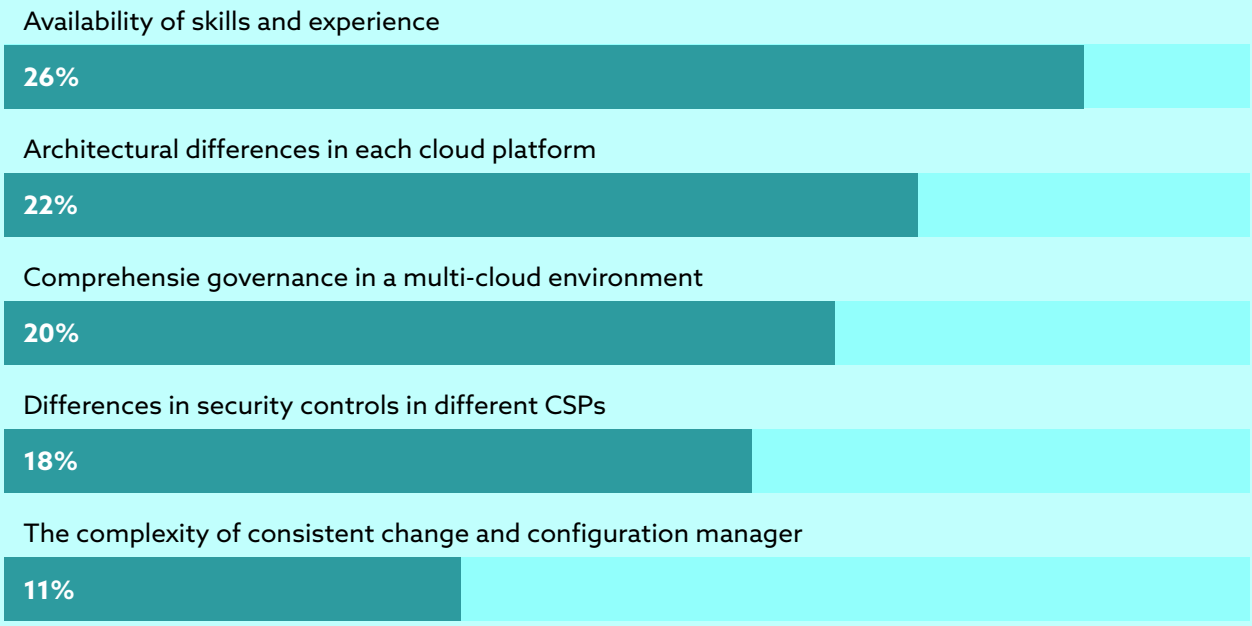
Introduction

Cloud is a continuously evolving space with new services, strategies, and technologies springing up seemingly overnight. Due to this, organizations regularly change and adapt their approach to cloud and cloud security. CSA developed and distributed a survey to better understand organizations' current and future plans regarding cloud strategy, security strategy, cloud services, and cloud-related technologies.

Key Finding 1

Organizations utilizing multi-cloud despite challenges

Organizations desire to use multi-cloud for several reasons including using best in breed features from various CSPs (29%), avoiding vendor lock-in (21%), and reducing cloud concentration risk (16%). However, multi-cloud does increase the complexity of the cloud environment and introduce other challenges that they must address.

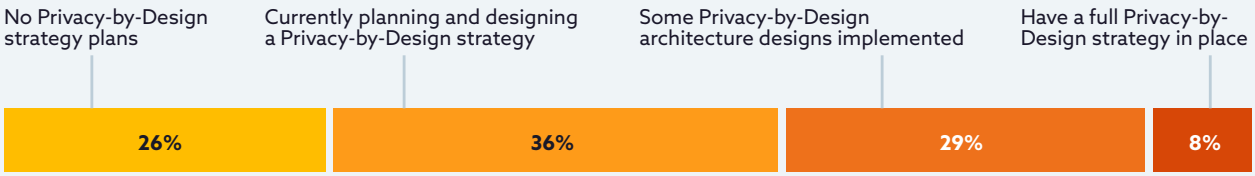


For **26%**, the top concern is the availability of skills and experience on their staff. This is an unsurprising finding since multi-cloud requires their staff to have skills and expertise with not just one CSP, but two or more. Those additional knowledge and skills include understanding the architectural differences (**22%**), gaining comprehensive governance (**20%**), and understanding differences in security controls among the cloud platforms (**18%**). As the complexity of the cloud environment increases so does the need for skills and knowledge in each of these areas.

Key Finding 2

Maturity of privacy-by-design lags

Although the concept of privacy-by-design was introduced over a decade ago, many organizations› privacy-by-design strategies are still developing. Nearly two-thirds of the organizations (65%) are either currently planning and designing (39%) or implementing (26%) their strategy. In fact only eight percent of respondents indicated having a fully implemented privacy-by-design strategy in their organization. This is particularly interesting as the European Union has formally incorporated this strategy into their privacy regulations with the introduction of the General Data Protection Regulation (GDPR) in 2018. It is no surprise then that when rating their maturity of privacy-by-design that meeting of regulatory compliance was the most mature with a rating between "somewhat mature" and "mature."

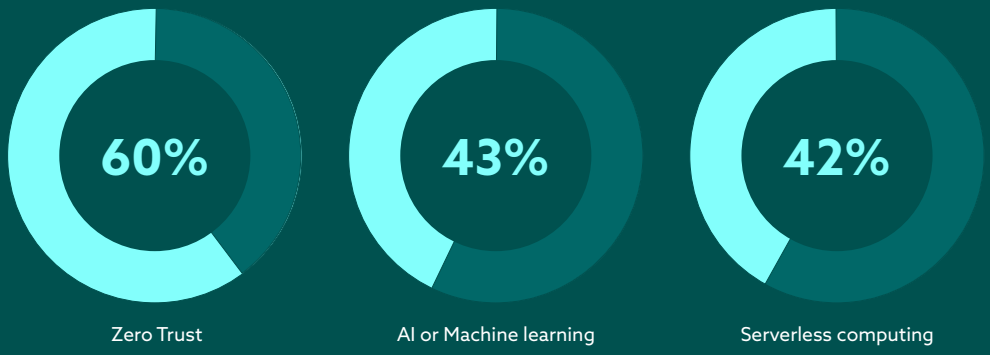


Key Finding 3

Use of Zero Trust, AI/Machine Learning and Serverless expanding in the next two years

Cloud technology is continuously evolving, incorporating new technologies. The top three cloud-related technologies that organizations plan to implement in the next two years: zero trust (**60%**), artificial intelligence (AI) or machine learning (**43%**), and serverless computing (**42%**).

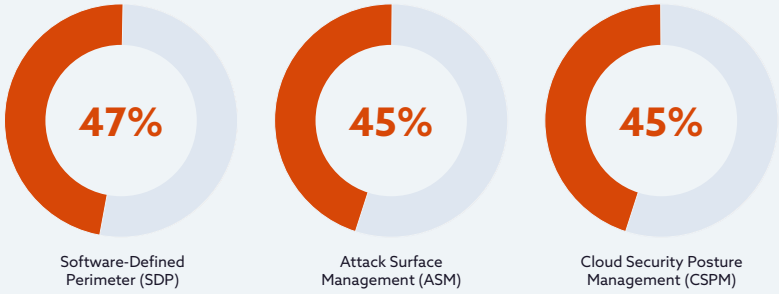
These findings follow the current technology trends. In the past few years, they have risen in popularity due to recent technological advancements and changing security strategies such as DevSecOps. Although technology trends may change rapidly, organizations require more time to implement these technologies effectively. The implementation rates of zero trust evidence this. Only 8% of organizations have fully implemented zero trust, but 71% of organizations have a partial implementation or are planning to implement.



Key Finding 4

Use of SDP, ASM, and CSPM expected to increase in the next two years

Cloud security and the available solutions are also on a continuous evolution. The three security solutions most organizations plan to implement in the next two years is software-defined perimeter (SDP, **47%**). This follows the zero trust trend as SDP solutions are a method of implementing zero trust. The second most common was attack service management (ASM, **45%**). This is a complementary solution to zero trust and SDP solutions with zero trust reducing the attack surface and ASM managing any remaining attack surface. The third most common is Cloud Security Posture Management (CSPM, **45%**). With recent supply chain attacks and the rise of misconfigurations leading to significant breaches, this rise in popularity this finding is a logical conclusion.



Key Finding 5

Organizations not planning for key technologies Blockchain, Quantum-safe security, 5G

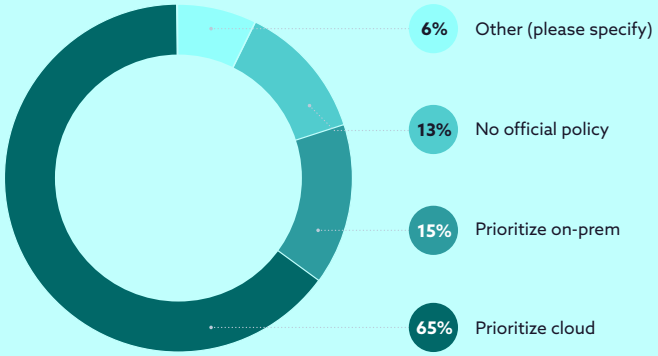
Although there are many different technology and solution trends organizations plan to implement, there are many more that they will not be implementing. The top technologies that organizations are not planning to use are:

- Blockchain (**59%**) – Blockchain/DLT was hyped many years ago and likely suffering from the "trough of disillusionment" phase of the Gartner Hype Cycle. Many organizations are likely seeking alternative solutions due to the high failure rates resulting from a lack of technical knowledge and high resource needs.
- Quantum-safe security (**54%**) – Quantum-safe security is still an emerging space with many ignorant or aloof to the quantum threat, while others are unsure of the current steps to take to begin preparing. Still, many others may be waiting for additional guidance from organizations such as NIST.
- 5G (**49%**) – 5G is more confounding than the others. This could be due to the cost of service and equipment needs. It could also be due to the potential for significant security changes.

Cloud Strategy

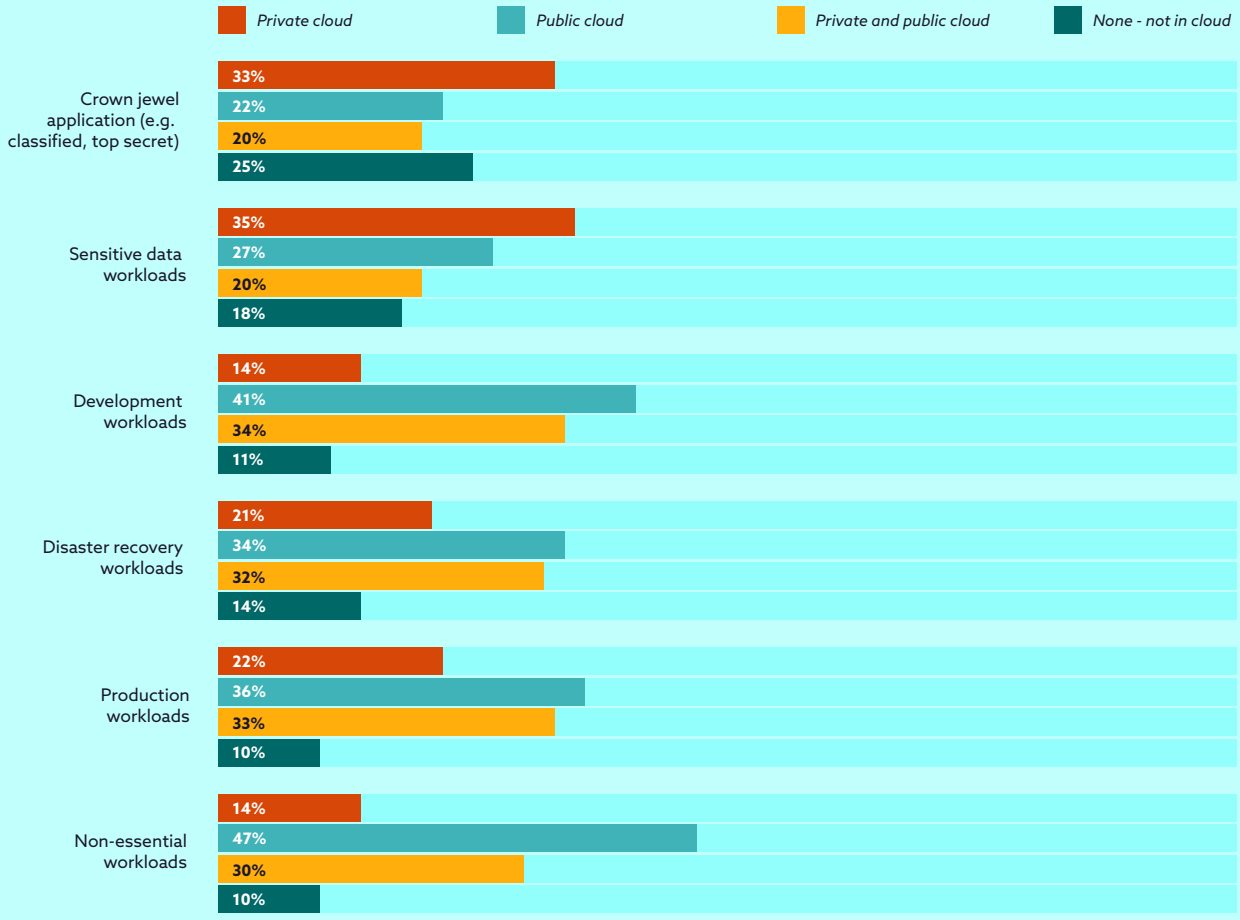
Cloud Policy

The majority of organizations reported having a policy that prioritizes cloud (**65%**). Only **15%** of organizations prioritized on-premises. Finally, **13%** reported not having an official policy.



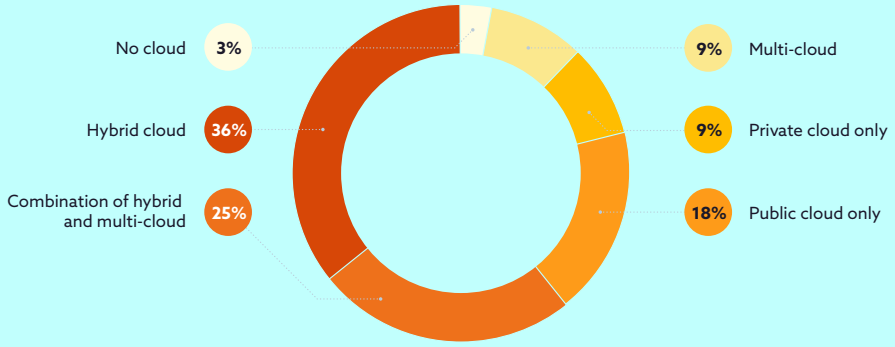
Types of Workloads Hosted in Cloud Environments

Organizations host a variety of types of workloads in cloud environments. Crown jewel (**33%**) applications and sensitive data (**35%**) workloads are primarily hosted in private cloud environments. These types of workloads were also more likely than others not to be hosted in the cloud - crown jewel applications - **25%**, sensitive data workloads - **18%**. This indicates some cautiousness in using the cloud with the more sensitive and important workloads. In contrast, development (**41%**), disaster recovery (**34%**), and non-essential (**47%**) workloads are most commonly hosted in the public cloud.



Cloud Deployment Model

The most common cloud deployment model is a hybrid cloud model (**36%**). The second most common is a combination of hybrid and multi-cloud (**25%**). This means 61% of organizations utilize some form of hybrid cloud, indicating continued use of on-premises in combination with the cloud. Other models such as public cloud only (**18%**), private cloud only (**9%**), and multi-cloud (**9%**) were less common.

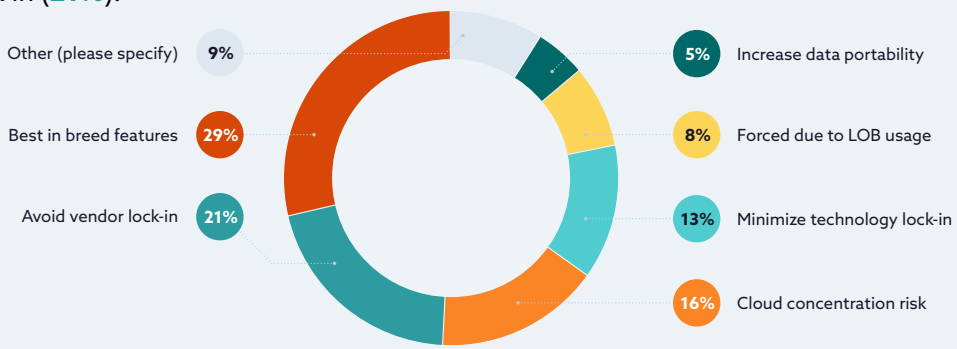


Multi-Cloud Users Only

This section of questions was asked only to those who indicated that they use some form of a multi-cloud model in their organization.

Reasons for Using Multi-Cloud Environment

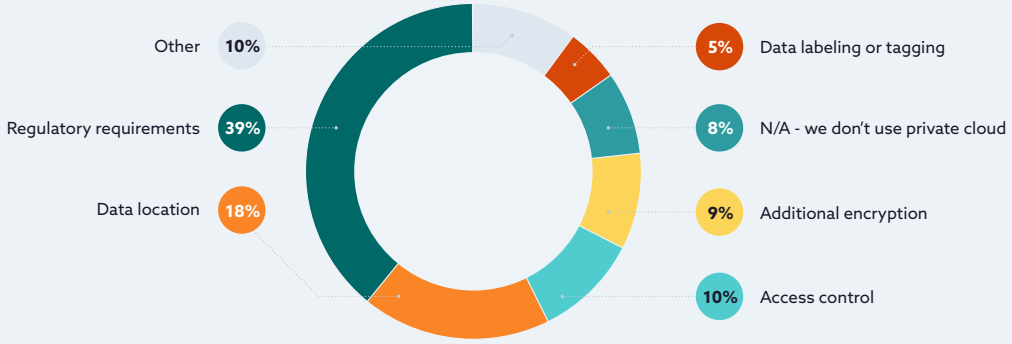
The top reasons for utilizing a multi-cloud environment are best in breed features (**29%**) and avoiding vendor lock-in (**21%**).



Reasons for Using Private Cloud in a Multi-Cloud Deployment

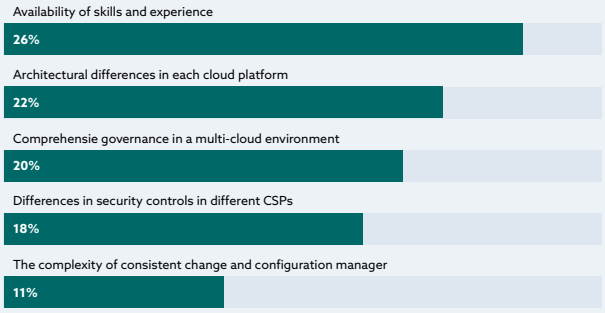
For those multi-cloud users that also use the private cloud as a part of their deployment model (approximately 30% of the total survey respondents), the primary reasons for utilizing the private cloud were due to regulatory requirements (**39%**) and data location (**18%**). These reasons could

be tied to one another since data location is usually tied into some regulatory requirements. This finding is unsurprising as previous surveys found that 57% of organizations have concerns about regulatory compliance and 44% have legal concerns when using public cloud.[1] These concerns stem from the challenges organizations experience with insufficient visibility into security and compliance gaps (60%).[2] Since these regulatory and compliance-based concerns and challenges exist for many organizations, it is unsurprising that they may turn to the private cloud.



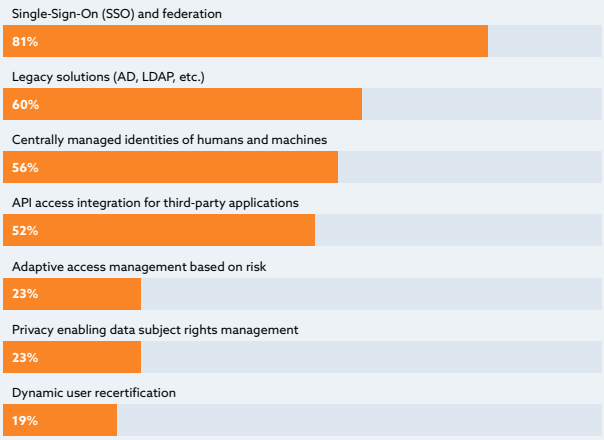
Concerns with Multi-Cloud

There are a multitude of concerns that organizations generally have with the cloud, such as loss of sensitive data (**64%**), improper configuration and security settings (**51%**), and unauthorized access (**51%**)[3]. When using multi-cloud, those top concerns change. The following were more frequently rated as the top concern for organizations: availability of skills and experience (**26%**), architectural differences in each platform (**22%**), and comprehensive governance (**20%**).



Methods for Managing Identity in Multi-Cloud

Organizations use multiple methods for managing identity. The most common methods are the following: single sign-on and federation (**81%**), legacy solutions (**60%**), and centrally managed identities (**56%**). This is unsurprising because they are more mature solutions. The more recent methods for managing identity in multi-cloud, such as adaptive access management (**23%**), privacy enabling data subject rights management (**23%**), and dynamic user recertification (**19%**) had lower rates of use. This indicates a potential opportunity for organizations to implement and improve identity management through these methods.



[1] Cloud Security Complexity: Challenges in Managing Security in Hybrid and Multi-Cloud Environments (2019). CSA.
[2] Secure DevOps and Misconfigurations (2021). CSA.
[3] Measuring Risk and Risk Governance (2021). CSA.

Security Strategy

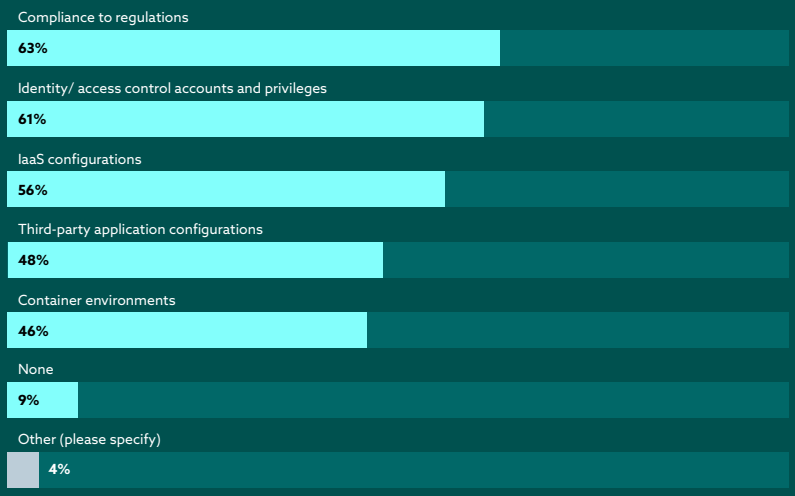
Security Budget

On average, the largest portions of organizations' IT security budget are dedicated to tools and services (**39%**) and staffing (**32%**), including hiring new staff and training existing staff. Tools and services are also likely a top selection due to the considerable expense and need to supplement staff. Staffing is likely a top selection because of the challenges with lack of skills and expertise[4]. The main types of training organizations are pursuing are industry training and certifications (55%), self-training (54%), and product-specific training from vendors (53%).

*Average percentages

Level of Vulnerability Scanning in Cloud

Organizations indicated the depth and breadth of their vulnerability scanning within their cloud environment. The most common levels of scanning reported were compliance to regulations (**63%**), identity/access control accounts and privileges (**61%**), and IaaS configuration (**56%**). The remaining levels, third-party application configuration (**48%**) and container environments (**46%**) fell below 50%. With the popularity of third-party applications and the use of containers, these rates will hopefully increase in the coming years.



Implementation and Maturity of Zero Trust

Zero trust has become an increasingly popular approach to cloud security. About half (45%) of organizations surveyed are planning and designing a zero-trust strategy. Over a quarter (28%) reported having some architecture designs implemented. Just 6% reported having their zero trust strategy fully implemented, which speaks to the newness of this strategy. Finally, 22% reported their

[4] The State of Cloud Security Risk, Compliance, and Misconfigurations (2021). CSA.

organization has no plans regarding zero trust. Some of the immaturity in this space could be due to revised plans in recent years with increased rates of work-from-home.

Organizations also rated the level of maturity of their zero trust strategy across several domains: network, data, identity, policy, applications, and user behavior. On average, all domains were rated as somewhat mature. However, there were a few notable differences. User behavior analytics was rated least mature out of all the categories. Network had the highest rate of very mature ratings. This is unsurprising given that zero trust is commonly known as a network-based segmentation strategy.

Implementation and Maturity of Privacy-by-Design

Privacy-by-design likewise has become popular with the introduction of the EU's GDPR policy several years ago. Just over a third (36%) indicated they are planning and designing a privacy-by-design strategy. Just under a third (29%) reported some implementation of a privacy-by-design architecture, and another 8% reported they have a strategy fully implemented. Finally, 26% reported they have no plans regarding a privacy-by-design strategy. Of those organizations with no plans, there is a roughly even split between the various regions (APAC 29%, EMEA 34%, and Americas 36%).

Individual domains of privacy-by-design were rated to assess their level of maturity are are listed below in order of their level of maturity:

1. Meeting of regulatory compliance
2. Design and architecture of IT system
3. Key management
4. Policy design
5. Data collection, use, and storage
6. Policy design
7. Technology enforcement of policies
8. Disclosure of data owners
9. Data subject access rights
10. Data discovery & governance

On average, all domains were rated as only somewhat mature. However, there were a few notable differences. The most mature category was meeting of regulatory compliance (mature – 40%, very mature – 15%), which is unsurprising given the implementation of many privacy laws and regulations over the past several years. The category most likely to be rated as not mature (26%) was surprising--data discovery and governance.

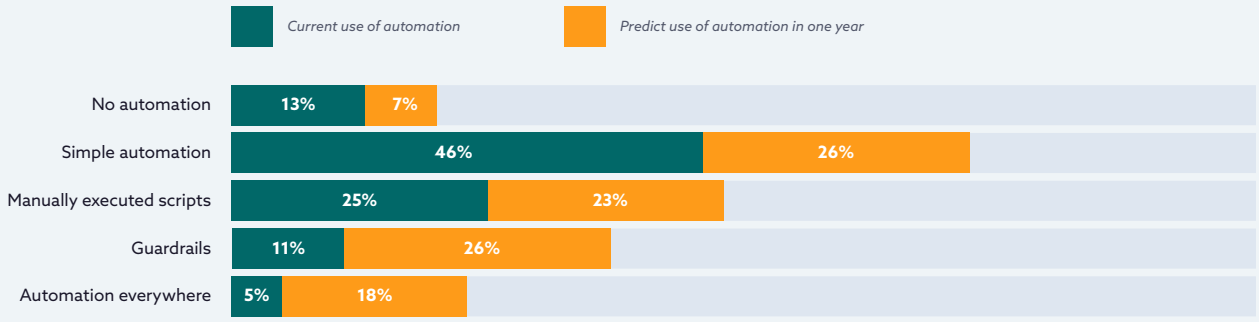
Current and Future Use of Cloud Security and Related Technologies

Current Use of Automation

With regard to the use and maturity of automation with cloud security, 84% of organizations report having no automation or are still on the journey to use automation. Only 5% of organizations report using automation everywhere. This could speak to the difficulty of implementation or lack of expertise on security teams. In a previous survey, lack of expertise was the top barrier to the use of auto-remediation4.are insufficient or non-existent.

Use of Automation in 1 year

A follow-up question asked about the expected use of automation within a year. The use of simple automation is expected to decrease (current **46%** to future **26%**). Manually executed scripts are expected to remain roughly the same (current **25%** to future **23%**). Guardrail usage is expected to increase (current **11%** to future **26%**). Finally, automation everywhere is expected to increase (current **5%** to future **18%**). No use of automation is also likely to decrease (**13%** current to future **7%**). Overall, it indicates a shift right toward automation.

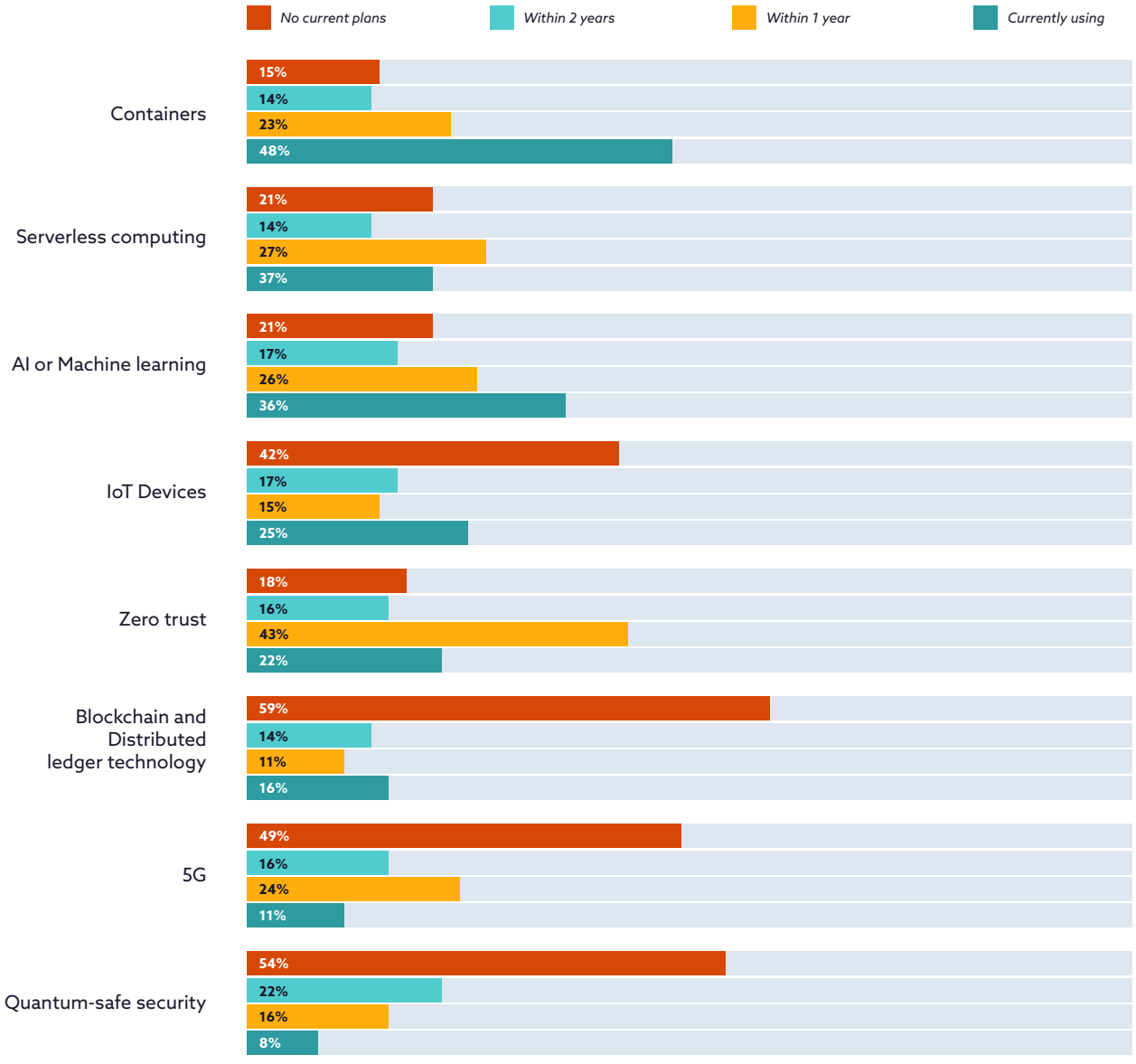


Current and Future Use of Cloud-Related Technologies

Organizations indicated whether they were currently using or planning to use various cloud-related technologies. The most common types of technology that organizations do not currently have plans to use include blockchain/DLT (**59%**), quantum-safe security (**54%**), 5G (**49%**), and IoT devices (**42%**). Many of these are surprising - blockchain has unique use cases and current phase in the hype curve, quantum-safe security is still new with many waiting for more guidance, and 5G is a relatively new technology. However, IoT devices in organizations are pretty common, so this result was surprising. It could be true that many organizations do not use IoT devices. Still, it could be equally true that IoT devices are well integrated into organizations, making them easy to overlook. The low numbers could also be due to the low survey participation rates from typical IIoT users such as oil, gas, automotive, and other such industries.

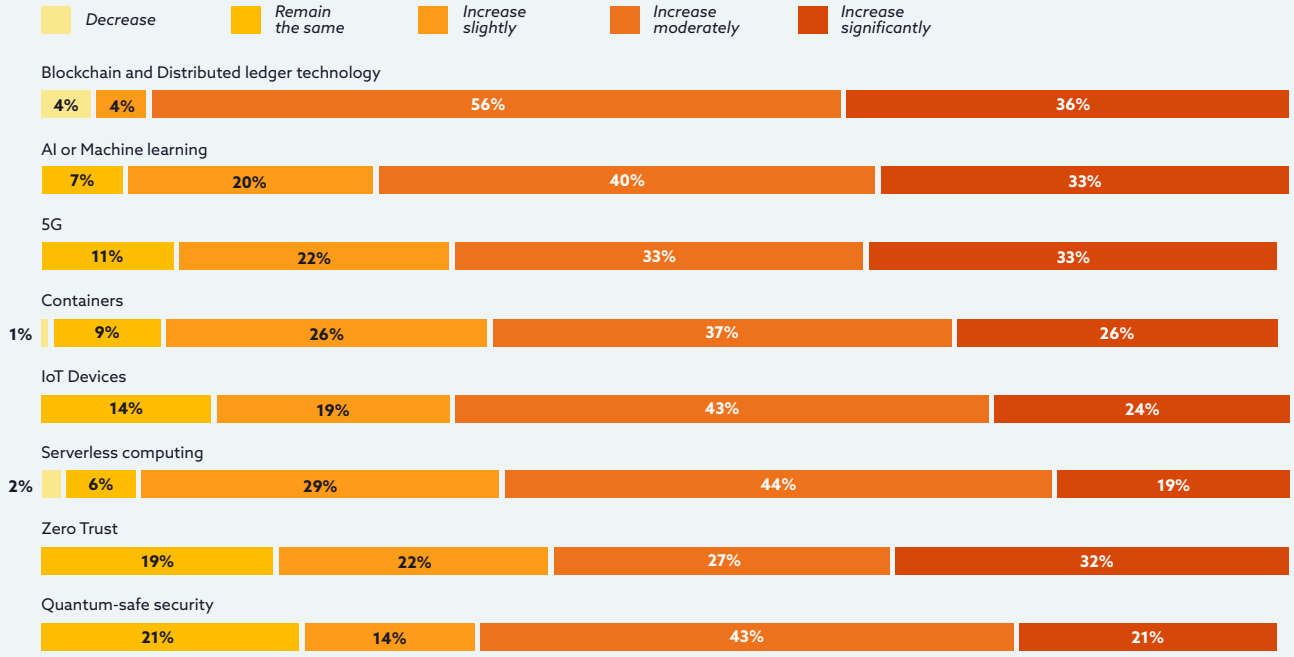
The most common technologies currently used are containers (**48%**), serverless computing (**37%**), and AI or Machine learning (**36%**). These results are consistent with current trends in the industry, including the rise in the use of a DevSecOps approach and the inclusion of AI or Machine learning in security products.

Finally, the most commonly reported technology expected to be used within one year was zero trust (**43%**). This is consistent with the earlier findings in this survey and suggests this approach will become increasingly popular over the next year.



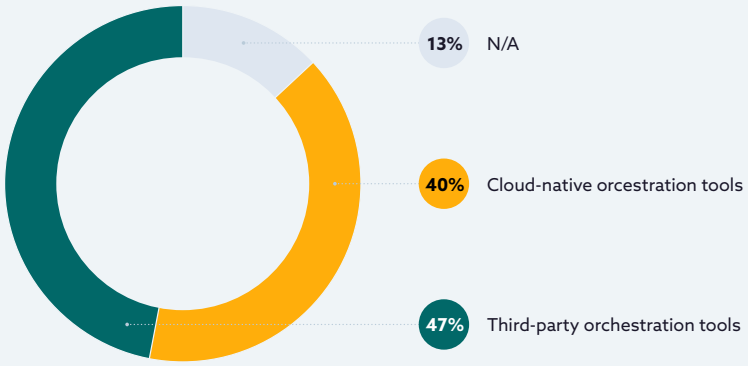
Expected Changes in Use of Cloud-Related Technologies

As a follow-up, organizations currently using these technologies were asked to indicate whether their use would increase or decrease over the next year. Overall, on average, current users of each of these technologies expect to use to increase moderately or significantly.



Tools for Orchestrating Containers in Cloud

Organizations were asked whether they use third-party or cloud-native tools for container orchestration in their cloud environments. It was most common for organizations to use third-party orchestration tools (**47%**) over cloud-native orchestration tools (**40%**).



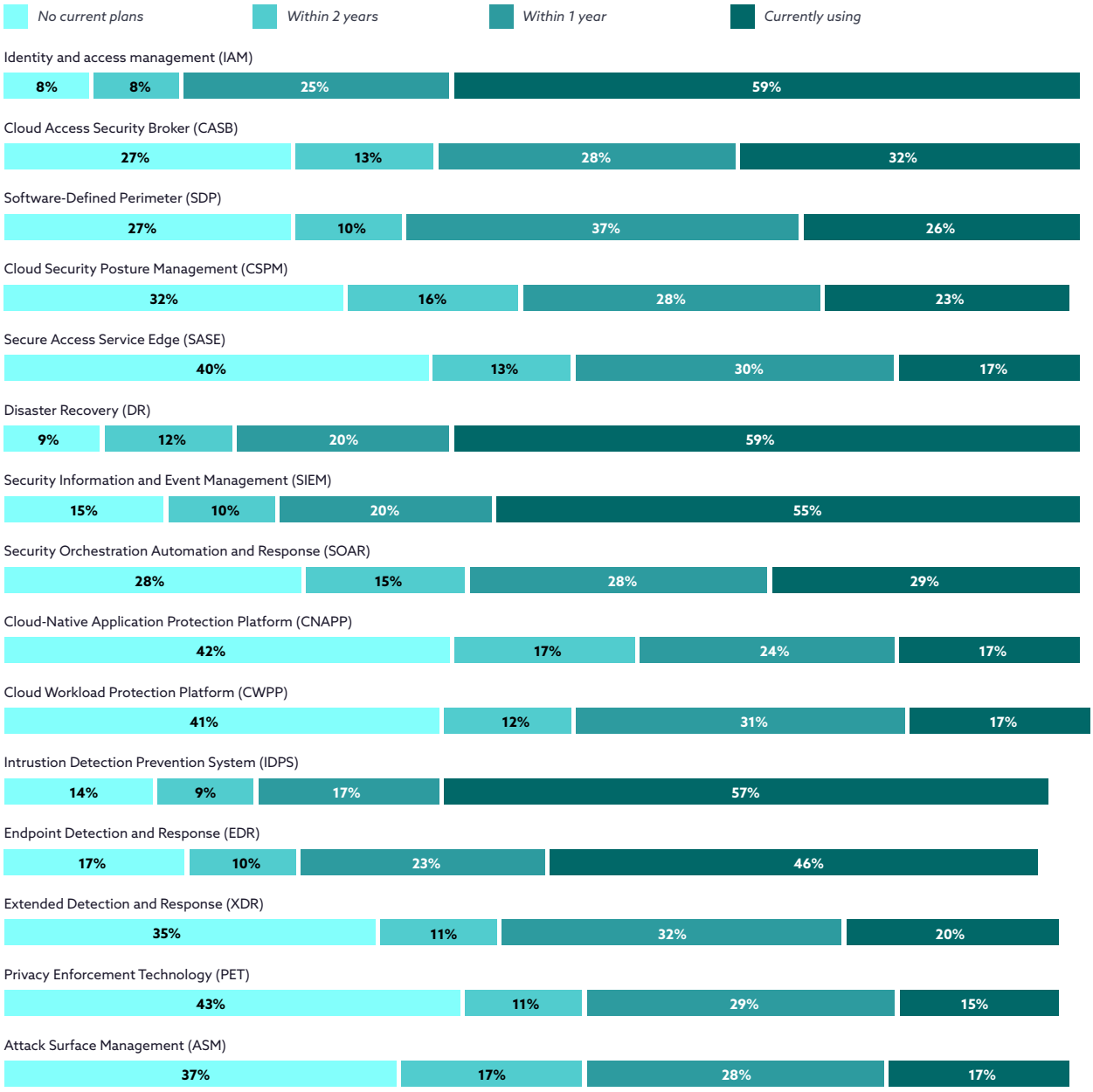
Current and Planned Use of Cloud Security Solutions

Organizations also indicated whether they were currently using or planning to use various cloud security solutions. The solutions most commonly reported to be in use currently are IAM (**59%**), Disaster Recovery (**59%**), Intrusion Detection Prevention Systems (**57%**), Security Information and Event Management (**55%**), and Endpoint Detection Response (**46%**).

The security solutions organizations most commonly reported they have no current plans to use include Privacy Enforcement Technology (43%), Cloud-Native Application Protection Platform (42%), Cloud Workload Protection Platform (41%), and Secure Access Service Edge (40%).

Note on IAM use: IAM capabilities that are expected to increase in use include:[5]

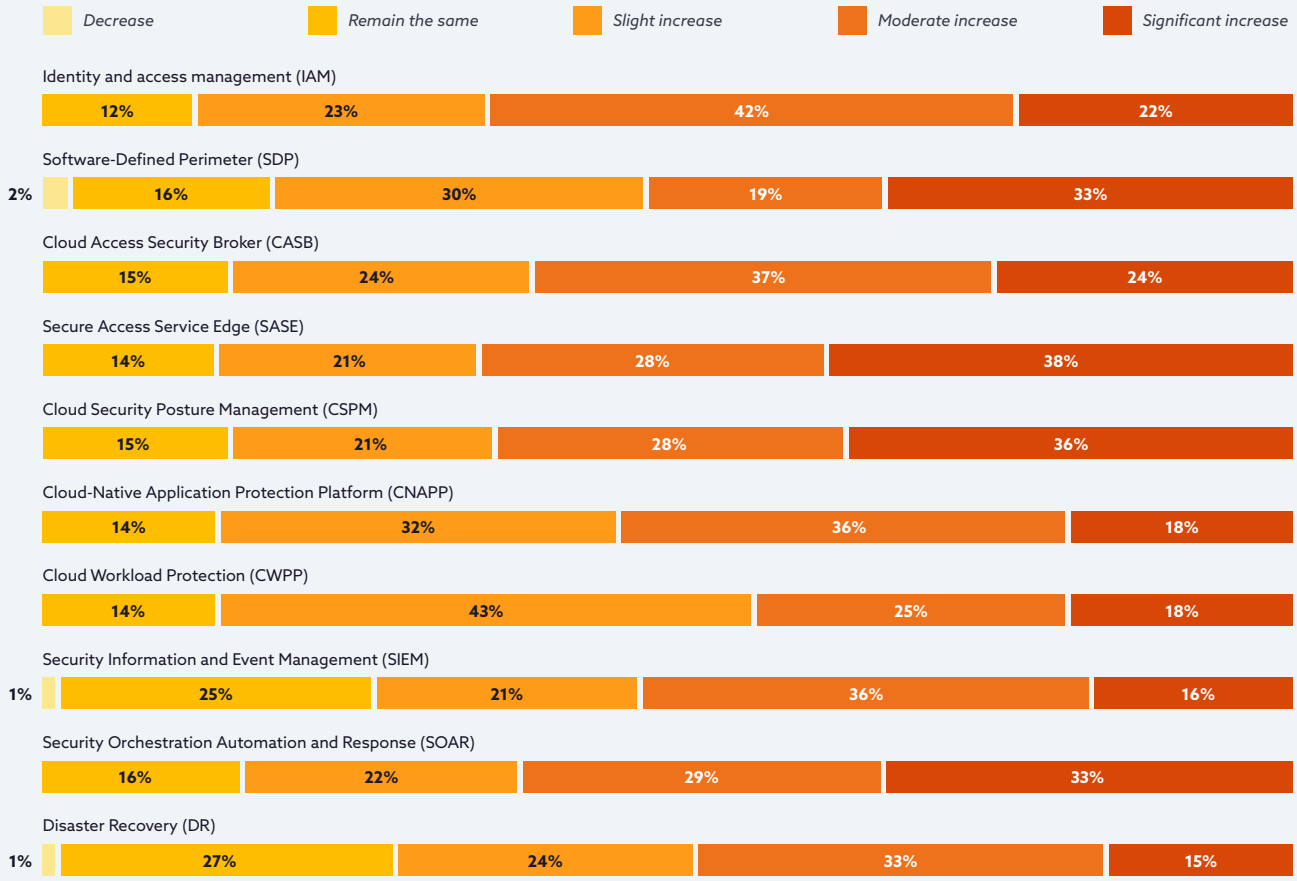
- MFA
- Federated identities
- Just-in-Time approach



[5] The 2020 State of Identity Security in the Cloud (2020). CSA.

Expected Change in Use of Cloud Security Services

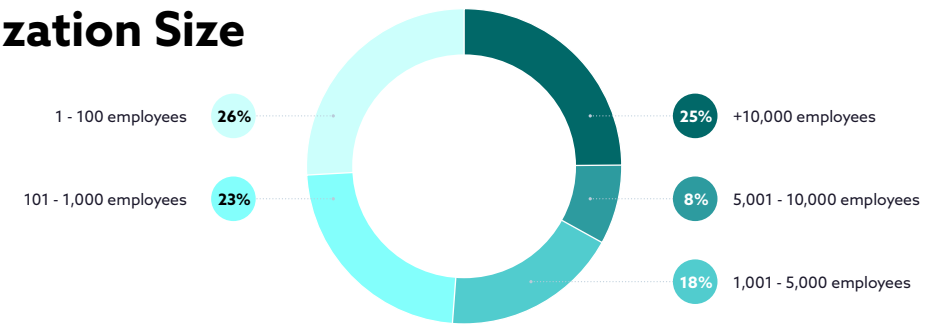
Current users of the cloud security services were asked to predict any changes in their use of these services over the next year. Overall, organizations expect to increase their use of all these cloud security services "slightly" to "significantly."



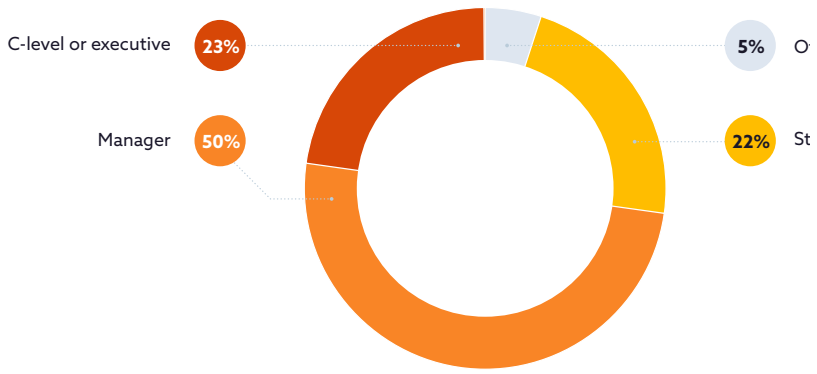
Demographics

This survey was conducted from October 2021 to November 2021 and gathered 256 responses from IT and security professionals from various organization sizes, industries, locations, and roles.

Organization Size

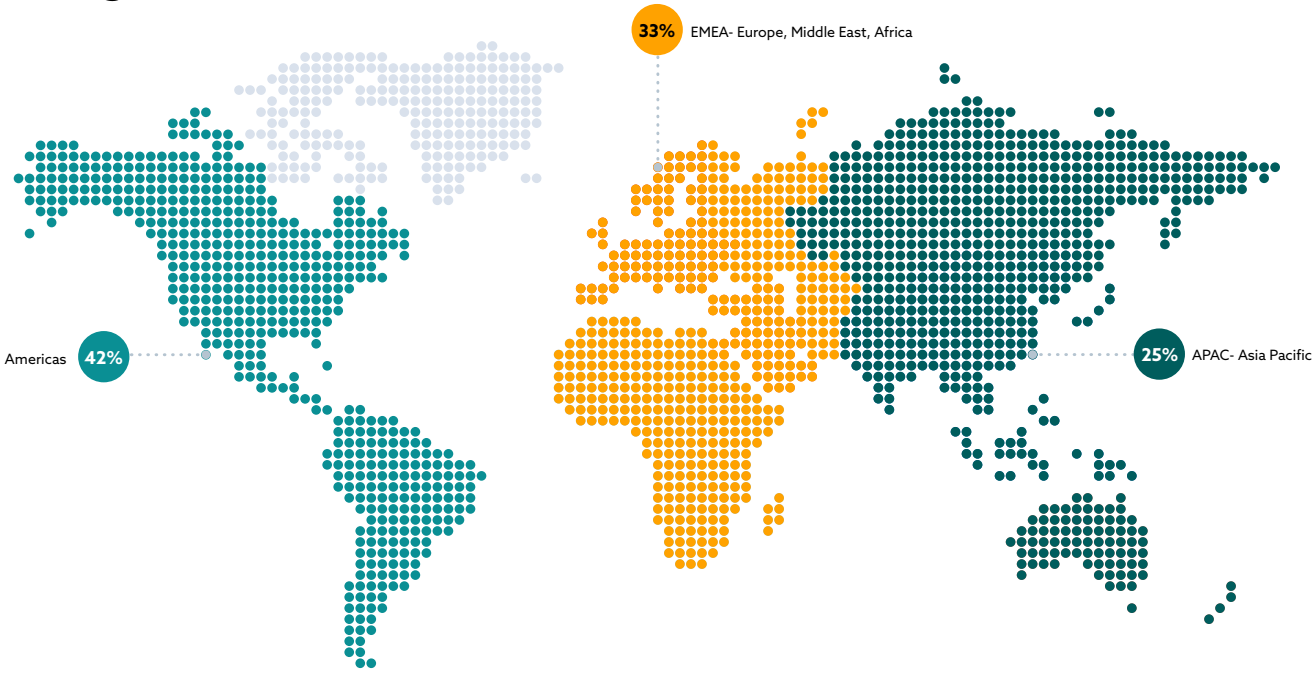


Primary Role



Organization Industry

Organization Location



About the Sponsor

CyberRes is a Micro Focus line of business. We bring the expertise of one of the world's largest security portfolios to help our customers navigate the changing threat landscape by building both cyber and business resiliency within their teams and organizations. We are here to help enterprises accelerate trust, reliability, and survivability through times of adversity, crisis, and business volatility.

We are a part of a larger set of digital transformation solutions that fight adverse conditions so businesses can continue to run today, keep the lights on, and transform to grow and take advantage of tomorrow's opportunities. Learn more at www.microfocus.com

Sponsors are CSA Corporate Members who support the research project's findings but have no added influence on the content development or editing rights of CSA research.