Cybersecurity INSIDERS

2023 Cloud Security Report

FORTINET®

INTRODUCTION

In 2023, the cloud is fundamentally delivering on its promised business outcomes, including flexible capacity and scalability, increased agility, improved availability, and accelerated deployment and provisioning.

However, security concerns remain a critical barrier to cloud adoption, showing little signs of improvement in the perception of cloud security professionals. Cloud adoption is further inhibited by a number of related challenges that prevent the faster and broader embracement of cloud services, including the continued lack of cloud security talent, proliferating compliance requirements, and the significant lack of visibility and control, especially in hybrid and multi-cloud environments.

This 2023 Cloud Security Report surveyed 752 cybersecurity professionals to reveal key challenges and priorities, including:

- Cloud security continues to be a significant issue, with 95% of surveyed organizations concerned about their security posture in public cloud environments. Misconfiguration remains the biggest cloud security risk, according to 59% of cybersecurity professionals. This is closely followed by exfiltration of sensitive data and insecure interfaces/APIs (tied at 51%), and unauthorized access (49%).
- Despite economic headwinds, cloud security budgets are increasing for the majority of organizations (60%) by an average of 33%.
- 44% of organizations are looking for ways to achieve better visibility and control in securing hybrid and multi-cloud networks, with 90% looking for a single cloud security platform to protect data consistently and comprehensively across their cloud footprint.

We would like to thank Fortinet 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

TABLE OF CONTENTS

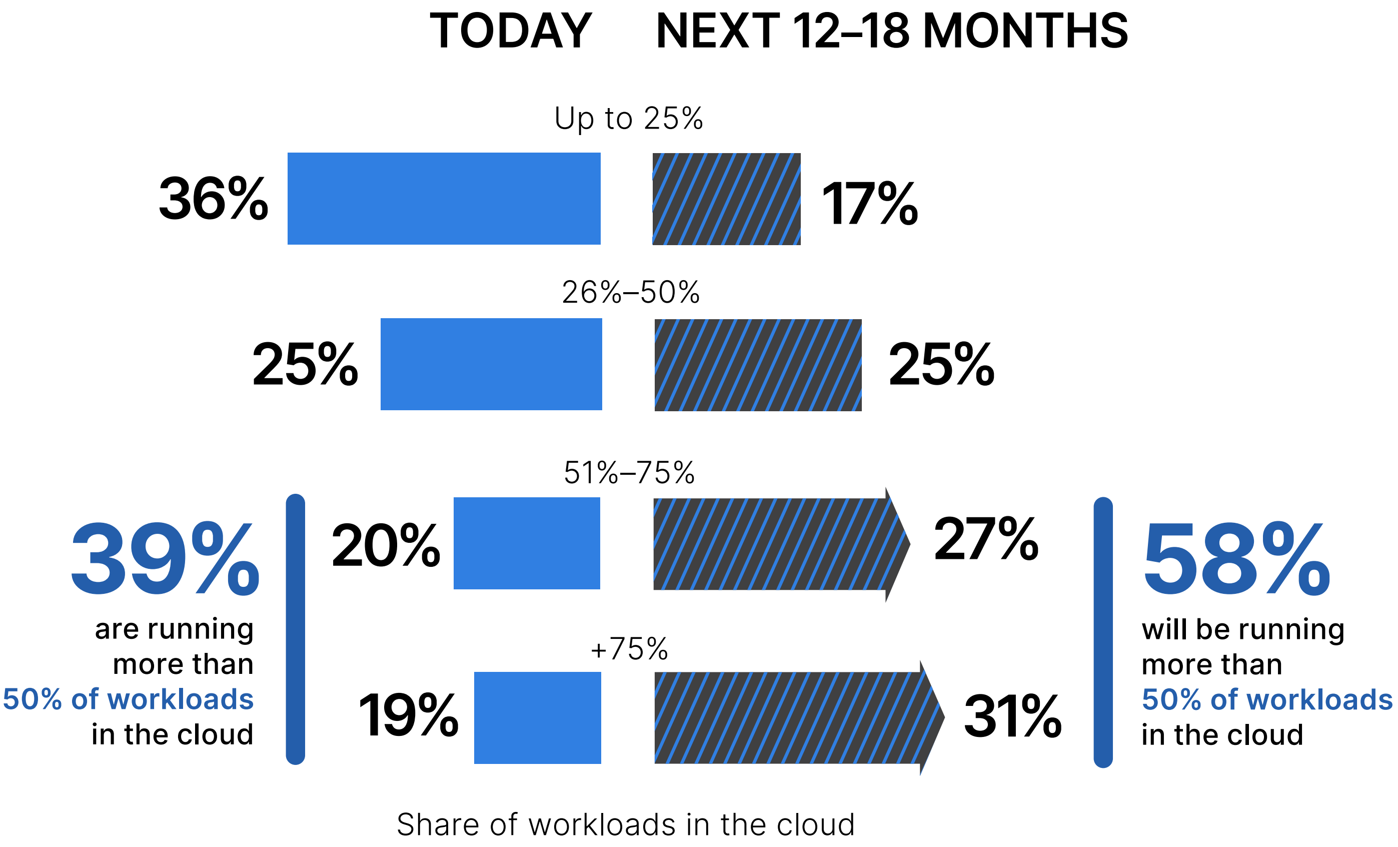
Current State of Cloud Adoption

WORKLOADS IN THE CLOUD

Despite a leveling out of cloud adoption year-over-year, the pace of moving workloads to the cloud remains strong. Today, 39% of respondents have more than half of their workloads in the cloud, while 58% plan to reach this level in the next 12–18 months.

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?

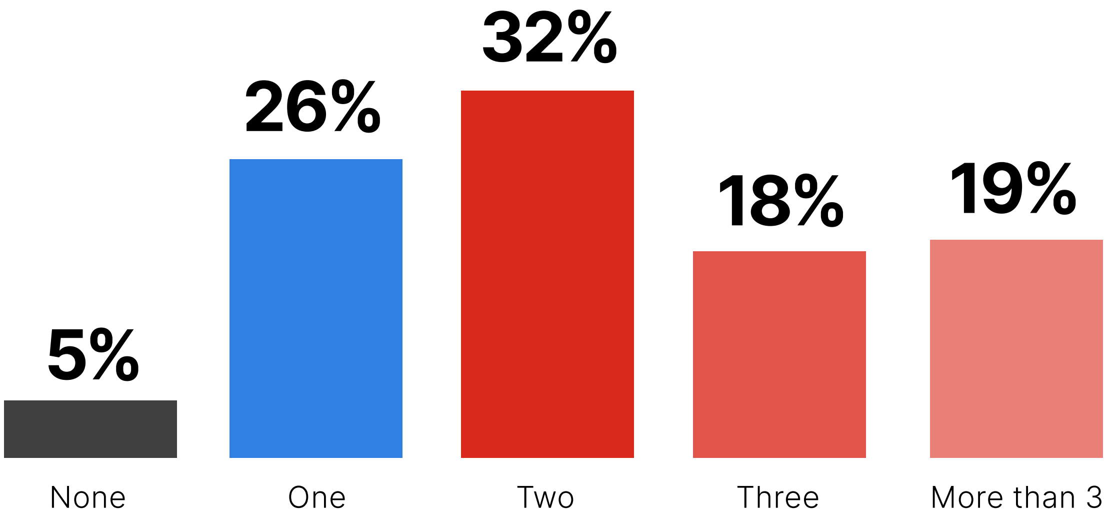


MULTI-CLOUD ADOPTION

As workloads move to the cloud, organizations are selecting the cloud platform that's the best fit for each project. This is driving multi-cloud proliferation with nearly seven out of 10 companies in our survey using two or more cloud providers (69%).

How many cloud providers does your organization currently use?

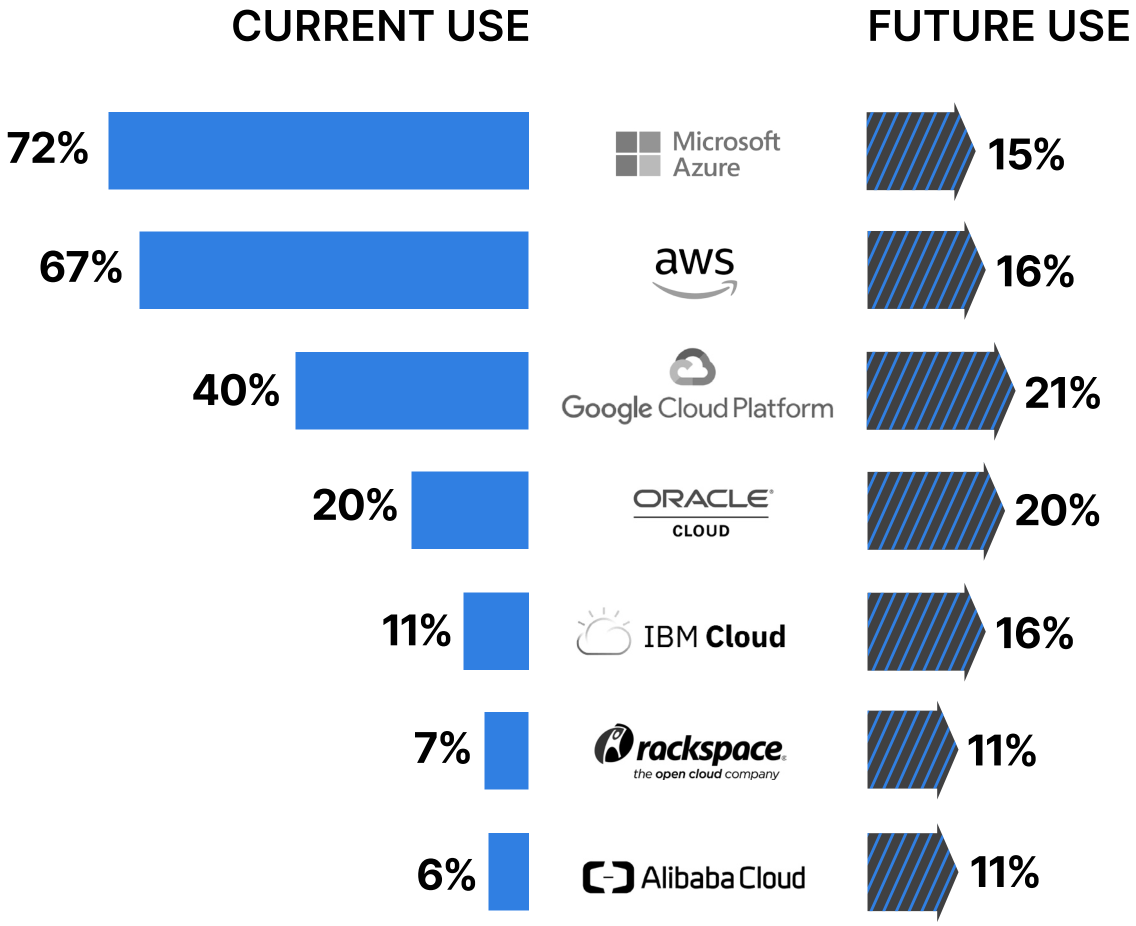
69% use two or more cloud providers



PREFERRED CLOUD PROVIDERS

Which cloud providers are organizations prioritizing? The big name providers, such as Microsoft Azure (72%) and Amazon Web Services (67%), continue to dominate the market. However, future cloud adoption is highest for Google Cloud Platform (+21%) and Oracle Cloud (+20%).

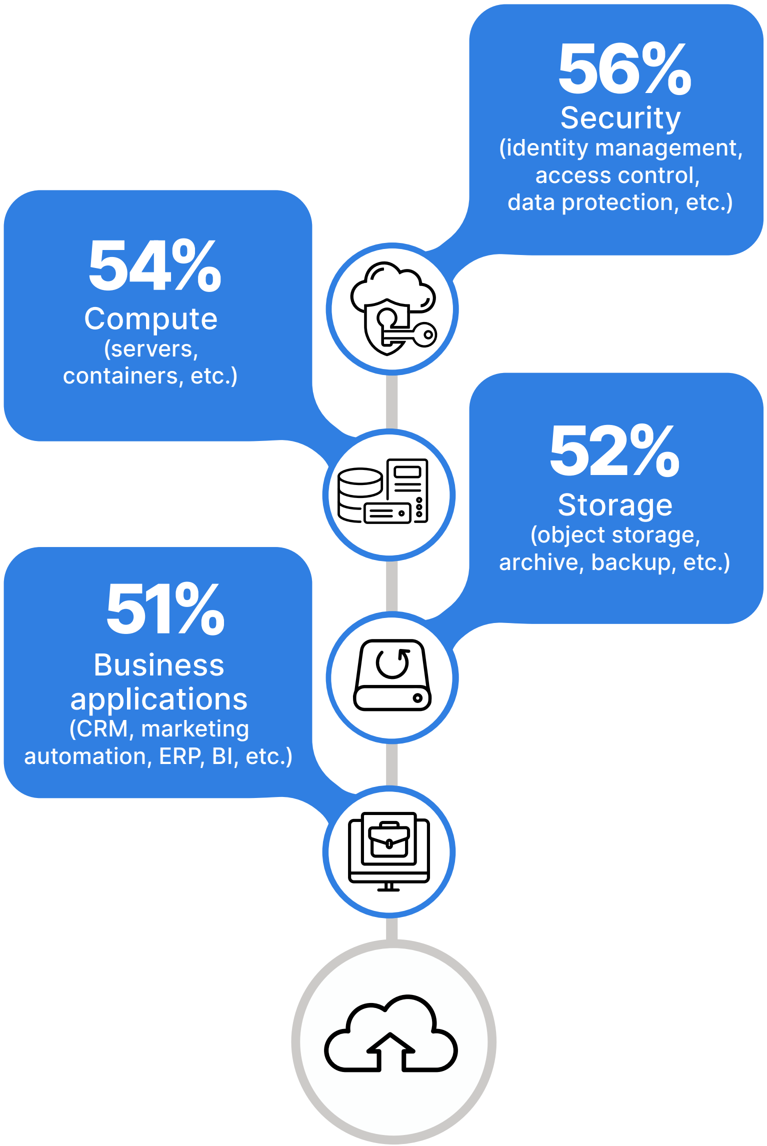
What cloud IaaS provider(s) do you currently use or plan to use in the future?



CLOUD SERVICES PRIORITIES

It seems the cloud is not just about compute and storage. Interestingly, security services are the top workload deployed in the cloud (56%), just ahead of compute (54%), storage (52%), and even applications (51%).

What services and workloads is your organization deploying in the cloud?



56% Security (identity management, access control, data protection, etc.)

54% Compute (servers, containers, etc.)

52% Storage (object storage, archive, backup, etc.)

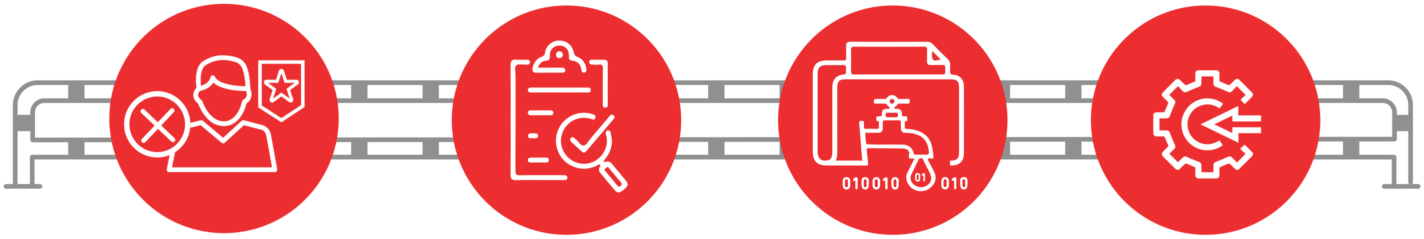
51% Business applications (CRM, marketing automation, ERP, BI, etc.)

Productivity applications (email, collaboration, instant messaging, etc.) 50% | Virtualization 49% | Database (relational, NoSQL, caching, etc.) 46% | IT operations applications (administration, backup, provisioning, monitoring, etc.) 45% | Developer/testing applications 40% | Networking and content delivery (virtual private cloud, DNS, etc.) 38% | Operating system 34% | Desktop and application streaming 22% | Middleware 22% | Runtime 14% | Don't know/other 6%

BARRIERS TO CLOUD ADOPTION

While the cloud offers important advantages, significant barriers to cloud adoption still exist. The biggest challenges organizations are facing are not primarily about technology, but people and processes. Most critical is the perennial lack of qualified staff (37%), which continues to be the largest impediment to faster adoption, despite dropping slightly from last year. This is closely followed by legal and regulatory compliance (30%), data security issues (29%), and integration with existing IT environments (27%).

What are the biggest barriers holding back cloud adoption in your organization?



37% Lack of staff resources or expertise

30% Legal and regulatory compliance

29% Data security, loss, and leakage risks

27% Integration with existing IT environment

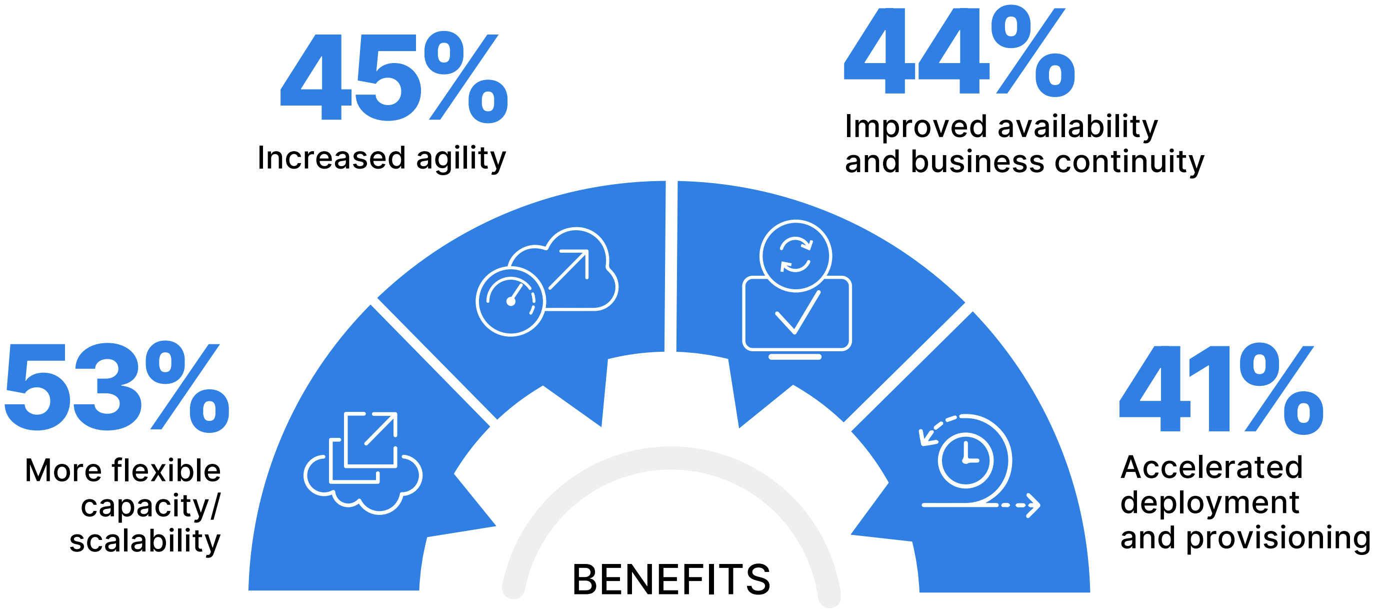
Fear of vendor lock-in 24% | General security risks 23% | Lack of budget 22% | Cost/lack of ROI 21% | Internal resistance and inertia 20% | Loss of control 19% | Complexity managing cloud deployment 18% | Lack of transparency and visibility 15% | Billing and tracking issues 14% | Lack of maturity of cloud service models 13% | Lack of management buy-in 13% | Dissatisfaction with cloud service offerings/performance/ pricing 12% | Lack of customizability 10% | Lack of support by cloud provider 8% | Performance of apps in the cloud 8% | Availability 8% | Other 5%

Benefits of the Cloud

KEY CLOUD BENEFITS

After years of cloud adoption, do organizations believe cloud computing is delivering on its promise? The answer is yes. Cloud users affirm that the cloud is delivering key business benefits, including flexibility and scale (53%), agility (45%), business continuity (44%), and accelerated deployment and provisioning (41%). This is the first year that accelerated deployment has made it into the top four, leapfrogging both performance and the move to variable OpEx.

What overall benefits have you already realized from your cloud deployment?

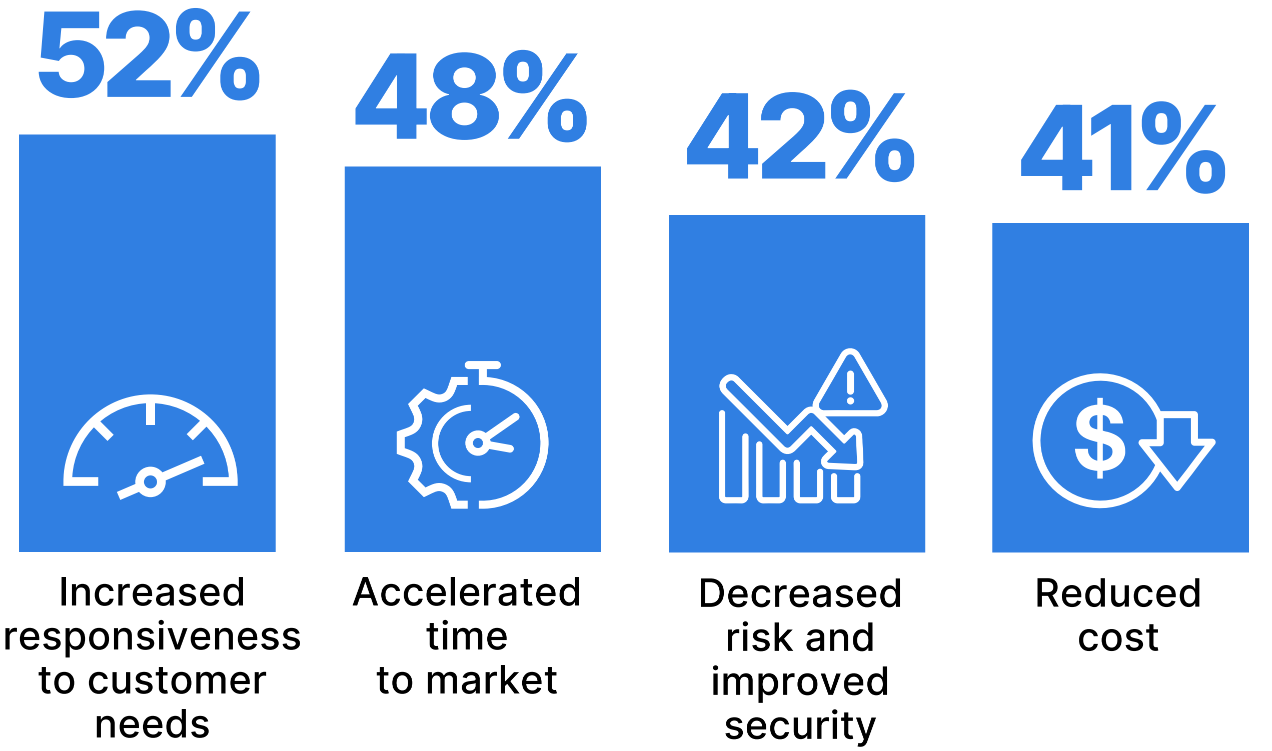


Improved performance 36% | Accelerated time to market 34% | Moved expenses from fixed CapEx (purchase) to variable OpEx (rental/ subscription) 34% | Reduced cost 32% | Improved security 32% | Increased geographic reach 27% | Increased employee productivity 25% Reduced complexity 23% | Improved regulatory compliance 22% | Not sure/other 12%

CLOUD BUSINESS OUTCOMES

The benefits of the cloud are driving key business outcomes, and this year responsiveness to customer needs (52%) becomes the top outcome instead of accelerated time to market (48%). Organizations that are smart about integrating cybersecurity into their move to the cloud are also seeing its value to the business in lower risk and improved security (42%) and in cost reductions (41%).

What business outcomes have you realized by moving to the cloud?



Expanded market reach to new markets 23% | Accelerated revenue growth in existing markets 22% | Achieved parity with competitors 22% | Other 7%

Security Challenges in the Cloud

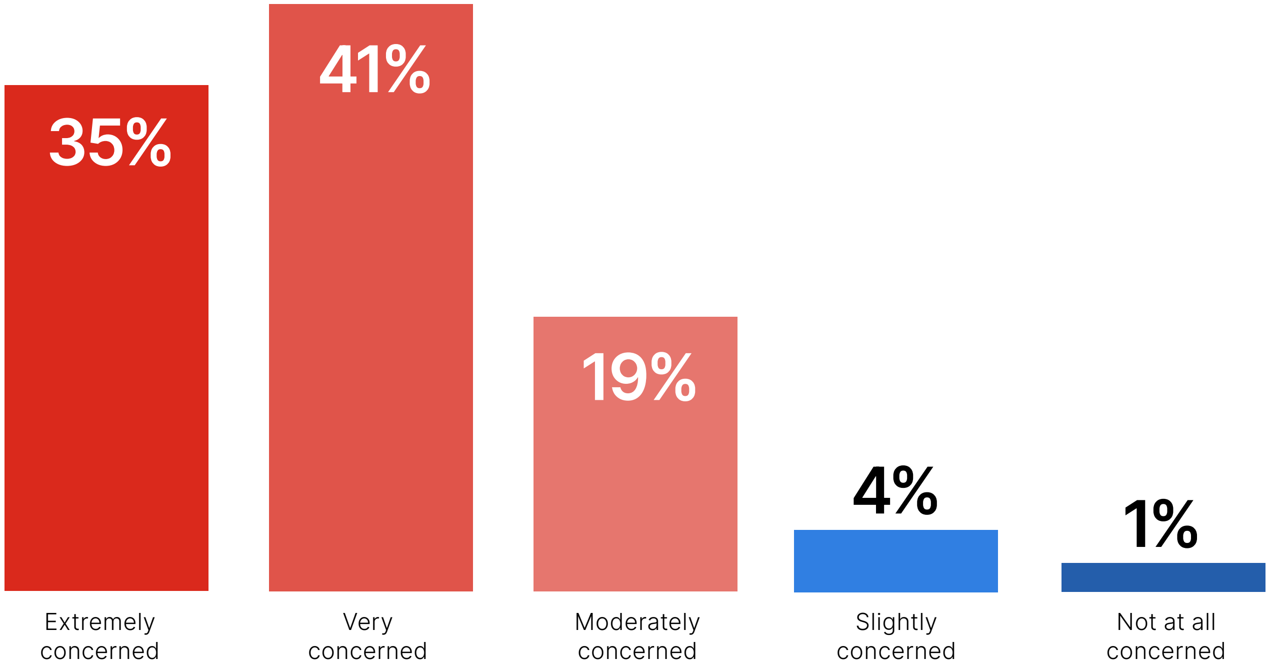
PUBLIC CLOUD SECURITY CONCERNS

Despite increasing cloud adoption, cloud security concerns show no signs of improving. Virtually all surveyed organizations are moderately to extremely concerned about their security posture in public cloud environments (95%). The number of organizations that are extremely concerned about public cloud security even increased this year — 35%, up from 32%.

How concerned are you about the security of public clouds?

95%

of organizations are moderately to extremely concerned about cloud security



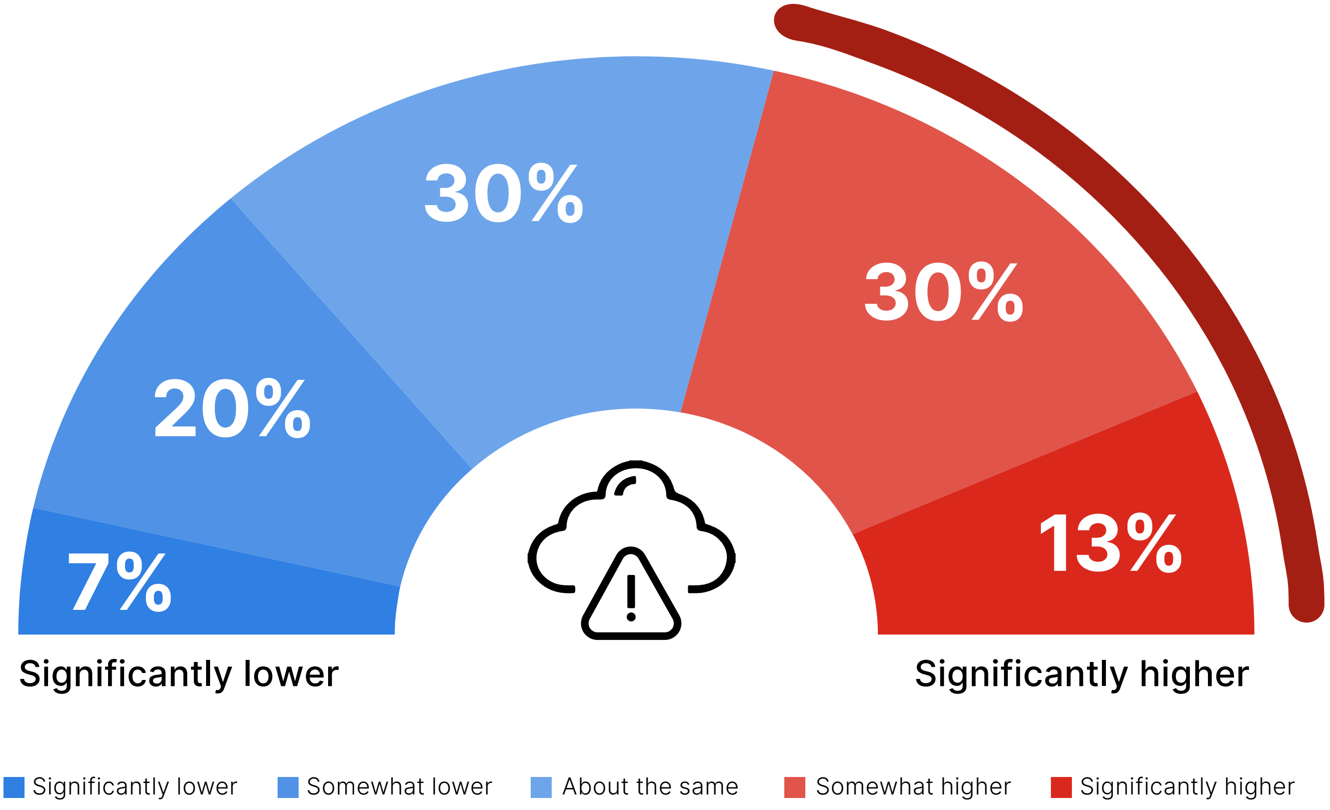
RISK OF A BREACH

Concerns about public cloud security, combined with a lack of resources and expertise, are driving the perception that the risk of a security breach in the public cloud is higher than in traditional on-premises environments (43%). Only 27% of security professionals perceive risk to be lower in a public cloud environment.

Compared to traditional, on-premises IT environments, would you say the risk of security breaches in a public cloud environment is higher or lower?

43%

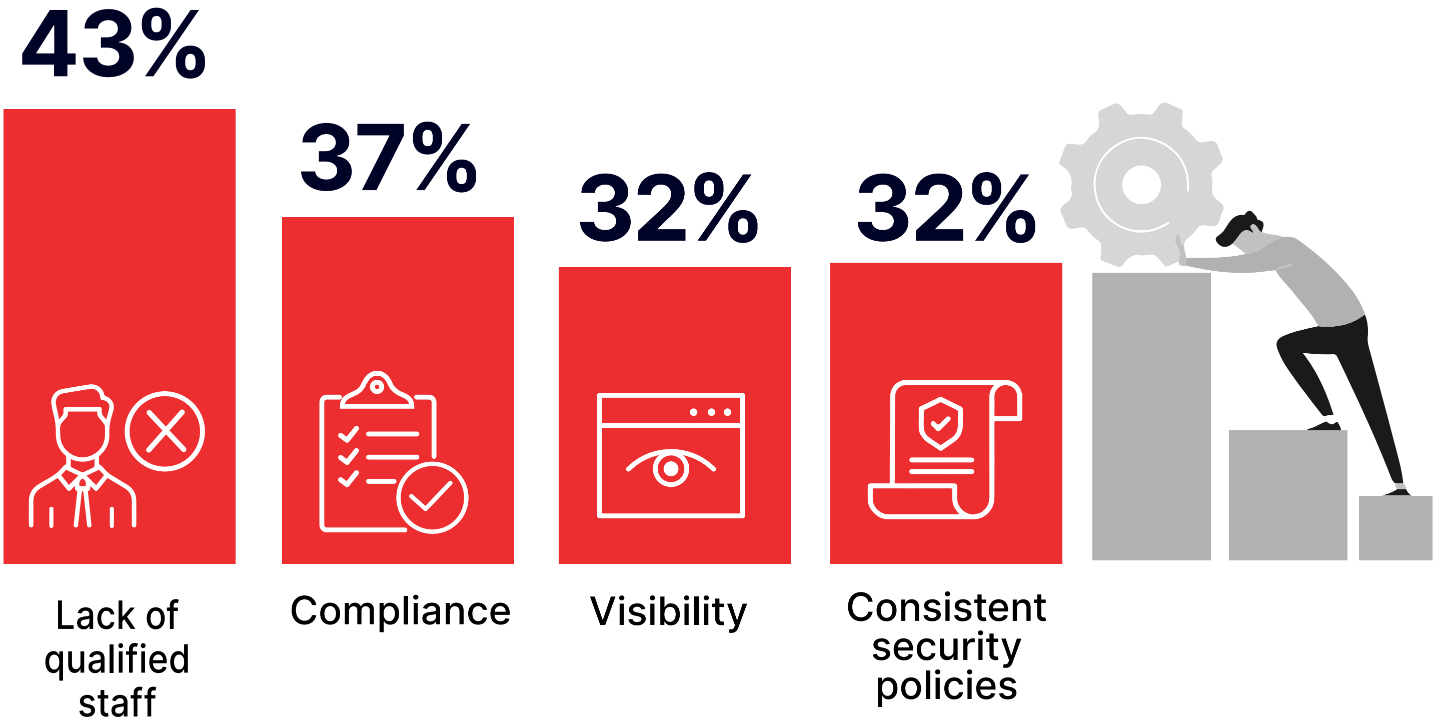
say public cloud risk is somewhat to significantly higher than on-premises



OPERATIONAL SECURITY HEADACHES

Cybersecurity professionals face numerous challenges when it comes to protecting cloud workloads. The people factor again sits at the top of the list, lack of qualified security staff (43%), closely followed by compliance (37%). Multi-cloud proliferation is almost certainly the reason behind the headache of delivering consistent security policies (32%).

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

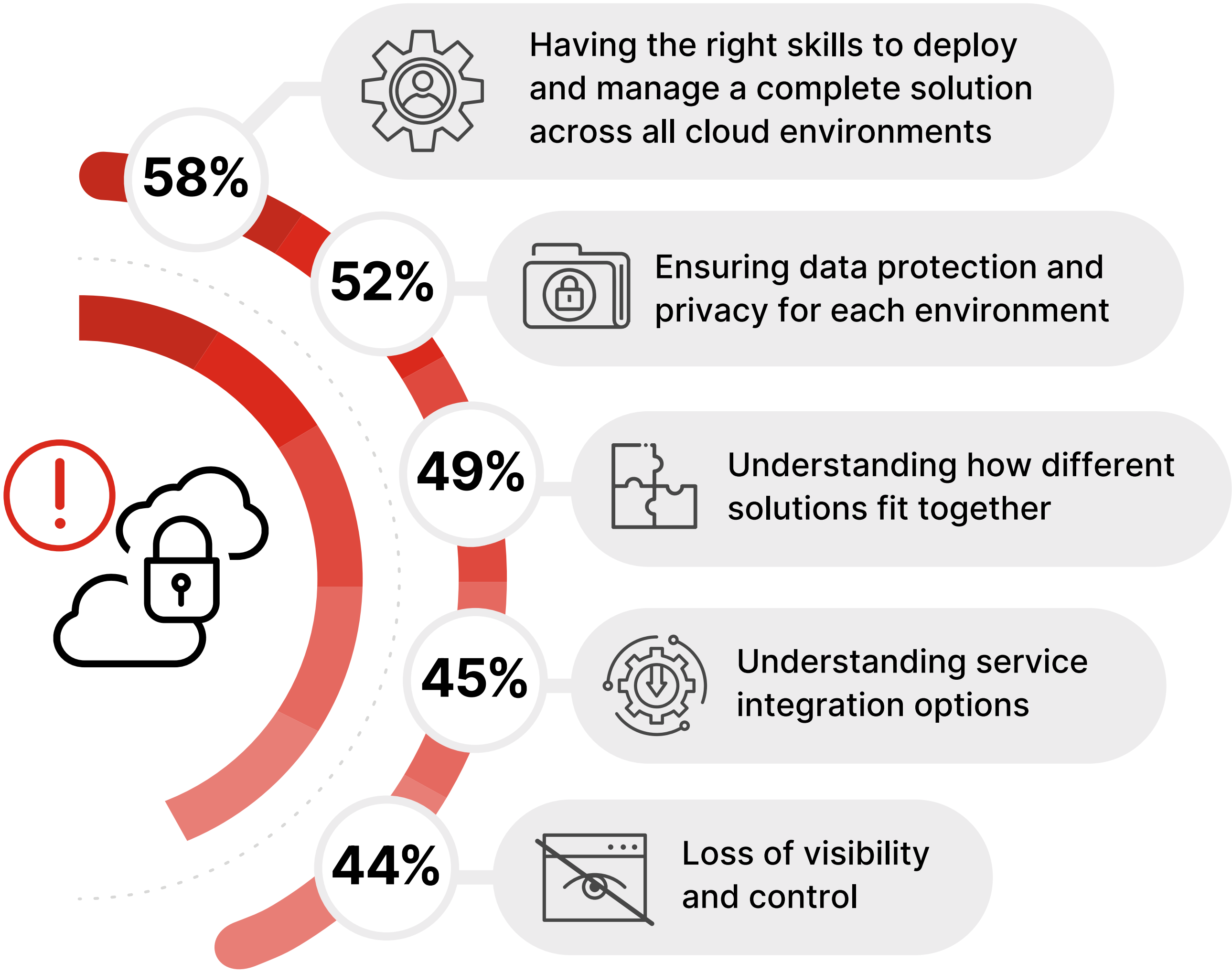


Controls and automation 30% | Can't identify misconfigurations quickly 29% | Automatically enforcing security across multiple clouds 29% | Complex cloud to cloud/cloud to on-premises security rule matching 25% | Securing traffic flows 25% | Securing access from personal and mobile devices 25% | Security can't keep up with the pace of changes to new/existing applications 25% | Lack of integration with on-premises security technologies 25% | Setting the correct user access privileges 24% | Remediating threats 24% | Justifying more security spending 24% | Understanding network traffic patterns 23% | No automatic discovery/visibility/control to infrastructure security 22% | Reporting security threats 21% | Lack of feature parity with on-premises security solution 21% | No flexibility 6% | Not sure/other 10%

MULTI-CLOUD SECURITY CHALLENGES

Multi-cloud environments increase the complexity and challenges of securing cloud workloads. The people factor and the expertise that multi-cloud environments demand is clearly highlighted in the fact that three out of the four top challenges are related to having the right skills, along with an in-depth understanding of each cloud platform.

What are your biggest challenges securing multi-cloud environments?



58% Having the right skills to deploy and manage a complete solution across all cloud environments

52% Ensuring data protection and privacy for each environment

49% Understanding how different solutions fit together

45% Understanding service integration options

44% Loss of visibility and control

Keeping up with the rate of change 38% | Managing the costs of different solutions 37% | Providing seamless access to users based on their credentials 37% | Selecting the right set of services 36% | Other 3%

CLOUD SECURITY THREATS

Which cloud security threats keep cybersecurity professionals up at night? The same top four as last year, with misconfiguration continuing to hold the top spot, according to 59% of cybersecurity professionals. This is closely followed by the exfiltration of sensitive data and insecure interfaces/APIs (tied at 51%), and unauthorized access (49%).

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

59% Misconfiguration of the cloud platform/wrong setup

51% Exfiltration of sensitive data

51% Insecure interfaces/APIs

49% Unauthorized access

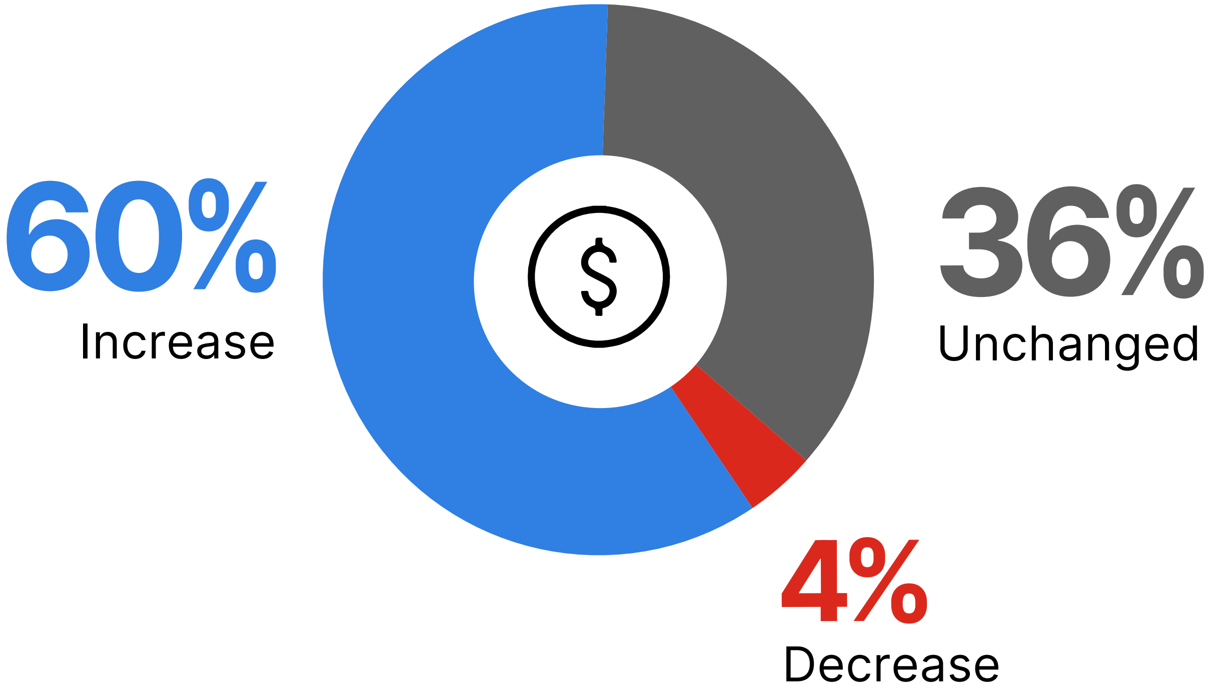
Hijacking of accounts, services, or traffic 45% | External sharing of data 39% | Malicious insiders 38% | Malware/ransomware 37% | Foreign state-sponsored cyberattacks 37% | Denial of service attacks 31% | Cloud cryptojacking 21% | Theft of service 20% | Lost mobile devices 13% | Don't know/other 7%

Key Priorities for Cloud Security

CLOUD BUDGET

Despite macroeconomic headwinds and a slowdown in workloads moving to the cloud compared to years past, most organizations (60%) will see a boost in their cloud security budget this year. That boost is expected to be a 33% increase in spending power year-over-year.

How is your cloud security budget changing in the next 12 months?



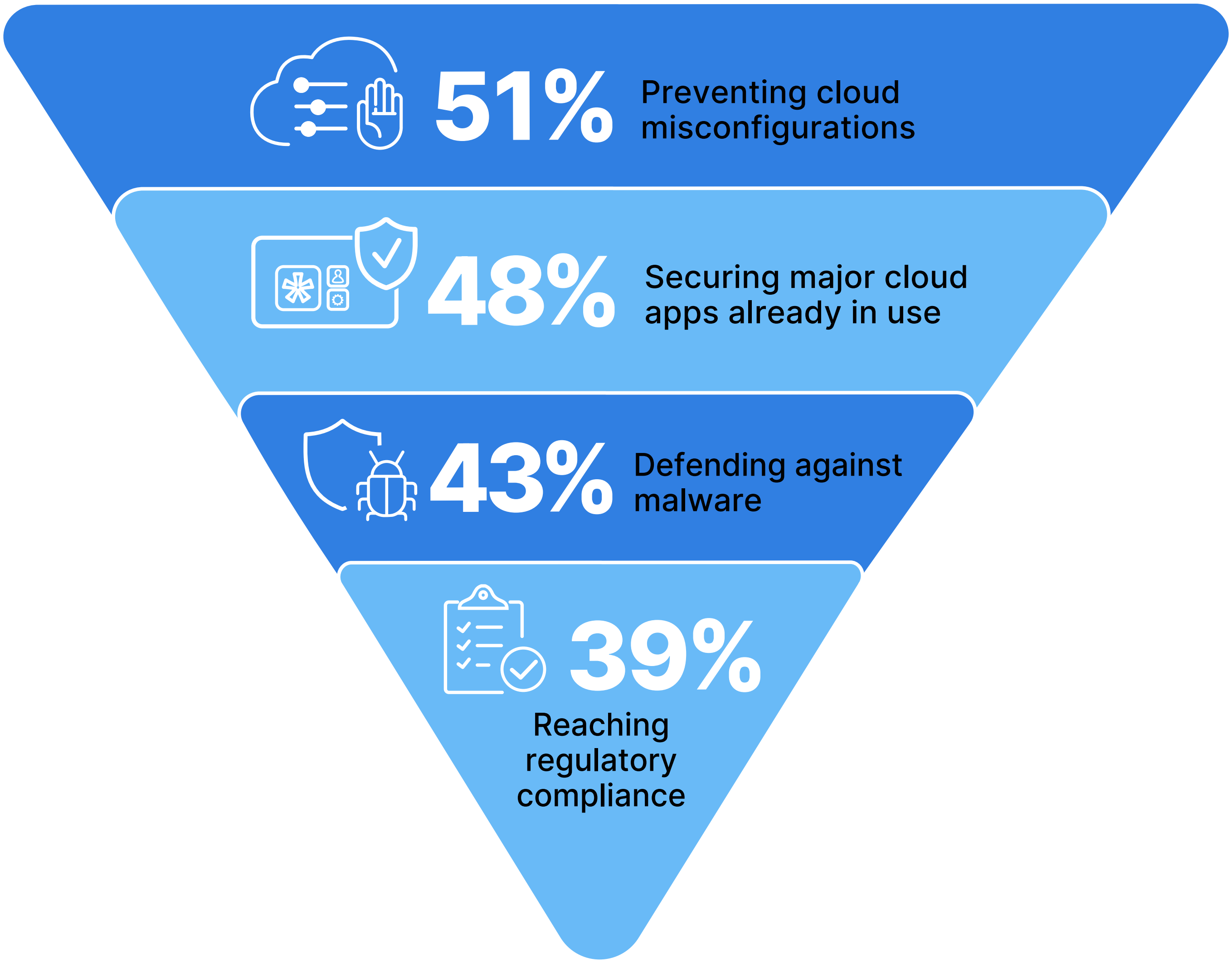
If the budget for your security program will increase, indicate by what percentage?

Budget will increase by 33%

CLOUD SECURITY PRIORITIES

Security professionals are using their cloud budgets wisely to address the threats and concerns that pose the biggest risk to the business. It may be no surprise that preventing misconfiguration is the number one priority (51%), but securing applications that have already moved to the cloud is a close second (48%).

What are your cloud security priorities for your company this year?

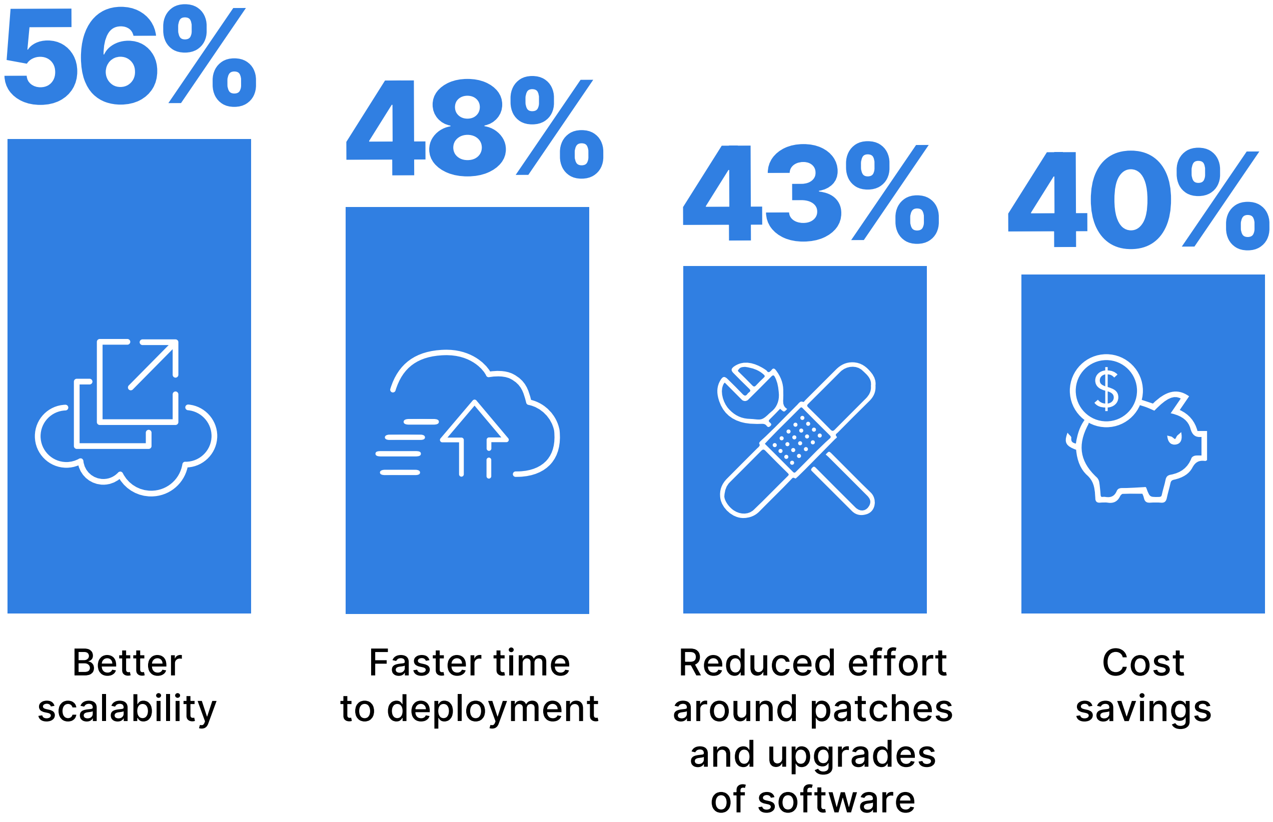


Cloud security training 12% | Securing mobile devices 7% | Discovering unsanctioned cloud apps in use 7% | Securing BYOD (bring your own device) 5% | Securing less popular cloud apps already in use 4%

KEY DRIVERS FOR CLOUD-BASED SECURITY

The cloud allows organizations to get the same advantages for their security services as they have for their applications and workloads. This includes better scalability (56%), faster time to deployment (48%), reduced effort around patches and upgrades of software (43%), and cost savings (40%).

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



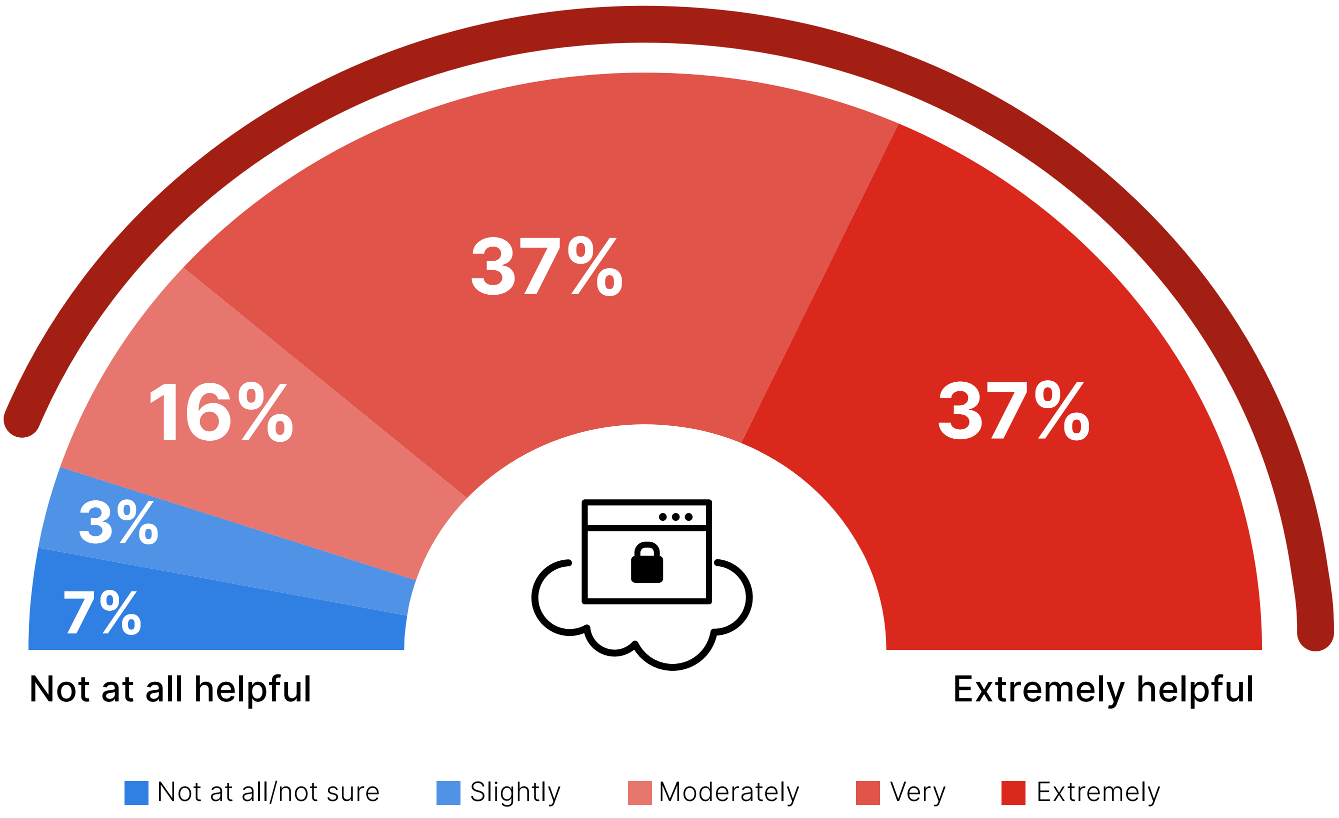
Better visibility into user activity and system behavior 38% | Better uptime 36% | Easier policy management 35% | Meet cloud compliance expectations 35% | Better performance 35% | Need for secure app access from any location 34% | Our data/workloads reside in the cloud (or are moving to the cloud) 30% | Reduction of appliance footprint in branch offices 29% | Other 3%

SINGLE CLOUD SECURITY PLATFORM

In light of the challenges regarding security visibility and lack of cyber talent, it comes as no surprise that the vast majority of respondents (90%) consider it moderately to extremely helpful to have a single cloud security platform and dashboard to protect data consistently and comprehensively across their cloud footprint.

How helpful would it be to have a single cloud security platform with a single dashboard where you could configure all of the policies needed to protect data consistently and comprehensively across your cloud footprint?

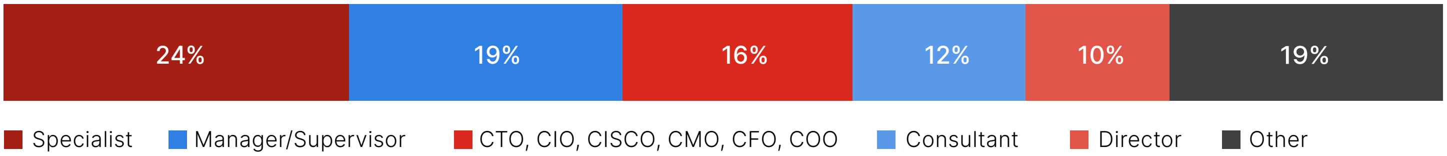
90% of professionals consider the use of a single cloud security platform with a single dashboard to be moderately to extremely helpful



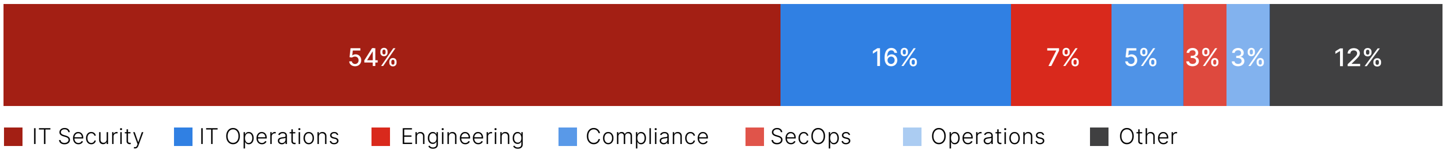
METHODOLOGY
& DEMOGRAPHICS

The 2023 Cloud Security Report is based on a comprehensive global survey of 752 cybersecurity professionals conducted in February 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.

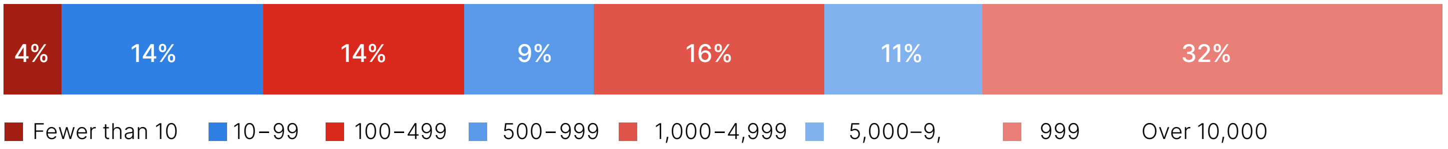
CAREER LEVEL



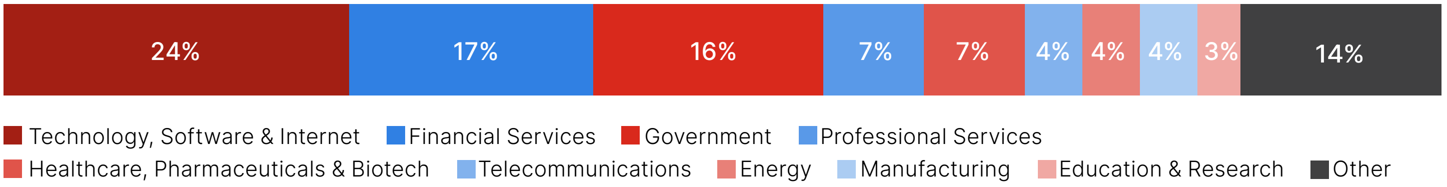
DEPARTMENT



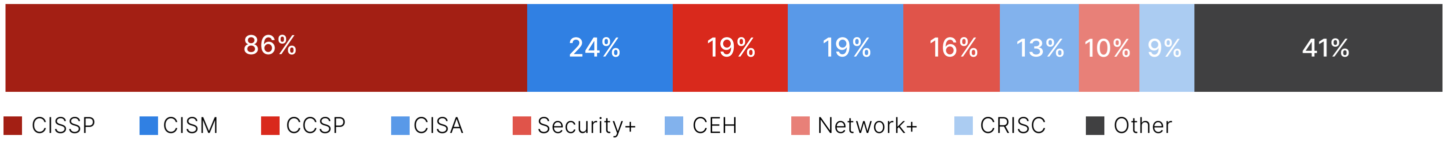
COMPANY SIZE



INDUSTRY



SECURITY CERTIFICATIONS HELD



FORTINET®

Fortinet (NASDAQ: FTNT) secures the largest enterprises, services providers, and government organizations around the world. Fortinet empowers our customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and into the future. Only the Fortinet Security Fabric platform can address the most critical security challenges and protect data across the entire digital infrastructure, whether in networks, application, multi-cloud, or edge environments. Fortinet ranks #1 as the company with the most security appliances shipped worldwide and more than 635,000 customers trust Fortinet to protect their businesses.

www.fortinet.com

Cybersecurity
INSIDERS

Cybersecurity Insiders is a 500,000+ 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