2021

Cybersecurity INSIDERS

AWS CLOUD SECURITY REPORT

CloudPassage

A Fidelis Cybersecurity Company

INTRODUCTION

Cloud security concerns remain high as the adoption of public cloud computing continues to surge in the wake of the COVID crisis and the resulting massive shift to remote work environments.

The 2021 AWS Cloud Security Report is based on a comprehensive survey of 316 cybersecurity professionals to uncover how AWS user organizations are responding to new security threats in the cloud, and what tools and best practices cybersecurity leaders are prioritizing in their move to the cloud.

This year's survey saw some significant changes in how organizations manage remediation of security and compliance issues with system owners. The reported remediation cadences of real-time, ad-hoc, and before-audit fire drills all declined between 10 and 13 percentage points since 2020. While the numbers for quarterly and weekly remediation cadences stayed the same, these declines indicate positive process improvements.

Key survey findings include:

- More than nine out of ten cybersecurity professionals (95%) confirm they are extremely to moderately concerned about public cloud security.
- Misconfiguration of the cloud platform remains the top concern (71%). Exfiltration of sensitive data came in second (59%), followed by insecure APIs (54%).
- Periodic vulnerability and compliance reports are still the primary method for organizations (58%) to communicate with system owners about security and compliance issues needing remediation. This is followed by automatically opened tickets (47%) using tools such as Jira, ServiceNow, etc.
- Organizations increasingly embrace hybrid cloud (44%) and multi-cloud deployments (43%) for planned redundancy because of commitments to legacy applications in traditional data centers. Single cloud deployments (11%) continue to diminish in importance. Ninety percent of organizations use more than two cloud providers.
- When selecting a cloud security provider, organizations prioritize cost-effectiveness (66%), scalability (52%), ease of deployment (51%), and tools that can be deployed with automation (48%) as the top four criteria.

We would like to thank CloudPassage for supporting this important industry research project.

We hope you find this report informative and helpful as you continue your efforts in securing your journey into the cloud.

Thank you,

Holger Schulze

Holger Schulze

CEO and Founder
Cybersecurity Insiders

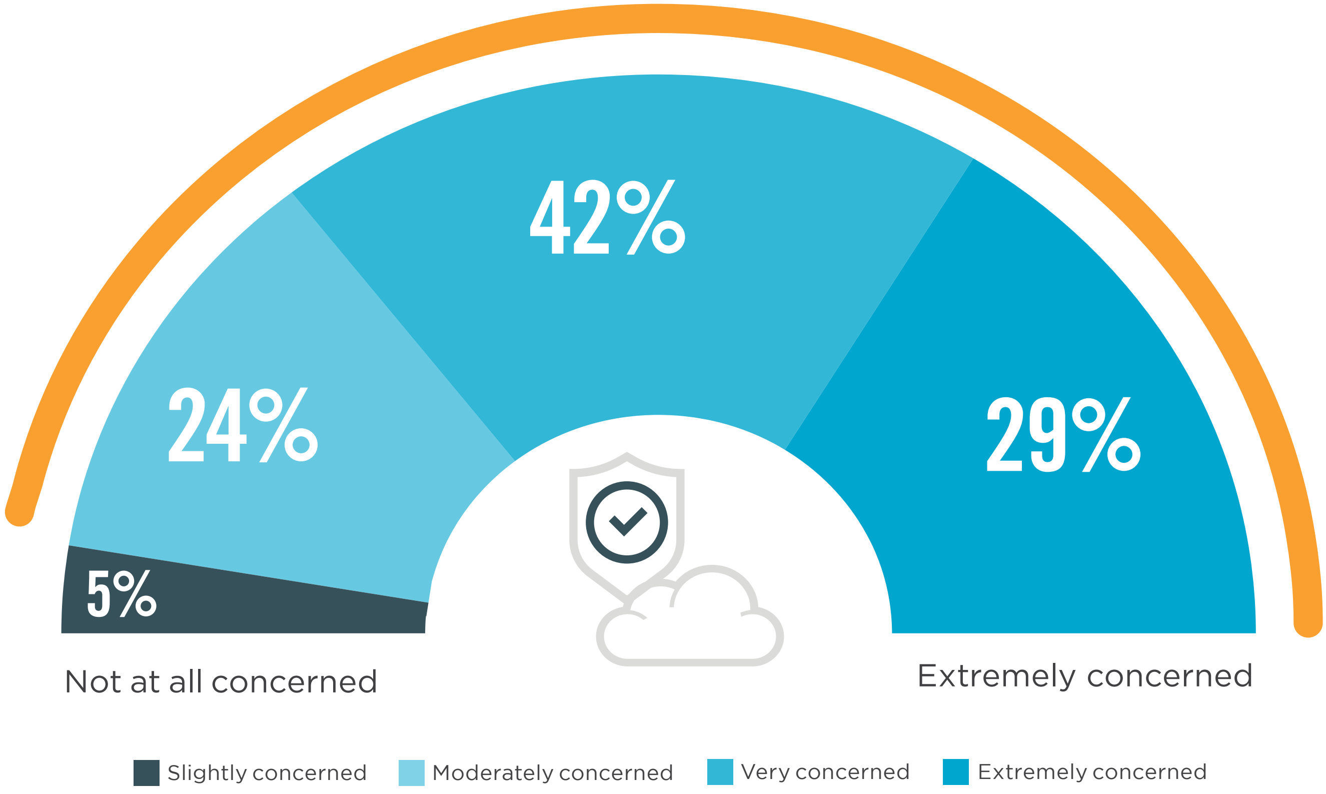
Cybersecurity INSIDERS

PUBLIC CLOUD SECURITY CONCERNS

Cloud security concerns are improving somewhat but remain high as the adoption of public cloud computing continues to surge in the wake of the COVID crisis and the resulting shift to remote work environments. Ninety-five percent of cybersecurity professionals confirm they are extremely to moderately concerned about public cloud security.

▶ How concerned are you about the security of public clouds?

95% of organizations are concerned about cloud security



CLOUD SECURITY CONCERNS

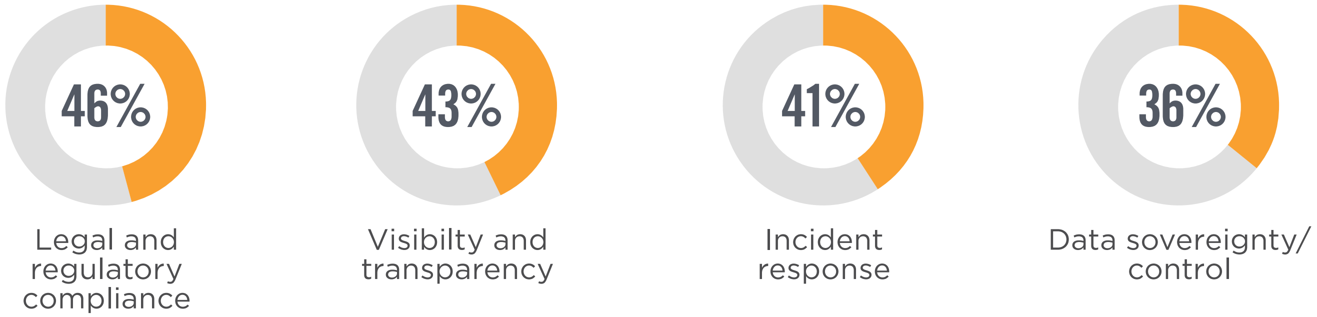
Despite the increasing security measures already offered by cloud providers, such as Amazon Web Services, cloud users are ultimately responsible for securing their own workloads in the cloud. When asked about their biggest cloud security challenges, cybersecurity professionals in our survey are highlighting the risk of data loss and leakage (67%), threats to data privacy (61%), and accidental exposure of credentials (49%) as the top three security concerns.

What are your biggest cloud security concerns?

67% Data loss/ leakage

61% Data privacy/ confidentiality

49% Accidental exposure of credentials



Lack of forensic data 26% | Business continuity 24% | Liability 23% | Availability of services, systems, and data 22% | Having to adopt new security tools 21% | Disaster recovery 20% | Performance 18% | Fraud (i.e., theft of SSN records) 17% | Not sure/other 4%

BIGGEST CLOUD SECURITY THREATS

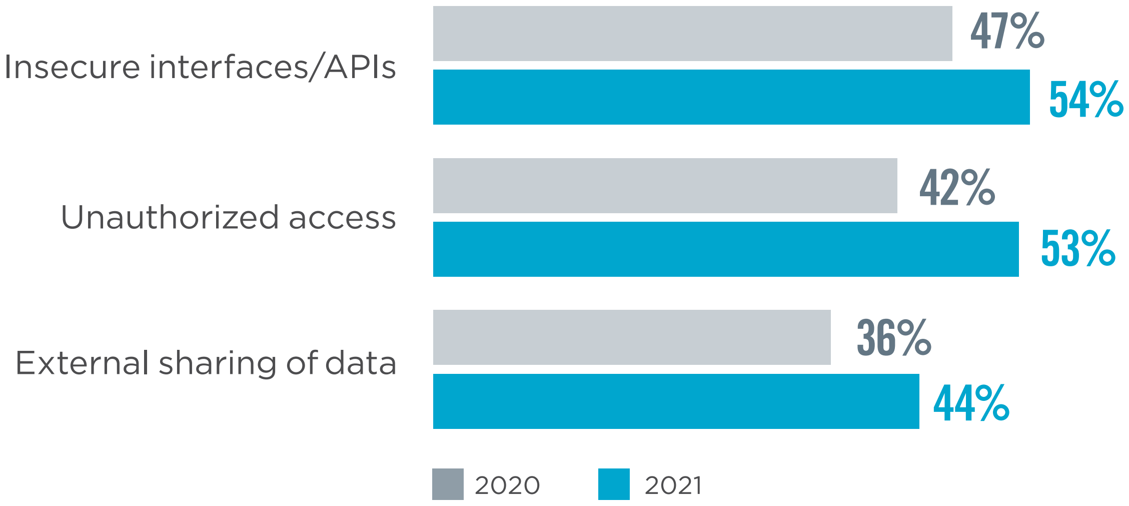
This year, we are observing some shifts in what security professionals see as the biggest cloud security threats. While misconfiguration of the cloud platform/wrong set-up remains the top concern (71% from 49% in 2020), exfiltration of sensitive data rose to second place (59%). This is followed by insecure APIs (54%, up from 47%), moving from the second highest concern to third place. Unauthorized access dropped from third to fourth place (53%) while external sharing of data remained in fifth place (44%).

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

71%
Misconfiguration of the cloud platform/wrong set-up

An increase of 22% from last year

59%
Exfiltration of sensitive data

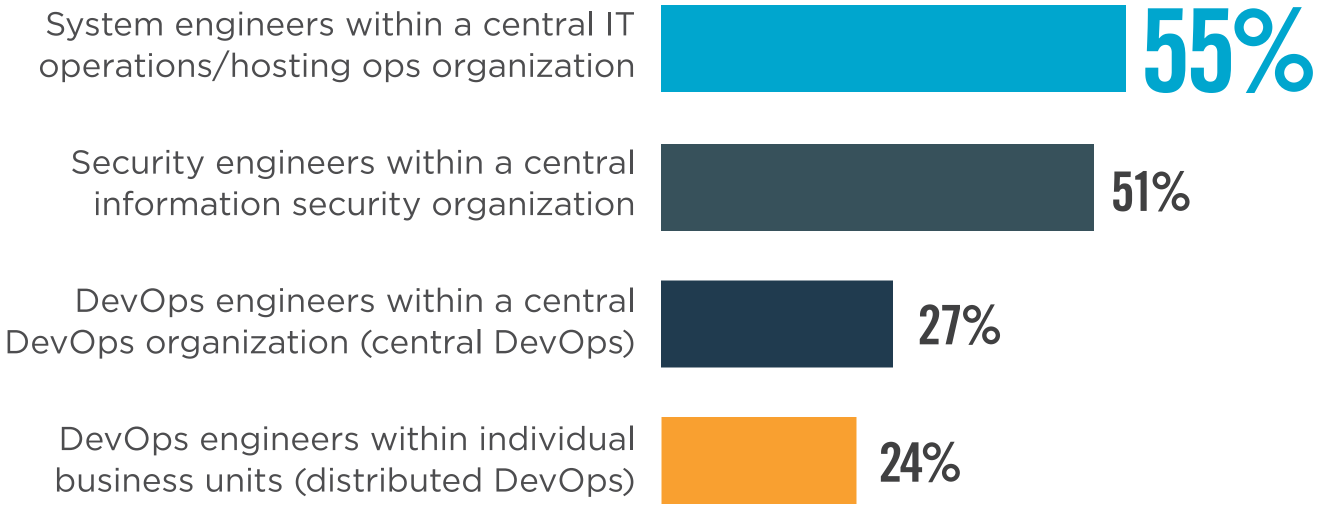


Malicious insiders 40% | Hijacking of accounts, services, or traffic 38% | Foreign state-sponsored cyber attacks 36% | Malware/ransomware 34% | Denial of service attacks 27% | Cloud cryptojacking 18% | Theft of service 13% | Lost mobile devices 9% | Don't know/other 6%

RESPONSIBLE FOR CHANGES

We asked cybersecurity pros who in their organization are accountable for technical changes to systems required to remediate security or compliance problems. The responsibility is spread fairly evenly among system engineers, security engineers, and DevOps engineers. This suggests that there is no single "best practice" yet regarding who should be making changes for security and compliance. While the majority of those responsible for changes are still in a centralized IT, InfoSec, or DevOps organization, 24% have moved to a model with distributed DevOps teams reporting to business units (up 2 points from 22% in 2020).

Who is accountable for actual technical changes to systems that are required to remediate security or compliance problems?



Other 4%

REMEDIATION METHODS

Periodic vulnerability and compliance reports (58%) are still the primary method for organizations to communicate with system owners about security and compliance issues needing remediation. This is followed by automated trouble tickets (47%) that are opened using tools such as Jira, ServiceNow, etc., and scheduled in-person meetings (42%, up from 31% in 2020). It is a positive sign that ad-hoc emails as a remediation method declined to 33% from 40% in 2020.

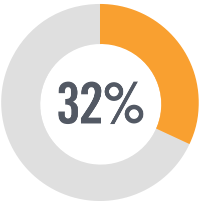
What is the primary method for managing remediation of security and compliance issues with system owners?

58% Periodic vulnerability and compliance reports

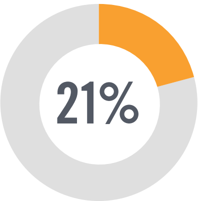
47% Tickets automatically opened in operational tools (e.g., Jira, Service Now, etc.)

42% Scheduled meetings

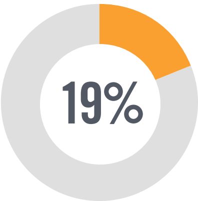
33% Ad-hoc emails



System owners have access to tools operated by information security



System owners operate their own security and compliance tools



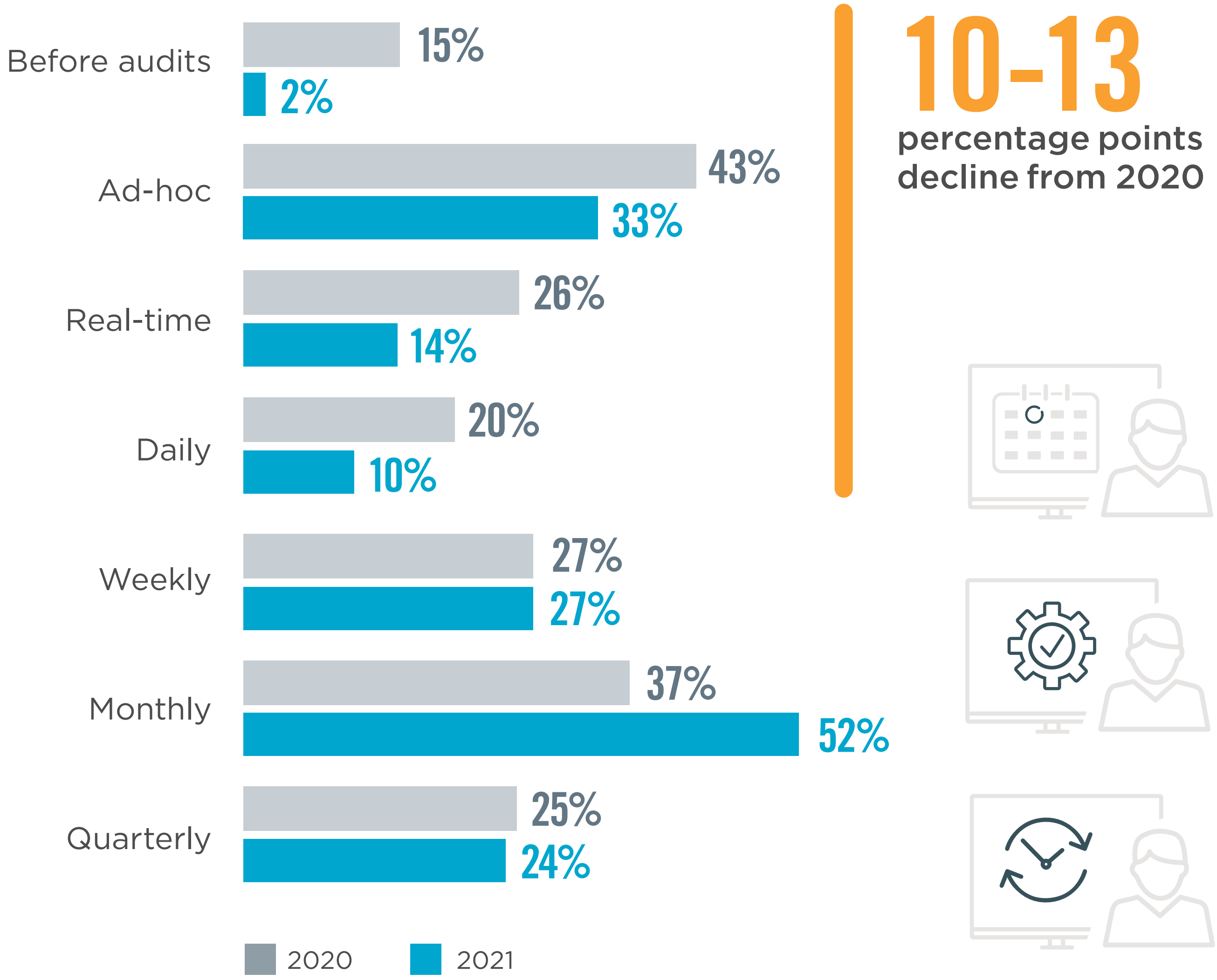
Integrations consume issues directly from security tools and auto-remediate

Other 4%

CADENCE FOR MANAGING REMEDIATION

This year's survey saw some significant changes in how organizations manage remediation of security and compliance issues with system owners. The reported remediation cadences of real-time, ad-hoc, and before-audit fire drills all declined between 10 and 13 percentage points in 2021 from 2020. However, the numbers for quarterly and weekly remediation cadences stayed the same, indicating positive process improvements. Of some concern is that monthly remediation cadence increased significantly from 37% to 52% year-over-year.

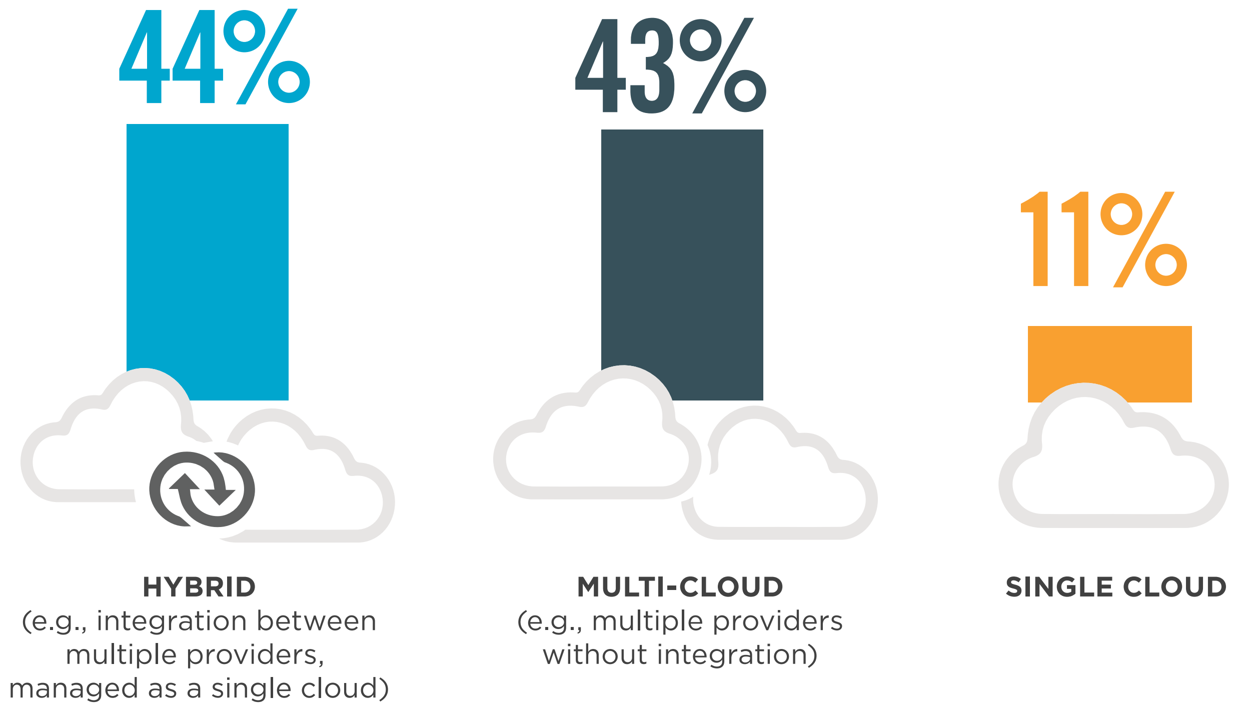
▶ **Outside of critical vulnerabilities, what is the cadence for managing remediation of security and compliance issues with system owners?**



CLOUD DEPLOYMENT STRATEGIES

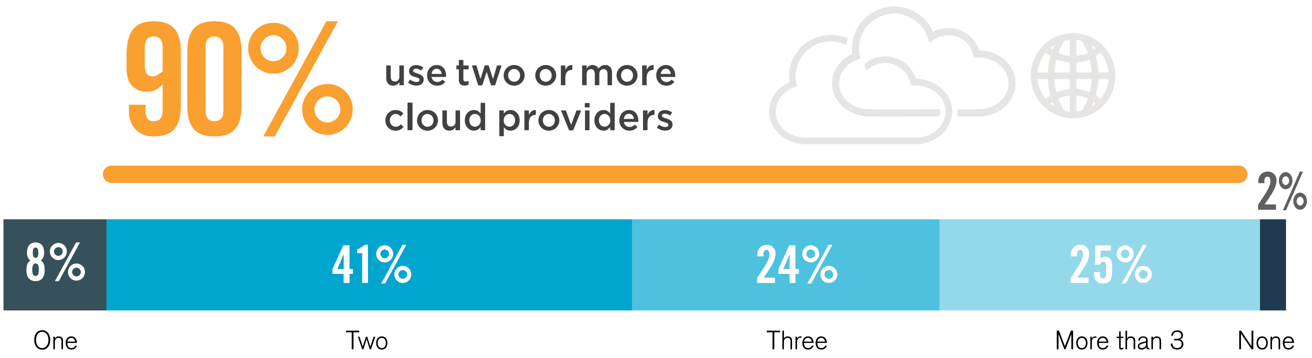
The survey results show that organizations are increasingly embracing hybrid cloud (44%) and multi-cloud deployments (43%) for planned redundancy because of commitments to legacy applications in traditional data centers. Single cloud deployments (11%) continue to diminish in importance. Ninety percent of organizations use two or more cloud providers.

What is your primary cloud deployment strategy?



Other 2%

How many cloud providers does your organization currently use?



CHALLENGES SECURING MULTI-CLOUD

We asked the survey participants what multi-cloud security challenges they are experiencing. Ensuring data protection and privacy for each environment leads the list with 58%. This is followed by the perennial challenge of procuring the right skillset in-house to deploy and manage security solutions across cloud environments (57%) and understanding how different solutions fit together (52%). These results suggest that organizations could reduce complexity and achieve productivity improvements with cloud security and compliance solutions that worked consistently across cloud service vendors.

What are your biggest challenges securing multi-cloud environments?

58%

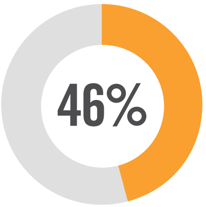
Ensuring data protection and privacy for each environment

57%

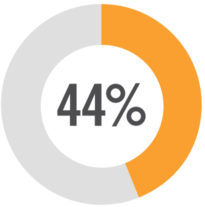
Having the right skills to deploy and manage a complete solution across all cloud environments

52%

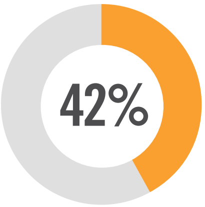
Understanding how different solutions fit together



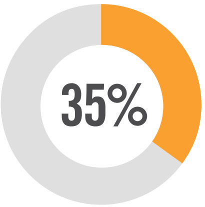
Loss of visibility and control



Keeping up with the rate of change



Understanding service integration options



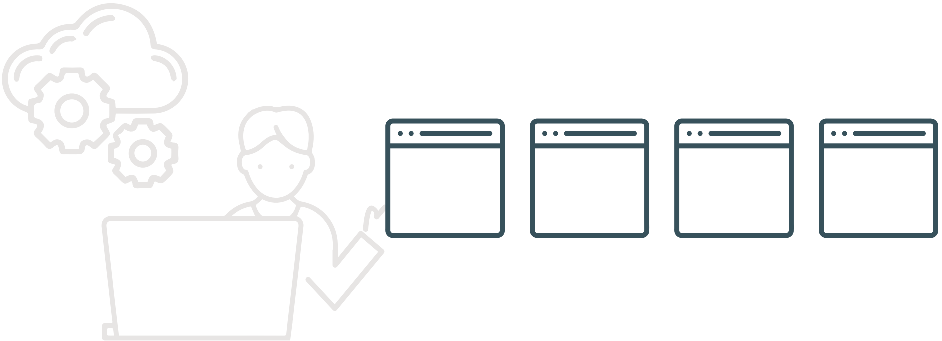
Selecting the right set of services

Providing seamless access to users based on their credentials 28% | Managing the costs of different solutions 28% | Other 3%

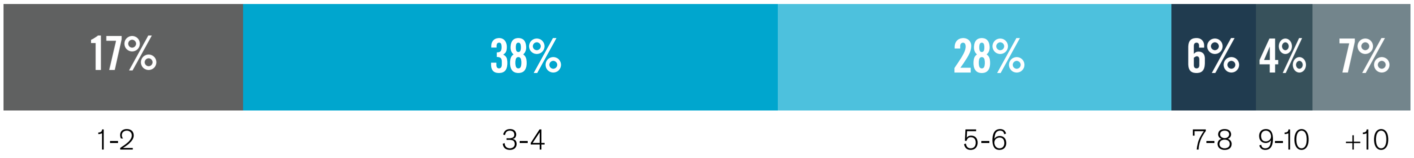
SECURITY DASHBOARDS

More than half of organizations use between three to six different dashboards to configure cloud security policies (66%). This requirement significantly increases the cost and complexity of managing security across multi-cloud environments and negatively impacts security posture. These results do not take into account the multiple dashboards that security professionals may have to access to secure assets hosted in-house, highlighting the need for vendors to offer comprehensive security solutions for multi-and hybrid cloud deployments.

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



66% need to access between three to six dashboards to configure cloud security policies

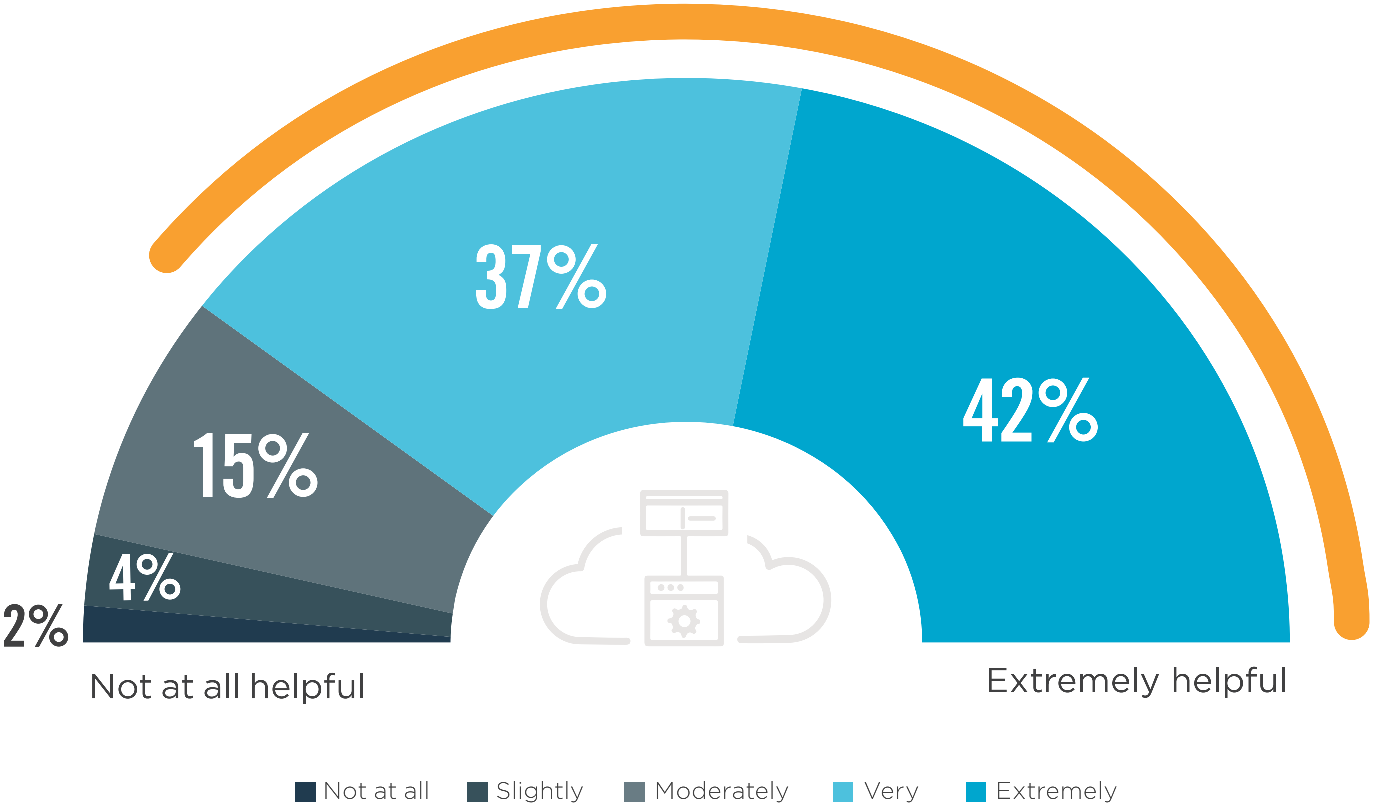


SINGLE CLOUD SECURITY PLATFORM

Eight of ten cybersecurity professionals prefer using a single cloud security platform with a single dashboard; they would consider this very to extremely helpful (79%) to comprehensively protect data across cloud environments.

▶ **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?**

79% of professionals would consider it very to extremely helpful to have a single cloud security dashboard



CLOUD-NATIVE SECURITY DRIVERS

Organizations recognize the advantages of deploying cloud-native security solutions. New this year, the top-reported driver is better scalability (55%). This is closely followed by faster time to deployment (54%) and reduced efforts for patching and upgrading software, which jumped from fifth place in 2020 (33%) to tie for third with cost savings (42%).

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

55%
Better scalability

54%
Faster time to deployment

42%
Reduced effort around patches and upgrades of software

42%
Cost savings

39%
Better performance

37%
Better visibility into user activity and system behavior

34%
Meet cloud compliance expectations

33%
Our data/workloads reside in the cloud (or are moving to the cloud)

Need for secure app access from any location 31% | Better uptime 31% | Easier policy management 28% | Reduction of appliance footprint in branch offices 24% | Other 1%

CLOUD SECURITY SOLUTIONS

We asked security professionals what they look for in a cloud security provider. When selecting a cloud security provider, organizations prioritize cost effectiveness (66%), scalability (52%), ease of deployment (51%), and tools that can be deployed with automation (48%).

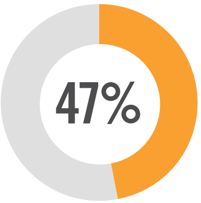
What do you look for in your cloud security provider?

66% Cost effectiveness

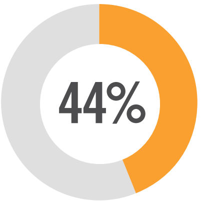
52% Scalable solution

51% Ease of deployment

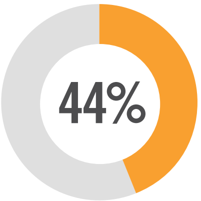
48% Tools can be deployed with automation



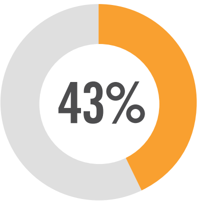
Multi-cloud support



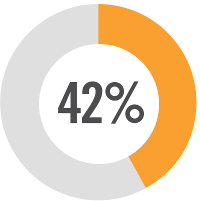
Security tools are cloud-native



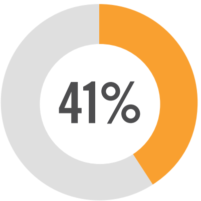
Interoperable with on-premises solutions



Easily manageable platform



Policy customization



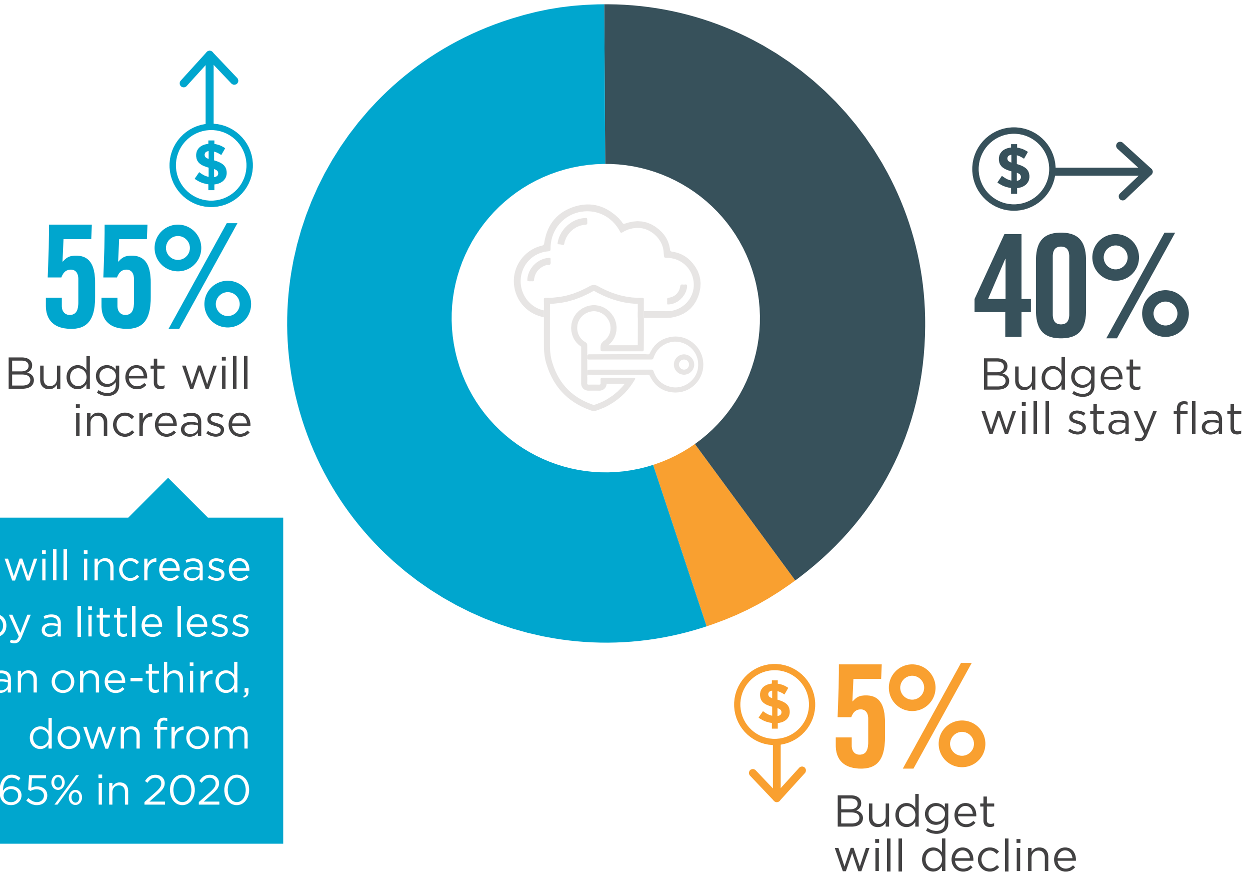
Integrates seamlessly with cloud platforms

Extends on-premises policies to the cloud 35% | Security uptime 32% | Demonstrate cloud knowledge 28% | All capabilities under one platform 28%

CLOUD SECURITY BUDGET

Cloud customers are recognizing the growing significance of addressing cloud security threats and are investing in cloud security accordingly. Looking ahead in 2021, 55% expect cloud security budgets to increase by a little less than one third, down from 65% in 2020. Forty percent expect their cloud security budgets to remain flat, up from 30% in 2020. Those anticipating their cloud security funding to shrink held steady at only five percent.

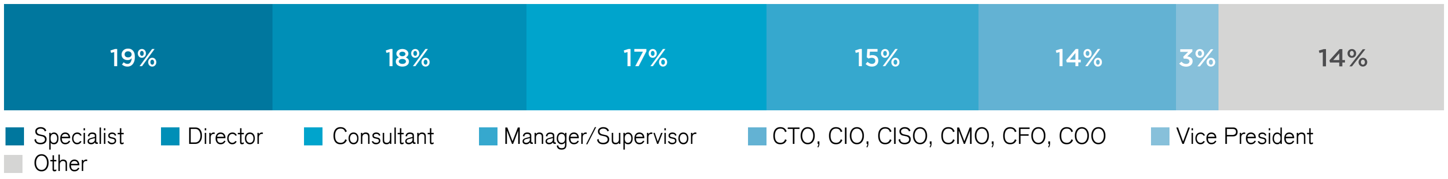
▶ **How is your cloud security budget changing in the next 12 months?**



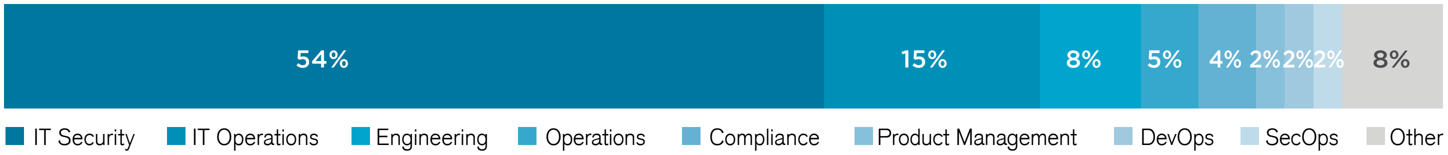
METHODOLOGY & DEMOGRAPHICS

This AWS Cloud Security Report is based on the results of a comprehensive online survey of 316 cybersecurity professionals, conducted in April 2021, to gain deep insight into the latest trends, key challenges, and solutions for cloud protection. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

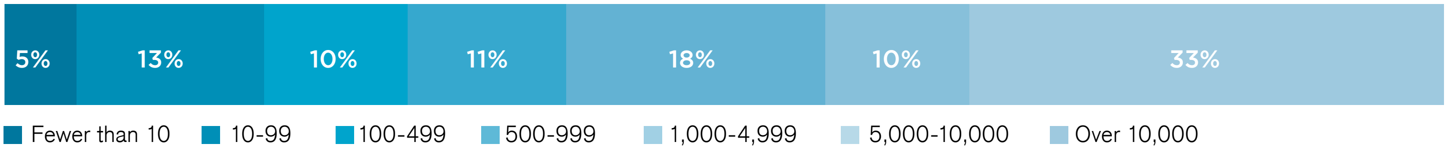
CAREER LEVEL



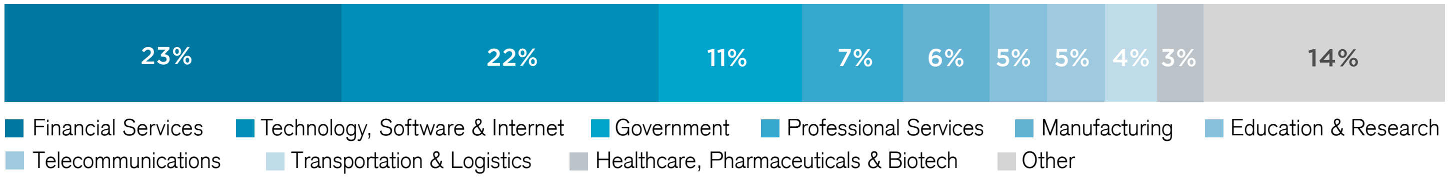
DEPARTMENT



COMPANY SIZE



INDUSTRY



CloudPassage

A Fidelis Cybersecurity Company

CloudPassage®, a Fidelis Cybersecurity® company, safeguards cloud infrastructure for the world's best-recognized brands in finance, e-commerce, gaming, B2B SaaS, healthcare, biotech, and digital media. Fidelis Cybersecurity combats the full spectrum of cyber-crime, data theft and espionage.

As the leading innovator of Active XDR solutions, Fidelis helps organizations detect, respond and neutralize threats earlier and deploy deception technologies to stop adversaries before they advance across the IT environment. The CloudPassage Halo® platform unifies security and compliance across servers, containers, and IaaS resources across any mix of public, private, hybrid, and multi-cloud environments including Amazon Web Services, Microsoft Azure, and Google Cloud Platform. Fidelis Cybersecurity is trusted by Global 1000s and Governments as their last line of defense. Fidelis Cybersecurity is a portfolio company of Skyview Capital.

www.cloudpassage.com | www.fidelissecurity.com