2020

Cybersecurity
INSIDERS

AWS CLOUD SECURITY REPORT

CloudPassage

INTRODUCTION

Organizations continue to rapidly migrate workloads from datacenters to the cloud, utilizing new technologies such as serverless, containers, and machine learning to benefit from increased efficiency, better scalability, and faster deployments from cloud computing.

Cloud security concerns remain high as the adoption of public cloud computing continues to surge, especially in the wake of the 2020 COVID crisis and the resulting massive shift to remote work environments.

The 2020 AWS Cloud Security Report is based on a comprehensive survey of 427 cybersecurity professionals to uncover how AWS user organizations are responding to security threats in the cloud, and what tools and best practices IT cybersecurity leaders are prioritizing in their move to the cloud.

Key survey findings include:

- 95% of cybersecurity professionals confirm they are extremely to moderately concerned about public cloud security – up from 91% in last year's survey.
- Specific cloud security challenges include the risk of data loss and leakage (63%), threats to data privacy (tied at 63%), and dealing with legal and regulatory challenges (40%) as the top three security concerns.
- Organizations rank misconfiguration of the AWS cloud platform as the single biggest vulnerability (49%), followed by insecure interfaces/APIs (47%) and unauthorized access through misuse of employee credentials and lack of proper access controls (46%).
- Only half of organizations (51%) embed security testing during the Software Development Life Cycle (SDLC).
- 67% still rely on periodic vulnerability and compliance reports as the primary method to manage remediation of security and compliance issues. Less than half have automation between security and DevOps in place.
- Organizations recognize the advantages of deploying cloud native security solutions, including faster time to deployment (44%) and cost savings (43%).
- 65% say cloud security budgets are increasing an average of 36%.

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

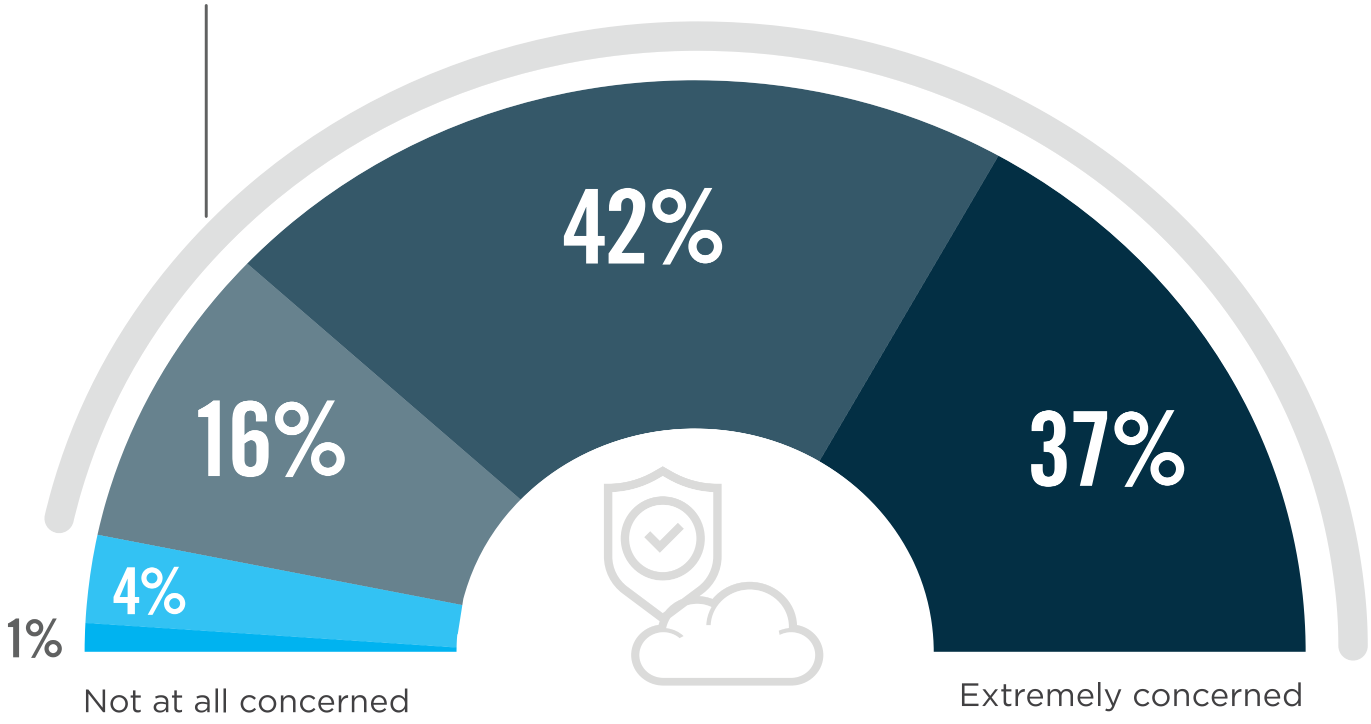
Cybersecurity
INSIDERS

CLOUD SECURITY CONCERNS REMAIN HIGH

Cloud security concerns remain high as the adoption of public cloud computing continues to surge, especially in the wake of the 2020 COVID crisis and the resulting massive shift to remote work environments. Nine of 10 cybersecurity professionals (95%) confirm they are extremely to moderately concerned about public cloud security – up from 91% in last year's survey.

Please rate your level of overall security concern related to adopting public cloud computing.

95% Organizations are concerned about cloud security.



🟦 Not at all concerned 🟦 Slightly concerned ▨ Moderately concerned ■ Very concerned ■ Extremely concerned

CLOUD SECURITY CONCERNS

Customer organizations are ultimately responsible for securing their own workloads in the cloud – despite the security measures offered by cloud providers such as Amazon Web Services. When asked about the specific cloud security challenges, cybersecurity professionals in our survey are highlighting the risk of data loss and leakage (63%), threats to data privacy (tied at 63%), and dealing with legal and regulatory challenges (40%) as the top three security concerns.

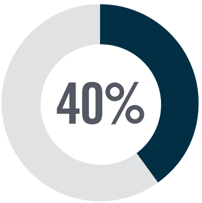
What are your biggest cloud security concerns?

63%

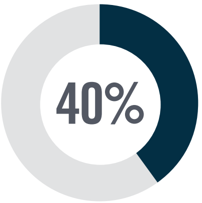
Data loss/leakage

63%

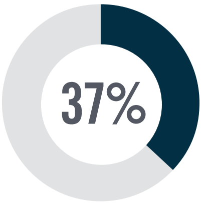
Data privacy/ confidentiality



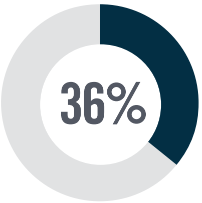
Legal and regulatory compliance



Accidental exposure



Incident response



Data sovereignty/ control

Lack of forensic data 29% | Visibility & transparency 29% | Fraud (i.e., theft of SSN records) 28% | Liability 25% | Availability of services, systems and data 25% | Disaster recovery 23% | Business continuity 21% | Performance 21% | Having to adopt new security tools 20% | Not sure/other 8%

BIGGEST CLOUD SECURITY THREATS

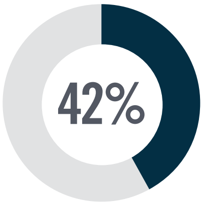
When asked about the biggest cloud security threats, organizations ranked misconfiguration of the AWS cloud platform as the single biggest vulnerability (49%). This is followed by insecure interfaces/APIs (47%), and unauthorized access through misuse of employee credentials and lack of proper access controls (46%).

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

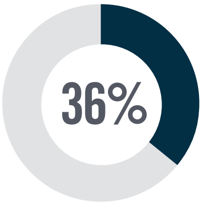
49%
Misconfiguration of the cloud platform/ wrong setup

47%
Insecure interfaces/APIs

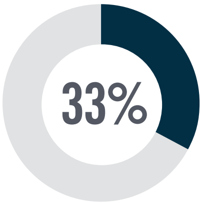
46%
Unauthorized access



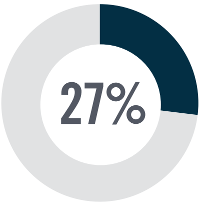
Hijacking of accounts, services or traffic



External sharing of data



Malicious insiders



Foreign state-sponsored cyber attacks

Malware/ransomware 26% | Denial of service attacks 23% | Cloud cryptojacking 20% | Theft of service 15% | Lost mobile devices 12% | Not sure/other 8%

OPERATIONAL SECURITY HEADACHES

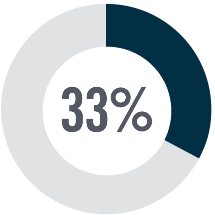
As more workloads move to the cloud, cybersecurity professionals are increasingly realizing the complications resulting from protecting these workloads. The biggest security operational headache organizations face is the perennial lack of qualified security staff (39%). This is followed by compliance (38%), lack of visibility into infrastructure security (36%), and setting consistent security policies across cloud and on-premises environments (33%).

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

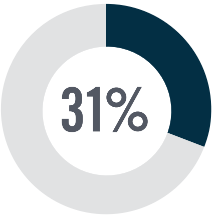
39% Lack of qualified staff

38% Compliance

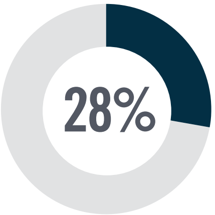
36% Lack of visibility into infrastructure security



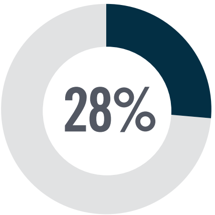
Setting consistent security policies



Security can't keep up with pace of change in applications



Lack of integration with on-premises security technologies



Can’t identify misconfiguration quickly

Securing traffic flow 26% | Complex cloud-to-cloud/cloud to on-prem security rule matching 26% | Understanding network traffic 26% | Securing access from personal and mobile devices 26% | Reporting security threats 25% | Justifying more security spend 25% | Remediating threats 22% | Automatically enforcing security across multiple datacenters 21% | No automatic discovery/ visibility/control to infrastructure security 20% | Lack of feature parity with on-premises security solutions 17% | No flexibility 8% | Not sure 6%

CLOUD COMPLIANCE CHALLENGES

When asked about the most challenging aspects of the compliance process, organizations report that audits and risk assessments of their cloud environment (44%) ranks highest. This is followed by monitoring for compliance with policies and procedures (42%) and monitoring for new vulnerabilities in cloud services (40%).

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

44%

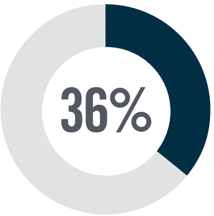
Going through audit/ risk assessment within the cloud environment

42%

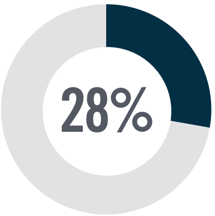
Monitoring for compliance with policies and procedures

40%

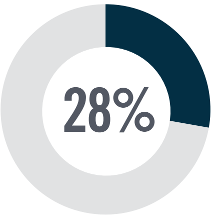
Monitoring for new vulnerabilities in cloud services that must be secured



Staying up to date about new/changing compliance and regulatory requirements



Applying/following the shared responsibility model



Data quality and integrity in regulatory reporting

Scaling and automating compliance activities 28% | Lack of staff expertise/knowledge 16% | Not sure/other 11%

DEVOPS SECURITY CHECKS

When asked about where in the Software Development Life Cycle (SDLC) organizations place DevOps security and/or compliance checks, the most frequently listed stage is system testing and production (58%). This is followed by feature development and unit testing (51%) and staging (42%).

▶ **In what stage(s) of your Software Development Life Cycle (SDLC) do you have DevOps security and/or compliance checks?**

58%
System testing and production

51%
Feature development and unit testing

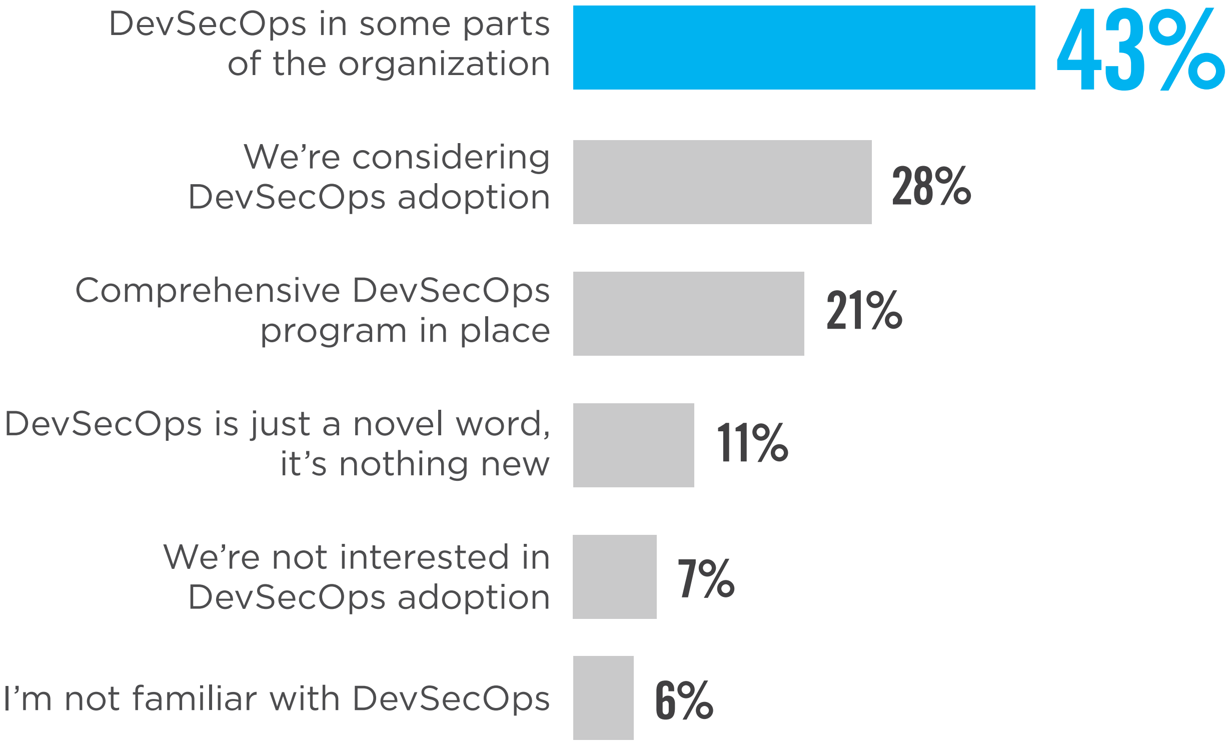
42%
Staging

We don't have security or compliance checks 11% | Not sure/other 20%

DEVSECOPS ADOPTION

We asked organizations about their adoption maturity of DevSecOps for cloud security. Most frequently, DevSecOps has been implemented in some parts of the organization (43%). A quarter of organizations are considering DevSecOps adoption (28%). Only 21% already have a comprehensive DevSecOps program in place.

▶ **What is your organization's current position on DevSecOps?**

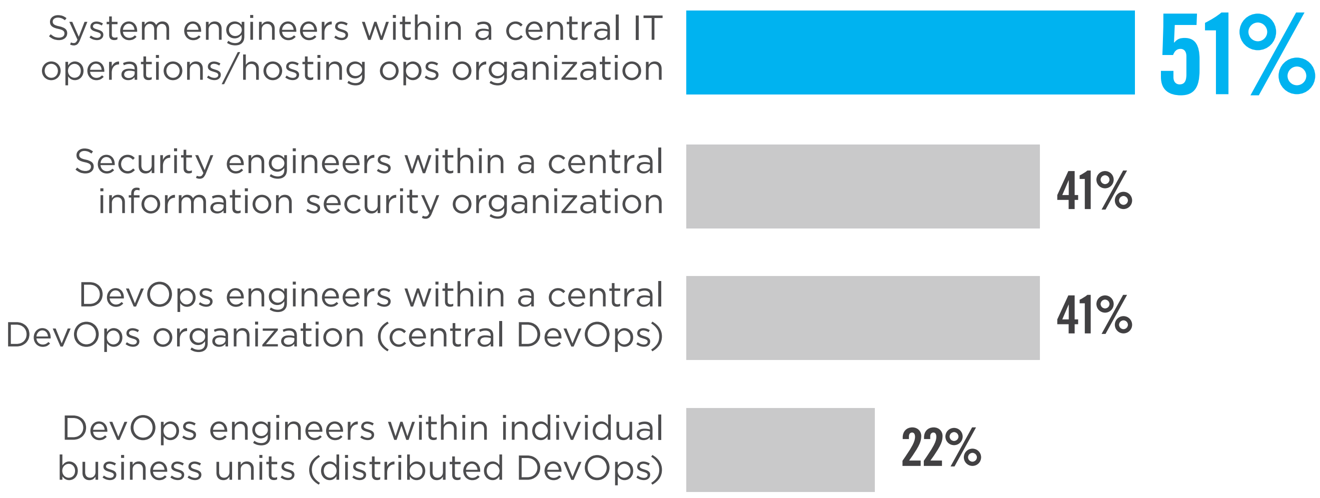

DevSecOps in some parts of the organization
43%
We're considering DevSecOps adoption
28%
Comprehensive DevSecOps program in place
21%
DevSecOps is just a novel word, it's nothing new
11%
We're not interested in DevSecOps adoption
7%
I'm not familiar with DevSecOps
6%

Other 3%

RESPONSIBLE FOR CHANGES

The responsibility for making changes to systems for security and compliance remediation is spread fairly even between system engineers, security engineers, and DevOps engineers. This suggests that there is no single "best practice" yet as to 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, 22% have moved to a model with distributed DevOps teams reporting into business units.

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



Other 7%

REMEDIATION METHODS

Periodic vulnerability and compliance reports (67%) are the primary method for organizations to manage remediation of security and compliance issues with system owners. This is followed by automatically opened tickets at 46% (in tools such as Jira, ServiceNow, etc.) , and manual, ad-hoc emails (40%). Thirty-one percent still rely on scheduled in-person meetings.

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

67%

Periodic vulnerability and compliance reports

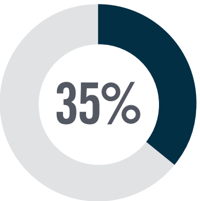
46%

Tickets automatically opened in operational tools

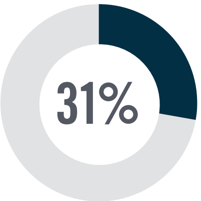
(e.g., Jira, Service Now, etc.)

40%

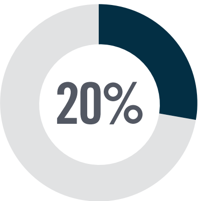
Ad-hoc emails



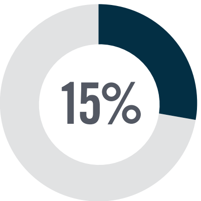
System owners have access to tools operated by information security



Scheduled meetings



Integrations consume issues directly from security tools and auto-remediate



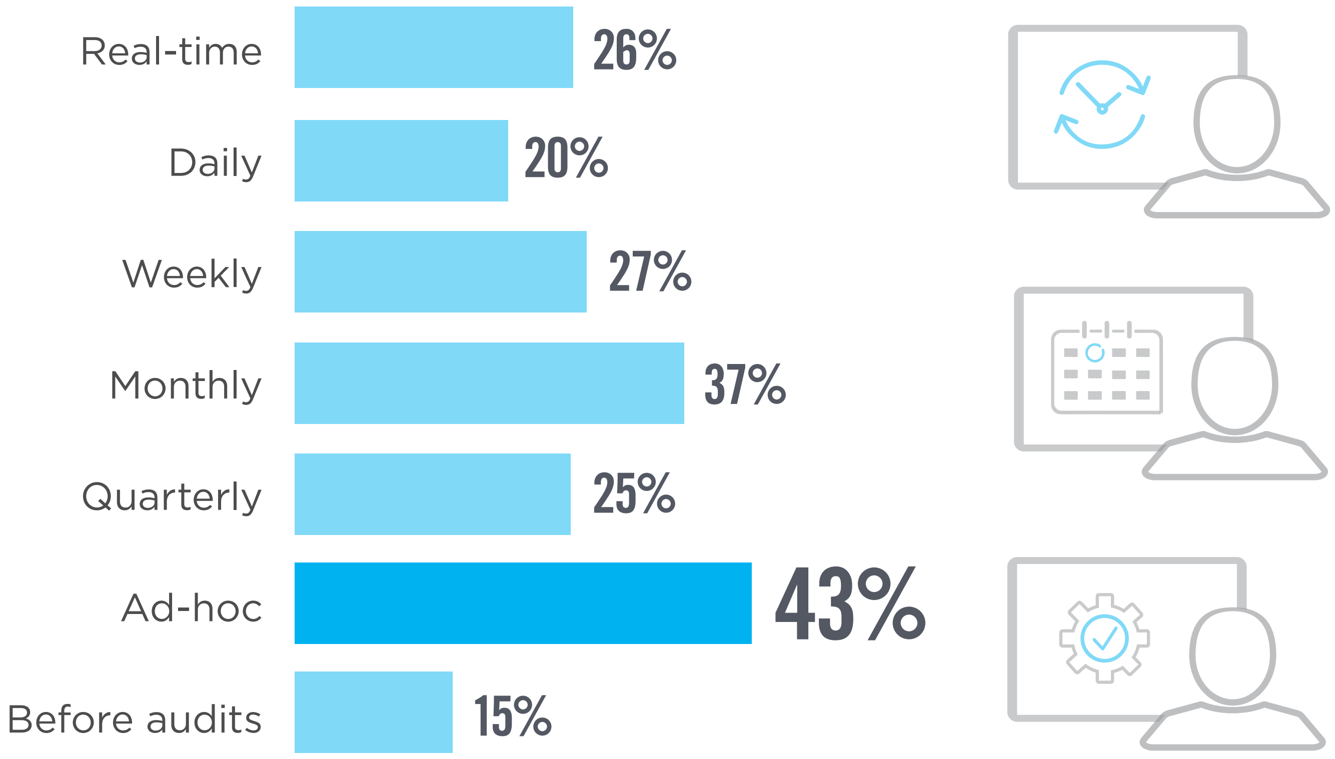
System owners operate their own security and compliance tools

Other 7%

CADENCE FOR MANAGING REMEDIATION

Outside of critical vulnerabilities, organizations typically manage remediation of security and compliance issues with system owners on an ad-hoc basis, as issues occur (43%) and in real-time (26%). This is followed by organizations who still follow a monthly (37%) or weekly (27%) cadence.

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



DRIVERS FOR CLOUD NATIVE SECURITY TOOLS

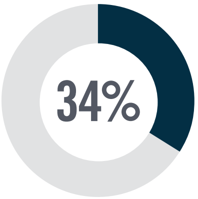
Organizations increasingly recognize the advantages of deploying cloud native security solutions, including faster time to deployment (44%), cost savings (43%), and moving more of their data and workloads in the cloud (36%).

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

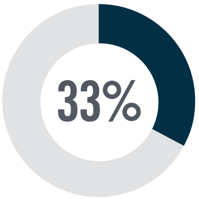
44%
Faster time
to deployment

43%
Cost savings

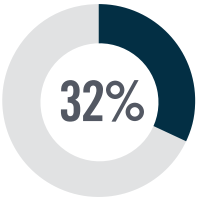
36%
Our data/workloads
reside in the cloud
(or are moving to the cloud)



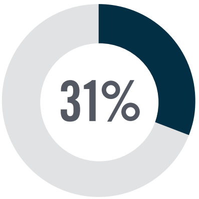
Better
performance



Reduced effort around
patches and upgrades
of software



Need for secure
app access from
any location



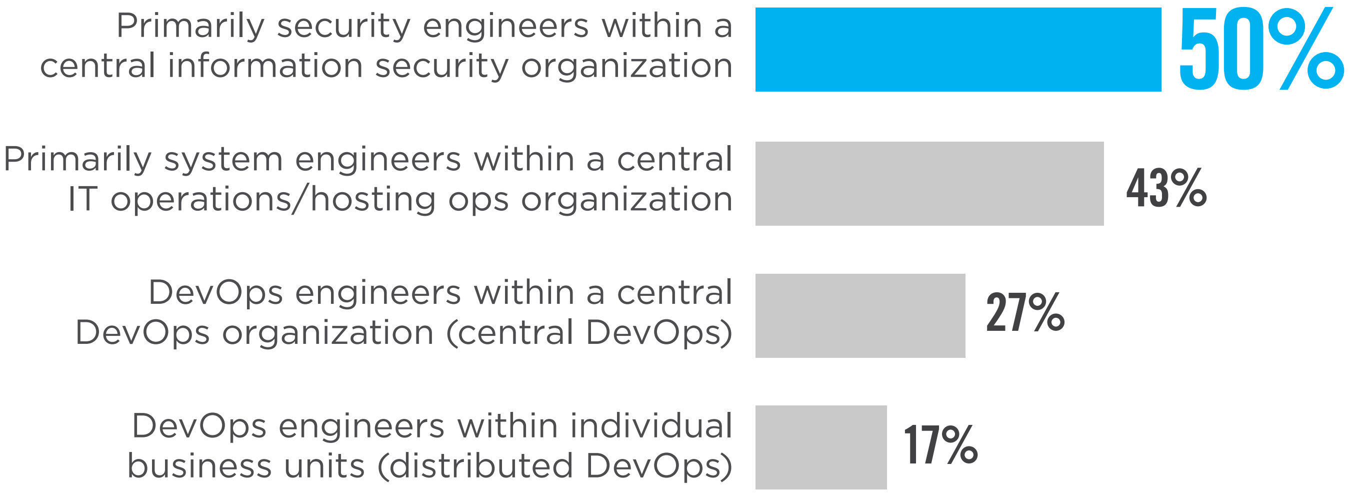
Meet cloud
compliance
expectations

Better visibility into user activity and system behavior 28% | Easier policy management 24% | Reduction of appliance footprint in branch offices 24% | Other 2%

SECURITY DECISION MAKING

In a majority of companies, security engineers within central information security organizations typically make decisions on what technologies are used to implement security control requirements and standards (50%).

Given that information security organizations typically establish security control requirements and standards, who actually makes decisions on what technologies are used to implement security control requirements and standards?

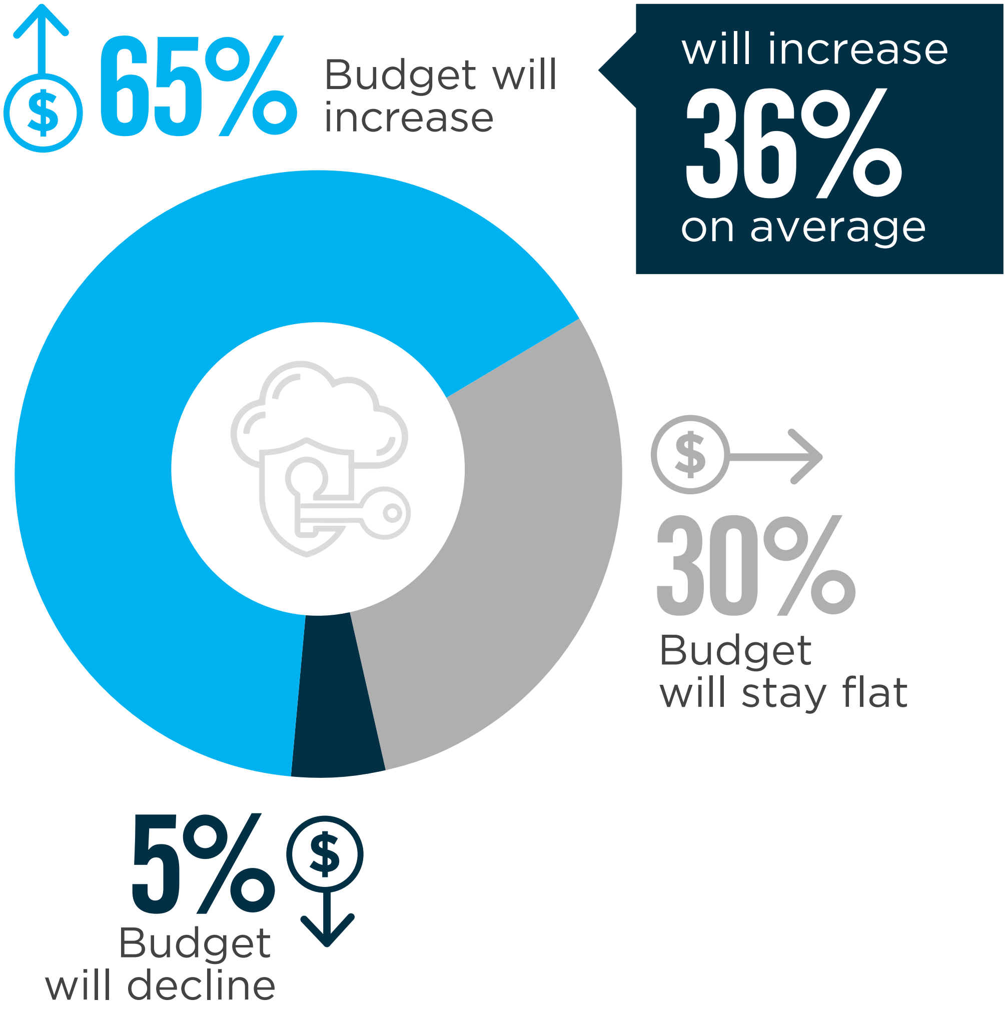


Other 10%

CLOUD SECURITY BUDGET

AWS cloud organizations are recognizing the growing significance of addressing cloud security threats and are investing in cloud security accordingly. Looking ahead, 65% expect cloud security budgets to increase by an average of 36% (up from 27% last year). About a third expect their cloud security budgets to remain flat (30%), while only 5% anticipate their cloud security funding to shrink.

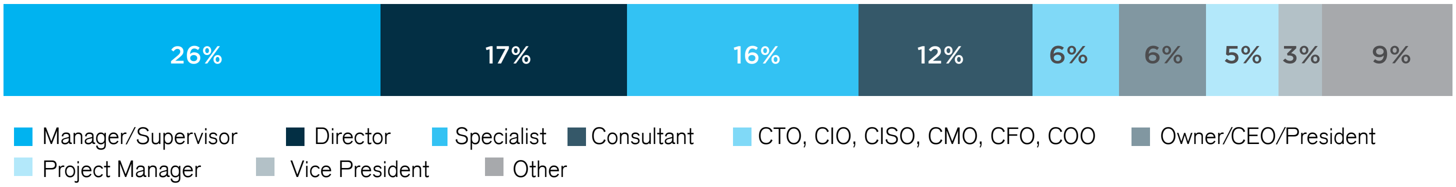
How is your cloud security budget changing in the next 12 months?



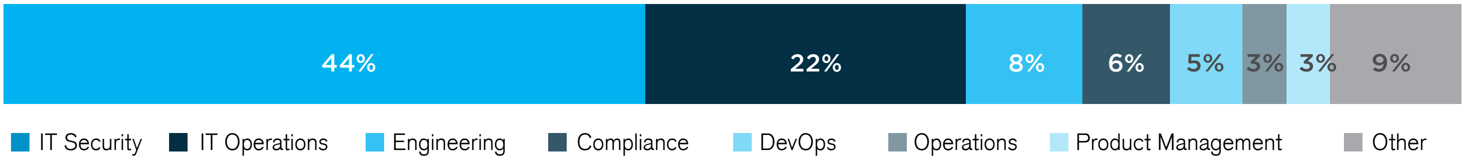
METHODOLOGY & DEMOGRAPHICS

This AWS Cloud Security Report is based on the results of a comprehensive online survey of 427 cybersecurity professionals, conducted in May of 2020 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.

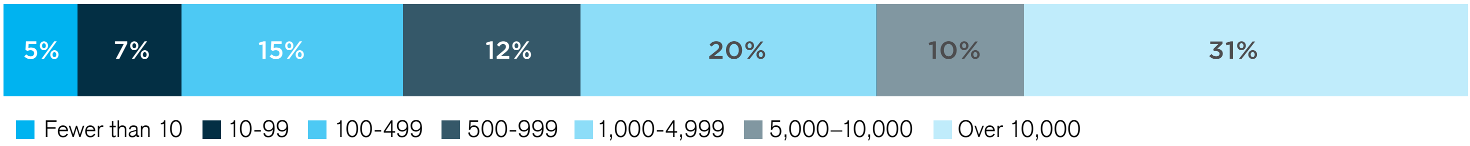
CAREER LEVEL



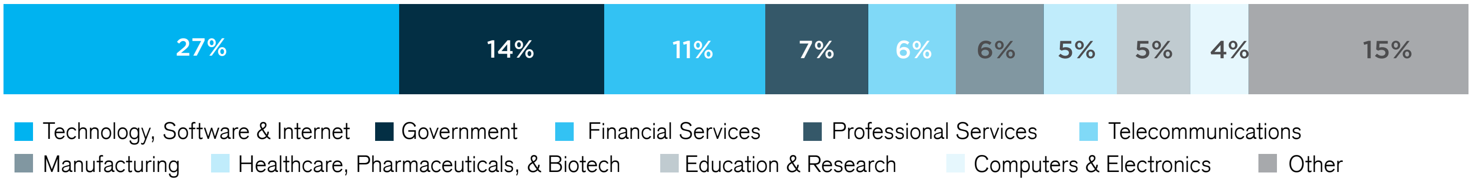
DEPARTMENT



COMPANY SIZE



INDUSTRY



CloudPassage

CloudPassage® safeguards cloud infrastructure for the world's best-recognized brands in finance, e-commerce, gaming, B2B SaaS, and digital media. Their Halo® platform unifies security and compliance across servers, containers, and IaaS resources across any mix of public, private, hybrid, and multi-cloud environments. Halo's extensive automation capabilities streamline and accelerate workflows between InfoSec and DevOps. CloudPassage is widely recognized as a cloud security pioneer, with ten patents granted since the first generation of the Halo platform launched in 2011.

www.cloudpassage.com