2019

Cybersecurity
RESEARCH

AWS CLOUD SECURITY REPORT

CloudPassage

INTRODUCTION

Organizations are rapidly migrating 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.

Amazon Web Services (AWS) continues to dominate the public cloud market with a market share of around one third as measured by revenue.

Despite massive investments in public cloud security, organizations still have reservations about the security of sensitive data, systems, and services in the cloud. The security technology challenge is only exacerbated by the dramatic shortage of skilled cybersecurity professionals.

This report has been produced by CloudPassage in partnership with the 400,000 member Cybersecurity Insiders community of IT security professionals to explore 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.

We hope you will enjoy the report.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

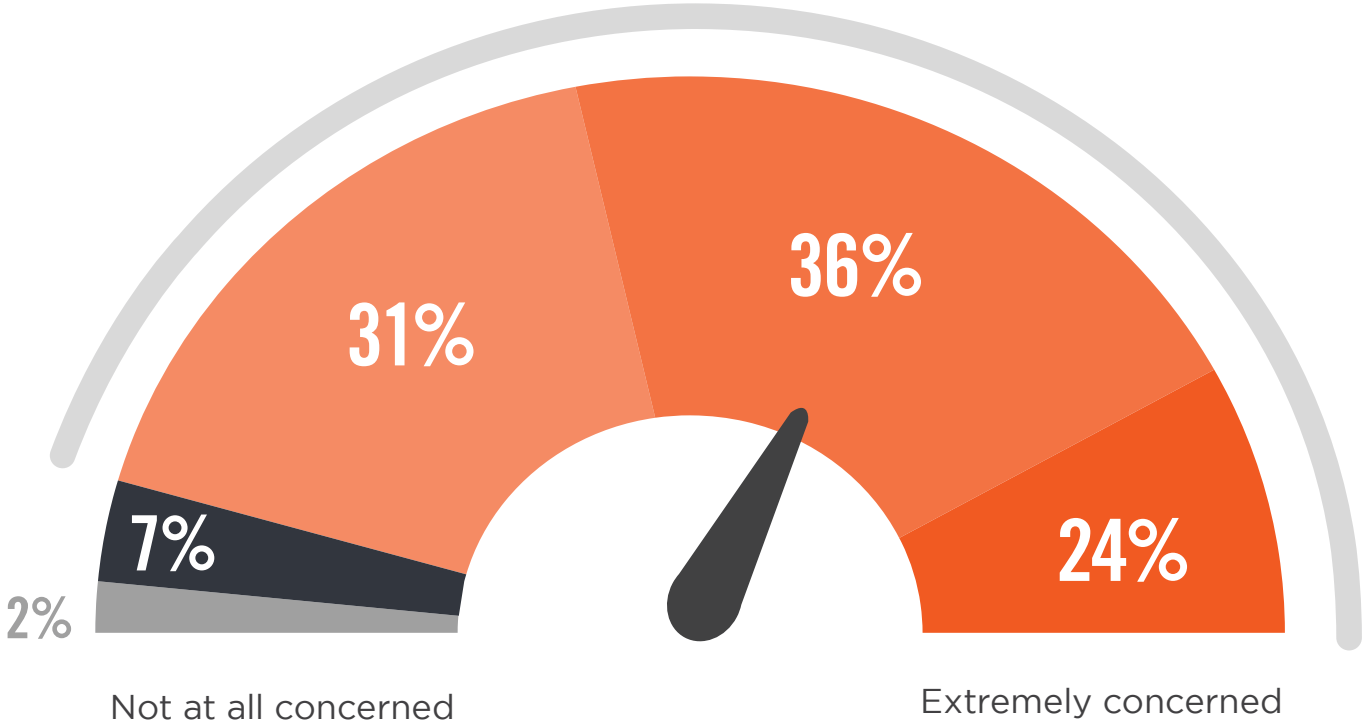
Cybersecurity
INSIDERS

CLOUD SECURITY CONCERNS REMAIN HIGH

While adoption for public cloud computing continues to surge, security concerns remain high. Nine of 10 cybersecurity professionals (91%) are extremely to moderately concerned about public cloud security.

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

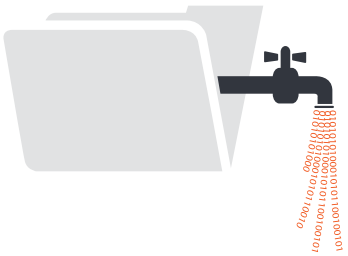
91% Organizations are concerned about cloud security



CLOUD SECURITY CONCERNS

While cloud providers such as Amazon Web Services offer multiple security measures, customer organizations are ultimately responsible for securing their own workloads in the cloud. The top three cloud security challenges highlighted by cybersecurity professionals in our survey are protecting against data loss and leakage (68%), threats to data privacy (61%), and breaches of confidentiality (52%).

What are your biggest cloud security concerns?

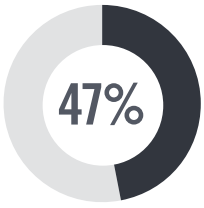


68%
Data loss/leakage

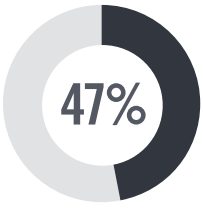
61%
Data privacy

52%
Confidentiality

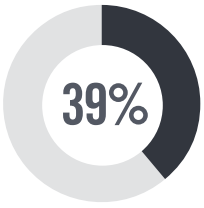
Legal and regulatory compliance



Accidental exposure



Data sovereignty/ control



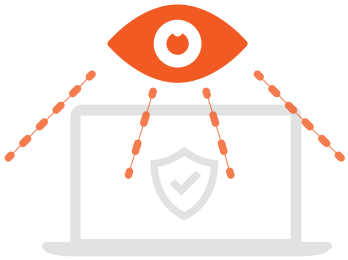
Incident response

Lack of forensic data 37% | Visibility & transparency 36% | Fraud (e.g., theft of SSN records) 31% | Liability 27% | Availability of services, systems and data 21% | Disaster recovery 20% | | Business continuity 20% | Performance 19% | Not sure/other 5%

OPERATIONAL SECURITY HEADACHES

As more workloads move to the cloud, cybersecurity professionals are increasingly realizing the complications to protect these workloads. The biggest security operations challenge organizations face is visibility into infrastructure security (44%), followed by setting consistent security policies across cloud and on-premises environments tying with compliance at 42% each.

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



44%

Visibility into infrastructure security

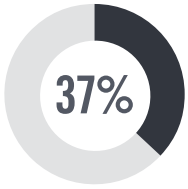
42%

Setting consistent security policies

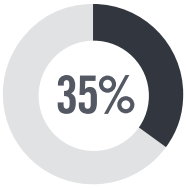
42%

Compliance

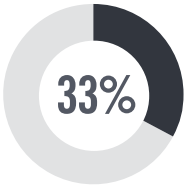
Security can't keep up with pace of change in applications



Lack of integration with on-premises security technologies



Can't identify misconfiguration quickly



Complex cloud to cloud on-premises security rule matching

No automatic discovery/visibility/control to infrastructure security 33% | Reporting security threats 29% | Remediating threats 28% | Automatically enforcing security across multiple datacenters 27% | Lack of feature parity with on-premises security solution 25% | No flexibility 8% | Understanding network traffic 6% | Securing traffic flow 5% | Not sure/other 12%

BIGGEST CLOUD SECURITY CHALLENGES

Misconfiguration of the AWS cloud platform takes the number one spot in this year's survey as the single biggest vulnerability to cloud security (62%). This is followed by unauthorized access through misuse of employee credentials and improper access controls (55%) and insecure interfaces/APIs (52%).

What do you think are the biggest security threats in public clouds?

#1 

62% Misconfiguration of thecloud platform/ wrong set-up

55%

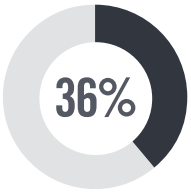
Unauthorized access

52%

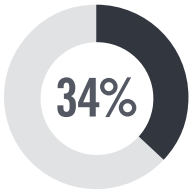
Insecure interfaces /APIs

49%

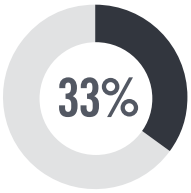
Hijacking of accounts, services or traffic



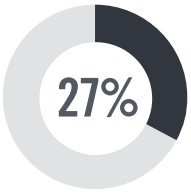
External sharing of data



Foreign state-sponsored cyberattacks



Malicious insiders



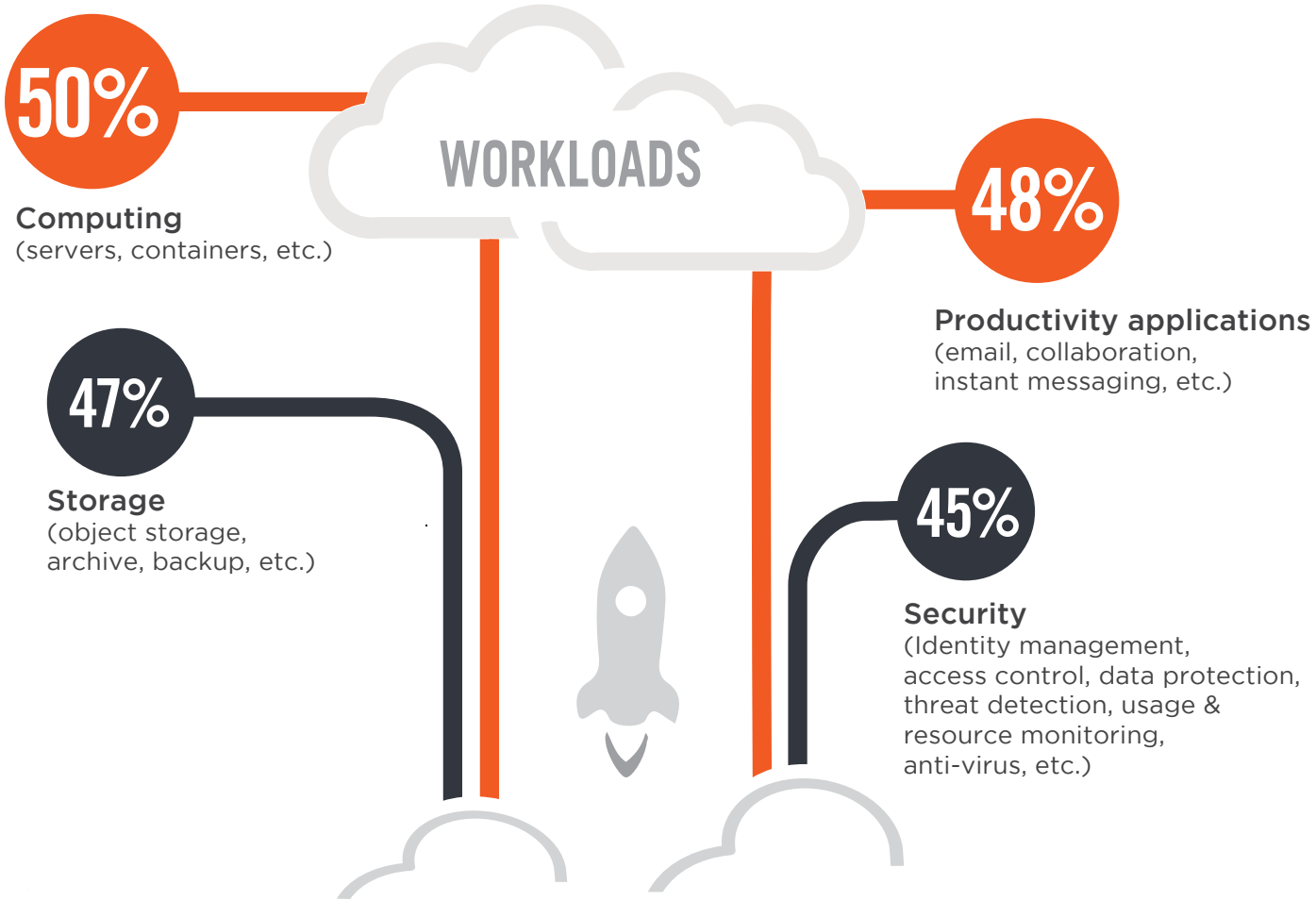
Malware/ ransomware

Denial of service attacks 24% | Theft of service 14% | Lost mobile devices 9% | Not sure/other 4%

MOST COMMON WORKLOADS

The top three cloud services and workloads organizations are deploying are computers (servers, containers, etc.) (50%), followed by productivity applications (email, etc.) (48%) and storage (archive, backup, etc.) (48%).

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



Business applications (CRM, marketing automation,ERP, BI, project management, etc.) 43% | Developer/testing applications 42% | Database (relational, NoSQL, caching, etc.) 41% | Networking (virtual private cloud, DNS, etc.) 40% | Virtualization 39% | IT operations applications (administration, backup, provisioning monitoring, etc.) 34% | Operating system 32% | Middleware 20% | Runtime 12% | Desktop virtualization 7% | Desktop and application streaming 4% | Not sure/other 11%

AWS SECURITY SERVICES

AWS Identity and Access Management (71%) and Amazon CloudWatch (65%) are the most widely used security services in the AWS cloud deployments, followed by AWS CloudTrail for user tracking (45%), AWS Directory Service (42%), and AWS Trusted Advisor (35%).

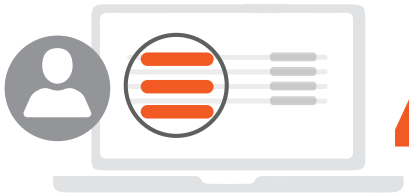
What AWS security and management services do you utilize?

71%

AWS Identity & Access Management
(Manage User Access and Encryption Keys)

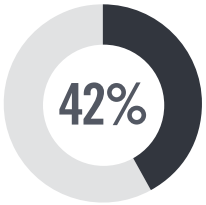
65%

Amazon CloudWatch
(Monitor and Track AWS Apps and Gain System-Wide Utilization Visibility)

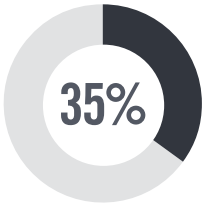


45%

AWS CloudTrail
(Track User Activity and API Usage)



AWS Directory Service (Host and Manage Active Directory)



AWS Trusted Advisor (Optimize Performance and Security)

Sign-on" to "AWS Trusted Advisor 35% | AWS Certificate Manager (Provision, Manage, and Deploy SSL/TLS Certificates) 32% | AWS Config (Create Automated Rules to Check the Configuration of AWS Resources) 29% | AWS Key Management Service (Managed Creation and Control of Encryption Keys) 26% | AWS Shield (DDoS Protection) 26% | Amazon Cloud Directory (Create Flexible Cloud-native Directories) 26% | Amazon GuardDuty (Managed Threat Detection Service) 22% | Amazon Inspector (Analyze Application Security) 22% | Amazon Cognito (Identity Management for your Apps) 22% | AWS Firewall Manager (Central Management of Firewall Rules) 19% | AWS CloudHSM (Hardware-based Key Storage for Regulatory Compliance) 19% | AWS Secrets Manager (Rotate, Manage, and Retrieve Secrets) 19% | AWS WAF (Filter Malicious Web Traffic) 16% | AWS Artifact (On-demand access to AWS compliance reports) 16% | Amazon Macie (Discover, Classify, and Protect Your Data) 16% | AWS Organizations 16% |

SECURITY CAPABILITIES

The most commonly deployed security control is data encryption (62%) and network encryption (52%), closely followed by SIEM and cloud access controls (tied at 51%).

What security capabilities have you deployed in the cloud?

62%

Data encryption

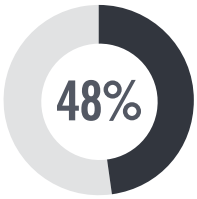
51%

Network encryption
(VPN, packet encryption, transport encryption)

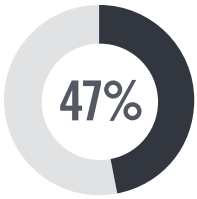
51%

Security Information and Event Management
(SIEM)

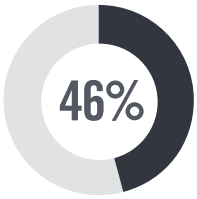
Access control (e.g., CASB/Cloud Access Security Brokers)



Trained cloud security professionals



Vulnerability assessment



Intrusion detection and prevention

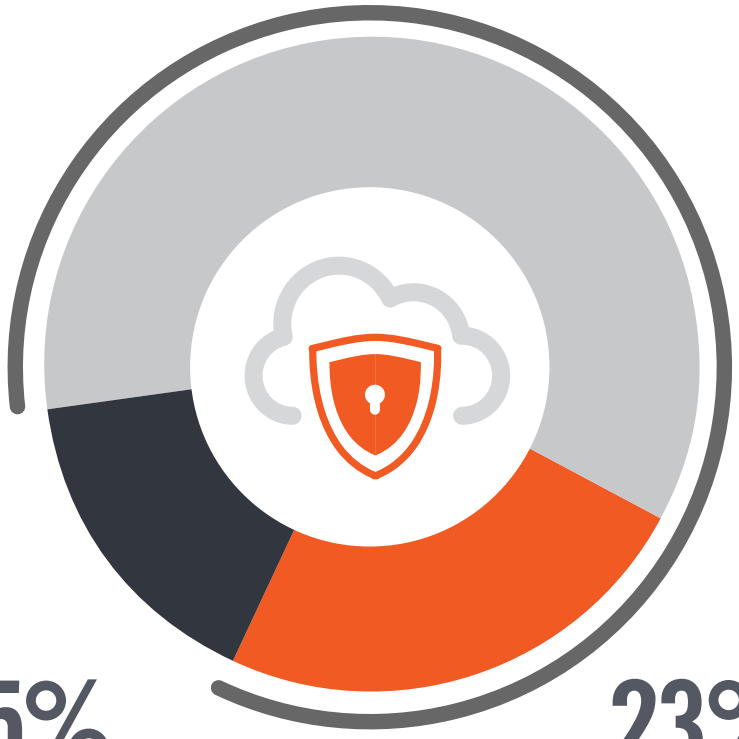
Log management and analytics 46% | Configuration management 46% | Data leakage prevention 45% | Privileged Access 44% | Single sign-on/user authentication 43% | Firewalls/NAC 42% | Endpoint security controls 41% | Patch management 41% | Anti-virus/anti-malware 39% | Network monitoring 37% | Application protection (WAF, scanners, etc.) 35% | Secure managed file transfer 29% | Employee usage monitoring 28% | Mobile Device Management (MDM) 28% | Cloud asset discovery 28% | Database scanning and monitoring 25% | Content filtering 21% | Cyber forensics 21% | Deception-based security 9% | Not sure/other 7%

TRADITIONAL SECURITY TOOLS IN AWS

While traditional network security tools made sense when users and applications were hosted in a static centralized data center, these legacy security tools and appliances are not designed for the dynamic, distributed virtual environment of the cloud. Eighty-five percent of respondents confirm that legacy security solutions either don't work at all in AWS cloud environments or have very limited functionality.

How well do your traditional network security tools / appliances work in cloud environments?

85% Confirm that legacy security solutions either don't work at all in AWS cloud environments or have very limited functionality



62%
Limited functionality

15%
All capabilities work in the cloud

23%
Our traditional network security tools don't work in the cloud

DRIVERS FOR CLOUD NATIVE SECURITY TOOLS

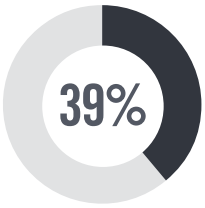
Organizations recognize the advantages of deploying cloud native security solutions, including faster time to deployment (52%) and lower cost (47%).

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

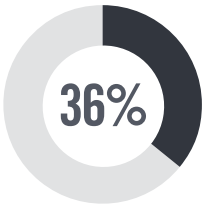
52%
Faster time to deployment

47%
Cost savings

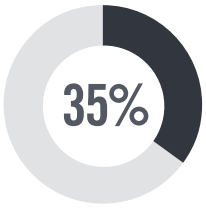
41%
Need for secure app access from any location



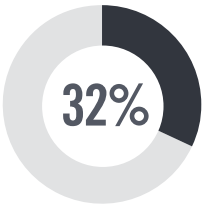
Reduced effort around patches and upgrades of software



Better visibility into user activity and system behavior



Meet cloud compliance expectations



Better performance

Reduction of appliance footprint in branch offices 31% | Easier policy management 26% | Not sure/other 9%

CLOUD COMPLIANCE CHALLENGES

Monitoring for compliance with policies and procedures (56%) is the single biggest cloud compliance-related challenge organizations face, followed by audits and risk assessments of their cloud environment (54%).

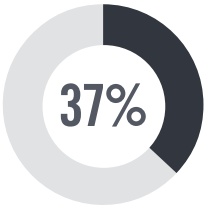
Which part of the cloud compliance process is the most challenging?

56%

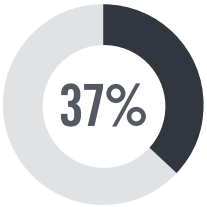
Monitoring for compliance with policies and procedures

54%

Going through audit/risk assessment within the cloud environment



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



Applying the Shared Responsibility Model

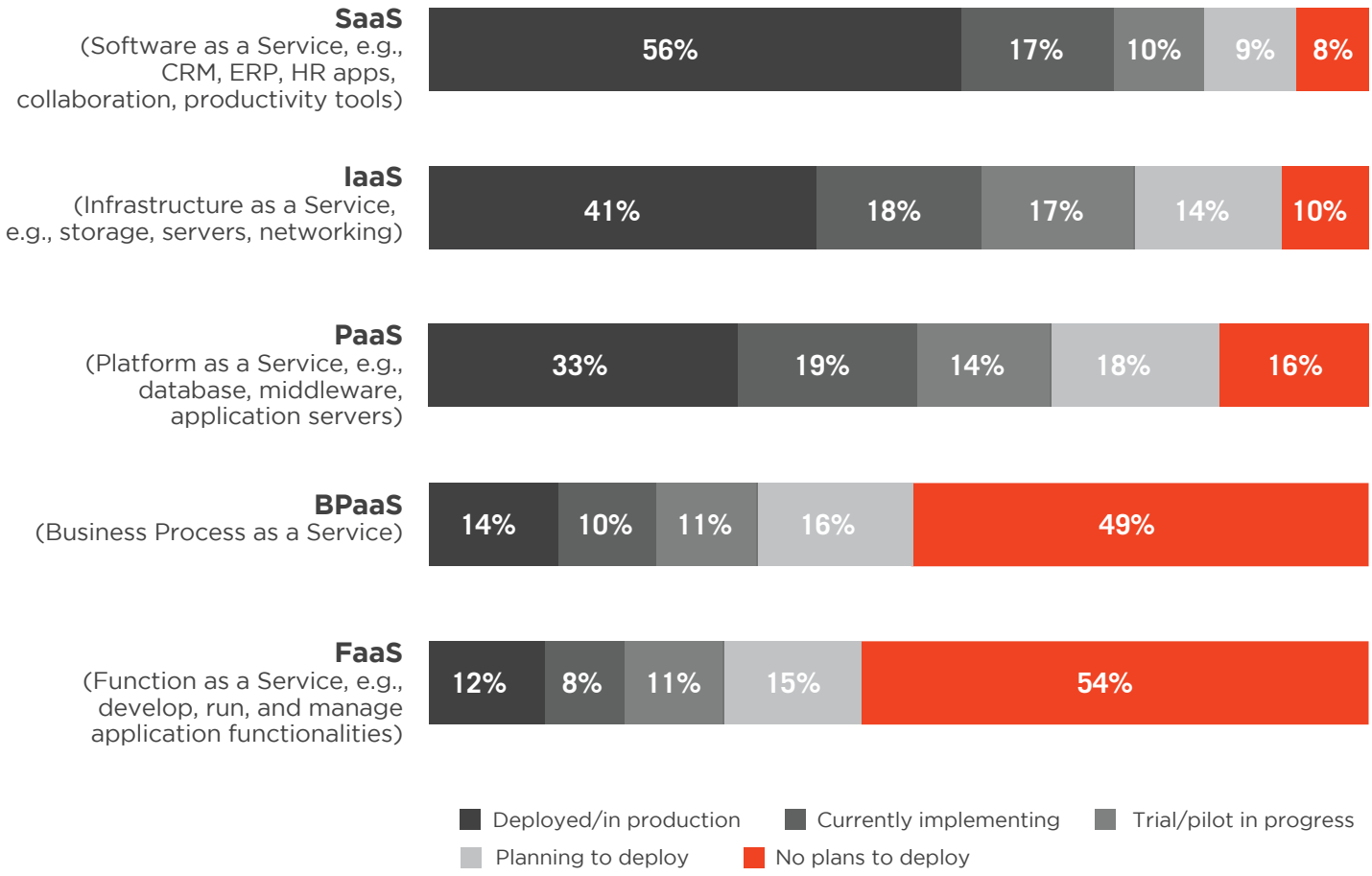
Scaling and automating compliance activities

Data quality and integrity in regulatory reporting 26% | Not sure/other 11%

CLOUD ADOPTION TRENDS

SaaS remains the most popular cloud model (56%), followed by IaaS (41%) and PaaS (33%), all showing strong adoption growth. To a lesser extent, newer deployment models such as BPaaS (14%) and FaaS (12%) still show lower rates of production deployments.

What is your organization's adoption of cloud computing?



PATHS TO STRONGER CLOUD SECURITY

Driven by the massive shortfall of qualified cybersecurity professionals, the training and certification of current IT staff (62%) remains organizations' preferred tactic to assure that their evolving security needs are met. Fifty-five percent of respondents use their cloud provider's native security tools and 36 percent deploy third-party security solutions to ensure the proper security controls are implemented across their cloud environments.

When moving to the cloud, how do you handle your changing security needs?

62%

Train and/or certify current IT staff

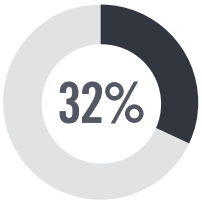
55%

Use cloud provider security tools

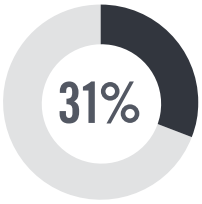
(e.g., GuardDuty in AWS)

36%

Deploy security software from independent software vendor(s)



Partner with a Managed Security Services Provider (MSSP)



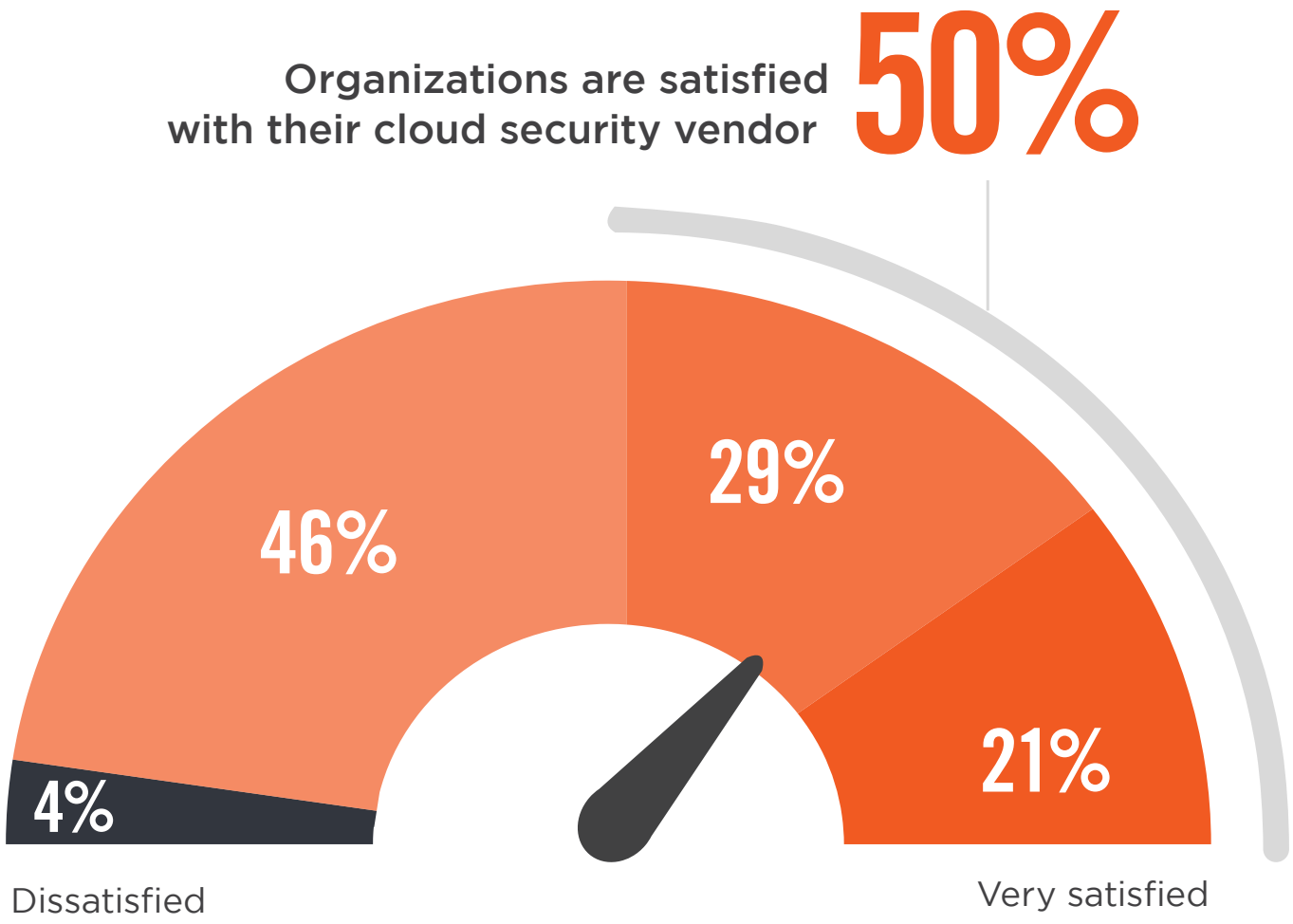
Hire staff dedicated to cloud security

Not sure/other 5%

CLOUD PROVIDER SATISFACTION

A solid half of organizations say they are satisfied with their current cloud security vendor (all participants in this survey are AWS users, among other cloud platforms).

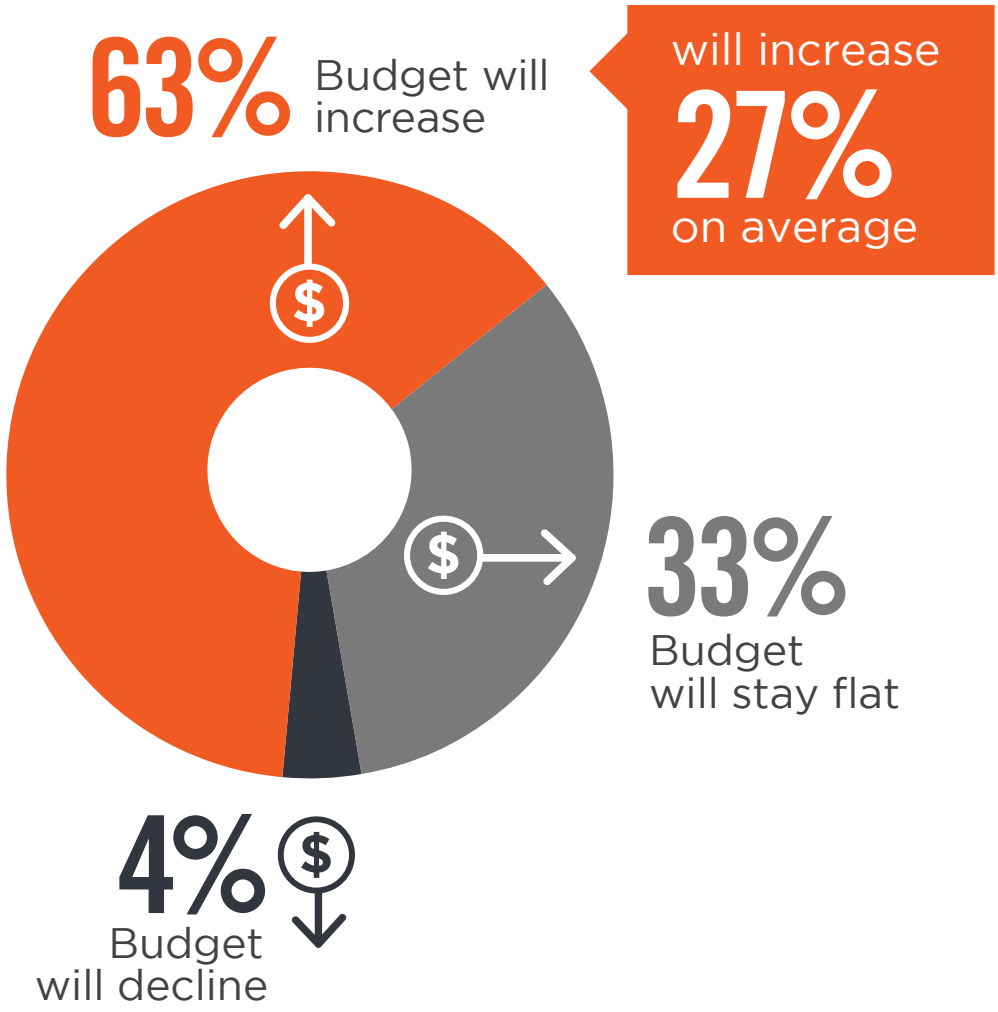
How satisfied are you with your current cloud security vendor?



CLOUD SECURITY BUDGET

The survey reveals that AWS user organizations are recognizing the growing significance of cloud security threats and are investing in cloud security accordingly. Looking ahead, a whopping 63% expect cloud security budgets to increase by an average of 27%. A third expect their cloud security budgets to remain flat, while only 4% anticipate their cloud security funding to shrink.

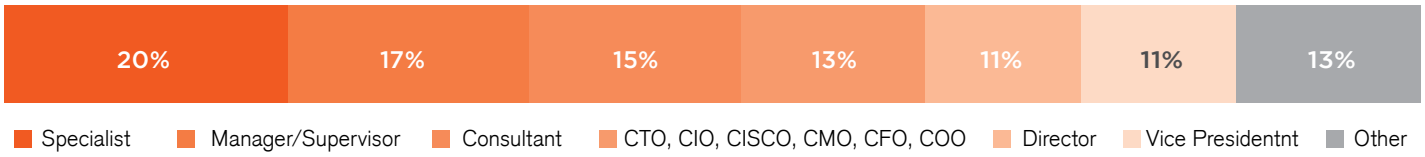
How is your cloud security budget changing in the next 12 months?



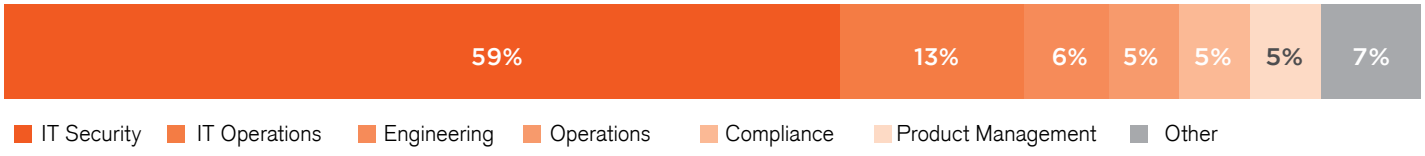
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of cybersecurity professionals to gain more insight into the latest trends, key challenges and solutions for AWS Cloud Security. 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.

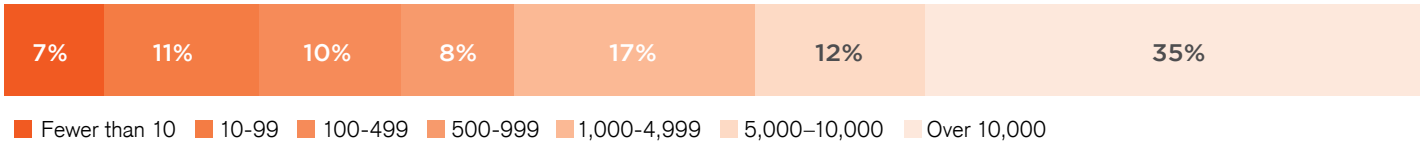
CAREER LEVEL



DEPARTMENT



COMPANY SIZE



INDUSTRY