2019

Cybersecurity
RESEARCH

AWS CLOUD SECURITY REPORT

cavirin

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 Cavirin 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.

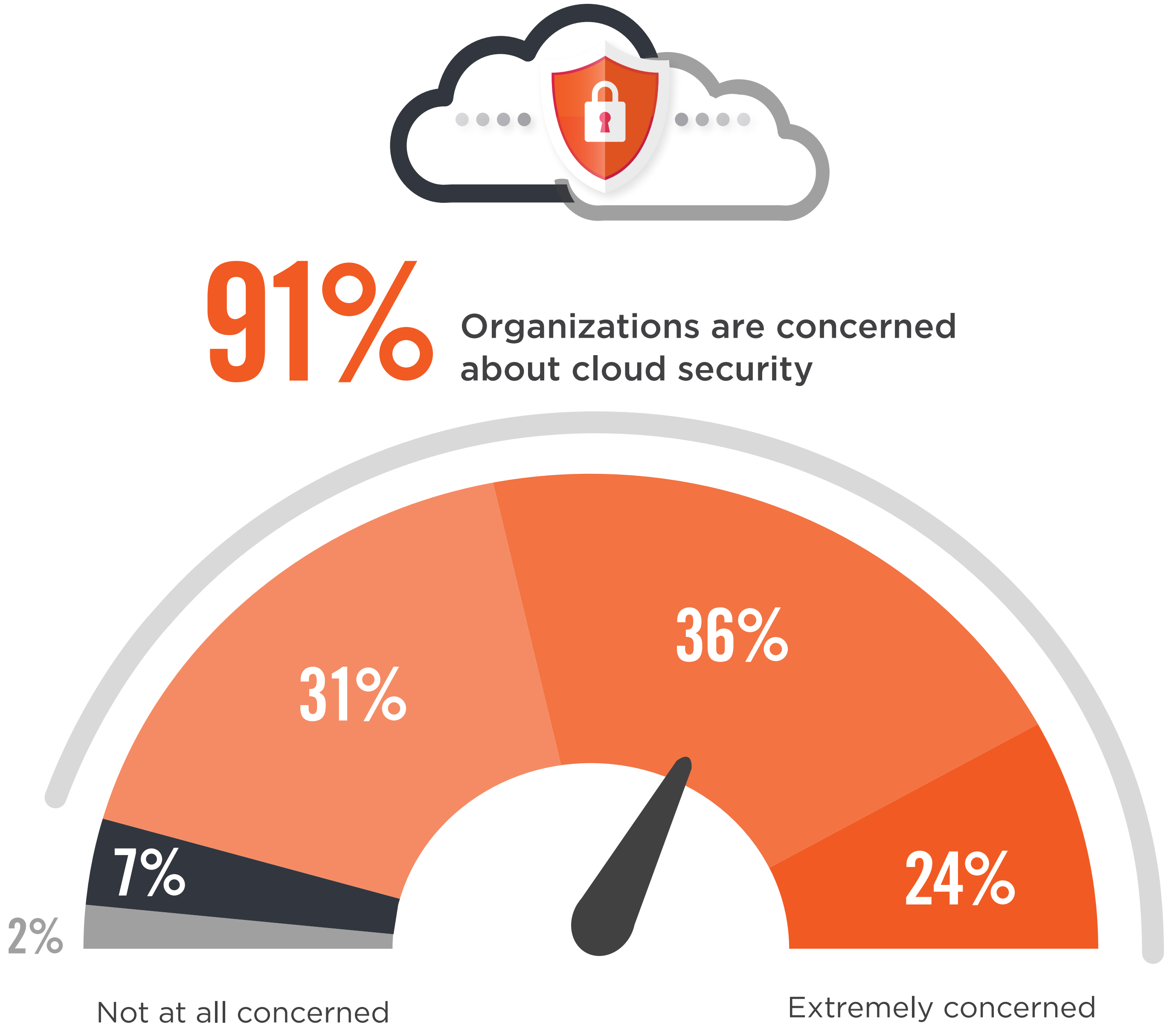
We hope you will enjoy the report.

Dave Ginsburg
VP Marketing
Cavirin

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**

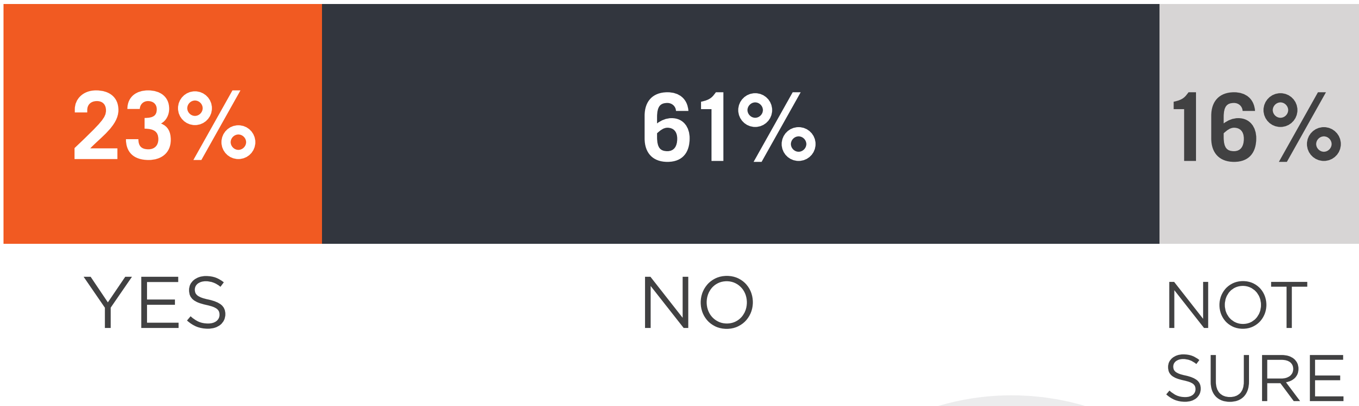


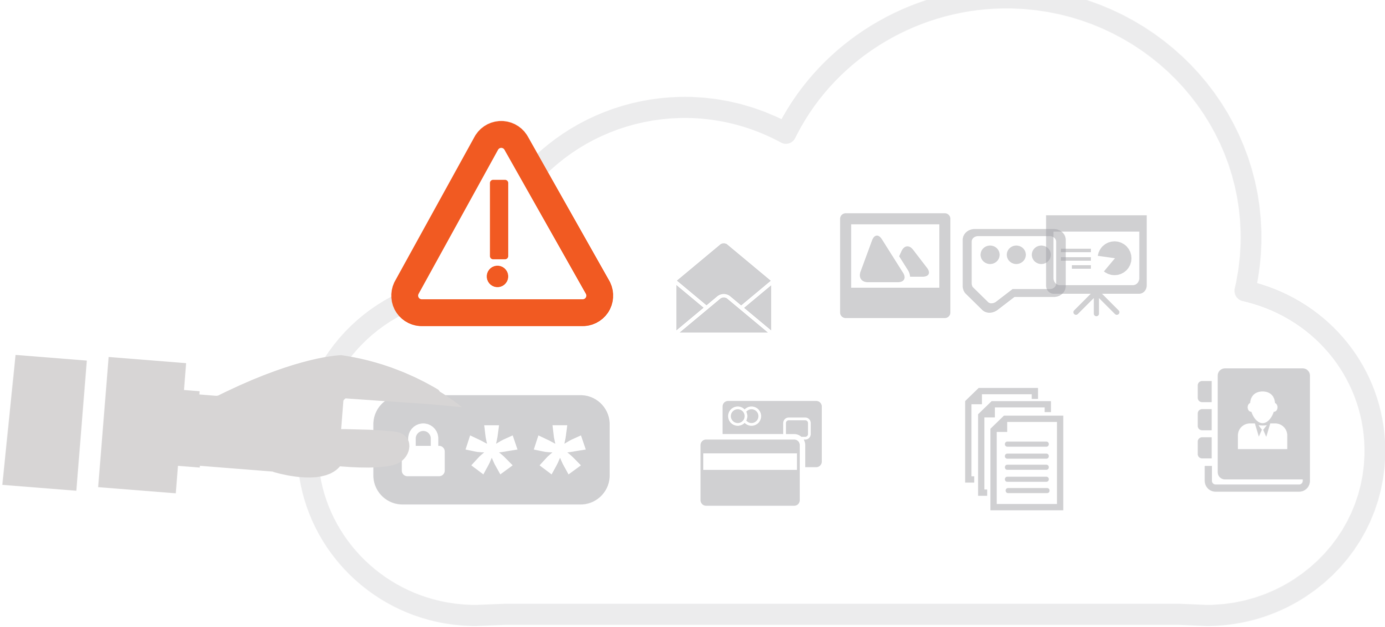
CLOUD SECURITY INCIDENTS

In the past 12 months, 23% of organizations have experienced a cloud security incident, a significant increase over the previous year.

The rise in observed cloud security incidents further serves to support the increased security concerns related to adoption of cloud computing.

Did your organization experience a cloud related security incident in the last 12 months?





CLOUD SECURITY CONCERNS

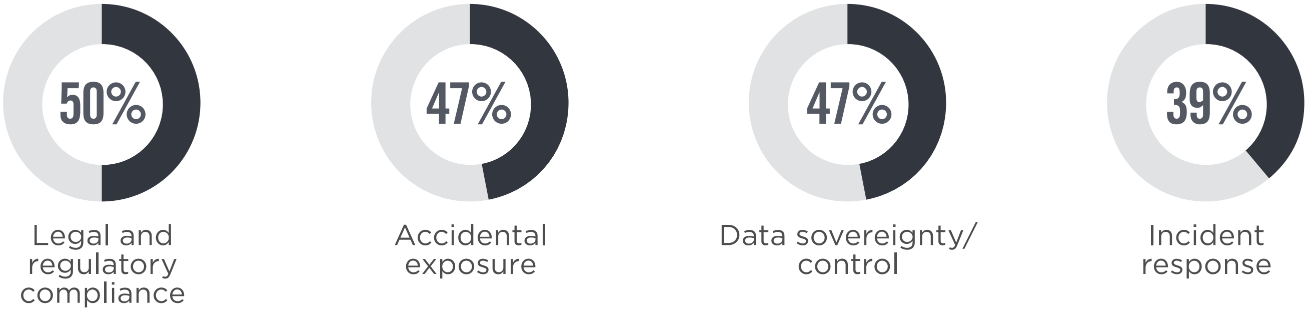
While cloud providers such as Amazon Web Services offer multiple security measures, customer organizations are ultimately responsible for securing their own workloads in the cloud. The top three cloud security challenges highlighted by cybersecurity professionals in our survey are protecting against 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



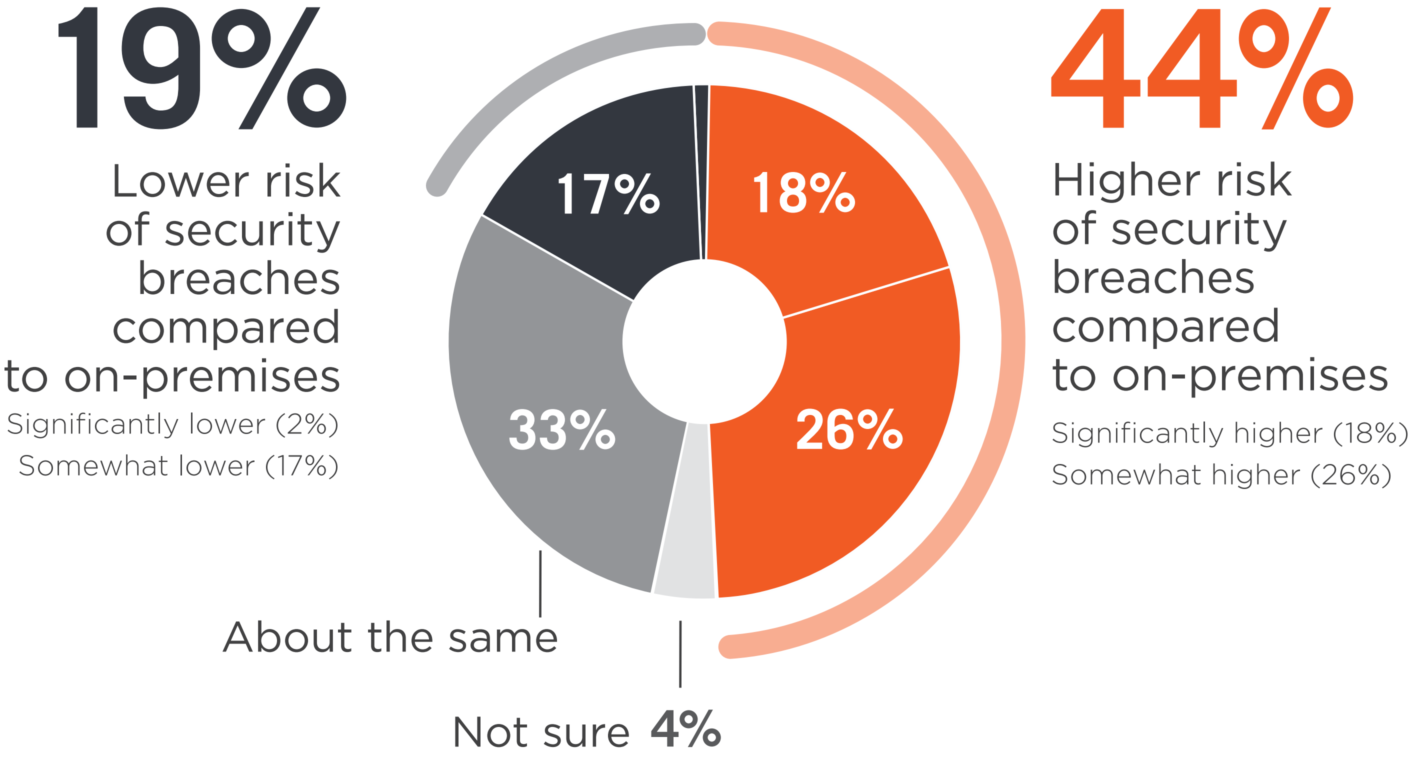
Lack of forensic data 37% | Visibility & transparency 36% | Fraud (e.g., theft of SSN records) 31% | Liability 27% | Availability of services, systems and data 21% | Disaster recovery 20% | | Business continuity 20% | Performance 19% | Not sure/other 5%

CLOUD VS ON-PREMISES SECURITY RISK

Organizations continue to believe public clouds are at higher risk of security breaches than traditional on-premises environments (44%).

The respondents who believe that public clouds are less risky to security breaches decreased proportionally (at 19%, a 4% drop compared to last year's 23%), further supporting the perception that the use of public clouds increases the probability of becoming a target for a cyberattack.

Compared to traditional IT environments, would you say the risk of security breaches in a public cloud environment is... ?



19%

Lower risk of security breaches compared to on-premises

Significantly lower (2%)

Somewhat lower (17%)

44%

Higher risk of security breaches compared to on-premises

Significantly higher (18%)

Somewhat higher (26%)

About the same

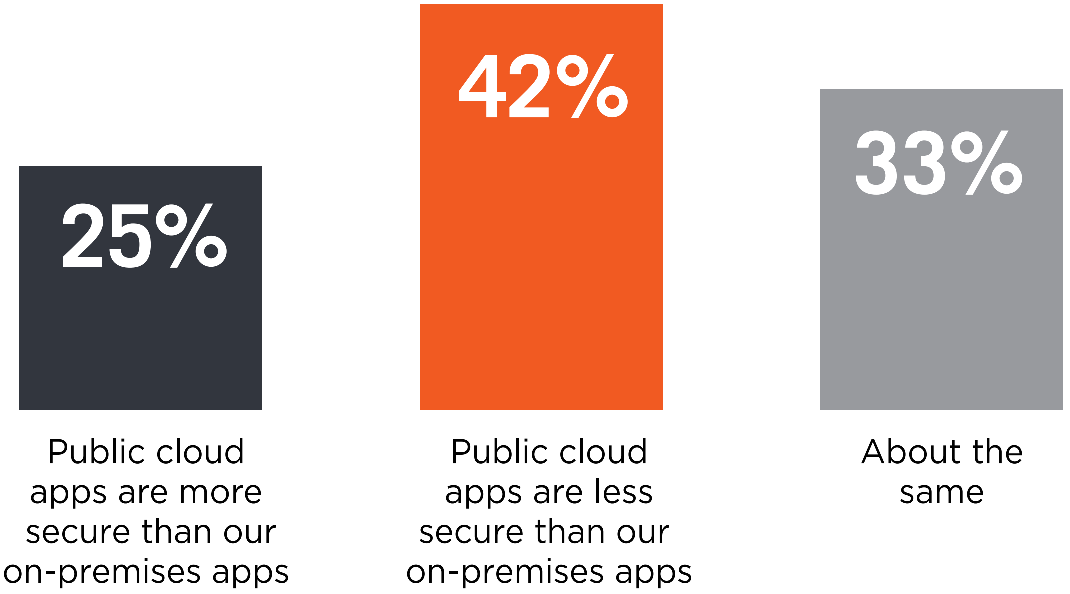
Not sure 4%

SAAS VS ON-PREMISES

Perceptions of SaaS security remain relatively unchanged this year. A majority, 58%, believe that cloud apps are as secure or more secure than on-premises applications.

Are public cloud apps/SaaS (such as Salesforce and Office 365) more or less secure than on-premises applications?

Public cloud apps/SaaS



OPERATIONAL SECURITY HEADACHES

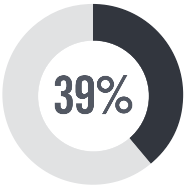
As more workloads move to the cloud, cybersecurity professionals are increasingly realizing the complications to protect these workloads. The biggest security operations challenge organizations face is visibility into infrastructure security (44%), followed by setting consistent security policies across 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?

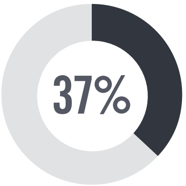
44%
Visibility into infrastructure security

42%
Setting consistent security policies

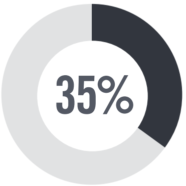
42%
Compliance



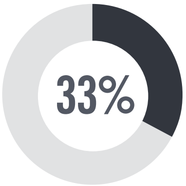
Security can't keep up with pace of change in applications



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%).

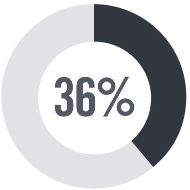
What do you think are the biggest security threats in public clouds?

#1 **62%** Misconfiguration of thecloud platform/ wrong set-up

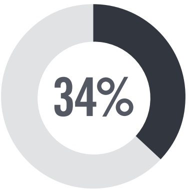
55% Unauthorized access

52% Insecure interfaces /APIs

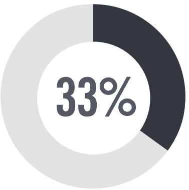
49% Hijacking of accounts, services or traffic



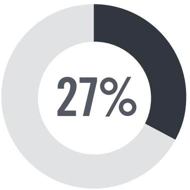
External sharing of data



Foreign state-sponsored cyberattacks



Malicious insiders



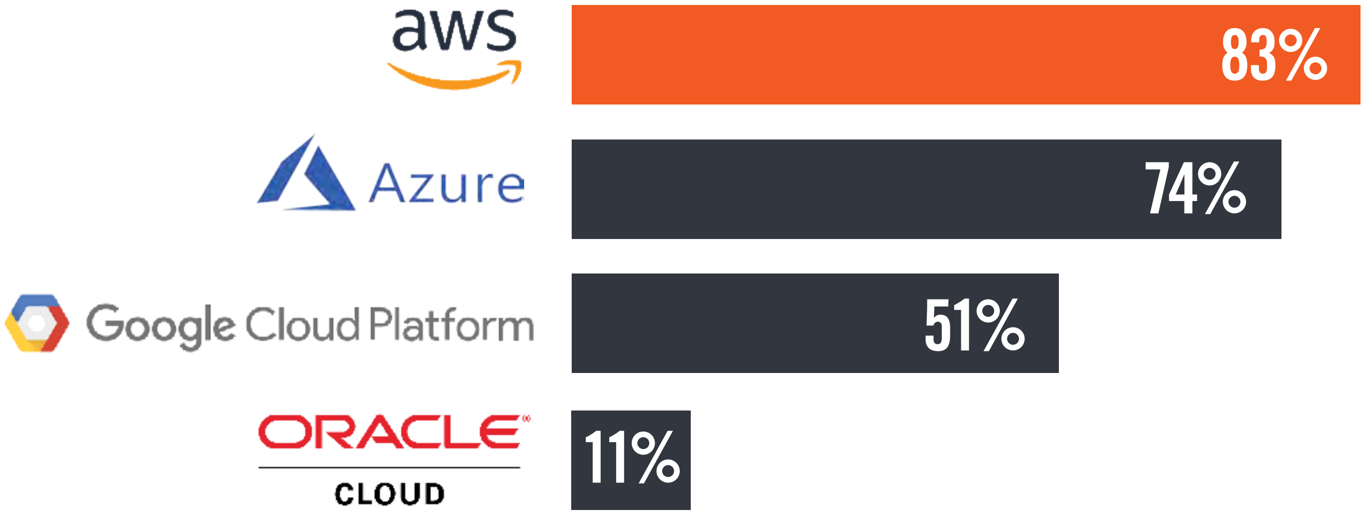
Malware/ ransomware

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

NATIVE SECURITY

Organizations rank AWS highest in their assessment of the cloud platform's native security controls (83%).

Which of the following platforms do you think provides sufficient native cloud security controls and services?



Other 3%

AWS SECURITY EFFECTIVENESS

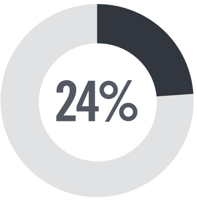
AWS users give the highest grades for effectiveness to AWS identity and access controls (44%), followed by infrastructure security (33%), and inventory and configuration management (28%).

How do you rate the effectiveness in the following AWS security tiers in use by your organization?

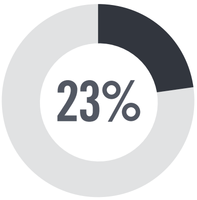
44%
Identity and Access Control
(AWS IAM, AWS Multi-Factor Authentication, AWS Directory Service)

33%
Infrastructure Security
(network firewalls, web application firewalls, network encryption)

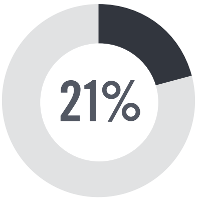
28%
Inventory and Configuration Management
(AWS Config, Amazon Inspector, AWS Cloud Formation)



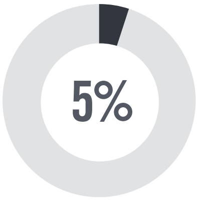
DDoS Protection



Data Encryption (incl. crypto key management and storage)



Monitoring and Logging (API call visibility with AWS Cloud Trail, Alert notification with mazon CloudWatch)



Penetration Testing

POPULAR 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%

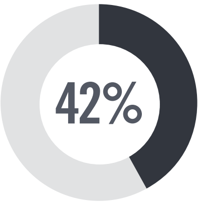
AWS Identity & Access Management
(Manage User Access and Encryption Keys)

65%

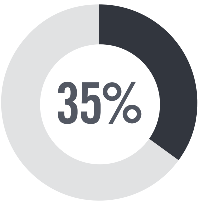
Amazon CloudWatch
(Monitor and Track AWS Apps and Gain System-Wide Utilization Visibility)

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% |

MOST DEPLOYED SECURITY CAPABILITIES

The most commonly deployed cloud security control is data encryption (62%) and network encryption (51%), tied with SIEM (51%), and cloud access controls (50%).

What security capabilities have you deployed in the cloud?

62%

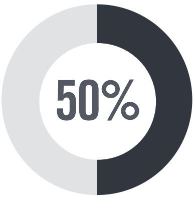
Data encryption

51%

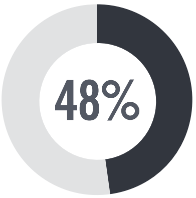
Network encryption
(VPN, packet encryption, transport encryption)

51%

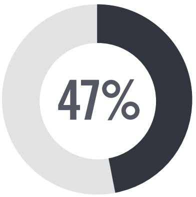
Security Information and Event Management (SIEM)



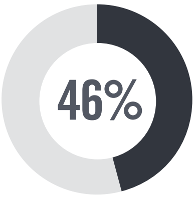
Access control
(e.g., CASB/Cloud Access Security Brokers)



Trained cloud security professionals



Vulnerability assessment



Intrusion detection and prevention

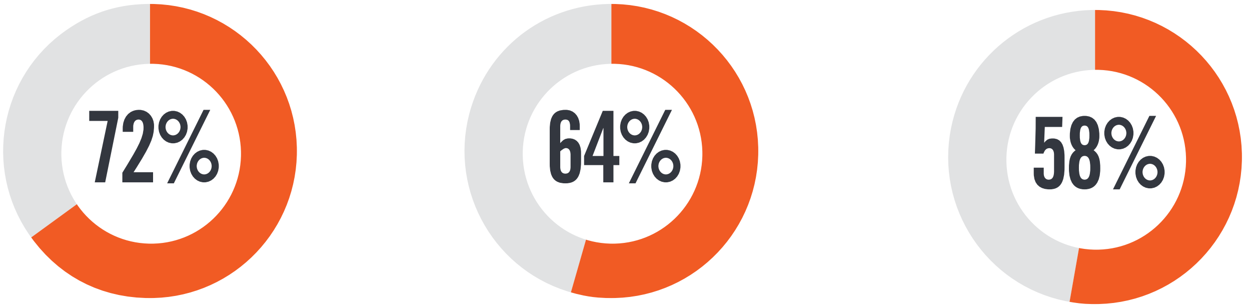
Log management and analytics 46% | Configuration management 46% | Data leakage prevention 45% | Privileged Access 44% | Single sign-on/user authentication 43% | Firewalls/NAC 42% | Endpoint security controls 41% | Patch management 41% | Anti-virus/anti-malware 39% | Network monitoring 37% | Application 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%

DATA PROTECTION IN THE CLOUD

With use of the cloud increasing every year, more data is stored in cloud environments. For the second year in a row, cybersecurity professionals say access controls (72%) are the primary method to protect data in the cloud, followed by encryption or tokenization (64%).

This year, the use of security services offered by the cloud provider (58%) jumped from fourth place to third, suggesting that organizations are looking toward their service providers to help provide additional data protection and risk mitigation as part of their services stack.

How do you protect data in the cloud?



We use access controls

We use encryption or tokenization

We use security services offered by the cloud provider

We connect to the cloud via protected networks 50% | We deploy cloud security monitoring tools 43% | We deploy additional security services offered by third-party vendors 37% | We don't protect data in the cloud 3% | Not sure/other 10%

CLOUD SECURITY CRITERIA

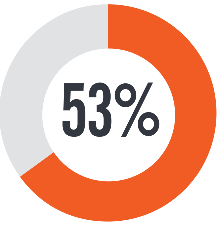
As organizations adopt the cloud, many recognize the need to partner with security providers for robust protection capabilities not available in-house. The top three attributes cybersecurity professionals look for in a cloud security provider include cloud native security tools (65%), cost effectiveness (60%), and seamless integration with cloud platforms (60%).

What do you look for in your cloud security provider?

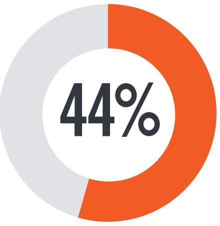
65% **Security tools are cloud native**
(are agile, can be deployed with automation, support scalability, etc.)

60%
Cost effectiveness

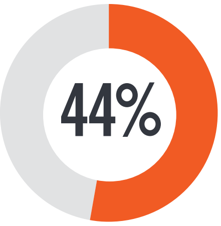
60%
Integrates seamlessly with cloud platforms



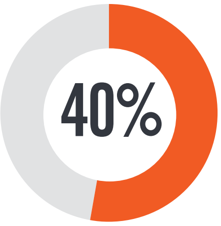
Ease of deployment



Demonstrates cloud knowledge



Policy customization



Multi-cloud support

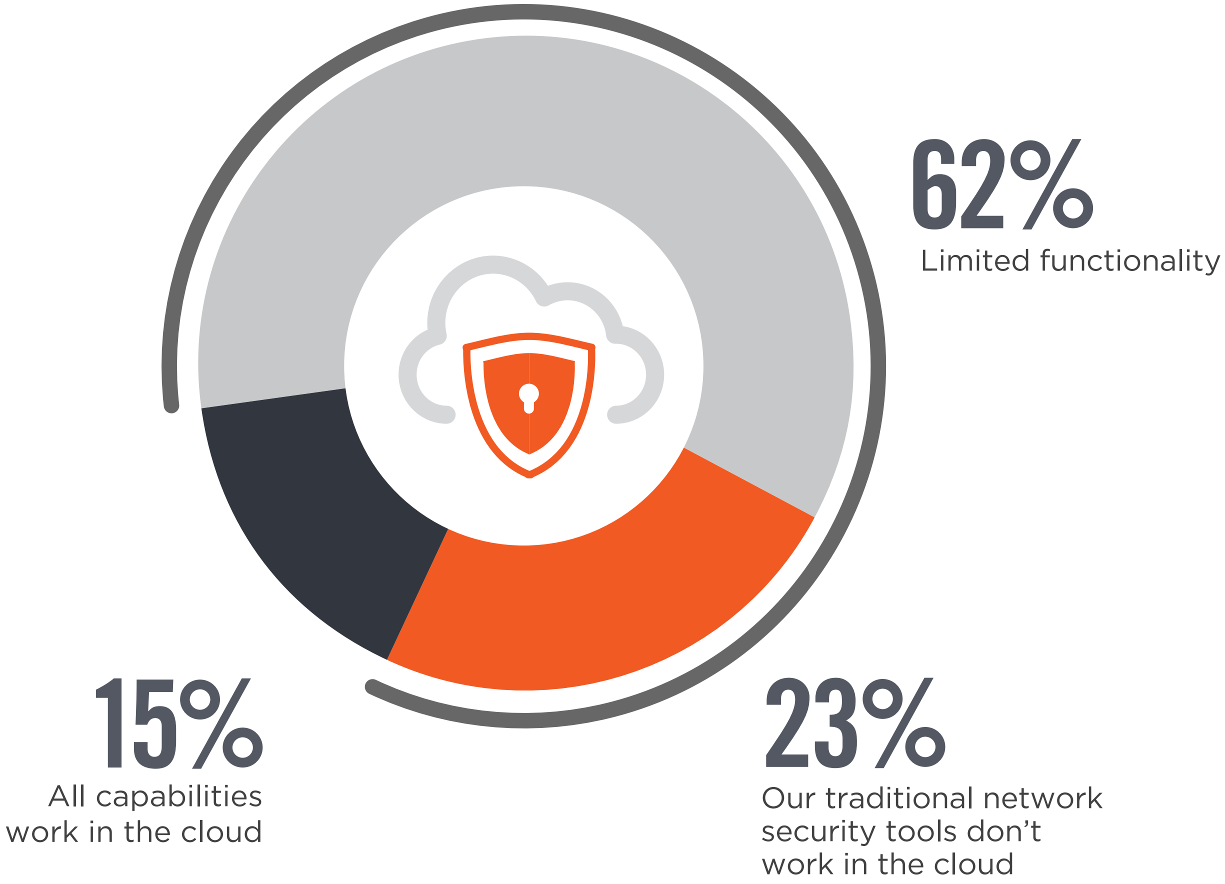
Not sure/other 7%

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



DRIVERS FOR CLOUD NATIVE SECURITY TOOLS

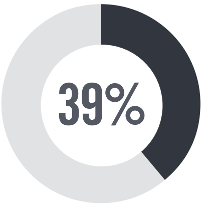
Organizations recognize the advantages of deploying cloud native security solutions, including faster time to deployment (52%) and lower cost (47%).

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

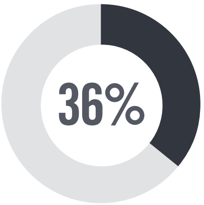
52%
Faster time to deployment

47%
Cost savings

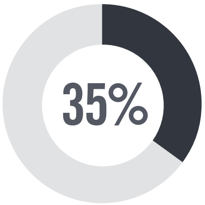
41%
Need for secure app access from any location



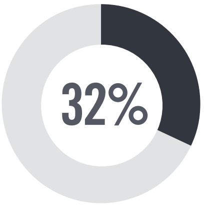
Reduced effort around patches and upgrades of software



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%

BARRIERS TO CLOUD-BASED SECURITY ADOPTION

Despite the significant advantages offered by cloud-based security solutions, barriers to adoption still exist. When it comes to business transformation and cloud adoption, three important aspects must be aligned: people, process and technology.

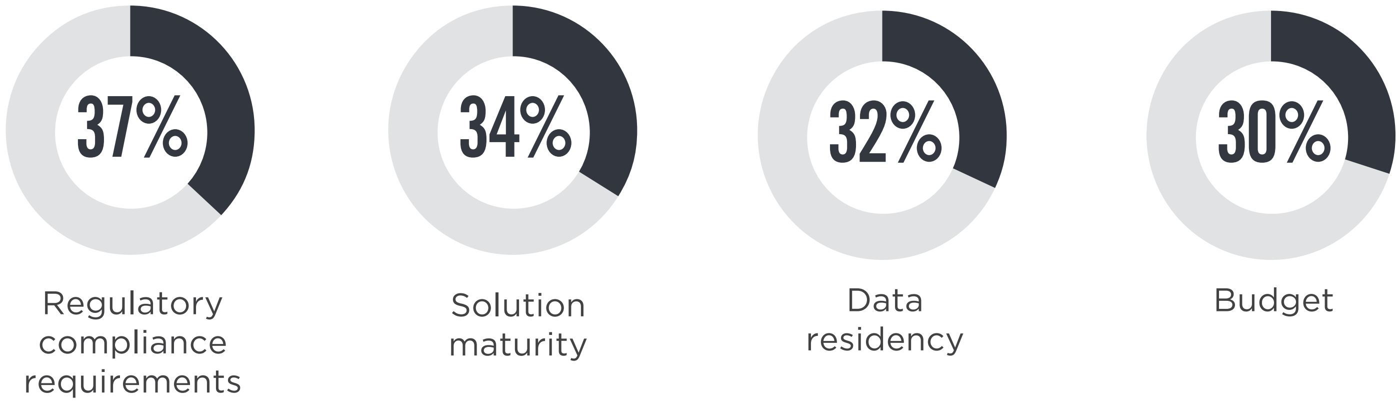
Our survey reveals that the biggest challenge organizations are facing is not technology, it's people and processes. Staff expertise and training (58%) ranked number one in the survey, followed by data privacy concerns (43%) and lack of integration with on-premises technology (37%).

What are the main barriers to migrating to cloud security solutions?

58% Staff expertise/ training

43% Data privacy

37% Lack of integration with on-premises security technologies



Limited control over encryption keys 25% | Sunk cost into on-premises tools 23% | Integrity of cloud security platform (DDoS attack, breach) 22% | Scalability and performance 13% | Not sure/other 11%

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%).

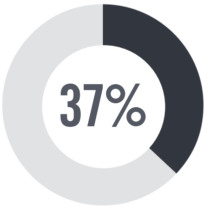
Which part of the cloud compliance process is the most challenging?

56%

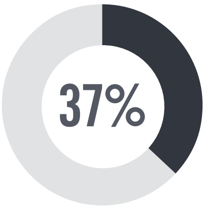
Monitoring for compliance with policies and procedures

54%

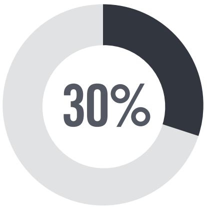
Going through audit/risk assessment within the cloud environment



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



Applying the Shared Responsibility Model



Scaling and automating compliance activities

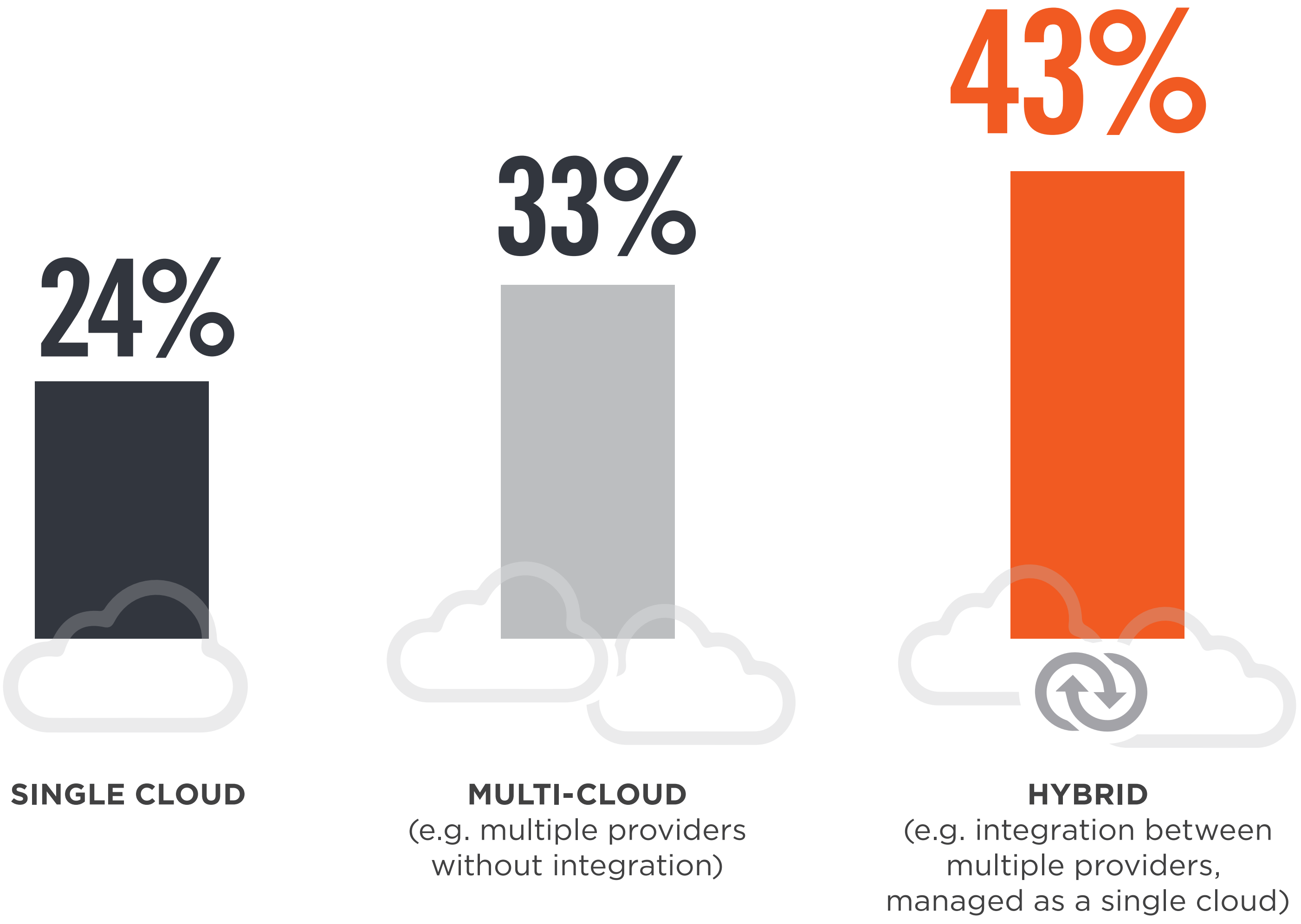
Data quality and integrity in regulatory reporting 26% | Not sure/other 11%

CLOUD STRATEGY

Forty-three percent of organizations say their primary cloud deployment strategy is a hybrid cloud, optimizing their investment by integrating multiple cloud providers to work together as a single seamless environment. The remaining respondents said their cloud deployment of choice was a non-integrated, multi-cloud solution (33%), followed by a single cloud (24%).

The growing trend is organizations are leveraging more than one cloud provider for a multitude of reasons, ranging from high availability (HA), disaster recovery (DR) and multi-vendor sourcing strategy to name a few.

▶ What is your primary cloud deployment strategy?

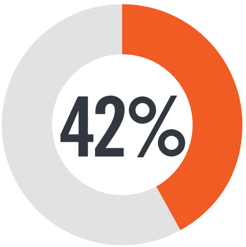


BARRIERS TO CLOUD ADOPTION

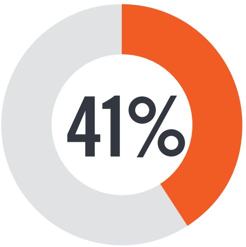
It’s important to recognize that with all of the benefits, cloud is not without its challenges. Lack of qualified staff or expertise tops the list as the primary barrier to cloud adoption (46%), followed by general security risks (42%), data security, loss & leakage risks (41%), and integration with existing IT environments (40%). The survey highlights a number of technical and organizational barriers that continue to hinder cloud adoption, as cloud technologies continue to mature, many of these barriers will be easier to overcome for organizations.

What is your primary cloud deployment strategy?

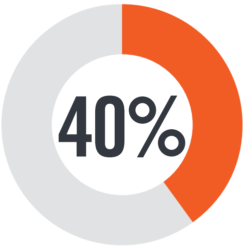
46% Lack of staff resources or expertise



General security risks



Data security, loss & leakage risks



Integration with existing IT environment

Legal & regulatory compliance 35% | Loss of control 27% | Fear of vendor lock-in 26% | Internal resistance and inertia 26% | Lack of maturity of cloud service models 23% | Complexity managing cloud deployment 21% | Lack of transparency and visibility 21% | Lack of management buy-in 19% | Lack of budget 18% | Cost/lack of ROI 15% | Billing & tracking issues 15% | Dissatisfaction with cloud service offerings/performance/pricing 12% | Performance of apps in the cloud 12% | Lack of customizability 11% | Lack of support by cloud provider 8% | Availability 5% | Not sure/other 15%

CLOUD CONFIDENCE BUILDERS

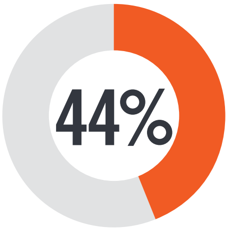
We asked organizations which actions cloud providers could take to improve their confidence in moving to the cloud. They identified five key confidence boosters to help alleviate their security concerns: encrypting data-at-rest (52%) was the number one issue to address, followed by APIs for reporting, auditing and alerting on security events (49%), and setting and enforcing security policies across clouds (47%).

Which of the following would most increase your confidence in adopting public clouds?

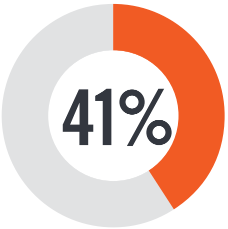
52%
Encryption of data-at-rest

49%
APIs for reporting, auditing and alerting on security events

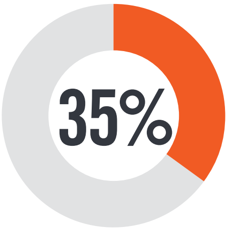
47%
Setting and enforcing security policies across clouds



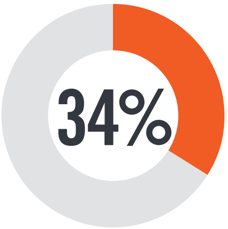
Automating compliance



Creating data boundaries



Isolation/protection of virtual machines



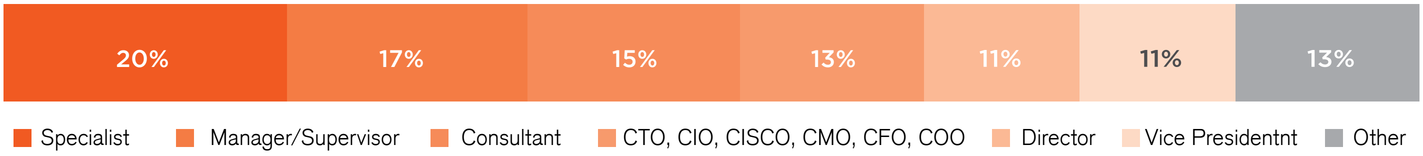
Leveraging data leakage prevention tools

Limiting unmanaged device access 31% | Protecting workloads 21% | Not sure/other 12%

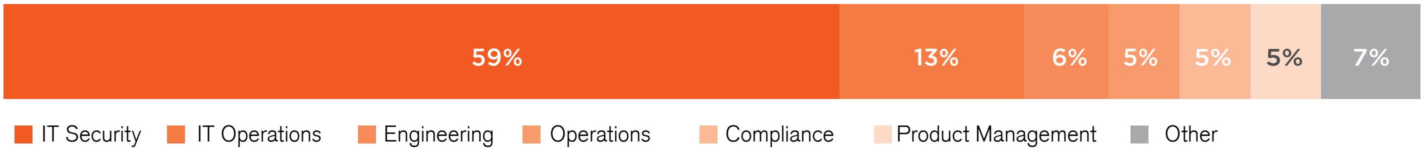
METHODOLOGY & DEMOGRAPHICS

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.

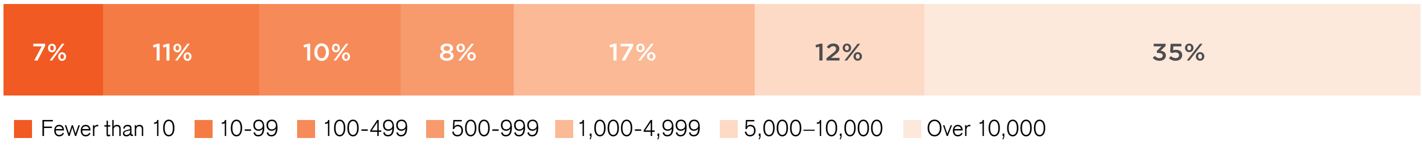
CAREER LEVEL



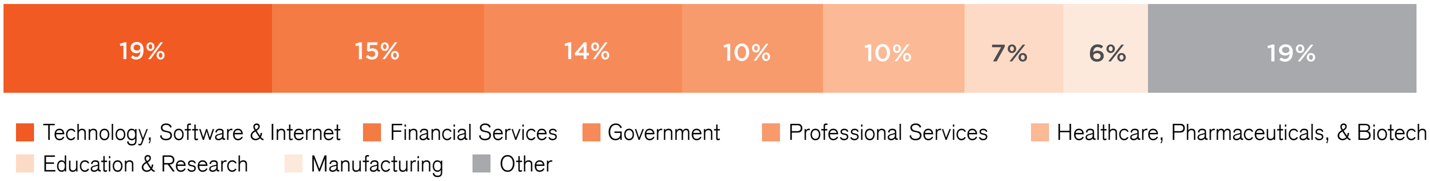
DEPARTMENT



COMPANY SIZE



INDUSTRY


Technology, Software & Internet
Financial Services
Government
Professional Services
Healthcare, Pharmaceuticals, & Biotech
Education & Research
Manufacturing
Other