CLOUD SECURITY

2017 SPOTLIGHT REPORT

Linked in Group Partner

Information Security

Crowd Research Partners

PRESENTED BY Quest

OVERVIEW

Cloud investment continues to grow over 20% annually as organizations are looking for faster time to deployment, scalability, reduced maintenance, and lower cost. But there is one aspect of cloud that consistently worries IT and security professionals – how to achieve high levels of security in the cloud. As cloud adoption increases, the fears of unauthorized access, stolen identities, data and privacy loss, and confidentiality and compliance issues are rising right along with it.

This report has been produced by the 350,000 member Information Security Community on LinkedIn in partnership with Crowd Research Partners to explore how organizations are responding to the security threats in the cloud and what tools and best practices IT cybersecurity leaders are considering in their move to the cloud.

This report reveals the latest data points and trends in cloud security, shares how your peers are approaching security, and provides valuable benchmark data that will help gauge how your own organization stacks up compared with others.

Many thanks to our sponsor Quest for supporting this exciting research project.

Thank you,

Holger Schulze

Holger Schulze
Founder
Information Security
Community on LinkedIn

✉ hhschulze@gmail.com

Linked in Group Partner
Information
Security

CLOUD SECURITY SPOTLIGHT REPORT

TABLE OF CONTENTS

KEY SURVEY FINDINGS

1 While cloud computing has become a mainstream delivery choice for applications, services and infrastructure, concerns about cloud security remain high. The top three cloud security concerns respondents need to address include protecting against data loss (57%), threats to data privacy (49%), and breaches of confidentiality (47%).

2 Moving to the cloud brings new security challenges that require new types of skills. To address these evolving security needs, 53% of organizations want to train and certify their current IT staff - by far the most popular approach. This is followed by partnering with a managed service provider (MSP) (30%), leveraging software solutions (27%) or hiring dedicated staff (26%).

3 As more workloads are moved to the cloud, organizations are increasingly realizing that traditional security tools are not designed for the unique challenges cloud adoption presents (78%). Instead, strong security management and control solutions designed specifically for the cloud are required to protect this new, agile paradigm.

4 Visibility into cloud infrastructure is the biggest security management headache for 37% of respondents, moving up to the top spot from being the second ranking concern in 2016. Compliance comes in second (36%) and setting consistent security policies as the third biggest headache at 33%.

5 A third of organizations predict cloud security budgets to increase over the next 12 months. With 33%, cloud security is receiving the largest share of predicted budget increase across all IT security areas.

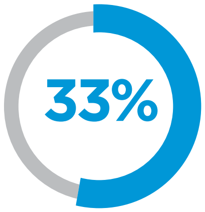
BARRIERS TO CLOUD ADOPTION

Cloud security risks still top the list of barriers to cloud adoption (33%). The most dramatic shift compared to the previous survey is the rise in the lack of staff and expertise to manage cloud security (28%) - moving from #5 to #2 and trading places with legal and regulatory concerns (24%) as key barriers to cloud adoption.

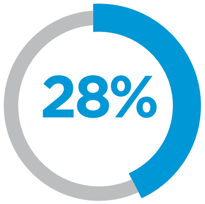
Q: What are the biggest barriers holding back cloud adoption in your organization?

Cloud Adoption Barriers

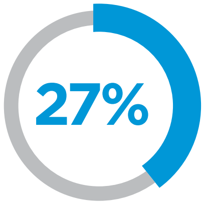
#1
General security risks



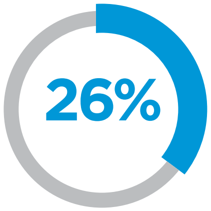
#2
Lack of staff resources or expertise



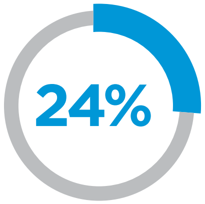
#3
Integration with existing IT environments



#4
Data loss & leakage risks



#5
Legal & regulatory compliance



Loss of control 23% | Management complexity 20% | Internal resistance and inertia 18% | Lack of budget 18% | None 17% | Fear of vendor lock-in 16% | Lack of maturity of cloud service models 15% | Cost/Lack of ROI 15% | Internal resistance and inertia | Management complexability 13% | Lack of transparency and visibility 13% | Lack of management buy-in 13% | Performance of apps in the cloud 10% | Dissatisfaction with cloud service offerings/performance/pricing 10% | Lack of customizability 8% | Billing & tracking issues 6% | Lack of support by cloud provider 6% | Availability 4% | Not sure/Other 12%

BIGGEST CLOUD SECURITY THREATS

Unauthorized access through misuse of employee credentials and improper access controls continues to be the single biggest threat to cloud security (61%). This is followed by hijacking of accounts (52%) and insecure interfaces/APIs (43%). Forty-two percent of organizations say external sharing of sensitive information is the biggest security threat. Insider threats also is a concern for organizations.

Q: What do you consider the biggest security threats in public clouds?

#1

Unauthorized access

61%

#2

Hijacking of accounts, services or traffic

52%

#3

Insecure interfaces /APIs

43%

#4

External sharing of data

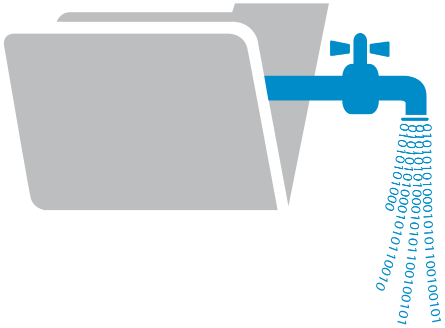
42%

Malicious insiders 34% | Denial of service attacks 33% | Foreign state sponsored cyber attacks 29% | Malware injection 22% | Theft of service 19% | Lost mobile devices 12% | Not sure/Other 12% |

CLOUD SECURITY CHALLENGES

Cloud providers offer many security measures; however, organizations are ultimately responsible for securing their own data, applications, and services in the cloud. The top three cloud security challenges highlighted by cybersecurity professionals are protecting against data loss (57%), threats to data privacy (49%), and breaches of confidentiality (47%) - virtually unchanged compared to the previous year.

Q: What are your biggest cloud security concerns?



57%
Data loss/leakage

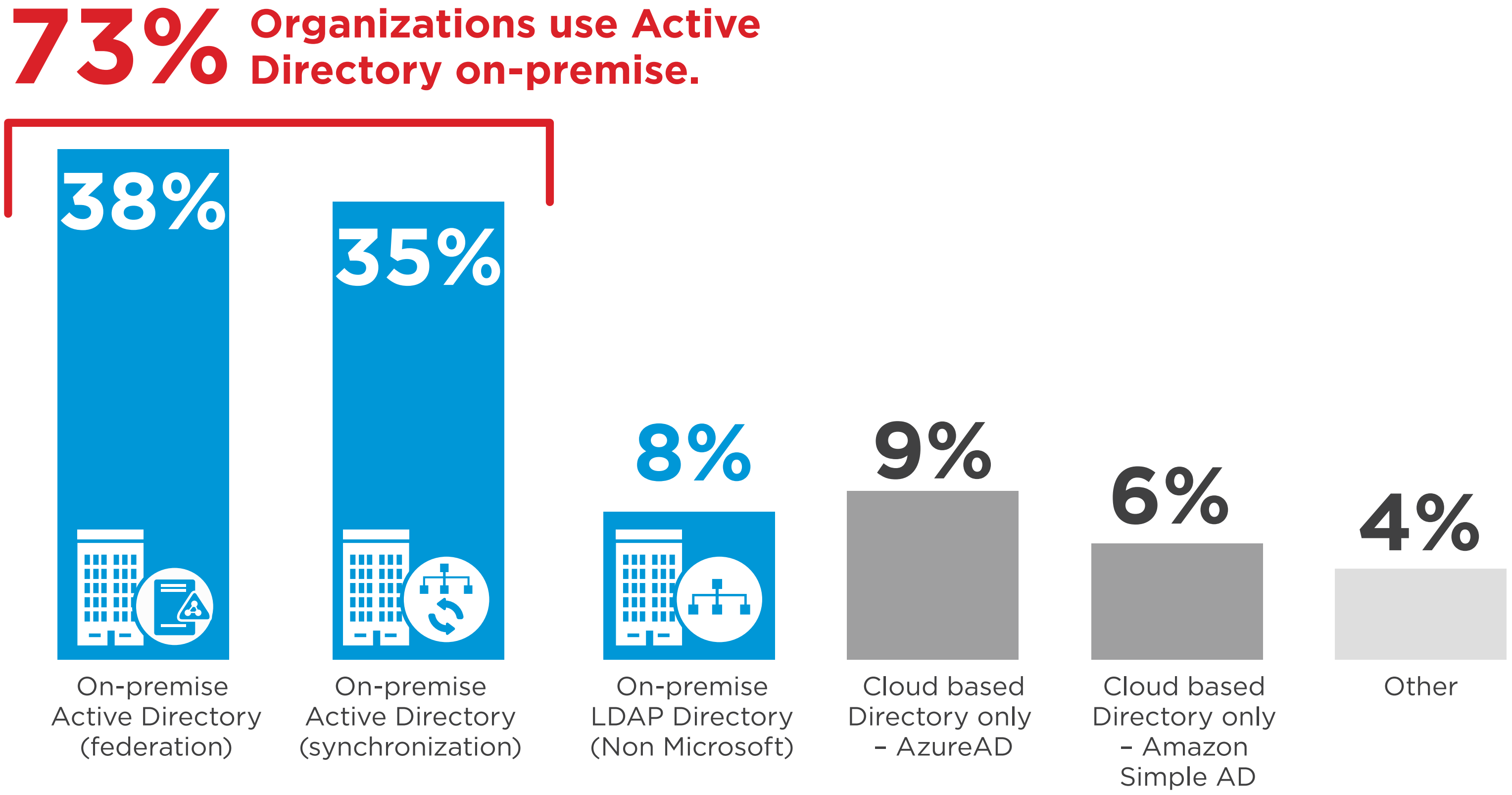
Data privacy	Confidentiality	Legal and regulatory compliance	Data sovereignty/ control
49%	**47%**	**36%**	**30%**

Accidental exposure of credentials 25% | Compliance 24% | Visibility & transparency 22% | Lack of forensic data 20% | Liability 18% | Availability of services, systems and data 17% | Fraud (e.g., theft of SSN records) 17% | Incident & problem management 17% | Disaster recovery 13% | Business continuity 12% | Performance 12% | None 1%

ACCESS TO CLOUD APPLICATIONS

Seventy-three percent of organizations use Active Directory on-premise as the authoritative directory to identify, authenticate and authorize access to cloud applications. Consequently, access to cloud based applications for a majority of organizations depends heavily on proper security controls around on-premise Active Directory infrastructure. The cloud enablement of Active Directory is a key enabler for moving to cloud-based security infrastructure.

Q: What is the authoritative directory you use for identity data identification and authentication, and authorization of access for your cloud based applications?



CLOUD SECURITY HEADACHES

Visibility into cloud infrastructure security is the biggest security management headache for 37% of respondents, moving up to the top spot from being the second ranking concern last year. Compliance comes in second (36%, moving up from #3), and setting consistent security policies is the third biggest headache at 33%, moving down from #1 previous year.

Q: What are your biggest cloud security headaches?

37%

Visibility into infrastructure security

Compliance

36%

Setting consistent security policies

33%

Reporting security threats

29%

Remediating threats

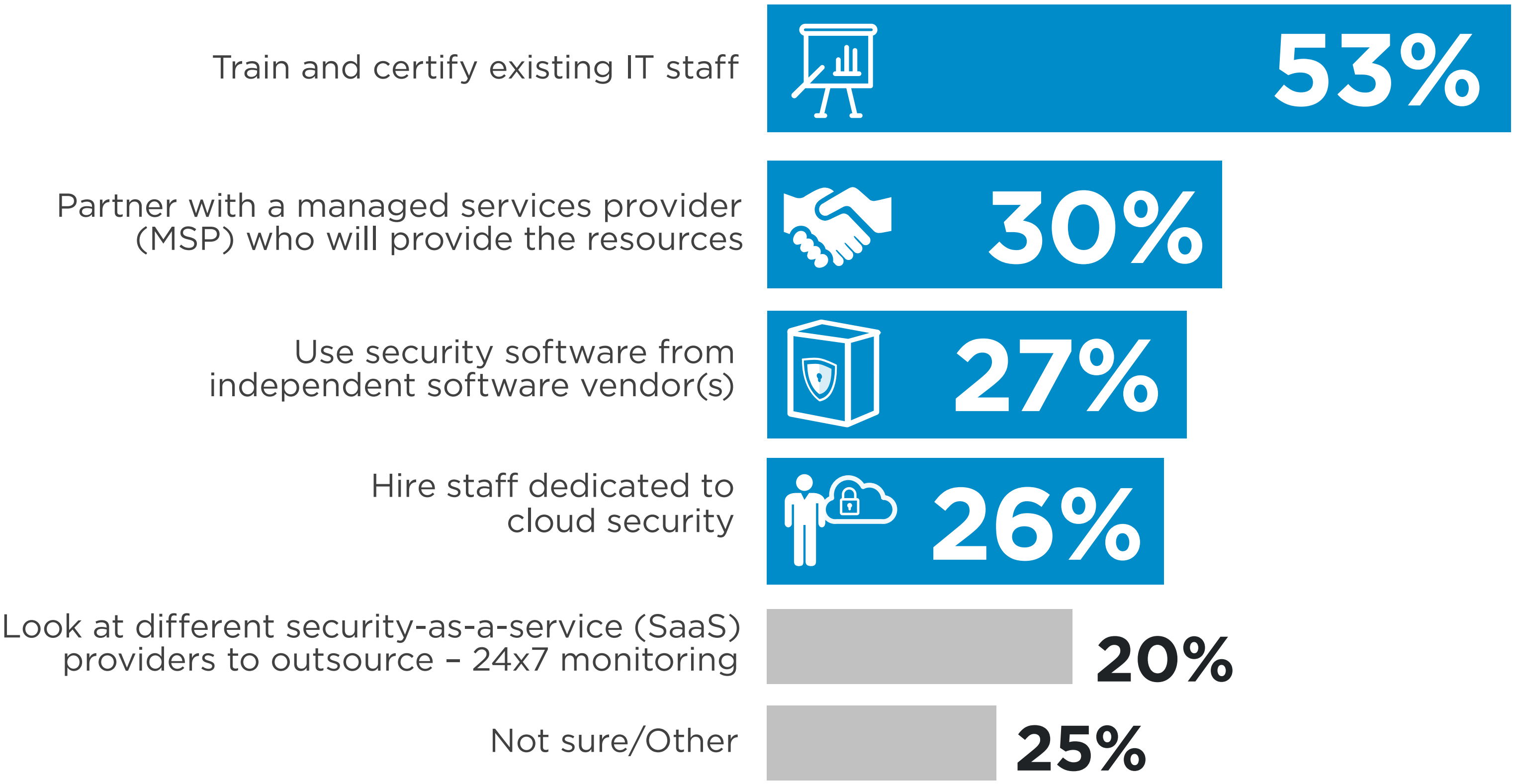
28%

Lack of integration with on-prem security technologies 27% | Can't identify misconfiguration quickly 24% | No automatic discovery/visibility/control to infrastructure security 24% | Automatically enforcing of security across multiple datacenters 21% | Complex cloud to cloud/cloud to on-prem security rule matching 21% | Security can't keep up with pace of changes to new/existing applications 20% | Lack of feature parity with on-prem security solution 16% | None 7% | No flexibility 7% | Not sure/other 15%

PATHS TO STRONGER CLOUD SECURITY

Moving to the cloud brings new security challenges that require new capabilities and skills. Fifty-three percent of organizations plan to train and certify their current IT staff to ensure the proper security controls are being implemented both internally and with third party cloud service providers. Thirty percent of organizations plan to partner with a a managed service provider (MSP), 27% plan to leverage software solutions, and 26% will hire dedicated cloud security staff.

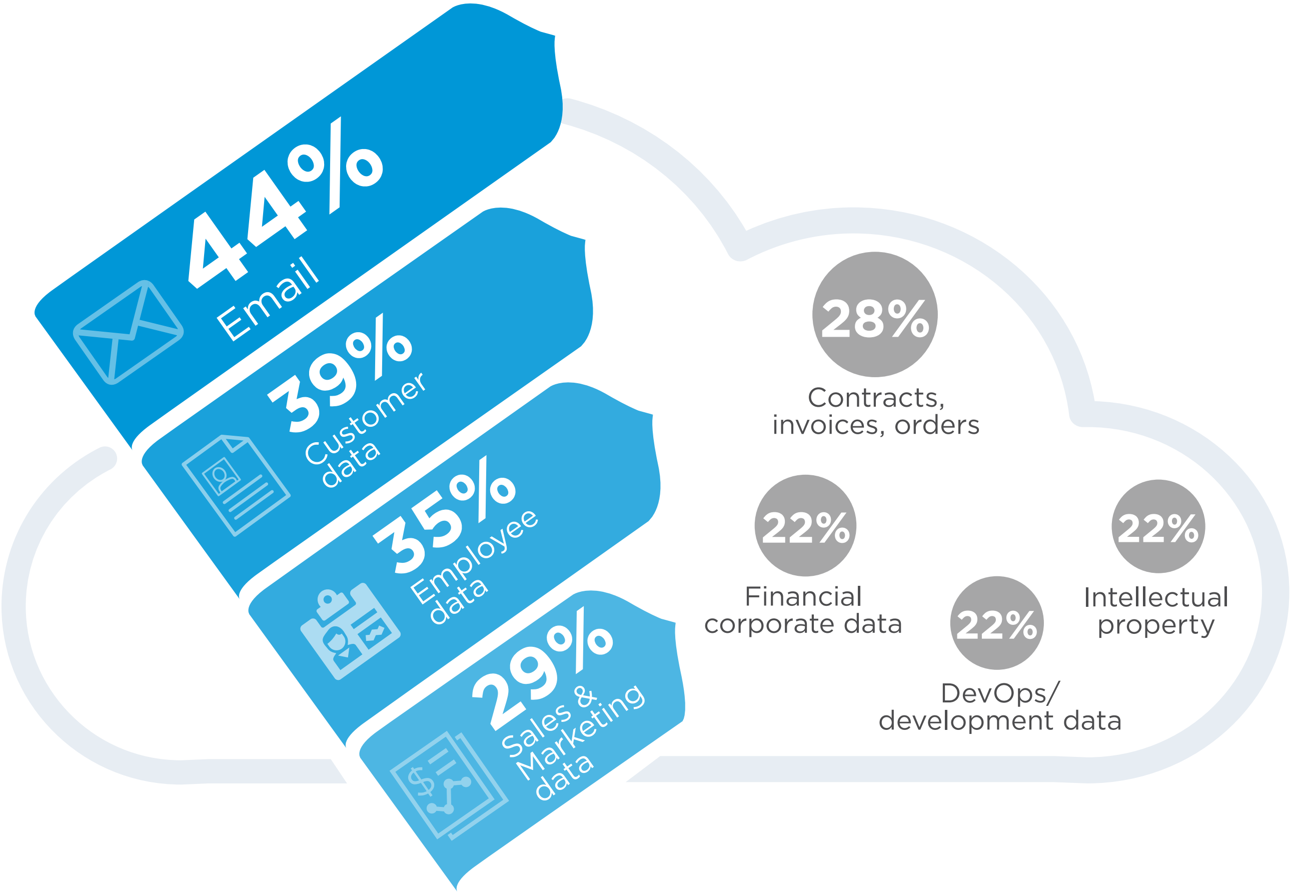
Q: When moving to the cloud, how do you plan to handle your security needs?



DATA STORED IN THE CLOUD

Email remains the most common corporate information stored in the cloud (44%), followed by customer data (39%) and employee data (35%). Fewer organizations store intellectual property information (22%), financial corporate data (22%) or DevOps/development data (22%) in the cloud.

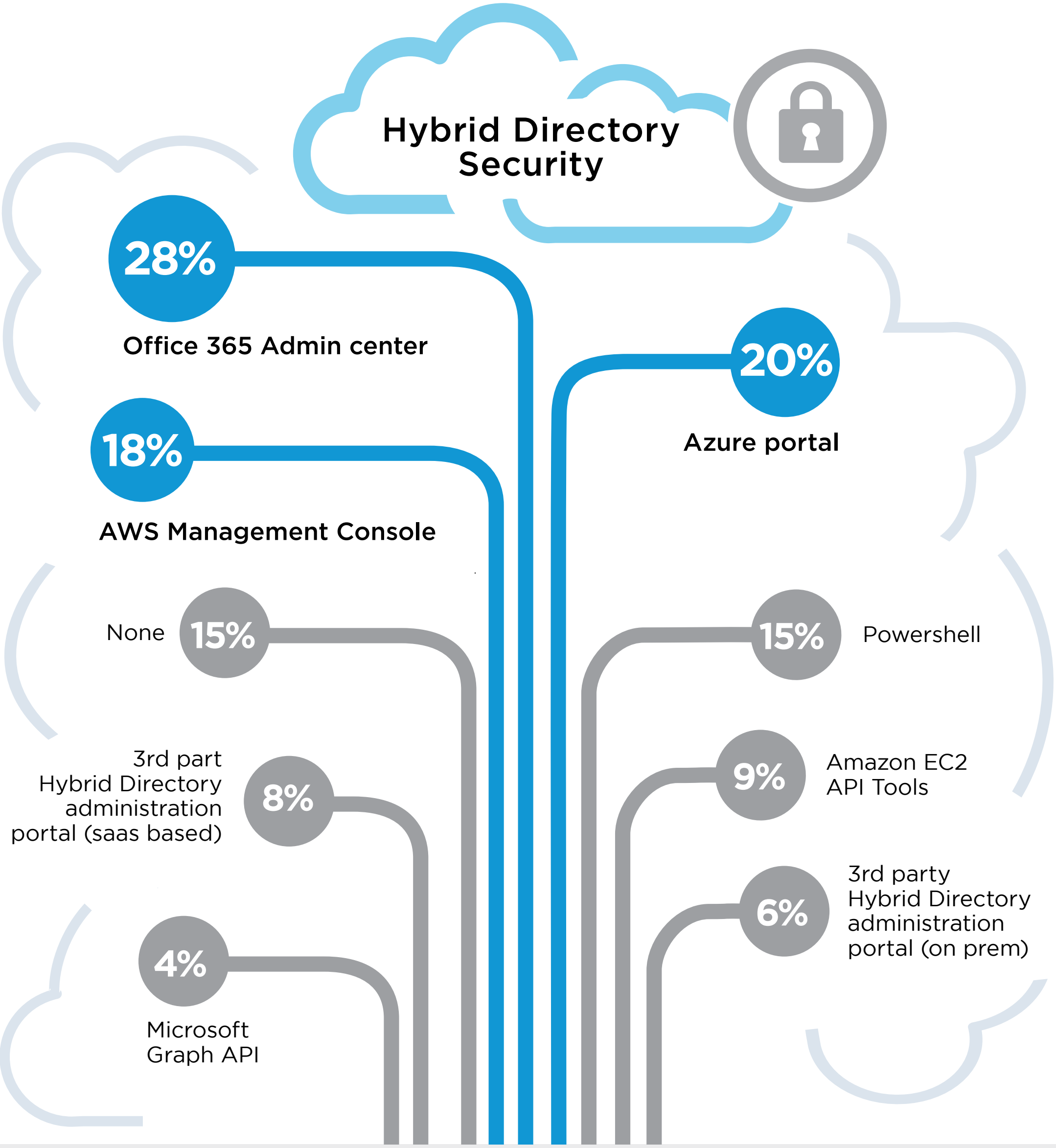
Q: What types of corporate information do you store in the cloud?



HYBRID DIRECTORY SECURITY MANAGEMENT

The most popular way to manage hybrid directory security is through the Office 365 Admin Center (28%), followed by cloud consoles for Azure (20%) and AWS (18%).

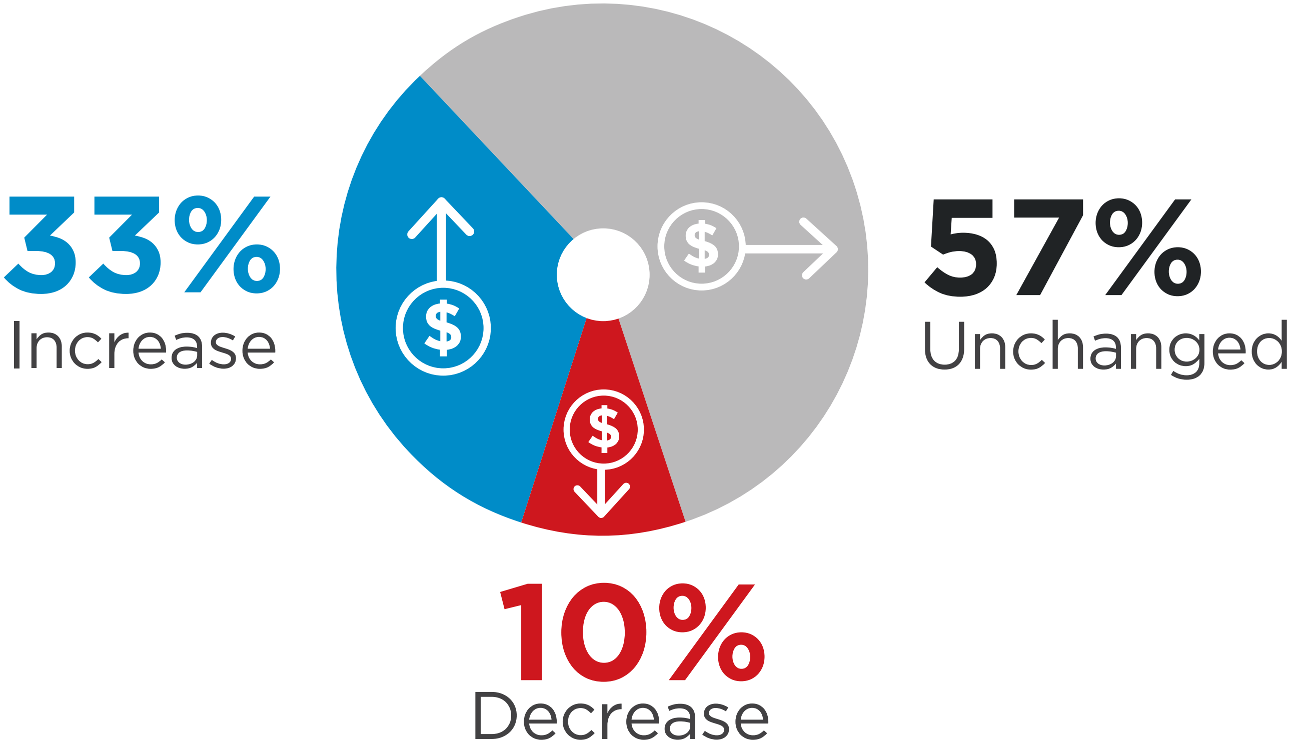
Q: How are you currently managing your hybrid directory security administration (permission reporting, change auditing, user / group administration, etc.)?



CLOUD SECURITY BUDGET

A third of organizations predict cloud security budgets to increase over the next 12 months. With 33%, cloud security is receiving the largest share of predicted budget increase across all IT security domains.

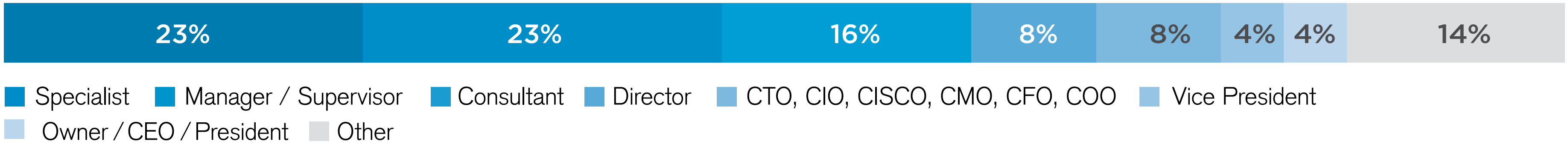
Q: What is your organization's budget outlook for cloud security?



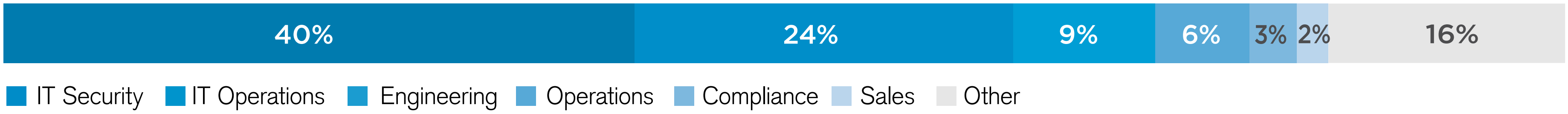
METHODOLOGY & DEMOGRAPHICS

The 2017 Cloud Security Report is based on the results of a comprehensive online survey of over 1,900 cybersecurity professionals to gain more insight into the latest security threats faced by organizations and the solutions to prevent and remediate them. The respondents range from technical executives to managers and IT security practitioners. They represent organizations of varying sizes across many industries. Their answers provide a comprehensive perspective on the state of cybersecurity today.

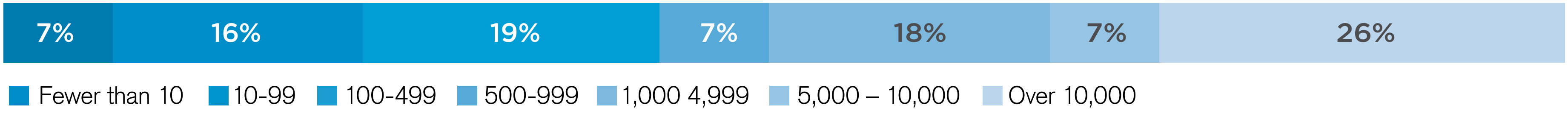
CAREER LEVEL



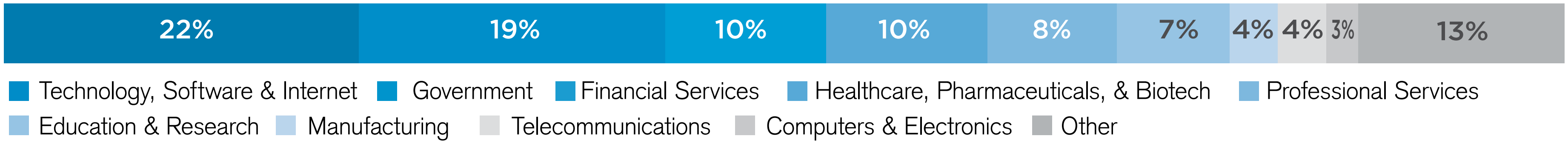
DEPARTMENT



COMPANY SIZE



INDUSTRY



SPONSOR OVERVIEW

Quest | www.quest.com

Quest® helps its customers reduce administration tasks so they can focus on growing their businesses. Combined with its invitation to the global community to be a part of the innovation, Quest continues to deliver the most comprehensive solutions for Microsoft Azure cloud management, SaaS, security, workforce mobility and data-driven insight.