CLOUD SECURITY

2017 SPOTLIGHT REPORT

LinkedIn Group Partner
Information Security

Crowd Research Partners

ALIEN VAULT
bitglass
CloudPassage
CLOUDVISORY
Dome9 SECURITY
EASTWIND NETWORKS
evident.io
(ISC)²
Quest
skyhigh
tenable

PRESENTED BY

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 sponsors for supporting this exciting research project:

AlienVault | Bitglass | CloudPassage | Cloudvisory
Dome9 Security | Eastwind Networks | Evident.io
(ISC)² | Quest | Skyhigh | Tenable

Thank you,

Holger Schulze

Holger Schulze
Founder
Information Security
Community on LinkedIn

hhschulze@gmail.com

LinkedIn Group Partner
Information Security

CYBERSECURITY TRENDS 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%.

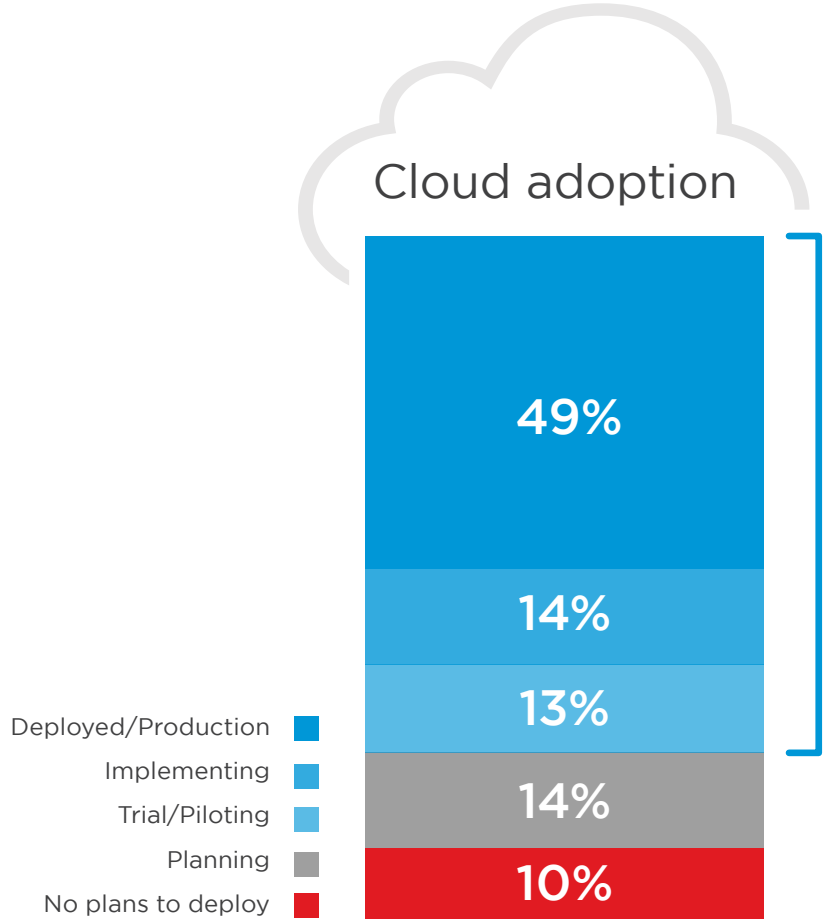
5. A third of organizations predict cloud security budgets to increase over the next 12 months. With 33%, cloud security is receiving the largest share of predicted budget increase across all IT security areas.

CLOUD ADOPTION TRENDS

CLOUD ADOPTION

Cloud adoption continues unabated. Ninety percent of respondents are in some stage of adoption and 49% are already operating in a live cloud environment (up from 41% last year). As organizations increase use of cloud services, software-as-a-service (SaaS) continues to be the most popular service model (67%, up from 61% last year).

Q: What is your organization's use of cloud today?



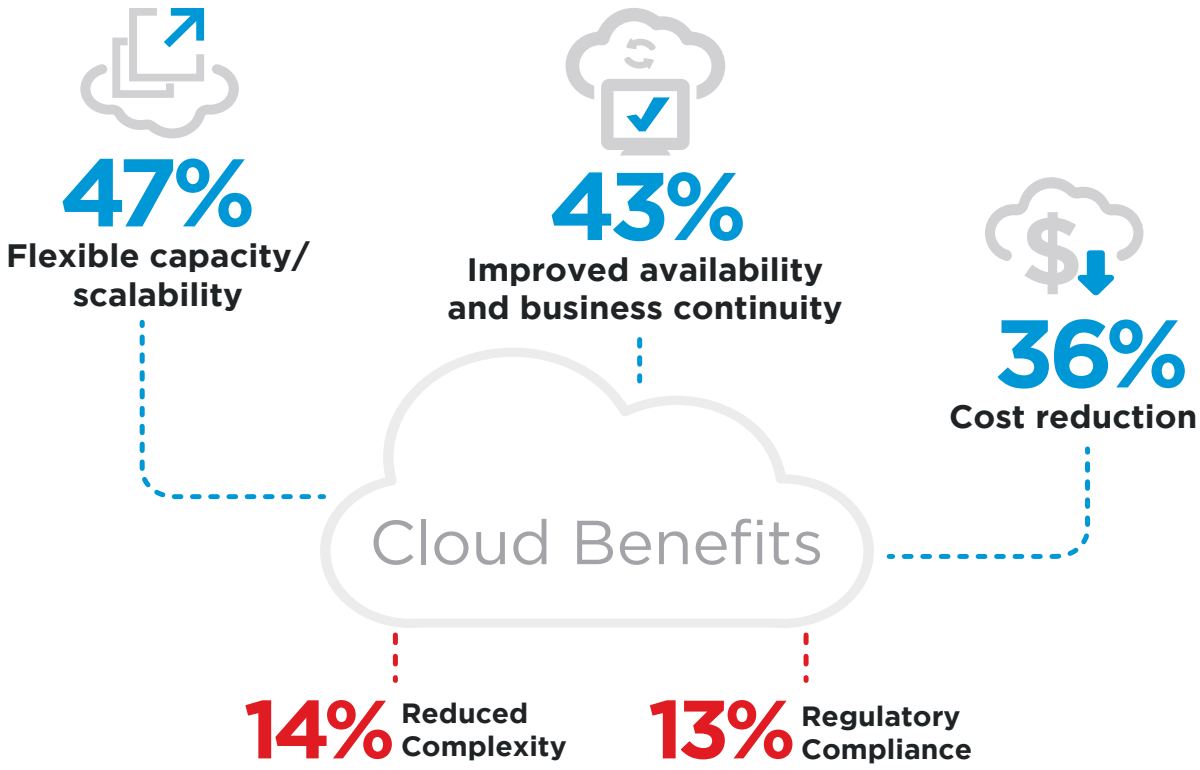
76%

of organizations are piloting, implementing or already operating in the cloud.

CLOUD BENEFITS

What's attracting survey respondents to the cloud? The highest ranked benefits have been shifting compared to last year's findings, now organizations are prioritizing the ability to have flexible capacity when needed (47%, up from 36%), followed by improved availability and business continuity (43%, down from 46%), and reduced cost (36%, down from 41%) compared to traditional on-premises IT.

Q: What overall benefits have you realized from your cloud deployment?



Moved expenses from fixed CAPEX (purchase) to variable OPEX (rental/subscription) 32% | Accelerated deployment and provisioning 31% | Increased agility 28% | Improved performance 27% | Increased efficiency 26% | Increased geographic reach 24% | Increased employee productivity 23% | Improved security 19% | Accelerated time to market 18% | Align cost model with usage 18% | Not Sure/Other 25%

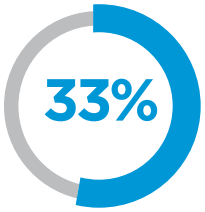
BARRIERS TO CLOUD ADOPTION

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

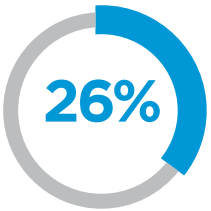
#1
General security risks



#2
Lack of staff resources or expertise

#3
Integration with existing IT environments

#4
Data loss & leakage risks



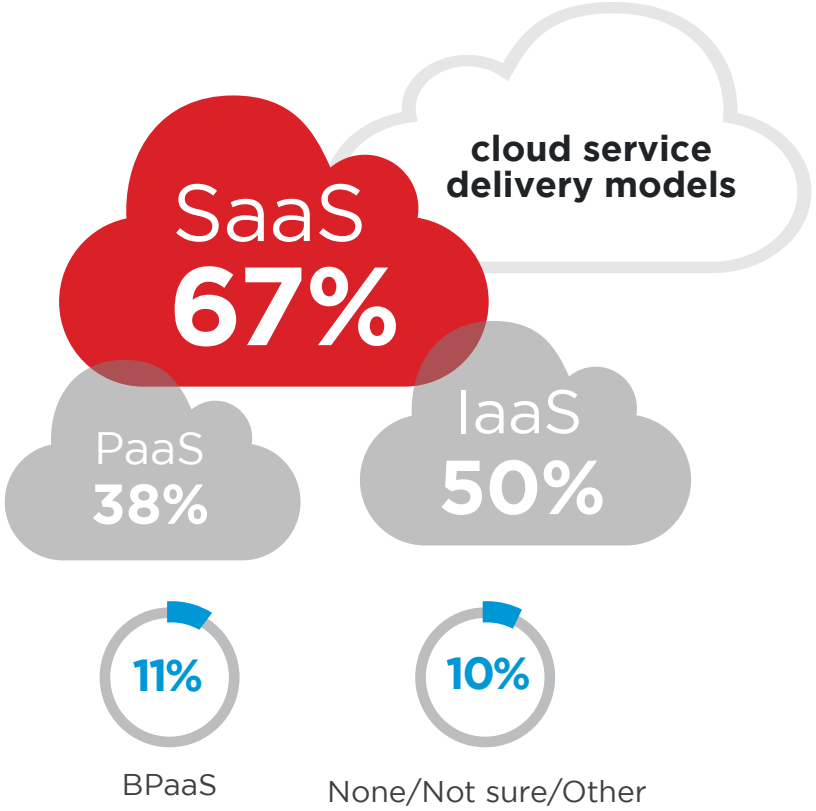
#5
Legal & regulatory compliance

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%

TOP CLOUD PROVIDERS

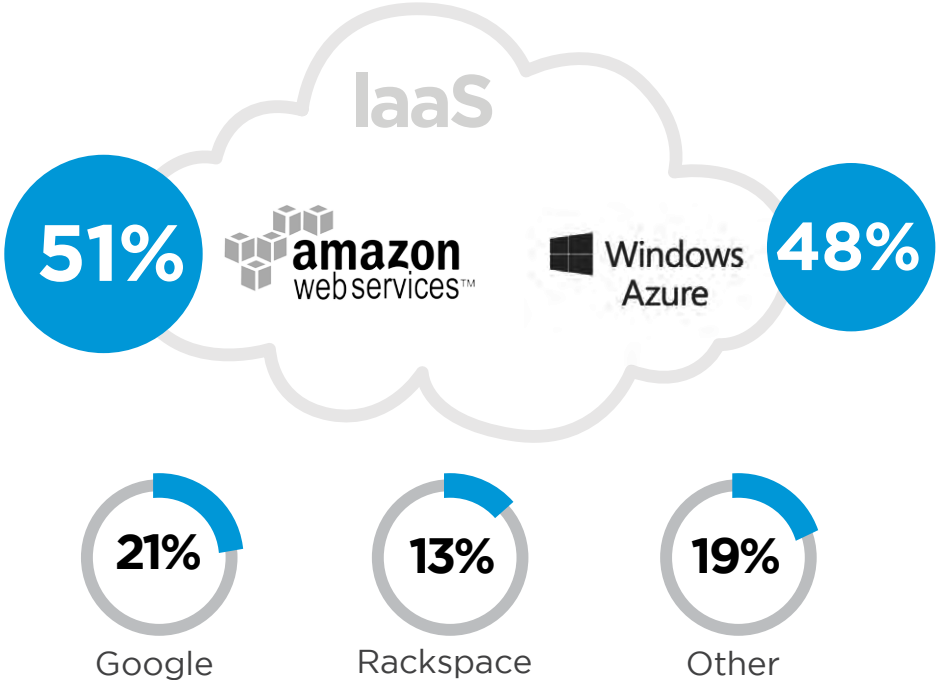
The dominance of both cloud applications and cloud infrastructure requires that organizations think about securing these different entities as part of a holistic vision for securing applications and infrastructure (both on premises and in the cloud). A majority of organizations (67%) uses SaaS models, followed by IaaS (50%) and PaaS (38%) as their cloud delivery model.

Q: What cloud service delivery model(s) is your organization using?



Amazon and Microsoft are the leading cloud providers - neck to neck based on this year's survey results.

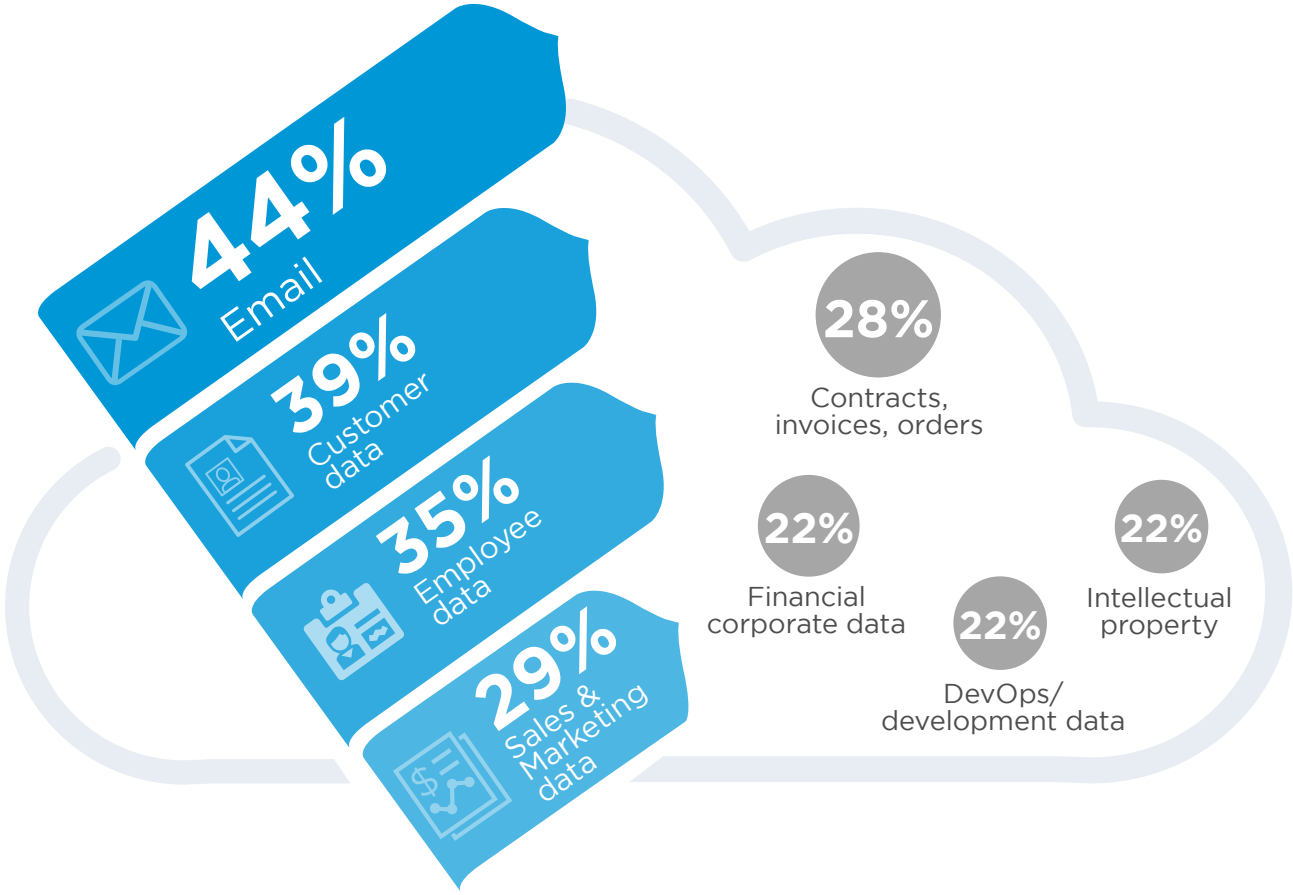
Q: What IaaS cloud provider(s) do you currently use?



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.

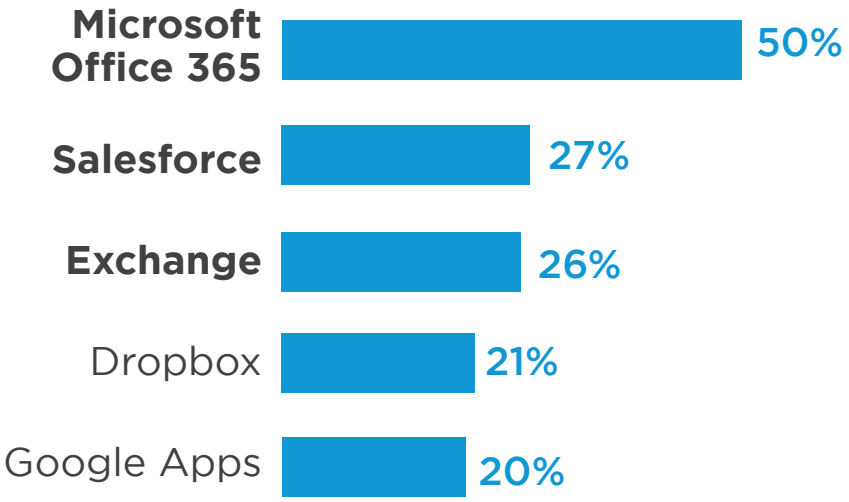
Q: What types of corporate information do you store in the cloud?



MOST POPULAR APPS

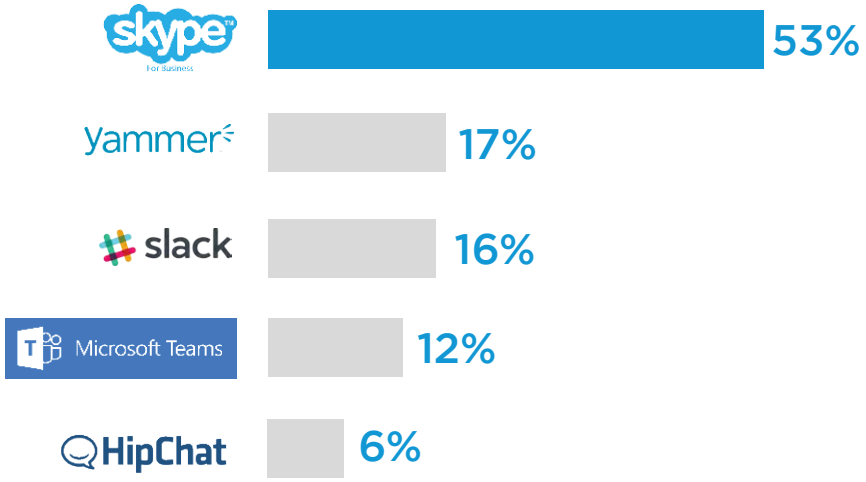
Microsoft Office 365 continues to be the leading cloud application that is deployed in the cloud. Salesforce follows second and is already deployed in 27% of organizations. The migration to Office 365 is one of the biggest changes to enterprise IT in recent years. It represents yet another step in the migration of enterprises to a utility-based model for IT services delivery that started with Salesforce.com many years ago.

Q: Which of the following cloud applications are deployed?



Cloud messaging platforms, or hosted message queue services, offer easy and reliable data exchange and is a common workload for today's IaaS platforms. Most organizations use Skype for Business (53%) as their messaging platform.

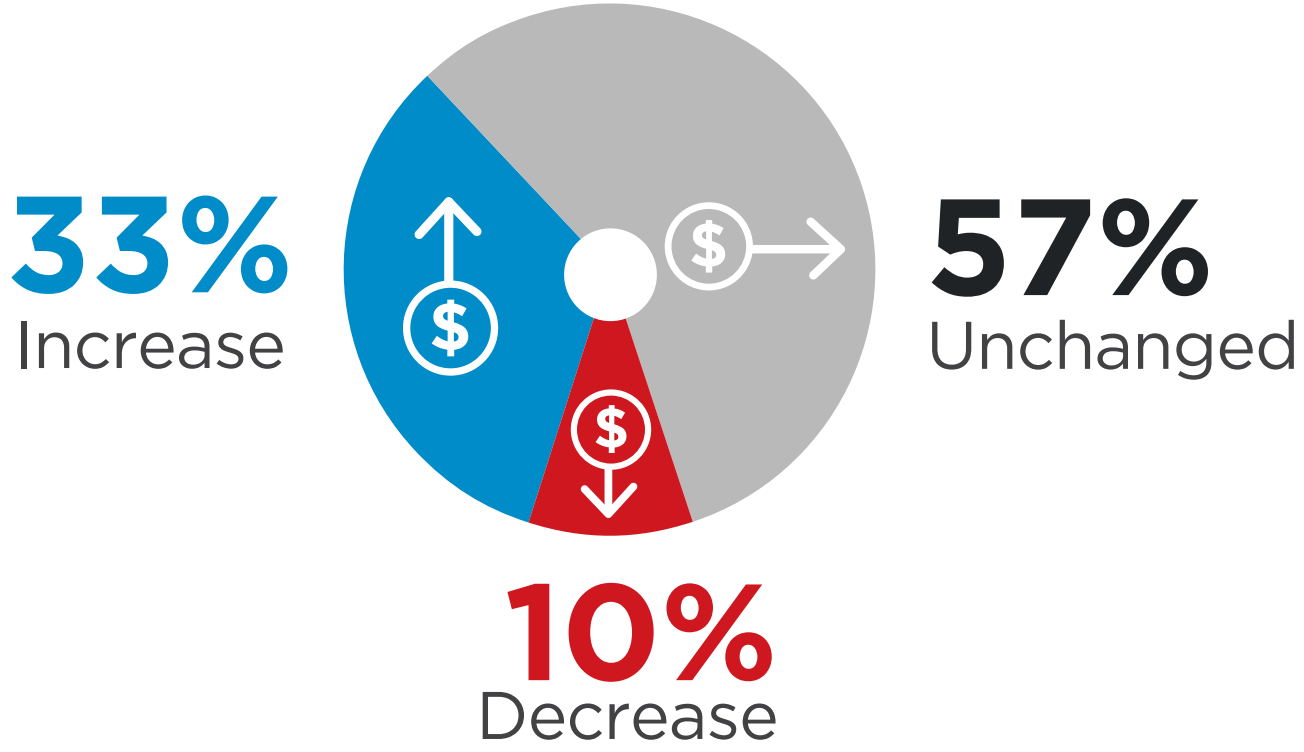
Q: Which of the following enterprise messaging apps are in use in your organization?



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?



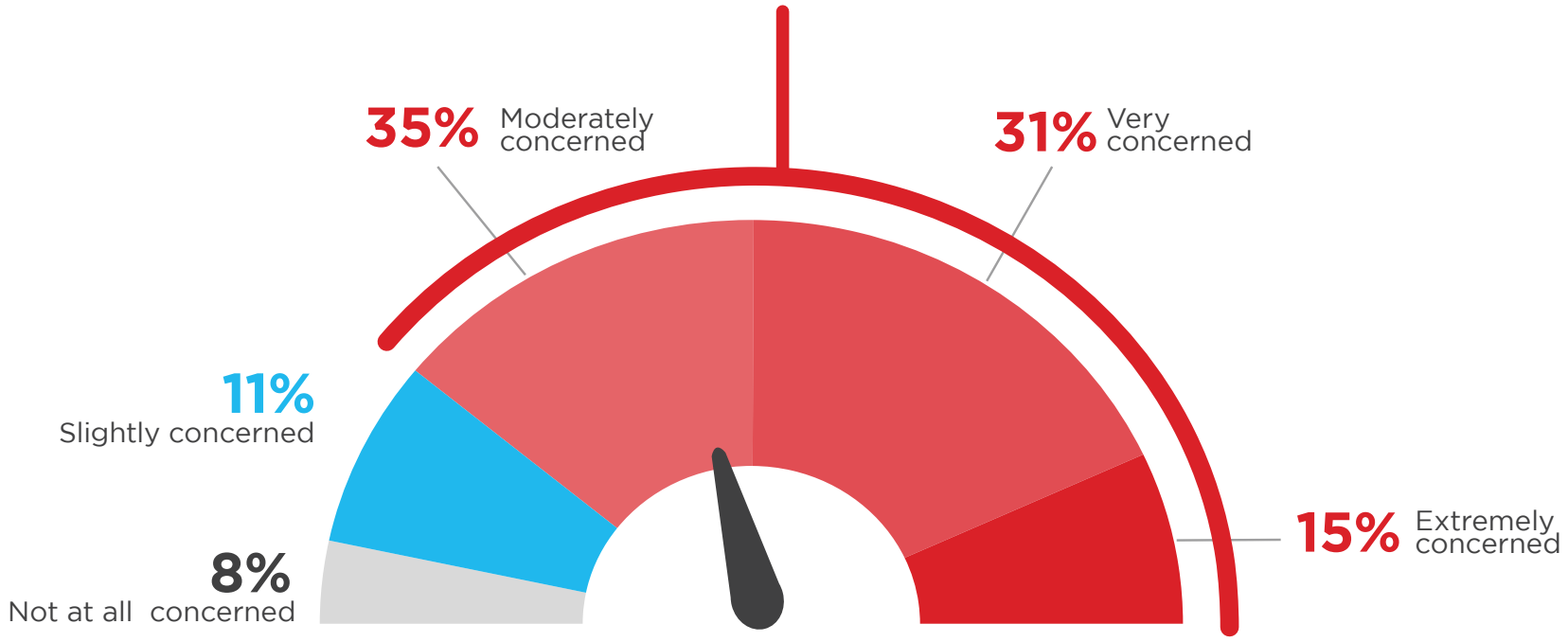
CLOUD SECURITY CHALLENGES

CLOUD SECURITY CONCERNS

Security concerns continue to be the single biggest factor holding back faster adoption of cloud computing. However, cloud security concerns are slowly decreasing compared to last year's study. This is a prime example of where security can have a profound impact on enabling business transformation.

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

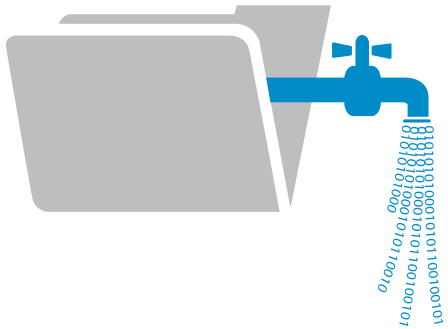
81% Organizations are concerned about cloud security



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

49%

Confidentiality

47%

Legal and regulatory compliance

36%

Data sovereignty/ control

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%

COMPLIANCE CONCERNS

As organizations mature their cloud adoption, compliance becomes a bigger headache, starting with audit and reporting (3.7), followed by contractual legal responsibilities (3.6) and concerns about an inability to meet specific compliance requirements (3.5).

Q: Please rate your level of concern with compliance issues as they relate to a public cloud. (from 1 to 5 with 5 being the highest level of concern)

Auditing and reporting requirements

CONCERN

3.7

Organization vs. provider legal responsibilities

CONCERN

3.2

Inability to meet specific requirements

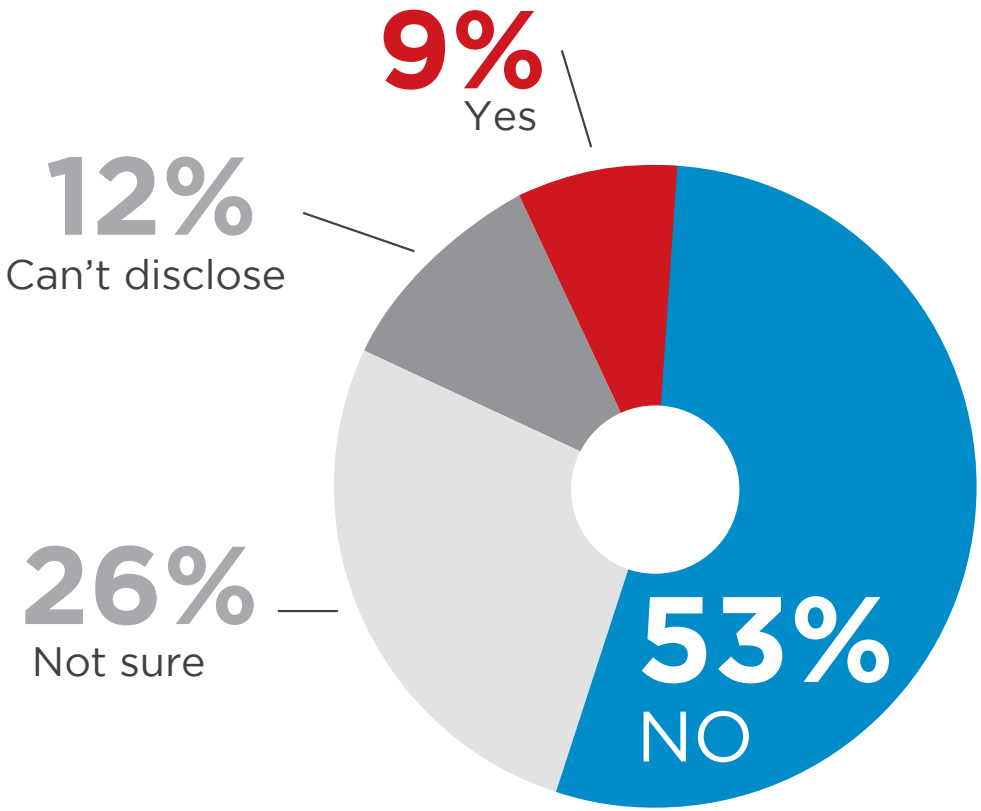
CONCERN

3.3

CLOUD SECURITY INCIDENTS

While cloud-related concerns are down 10 percentage points over last year, there is very little change in the percentage of respondents who experienced a cloud related security incident, roughly one out of ten.

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



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%

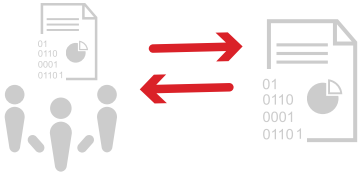
#3

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 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%

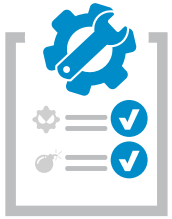
Setting consistent security policies

33%

Reporting security threats

29%

Remediating threats



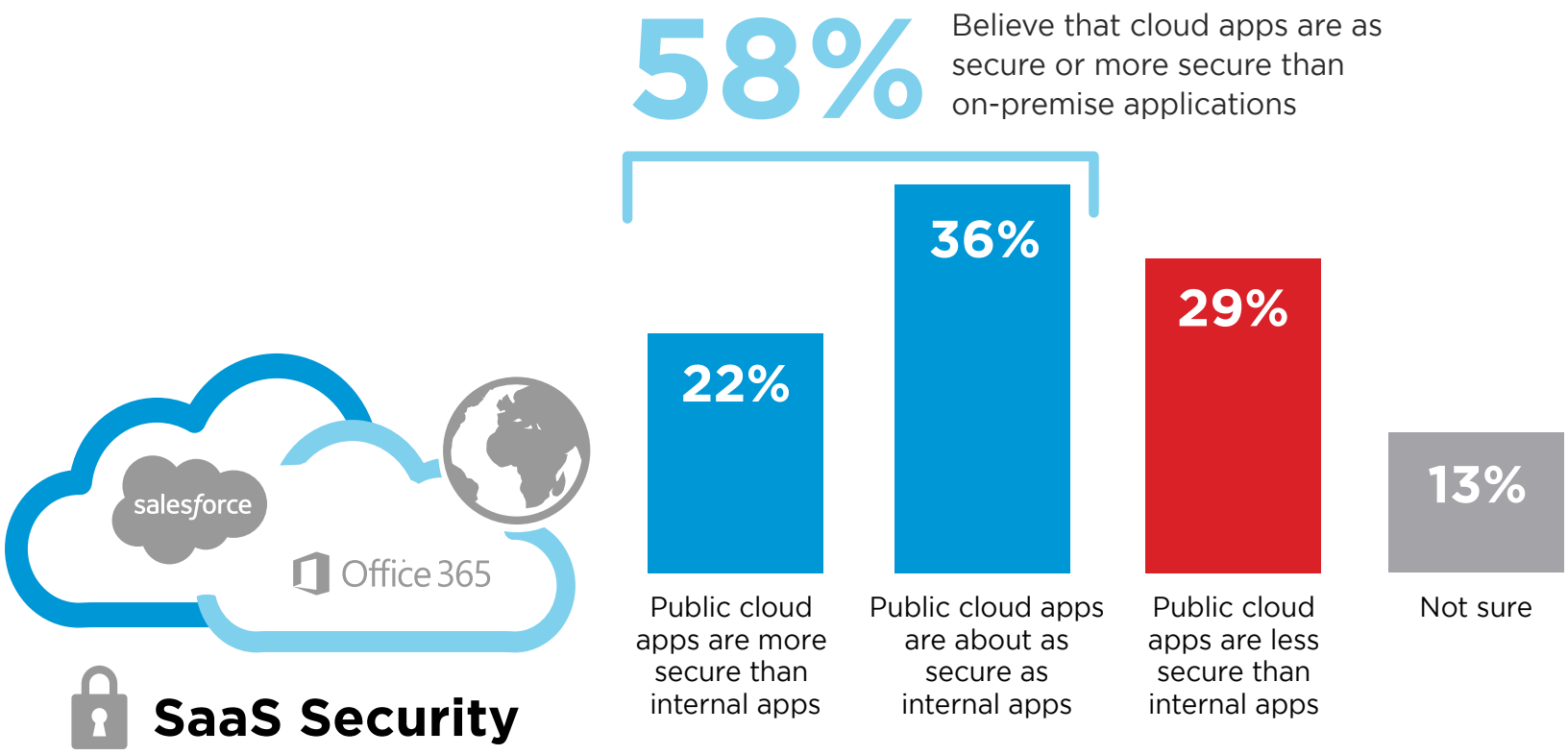
28%

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%

CLOUD APPS VS. ON-PREMISE APPS

Perceptions of SaaS security continue to improve year over year. A majority of 58% believe that cloud apps are as secure or more secure than on-premise applications, up from 52% in last year's survey. The math is simple: Large cloud providers can outspend any individual enterprise in securing their infrastructure and apply cutting-edge expertise and manpower in protecting a shared infrastructure. The results are often superior in terms of availability, performance and security of public cloud environments.

Q: Do you believe public cloud apps/SaaS like Salesforce and Office 365 are more or less secure than your internally hosted applications?



SECURITY RISKS IN THE CLOUD

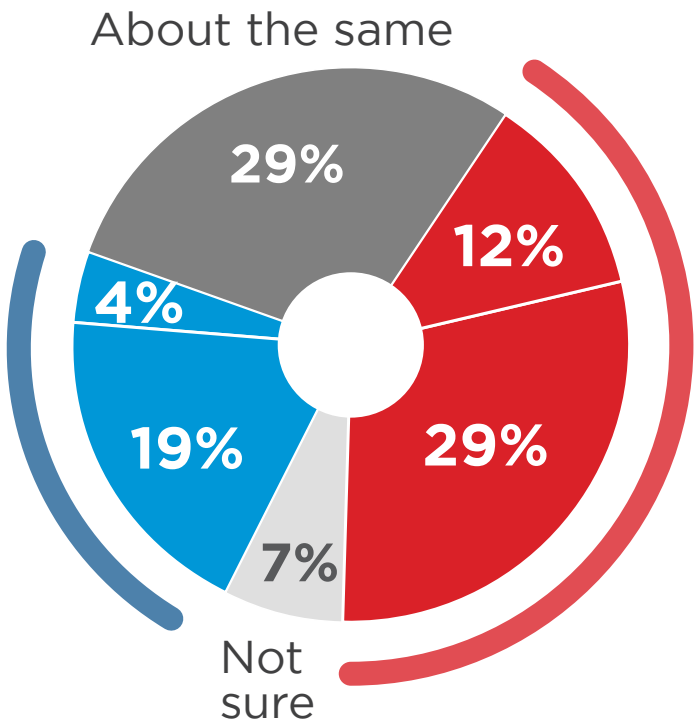
The perception of cloud security risk is still significantly higher relative to traditional enterprise IT environments. The share of organizations that see a higher risk of security breaches in the cloud compared to traditional IT environments is 41% compared to last year's 21% - a significant and surprising trend reversal.

Q: Compared to your traditional IT environment, would you say the number of security breaches you experienced in a public cloud is?

23%

Lower risk of security breaches compared to on-premise

Significantly lower (4%)
Somewhat lower (19%)



41%

Higher risk of security breaches compared to on-premise

Significantly higher (12%)
Somewhat higher (29%)

BARRIERS TO CLOUD MESSAGING APPS

Cloud messaging applications allow people to communicate from any location and any device. However, there are some barriers to adoption. Twenty-seven percent of respondents say compliance requirements is the number one adoption hurdle, followed by inadequate native security (23%), high costs (18%) and fear of lock-in (18%).

Q: What is the biggest barrier to adopting cloud messaging apps?

27%
Compliance requirements

Inadequate Native Security

High Costs

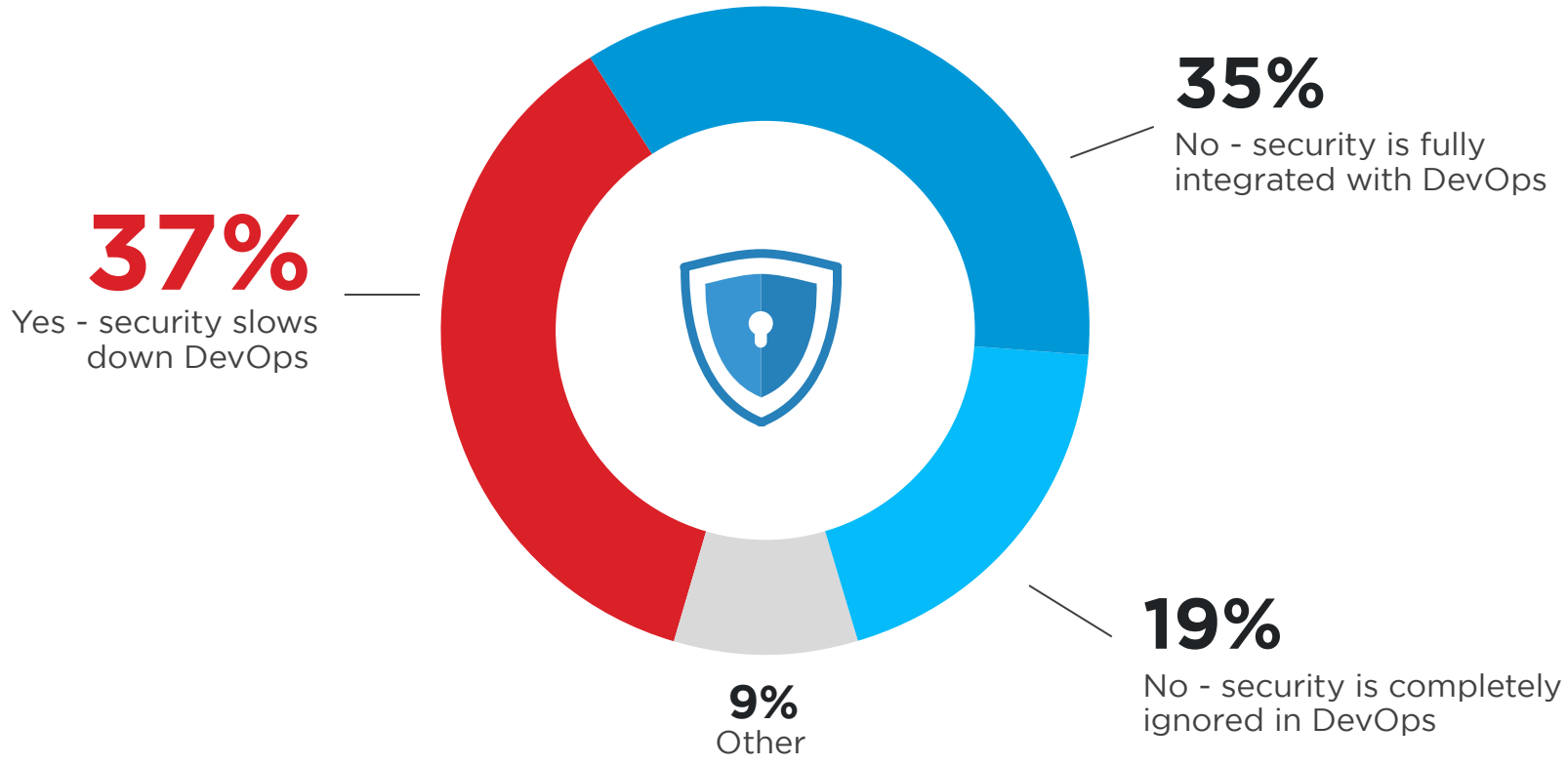
Fear of lock-in

Other

SECURITY IMPACT ON DEVOPS

Thirty-seven percent of respondents say that security slows down continuous development methods like DevOps, another 19% noted that security is ignored completely in their DevOps process. Agility and accelerated deployments are among the key cloud adoption benefits, yet security slows down DevOps. Utilization of "built for the cloud" security products provides security governance directly integrated into the DevOps process and is key to fully realizing the benefits of the cloud.

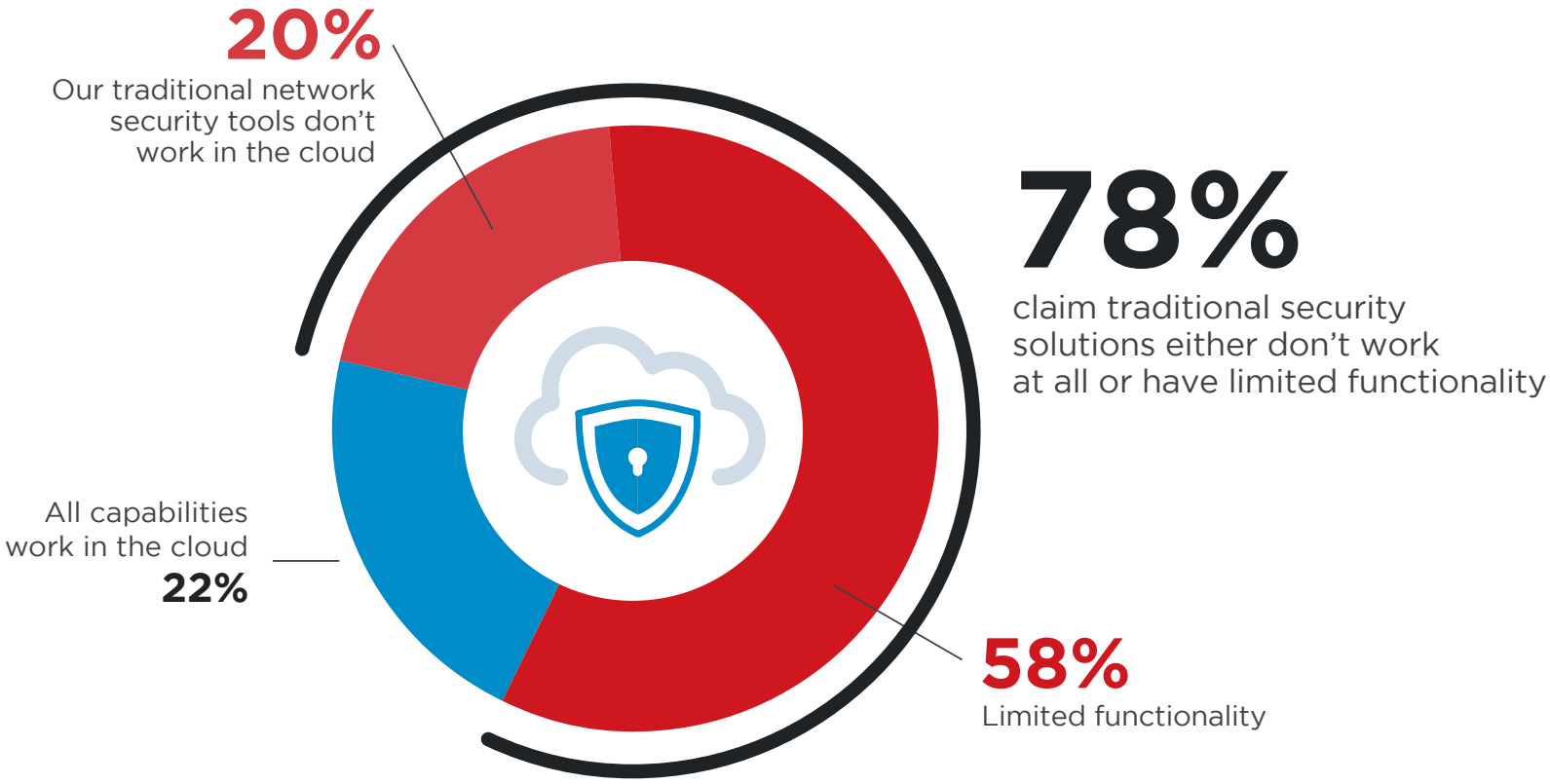
Q: Does security slow down continuous development methods like DevOps at your organization?



TRADITIONAL SECURITY TOOLS

As more workloads are moving to cloud, organizations are realizing that many traditional security tools do not work well in cloud environments. Cloud requires new types of security tools as most traditional security tools have not been designed for dynamic, virtual cloud environments and the unique challenges they present. Seventy-eight percent of respondents say traditional security solutions either don't work at all in cloud environments or have only limited functionality.

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



CLOUD SECURITY SOLUTIONS

MOST EFFECTIVE SECURITY CONTROLS

Security policies and capabilities are implemented through processes and technology. What security technologies are most effective to protect data and platforms in the cloud? Similar to last year, this year's results reveal that cybersecurity professionals prioritize encryption of both data at rest and data in motion as the most effective technologies for protecting data in the cloud. Access control (52%) replaces intrusion detection and prevention as the third most effective approach for protecting information in the cloud, compared to last year.

Q: What security technologies and controls are the most effective to protect data in the cloud?

74%

Data encryption

64%

Network encryption

52%

Access control

Trained cloud security professionals 47% | Intrusion detection & prevention 44% | Firewalls/NAC 37% | Log management and analytics 36% | Data leakage prevention 34% Log management and analytics 33% | Security Information and Event Management | (SIEM) 33% | Network monitoring 32% | Endpoint security controls 30% | Single sign-on/ user authentication 29% | Anti-virus/ Anti-malware 27% | Employee usage monitoring 25% | Cyber forensics 22% | Application security scanners 21% | Mobile device management (MDM) 18% | Database scanning andmonitoring 17% | Content filtering 16% | Deception-based security 11% | Not sure/Other 12%

CLOUD APPLICATION SECURITY

A majority of organizations are taking proactive measures to protect their business applications. We dug deeper to find out how companies were protecting their applications in the cloud. The most popular application security measures are penetration testing (60%, virtually unchanged from 59% last year), followed by security monitoring (57%, significantly up from 38% last year), and web application firewalls (47%, down from 54% last year).

Q: What Application Security measures are you taking in order to protect your business applications?

60%

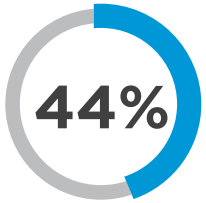
Penetration testing

57%

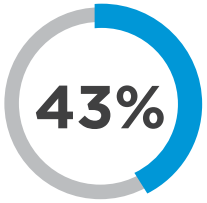
Security monitoring

47%

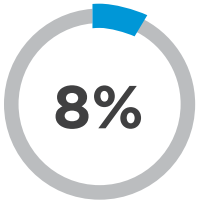
Web application firewalls



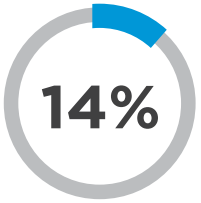
Developer education



Static/Dynamic testing



Bug Bounty programs



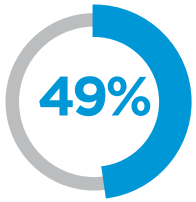
Not sure/Other

CLOUD CONFIDENCE BUILDERS

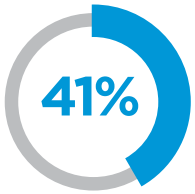
Data encryption is by far the most requested capability to increase confidence in clouds (51%), followed by setting and enforcing security policies across cloud environments (49%), and the ability to create data boundaries (41%).

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

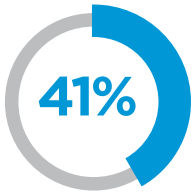
51% Data Encryption



Setting and enforcing security policies across clouds

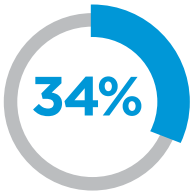


Ability to create data boundaries



APIs for reporting, auditing and alerting on security events

Isolation/protection of virtual machines



Leveraging data leakage prevention tools

Limiting unmanaged device access 27% | Protecting workloads 17% | Not sure/Other 21%

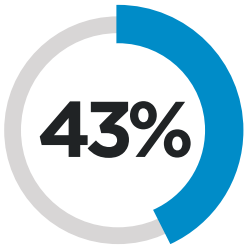
DRIVERS OF CLOUD-BASED SECURITY SOLUTIONS

Cloud security solutions continue to evolve as organizations move more diverse workloads to the cloud. Traditional security tools often do not work or are significantly deficient in protecting against new threats in dynamic cloud environments. Respondents name faster time to deployment (52%), reduced effort around patches and upgrades of software (43%), and the need for secure application access from any location (34%) as the top three reasons they deploy cloud-based security services.

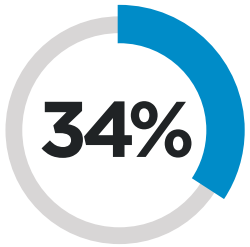
Q: What are your main drivers for considering cloud-based security solutions?

52%

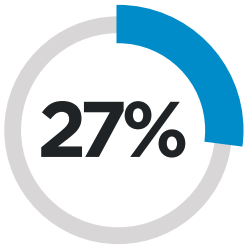
Faster time to deployment



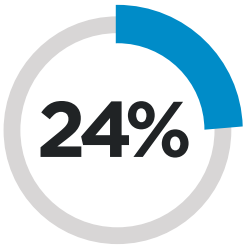
Reduced effort around patches and upgrades of software



Need for secure app access from any location



Reduction of appliance footprint in branch offices



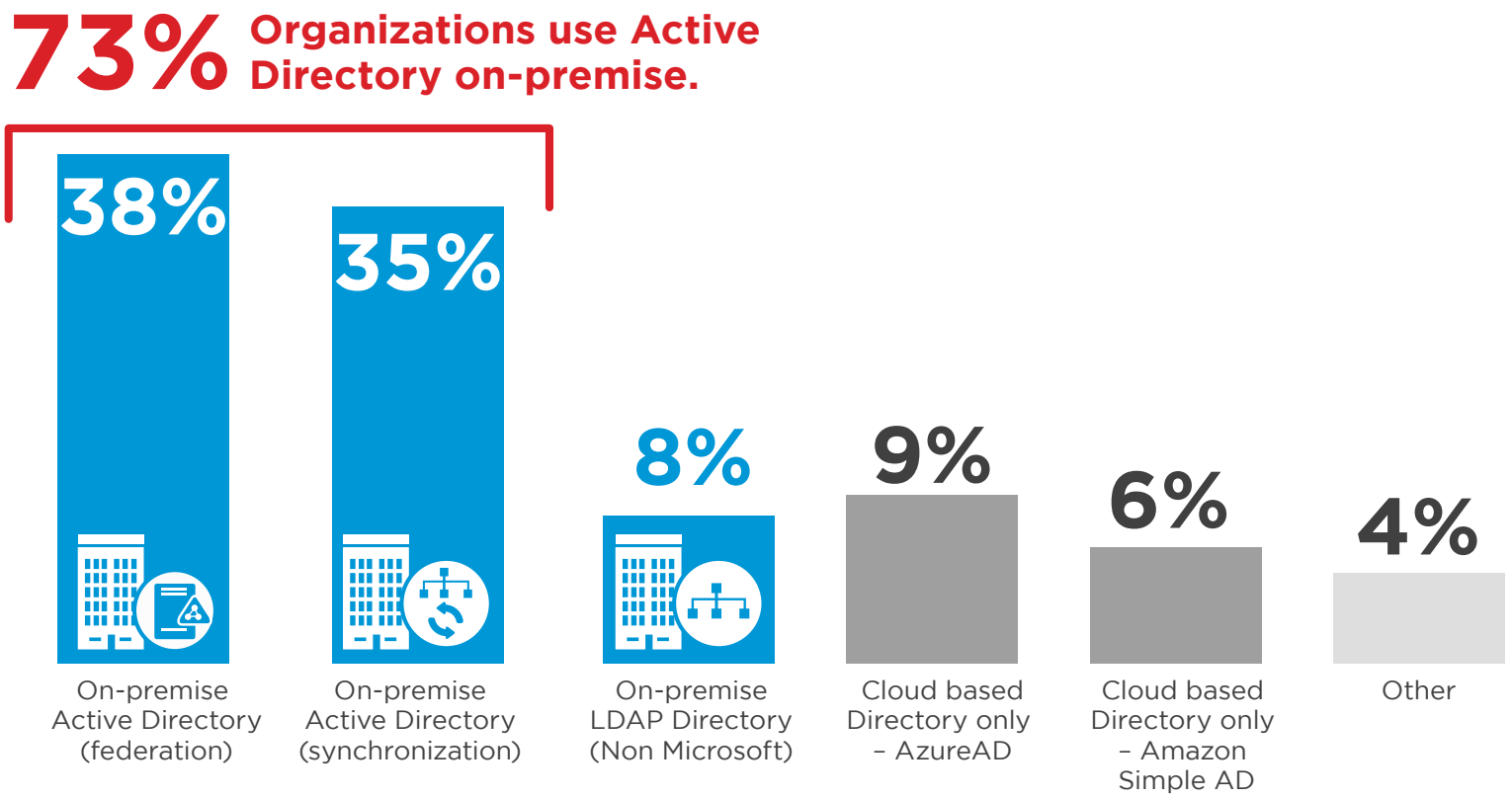
Easier policy management

Better performance 23% | Better visibility into user activity and system behavior 20% | Meet cloud compliance expectations 17% | None 5% | Not sure/other 21%

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.

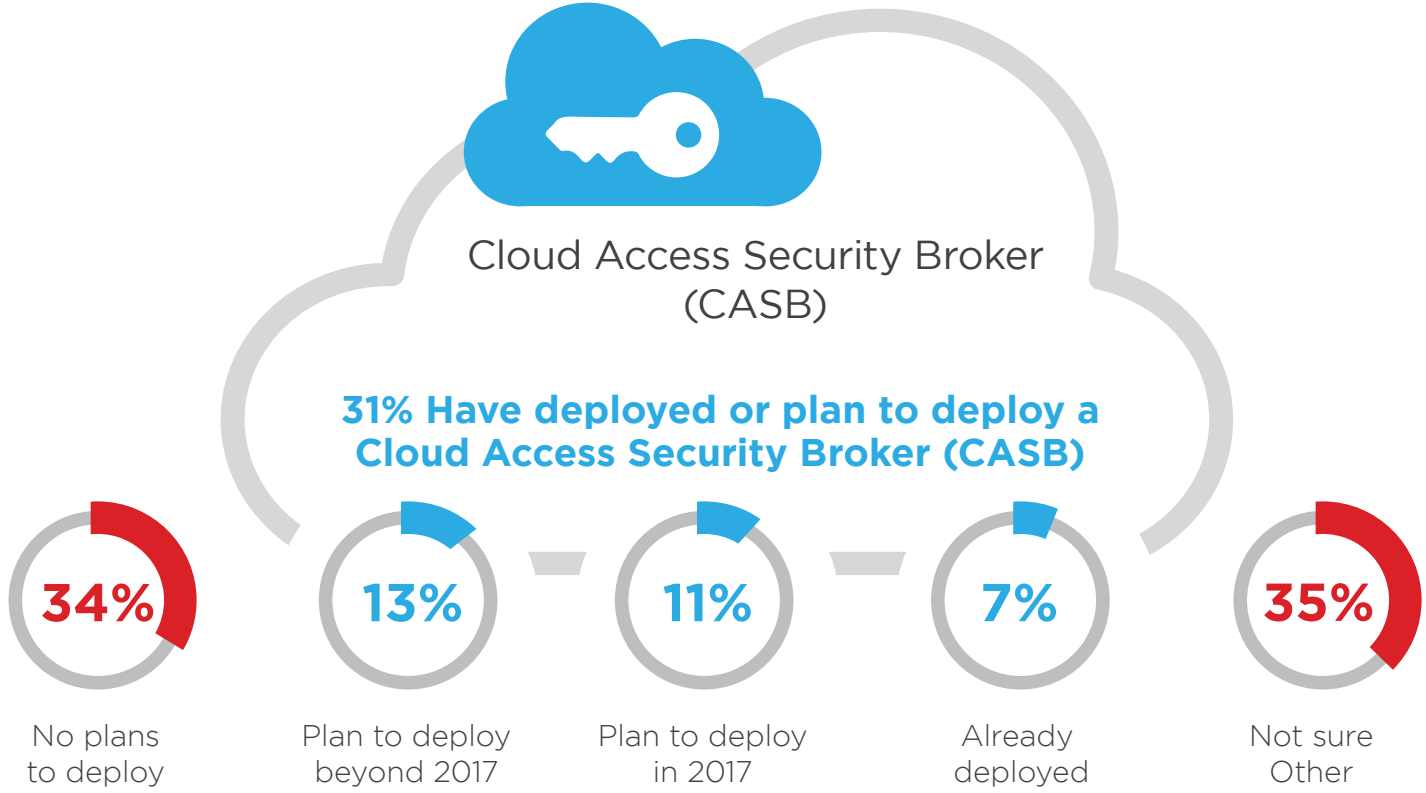
Q: What is the authoritative directory you use for identity data identification and authentication, and authorization of access for your cloud based applications?



CASB PRIORITIES

Placed between cloud service consumers and cloud service providers, Cloud Access Security Broker (CASB) solutions can provide extensive capabilities to protect cloud environments and enforce security policy as the cloud-based resources are accessed (including authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention, and more). However, their deployment is not trivial. CASBs require significant understanding of an organization's use cases to be effective as well as trained cloud security personnel to implement them properly. Seven percent of organizations have already deployed CASB solutions, and 24% plan to deploy them in 2017 and beyond.

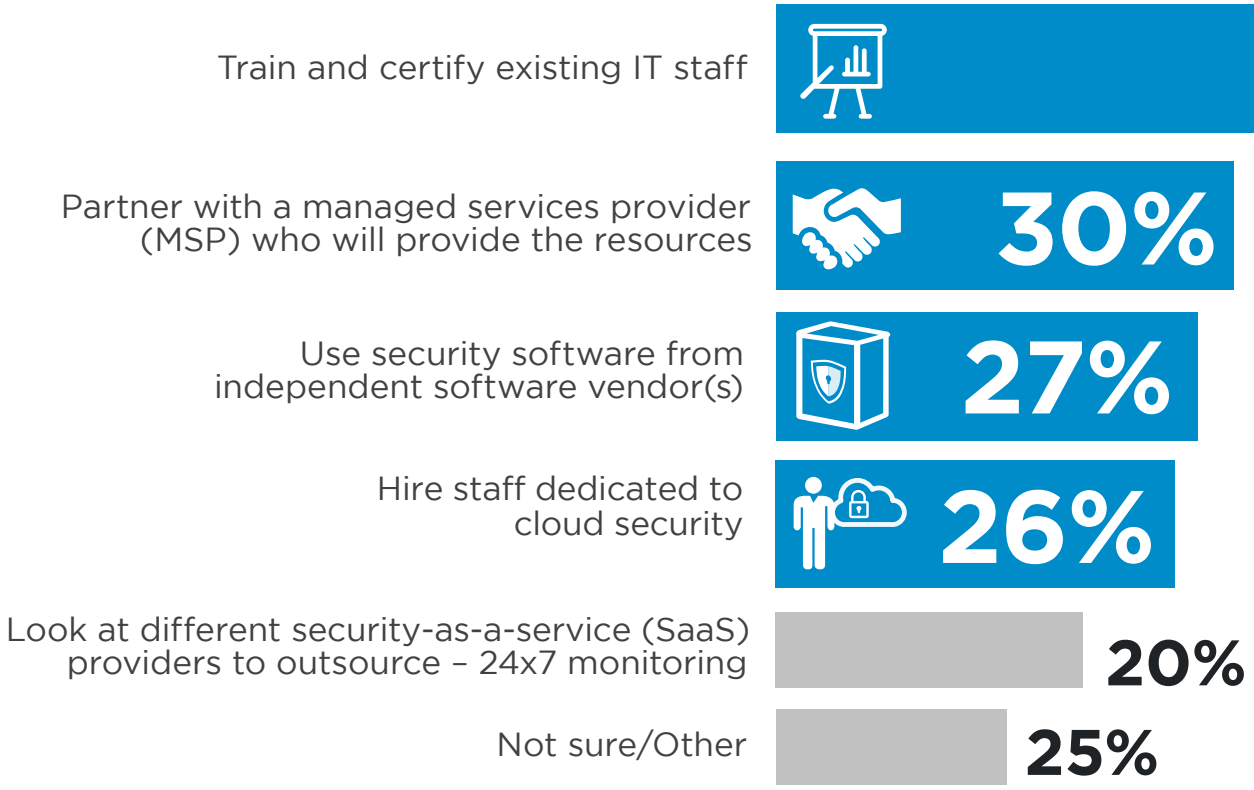
Q: What are your organization's plans for Cloud Access Security Broker (CASB) deployment?



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.

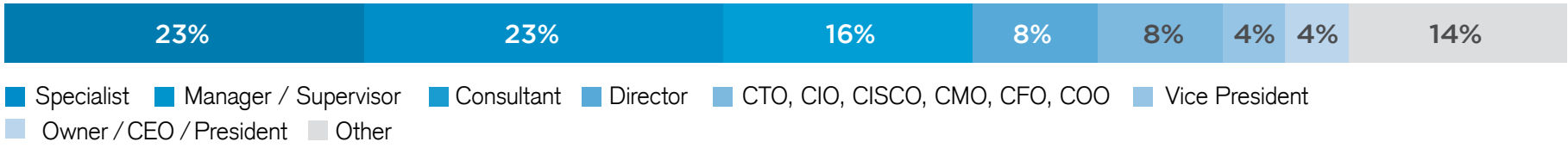
Q: When moving to the cloud, how do you plan to handle your security needs?



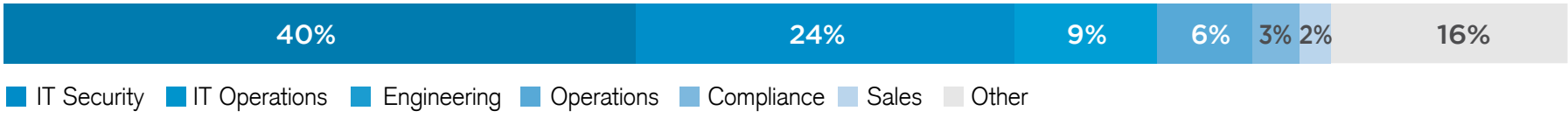
METHODOLOGY & DEMOGRAPHICS

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.

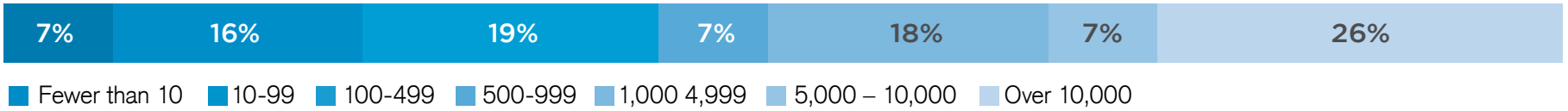
CAREER LEVEL



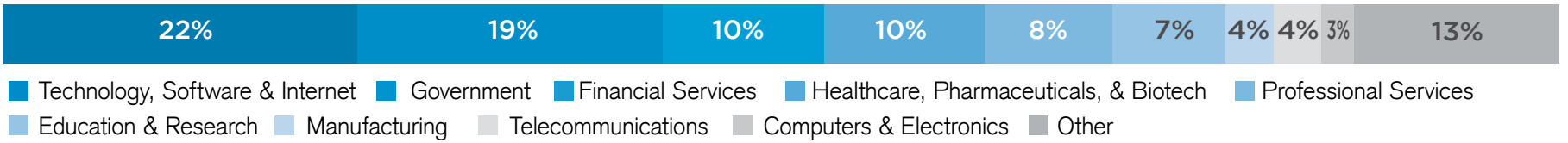
DEPARTMENT



COMPANY SIZE



INDUSTRY



SPONSORS

AlienVault | www.alienvault.com

AlienVault has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award winning approach combines our all-in-one platform, AlienVault Unified Security Management, with the power of AlienVault's Open Threat Exchange, making effective and affordable threat detection attainable for resource constrained IT teams.

Bitglass | www.bitglass.com

Bitglass' Cloud Access Security Broker (CASB) solution provides enterprises with end-to-end data protection from the cloud to the device. It deploys in minutes and works across apps like Office 365, Salesforce, and AWS. Bitglass also protects data on mobile devices without the hassles of MDM.

CloudPassage | www.cloudpassage.com

CloudPassage® Halo® is the world's leading agile security platform that provides instant visibility and continuous protection for servers in any combination of data centers, private clouds and public clouds. The Halo platform is delivered as a service, so it deploys in minutes and scales on-demand.

Cloudvisory | www.cloudvisory.com

The Cloudvisory Security Platform (CSP), for hybrid/multi-cloud environments, delivers powerful visualization, centralized security policy automation and valuable micro-segmentation. Continuous compliance enforcement and efficient multi-tenant, self-service capabilities streamline DevSecOps, improves business agility and halts nation-state hackers. The CSP is enterprise-class, highly scalable, and trusted by F500 customers.

SPONSORS

Dome9 Security | www.dome9.com

Dome9 delivers verifiable cloud infrastructure security and compliance to enterprises across every public cloud. Using the Dome9 Arc SaaS platform, organizations can assess the security posture of their cloud environments, detect and fix misconfigurations, model gold standard policies, protect against attacks and identity theft, and conform to security best practices.

Eastwind Networks | www.eastwindnetworks.com

Eastwind Breach Analytics Cloud provides complete visibility of an organization's key cyber terrain including cloud technologies such as AWS, Office 365, G Suite, and Dropbox. Our technology analyzes, automatically and on-demand, months of information to identify malicious activity that evades other security solutions and accelerates incident response and forensics.

Evident.io | www.evident.io

Evident.io was founded to fill the need for security and compliance for public clouds. The Evident Security Platform (ESP) helps organizations gain visibility and automate policy enforcement across all their cloud infrastructure.

(ISC)² | www.isc2.org/ccsp

(ISC)² is the largest not-for-profit membership body of certified cyber, information, software and infrastructure security professionals worldwide, with over 120,000 members. (ISC)²'s flagship certification is the CISSP®. In 2015, (ISC)² and the Cloud Security Alliance (CSA) partnered to launch the Certified Cloud Security Professional (CCSP®) credential for security professionals whose day-to-day responsibilities involve procuring, securing and managing cloud environments or purchased cloud services. (ISC)² offers education programs and services based on its CBK®.

SPONSORS

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.

Skyhigh Networks | www.skyhighnetworks.com

Skyhigh Networks, the world's leading Cloud Access Security Broker (CASB), enables enterprises to safely adopt SaaS, PaaS and IaaS cloud services, while meeting their security, compliance and governance requirements. With more than 600 enterprise customers globally, Skyhigh provides organizations the visibility and management for all their cloud services, including enforcement of data loss prevention policies; detecting and preventing internal and external threats; encrypting data with customer-controlled keys; and implementing access-control policies.

Tenable | www.tenable.com

Tenable transforms security technology through comprehensive solutions providing continuous visibility and critical context, enabling decisive actions to protect organizations of all sizes. Tenable eliminates blind spots, prioritizes threats and reduces exposure and loss.

CONTACT US

Interested in joining the next security research report?

Contact Crowd Research Partners for more information.

info@crowdresearchpartners.com

Produced by:

Crowd Research Partners

LinkedIn Group Partner
Information Security