2018

CLOUD SECURITY REPORT

Cybersecurity INSIDERS

Crowd Research Partners

Presented By:

SECURONIX

Security Analytics. Delivered.

CLOUD SECURITY
2018 REPORT

TABLE OF CONTENTS

SECURONIX
Security Analytics. Delivered.

INTRODUCTION

Organizations continue to adopt cloud computing at a rapid pace to benefit from increased efficiency, better scalability, and faster deployments.

As more workloads are shifting to the cloud, cybersecurity professionals remain concerned about security of data, systems, and services in the cloud. To cope with new security challenges, security teams are forced to reassess their security posture and strategies as traditional security tools are often not suited for the challenges of dynamic, virtual and distributed cloud environments. This technology challenge is only exacerbated by the dramatic shortage of skilled cybersecurity professionals.

SECURONIX
Security Analytics. Delivered.

This report has been produced by the 400,000 member Information Security Community on LinkedIn in partnership with Cybersecurity Insiders 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.

We would like to thank the study sponsor Securonix for supporting this research.

We hope you will enjoy the report.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

✉ Holger.Schulze@Cybersecurity-Insiders.com

Cybersecurity
INSIDERS

KEY SURVEY FINDINGS

1 **Cloud security concerns** – While adoption of cloud computing continues to surge, security concerns are showing no signs of abating. Reversing a multi-year downward trend, nine out of ten cybersecurity professionals confirm they are concerned about cloud security, up 11 percentage points from last year's cloud security survey. The top three cloud security challenges include protecting against data loss and leakage (67 percent), threats to data privacy (61 percent), and breaches of confidentiality (53 percent).

2 **Biggest threats to cloud security** – Misconfiguration of cloud platforms jumped to the number one spot in this year's survey as the single biggest threat to cloud security (62 percent). This is followed by unauthorized access through misuse of employee credentials and improper access controls (55 percent), and insecure interfaces/APIs (50 percent).

3 **Cloud security headaches** – As more workloads move to the cloud, cybersecurity professionals are increasingly realizing the complications to protect these workloads. The top three security control challenges SOCs are struggling with are visibility into infrastructure security (43 percent), compliance (38 percent), and setting consistent security policies across cloud and on-premises environments (35 percent).

4 **Legacy security tools limited in the cloud** – Only 16 percent of organizations report that the capabilities of traditional security tools are sufficient to manage security across the cloud, a 6 percentage point drop from our previous survey. Eighty-four percent say traditional security solutions either don't work at all in cloud environments or have only limited functionality.

5 **Paths to stronger cloud security** – For the second year in a row, training and certification of current IT staff (57 percent) ranks as the most popular path to meet evolving security needs. Fifty percent of respondents use their cloud provider's security tools and 35 percent deploy third-party security software to ensure the proper cloud security controls are implemented.

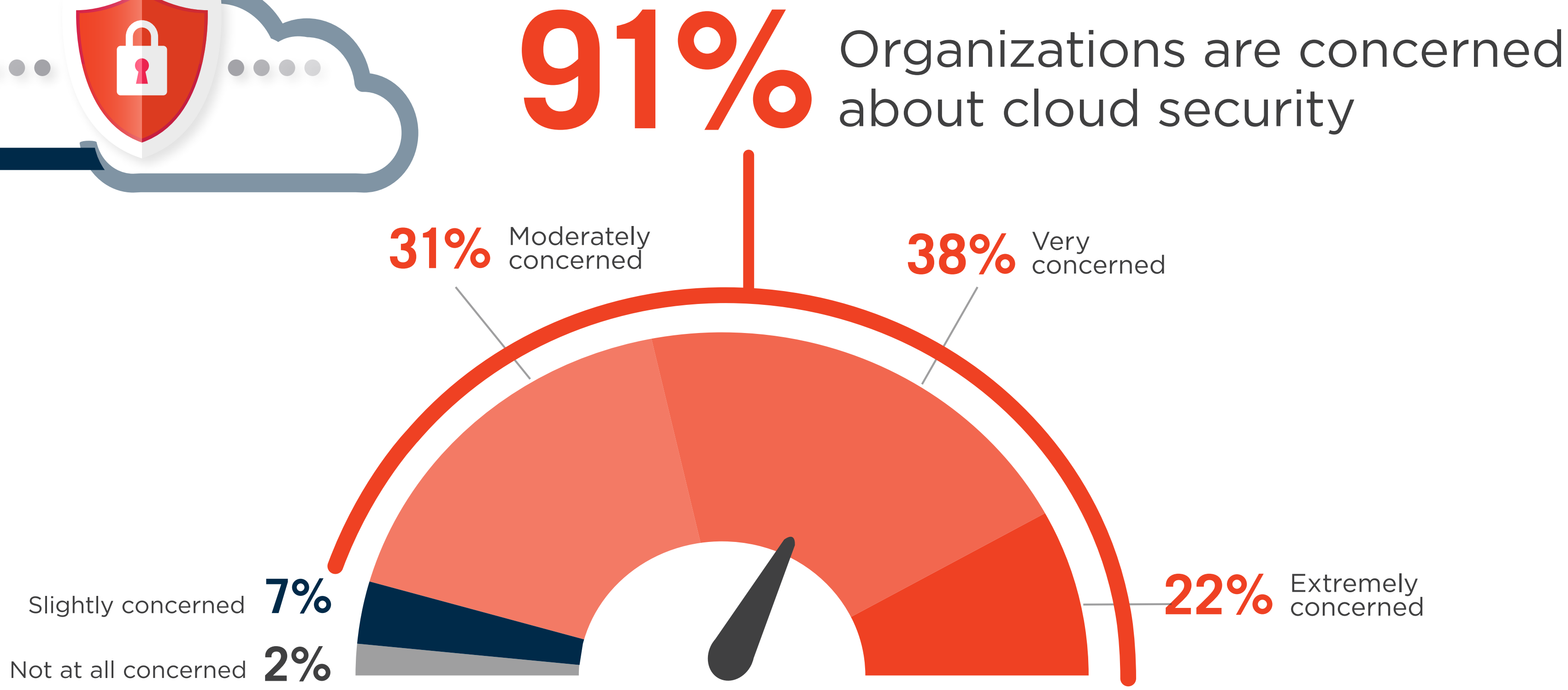
6 **Cloud security budgets increase** – Looking ahead, close to half of organizations (49 percent) expect cloud security budgets to go up, with a median budget increase of 28 percent.

CLOUD SECURITY CHALLENGES

CLOUD SECURITY CONCERNS ON THE RISE

While adoption for public cloud computing continues to surge, security concerns are showing no signs of abating. An overwhelming majority of cybersecurity professionals (91 percent) say they are extremely to moderately concerned about public cloud security, up 11 percentage points from last year.

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

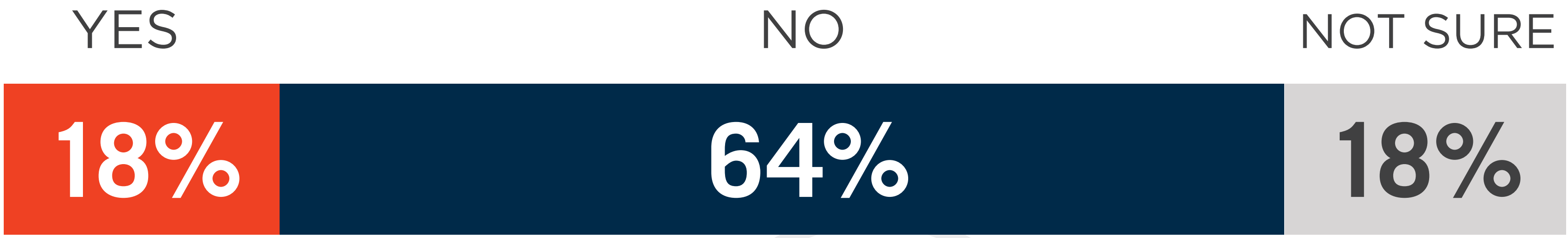


CLOUD SECURITY INCIDENTS

In the past 12 months, 18 percent 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

SECURONIX Security Analytics. Delivered.

While cloud providers offer many 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 (67 percent), threats to data privacy (61 percent), and breaches of confidentiality (53 percent) – all up compared to the previous year.

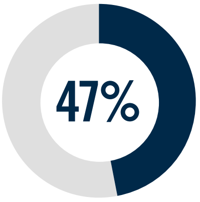
Concerns about accidental exposure have seen the biggest gain compared to last year, moving from the number 6 spot (26 percent in 2017) to number 4 (47 percent in 2018) on the list.

What are your biggest cloud security concerns?

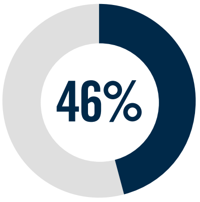
67% Data loss/leakage

61% Data privacy

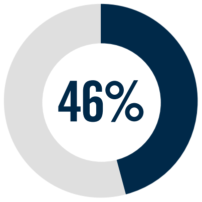
53% Confidentiality



Accidental Exposure



Legal and regulatory compliance



Data sovereignty/ control

Lack of forensic data 37% | Incident response 35% | Visibility & transparency 34% | Fraud (e.g., theft of SSN records) 27% | Liability 25% | Availability of services, systems and data 21% | Business continuity 18% | Disaster recovery 18% | Performance 16% | Other 7%

OPERATIONAL SECURITY HEADACHES

SECURONIX
Security Analytics. Delivered.

As more workloads move to the cloud, cybersecurity professionals are increasingly realizing the complications to protect these workloads.

The top two security control challenges SOCs are struggling with are visibility into infrastructure security (43 percent) and compliance (38 percent). Setting consistent security policies across cloud and on-premises environments (35 percent) is tied with security not keeping up with the pace of change in applications (35 percent).

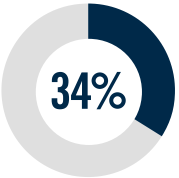
▶ **What are your biggest operational, day-to-day headaches trying to protect cloud workloads?**

43%
Visibility into infrastructure security

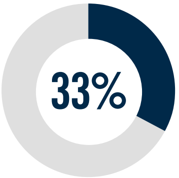
38%
Compliance

35%
Setting consistent security policies

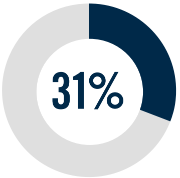
35%
Security can't keep up with pace of change in applications



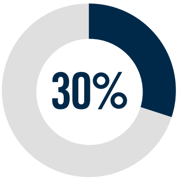
Lack of integration with on-premises security technologies



No automatic discovery/ visibility/control to infrastructure security



Can’t identify misconfiguration quickly



Complex cloud to cloud on-premises security rule matching

Reporting security threats 27% | Remediating threats 23% | Automatically enforcing security across multiple datacenters 23% | Lack of feature parity with on-premises security solution 21% | No flexibility 8% | Not sure/other 16%

BIGGEST CLOUD SECURITY THREATS

SECURONIX
Security Analytics. Delivered.

Misconfiguration of the cloud platform jumped to the number one spot in this year's survey as the single biggest threat to cloud security (62 percent).

This is followed by unauthorized access through misuse of employee credentials and improper access controls (55 percent), and insecure interfaces/APIs (50 percent).

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

#1

Misconfiguration of the cloud platform/wrong set-up

62%

#2

Unauthorized access

55%

#3

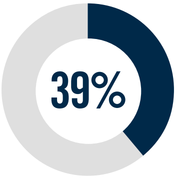
Insecure interfaces /APIs

50%

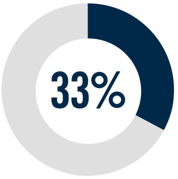
#4

Hijacking of accounts, services or traffic

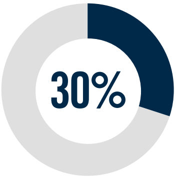
47%



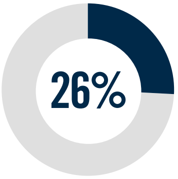
External sharing of data



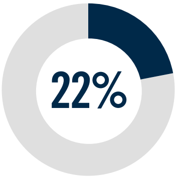
Foreign state sponsored cyberattacks



Malicious insiders



Malware/ ransomware



Denial of service attacks

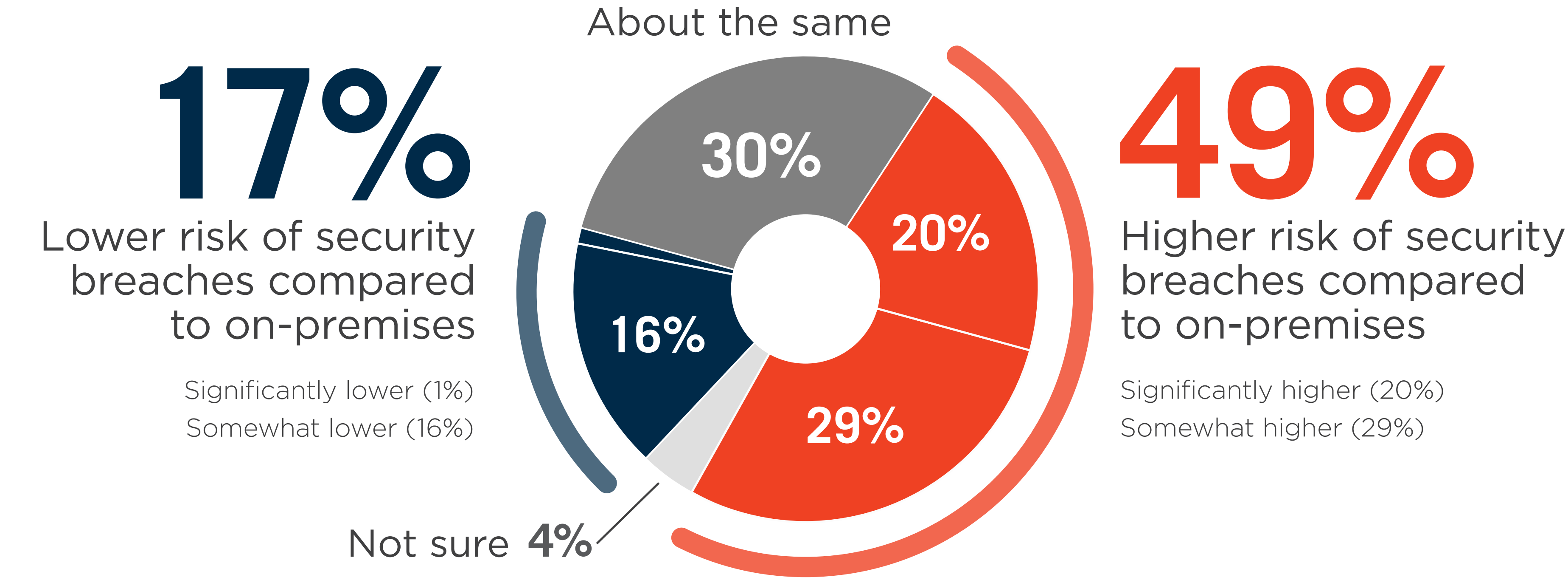
Theft of service 12% | Lost mobile devices 7% | Not sure/other 7%

CLOUD VS ON-PREMISES SECURITY RISK

Organizations continue to believe public clouds are at higher risk of security breaches than traditional on-premises environments (49 percent), an 8 percent increase relative to last year's 41 percent.

The respondents who believe that public clouds are less risky to security breaches decreased proportionally (at 17 percent, a 6 percent drop compared to last year's 23 percent), further supporting the perception that the use of public clouds increases the probability of becoming a target for a cyberattack.

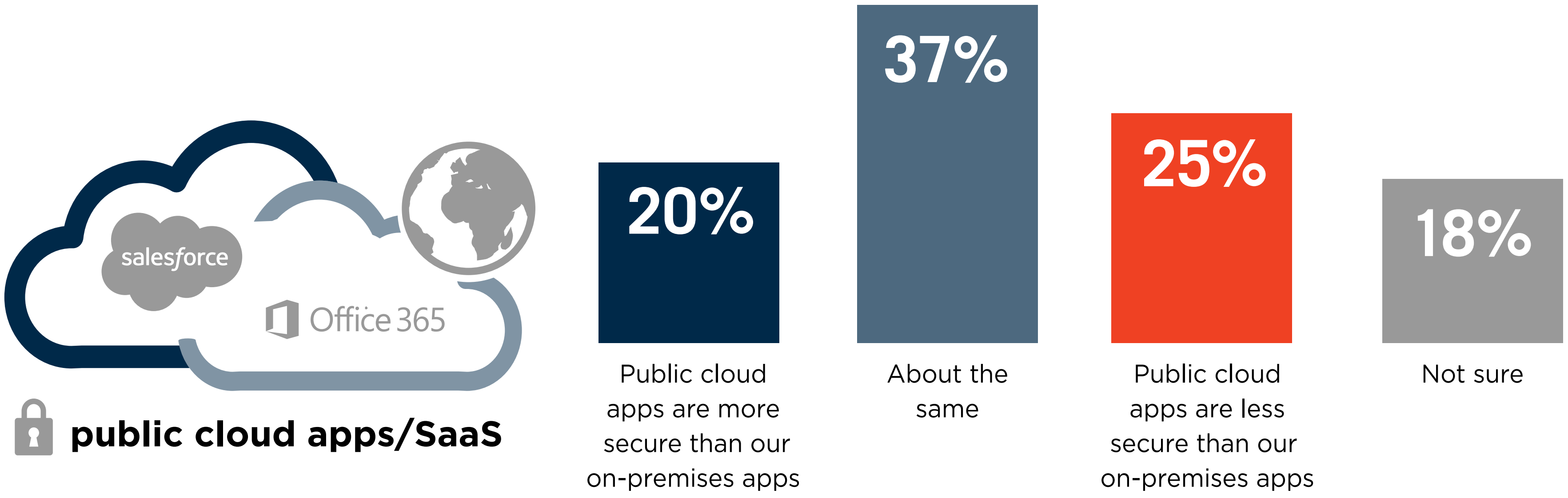
Compared to traditional IT environments, what would you say is the risk of security breaches in a public cloud environment?



SAAS VS ON-PREMISES

Perceptions of SaaS security remain relatively unchanged this year. A majority, 57 percent, believe that cloud apps are as secure or more secure than on-premises applications, down slightly from 58 percent in last year's survey.

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



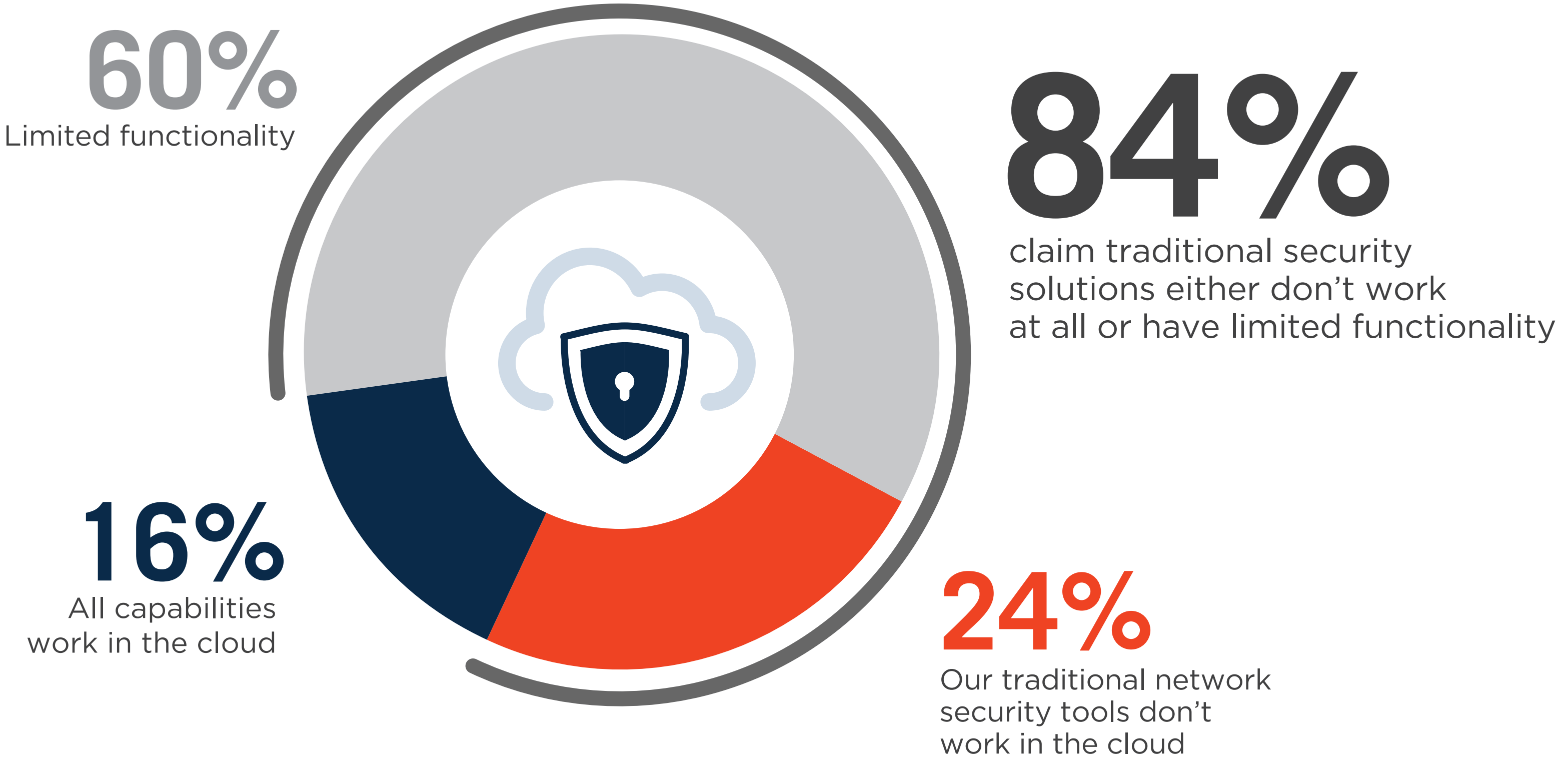
CLOUD SECURITY SOLUTIONS

TRADITIONAL TOOLS IN THE CLOUD

As more workloads move into the cloud, organizations are faced with unique security challenges that cloud adoption presents. Traditional network security tools made sense when an organization's users and applications were hosted in a static centralized data center. Many of these legacy security tools/appliances are not designed for the dynamic, distributed virtual environment of the cloud.

Only 16 percent feel that traditional security tools are sufficient to manage security across the cloud, a six percent point drop from our previous survey. Eighty-four percent of respondents say traditional security solutions either don't work at all in cloud environments or have only limited functionality, up six percent points from the previous year (78 percent).

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



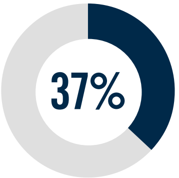
DRIVERS OF CLOUD-BASED SECURITY SOLUTIONS

Organizations recognize several key advantages of deploying cloud-based security solutions. As in previous years, respondents selected faster time to deployment (47 percent) along with cost savings (47 percent) at the number one factors for selecting cloud-based security solutions.

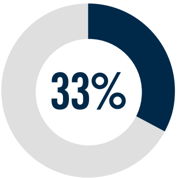
What are the main drivers for considering cloud-based security solutions?

47%
Faster time to deployment

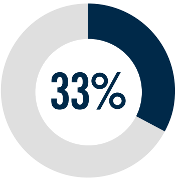
47%
Cost savings



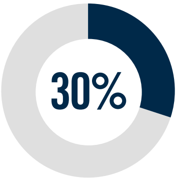
Need for secure app access from any location



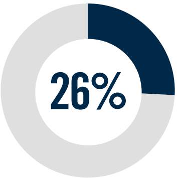
Reduced effort around patches and upgrades of software



Meet cloud compliance expectations



Better visibility into user activity and system behavior



Reduction of appliance footprint in branch offices

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.

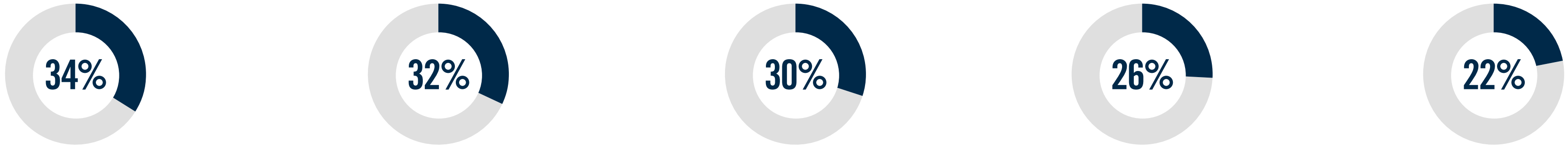
Our survey reveals that the biggest challenge organizations are facing is not technology, it's people and processes. Staff expertise and training (56 percent) ranked number one in the survey, followed by data privacy concerns (41 percent) and lack of integration with on-premises technology (37 percent).

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

56% Staff expertise/ training

41% Data privacy

37% Lack of integration with on-premises security technologies



Regulatory compliance requirements | Solution maturity | Data residency | Budget | Integrity of cloud security platform (DDoS attack, breach)

Limited control over encryption keys 21% | Sunk cost into on-premises tools 19% | Scalability and performance 11% | Not sure/other 14%

MOST EFFECTIVE SECURITY TECHNOLOGIES

SECURONIX
Security Analytics. Delivered.

In a data-driven economy, it is imperative that organizations protect and secure workloads in the cloud. As in previous years, data and network encryption technologies top the list as the most effective security technologies (data encryption at 64 percent and network encryption at 54 percent) followed by Security Information and Event Management (SIEM) (52 percent).

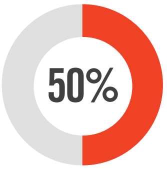
What security technologies and controls are most effective to protect data in the cloud?

64%
Data encryption

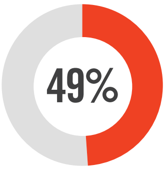
54%
Network encryption
(VPN, packet encryption, transport encryption)

52%
Security Information and Event Management
(SIEM)

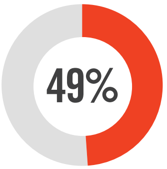
51%
Trained cloud security professionals



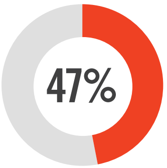
Intrusion detection and prevention



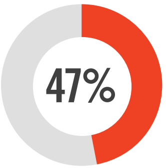
Vulnerability assessment



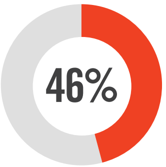
Access control (e.g., CASB/Cloud Access Security Brokers)



Log management and analytics



Privileged Access Management (PAM)



Data leakage prevention

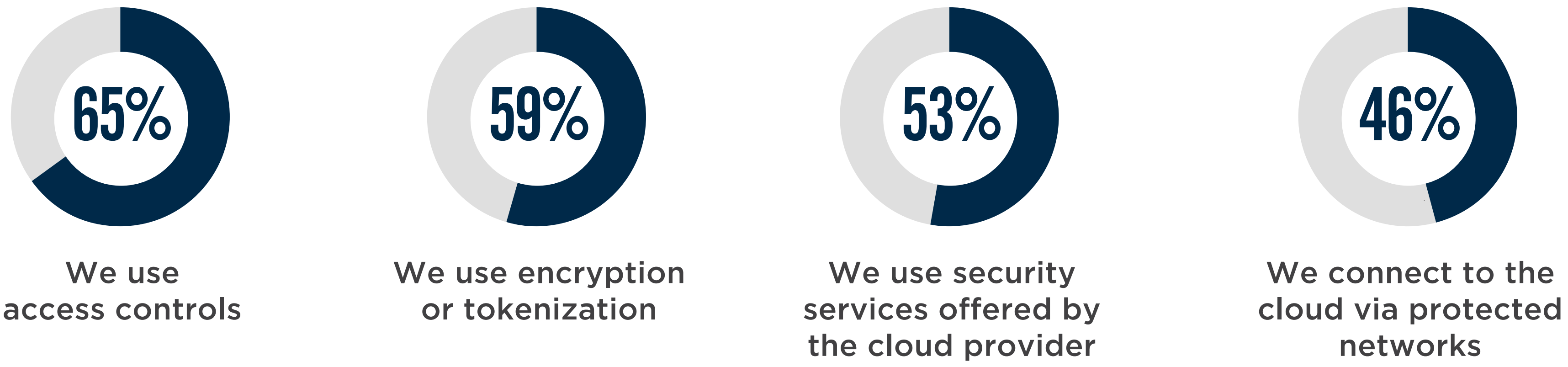
Patch management 46% | Configuration management 46% | Single sign-on/user authentication 43% | Endpoint security controls 42% | Firewalls/NAC 41% | Network monitoring 39% | Anti-virus/anti-malware 37% | Application security scanners 32% | Secure managed file transfer 30% | Employee usage monitoring 30% | Mobile Device Management (MDM) 30% | Database scanning and monitoring 26% | Cloud asset discovery 23% | Cyber forensics 22% | Content filtering 22% | Not sure/other 20%

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 (65 percent) are the primary method to protect data in the cloud, followed by encryption (59 percent).

This year, the use of security services offered by the cloud provider (53 percent) 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 deploy cloud security monitoring tools 41% | We deploy additional security services offered by third-party vendors 35% | We don't protect data in the cloud 4% | Not sure/other 15%

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 five attributes cybersecurity professionals look for in a cloud security provider include cloud native security tools (68 percent), cost effectiveness (64 percent), seamless integration with cloud platforms (57 percent), ease of deployment (53 percent) and demonstrated cloud knowledge (50 percent) — all are ranked by at least 50 percent of the survey participants, suggesting that SOCs are looking for a broad array of capabilities.

What do you look for in your cloud security provider?

68% **Security tools are cloud native**
(are agile, can be deployed with automation, support scalability, etc.)

64%
Cost effectiveness

57%
Integrates seamlessly with cloud platforms

53%
Ease of deployment

50%
Demonstrates cloud knowledge

Not sure/other 11%

PATHS TO STRONGER CLOUD SECURITY

SECURONIX
Security Analytics. Delivered.

For the second year in a row, training and certifying current IT staff (57 percent) ranked number one by organizations to assure that their evolving security needs are met. Fifty percent of respondents use their cloud provider's security tools and 35 percent deploy third-party security software to ensure the proper security controls are implemented across on-premises and the cloud.

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

57%

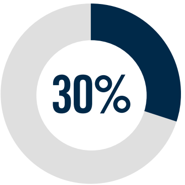
Train and/or certify current IT staff

50%

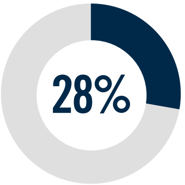
Use cloud provider security tools
(e.g., GuardDuty in AWS)

35%

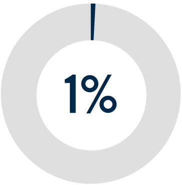
Deploy security software from independent software vendor(s)



Partner with a Managed Security Services Provider (MSSP)



Hire staff dedicated to cloud security



Look at security-as-a-service providers to outsource 24x7 monitoring

Not sure/other 19%

CLOUD CONFIDENCE BUILDERS

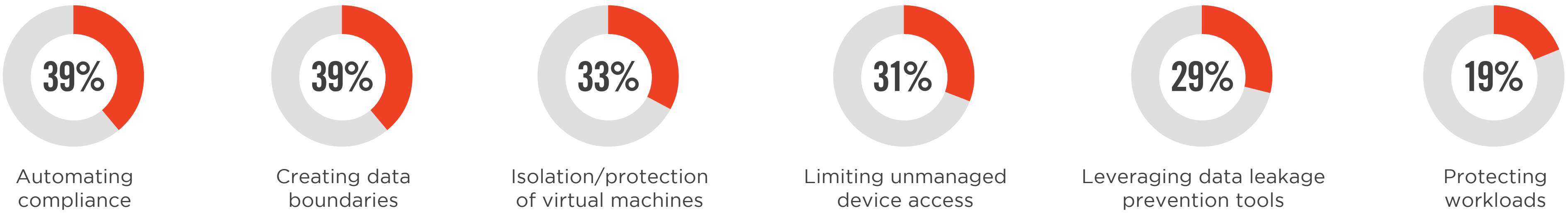
We asked organizations which actions cloud providers could take to improve their confidence in moving to the cloud. They identified five key confidence boosters to help alleviate their security concerns. Encrypting data-at-rest (49 percent) was the number one issue to address, followed by APIs for reporting, auditing and alerting on security events (46 percent), and setting and enforcing security policies across clouds (45 percent).

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

49%
Encryption of data-at-rest

46%
APIs for reporting, auditing and alerting on security events

45%
Setting and enforcing security policies across clouds



Not sure/other 15%

SECURITY TRAINING

Organizations realize that security training, certification and awareness is a key cornerstone in the defense against security breaches. Training and expertise remains the highest concern among IT professionals as the biggest barrier to better security management, a majority (67 percent) consider training and certification valuable to their employees in reducing risk and helping protect the organization from both internal and external cyber threats.

What percentage of your employees would benefit from security training and/or certification for their job?

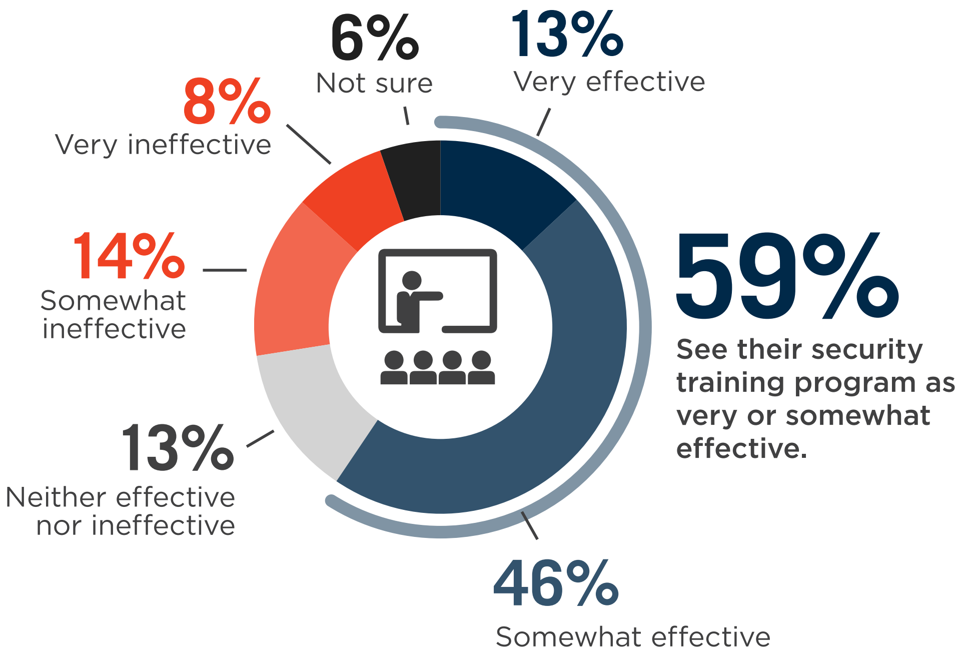
67%

Consider training and certification valuable to their employees in reducing risk and helping protect the organization

Security training is an important component of an organization's security posture. A well planned security training program will ensure there is a continual focus on IT security, helping employees identify what data is protected, assessing risk, mitigating procedures, compliance requirements, and how often the program will be revised and refreshed.

A majority, 59 percent, see their security training program as very or somewhat effective.

How effective is your current security training program?

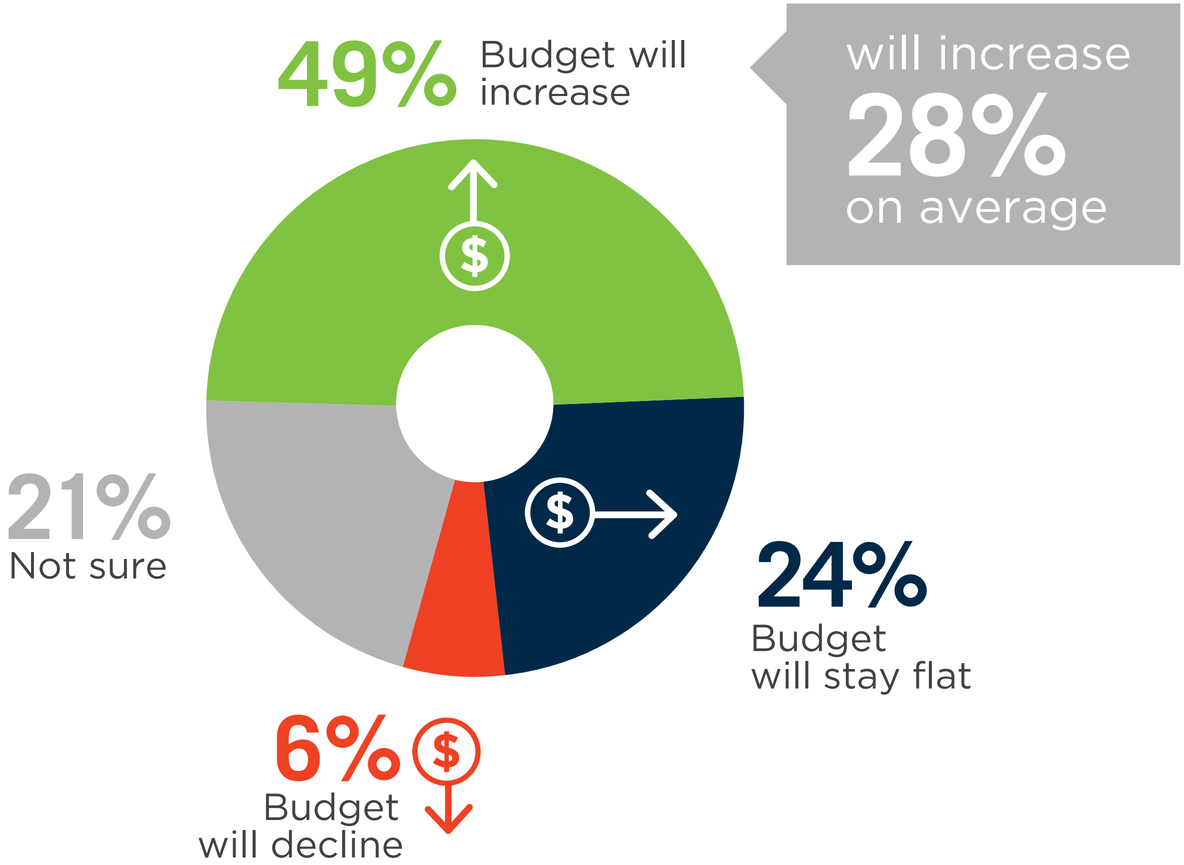


CLOUD SECURITY BUDGET

The survey reveals that organizations are recognizing the growing significance of cloud security threats and are investing resources accordingly. Looking ahead, close to half of organizations (49 percent) expect budget increases. Twenty-four percent expect their IT budgets to remain flat, while only 6 percent foresee their cloud security funding to shrink.

When asked about the degree of their security budget increases, cybersecurity professionals anticipate their program funding would increase by 28 percent, on average.

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

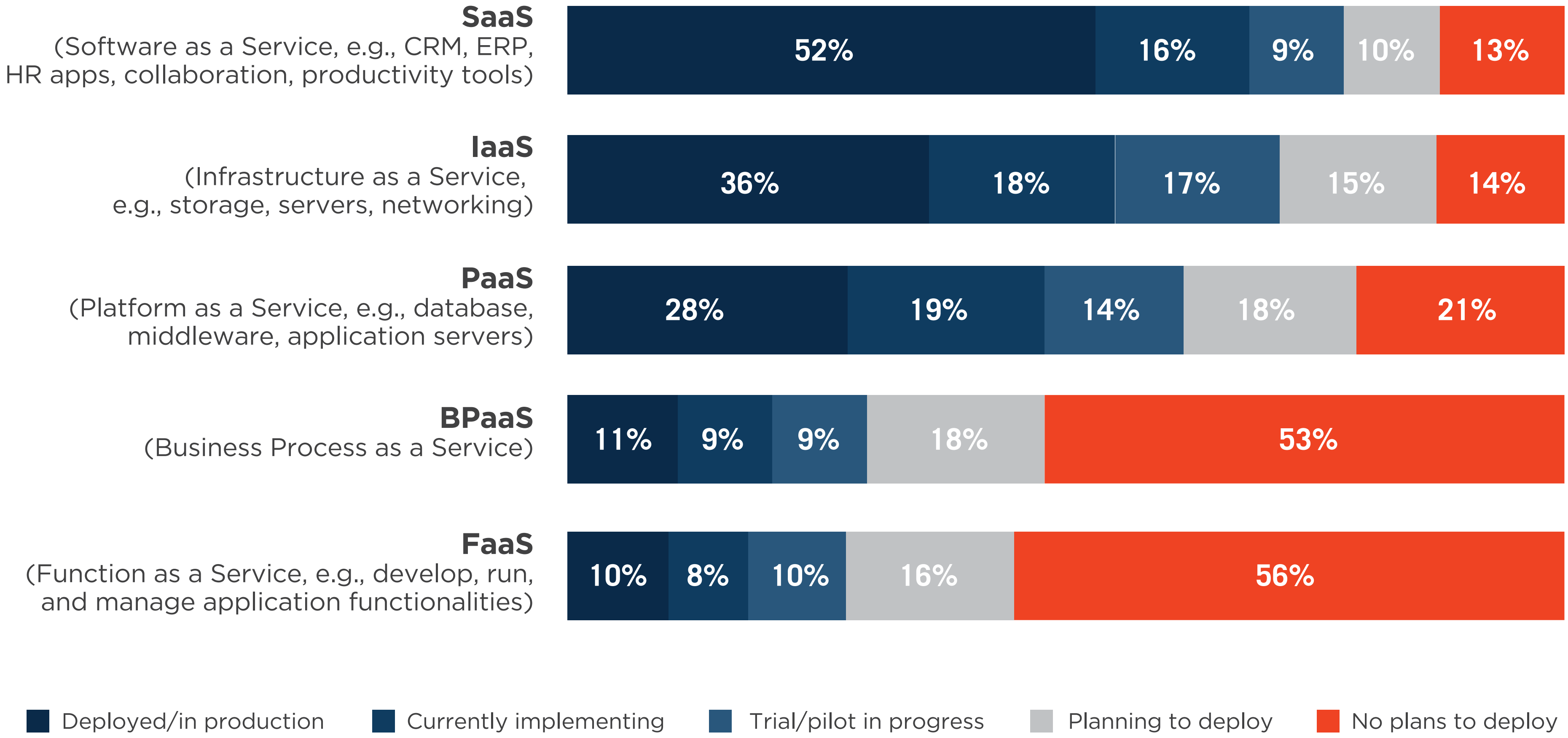


CLOUD ADOPTION TRENDS

CLOUD ADOPTION

SaaS remains the most deployed cloud model (52 percdent) as software stacks are maturing, followed by IaaS (36 percent) and PaaS (28 percent), both showing strong adoption by organizations. To a lesser extent, newer deployment models such as BPaaS (11 percent) and FaaS (10 percent) have lower rates of production deployments.

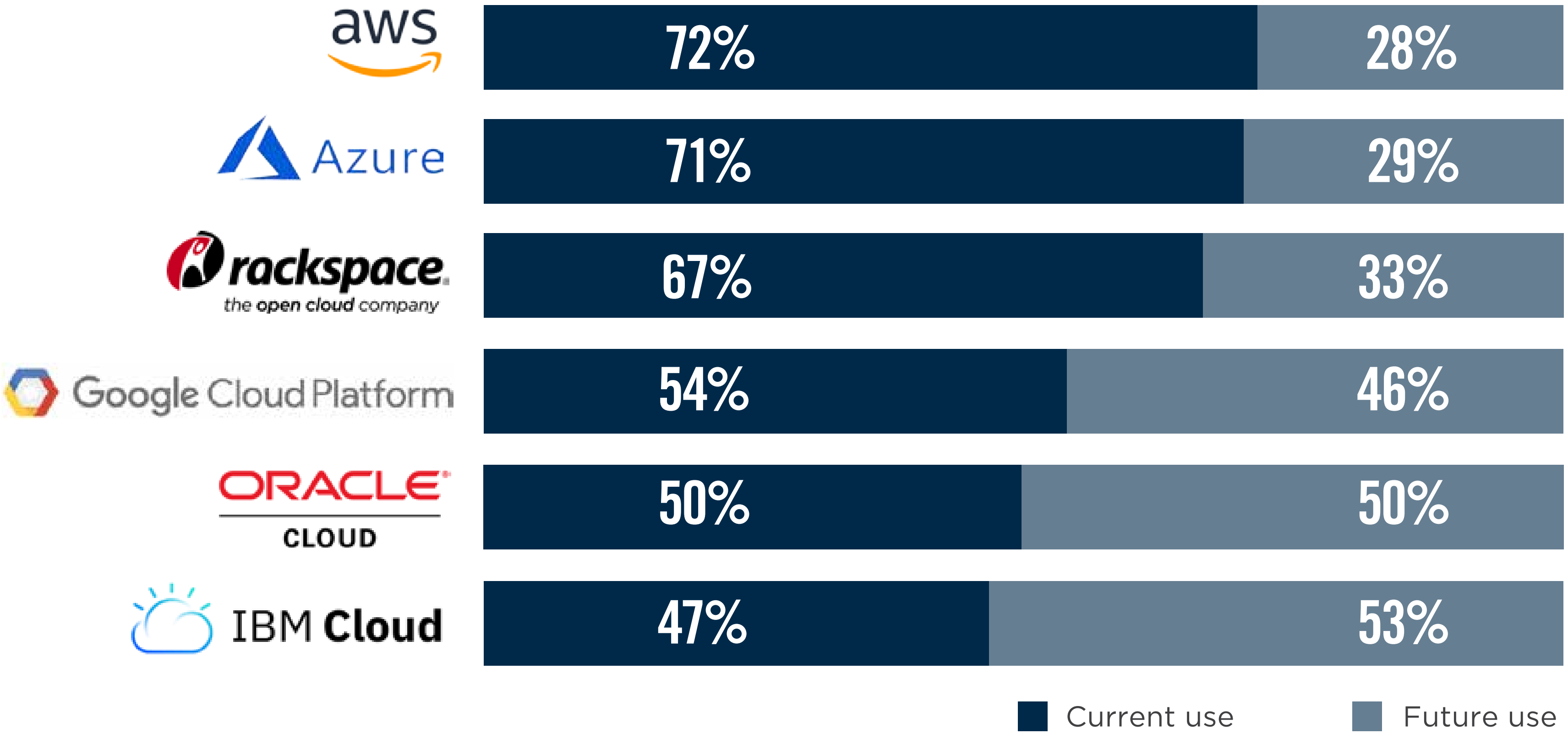
▶ What is your organization's adoption of cloud computing?



TOP CLOUD PROVIDERS

Over the past few years, public cloud providers have continued to mature and expand their service offerings. The two biggest cloud providers continue to compete for the lead in our survey: Amazon Web Services (72 percent) and Microsoft Azure (71 percent). Interestingly, Rackspace Cloud (67 percent) displaced Google Cloud Platform (54 percent) among our survey participants to claim third place this year.

What cloud IaaS provider(s) do you currently use or plan to use in the future?

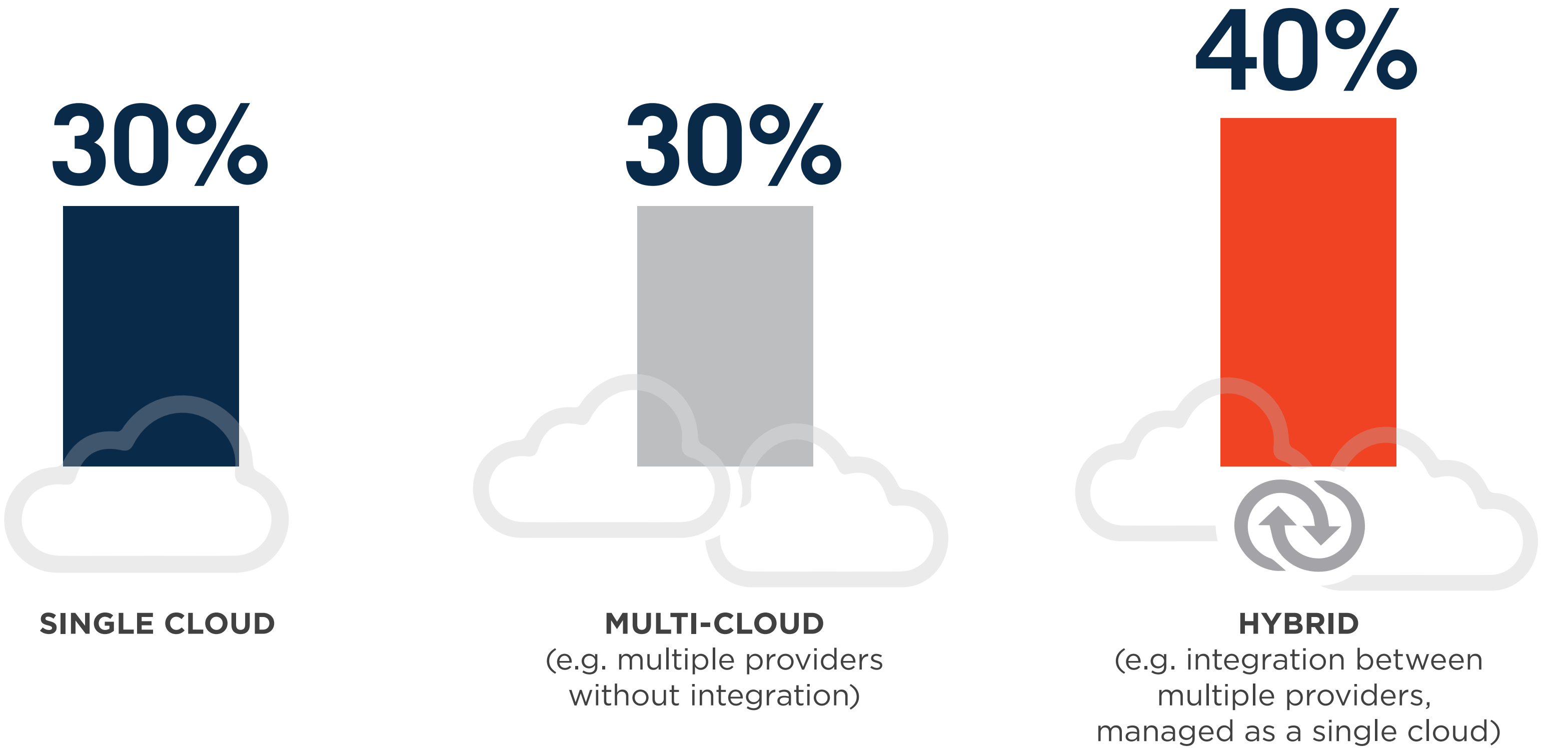


CLOUD STRATEGY

Forty 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 equally said their cloud deployment of choice was either a single cloud (30 percent) or a non-integrated, multi-cloud solution (30 percent).

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?

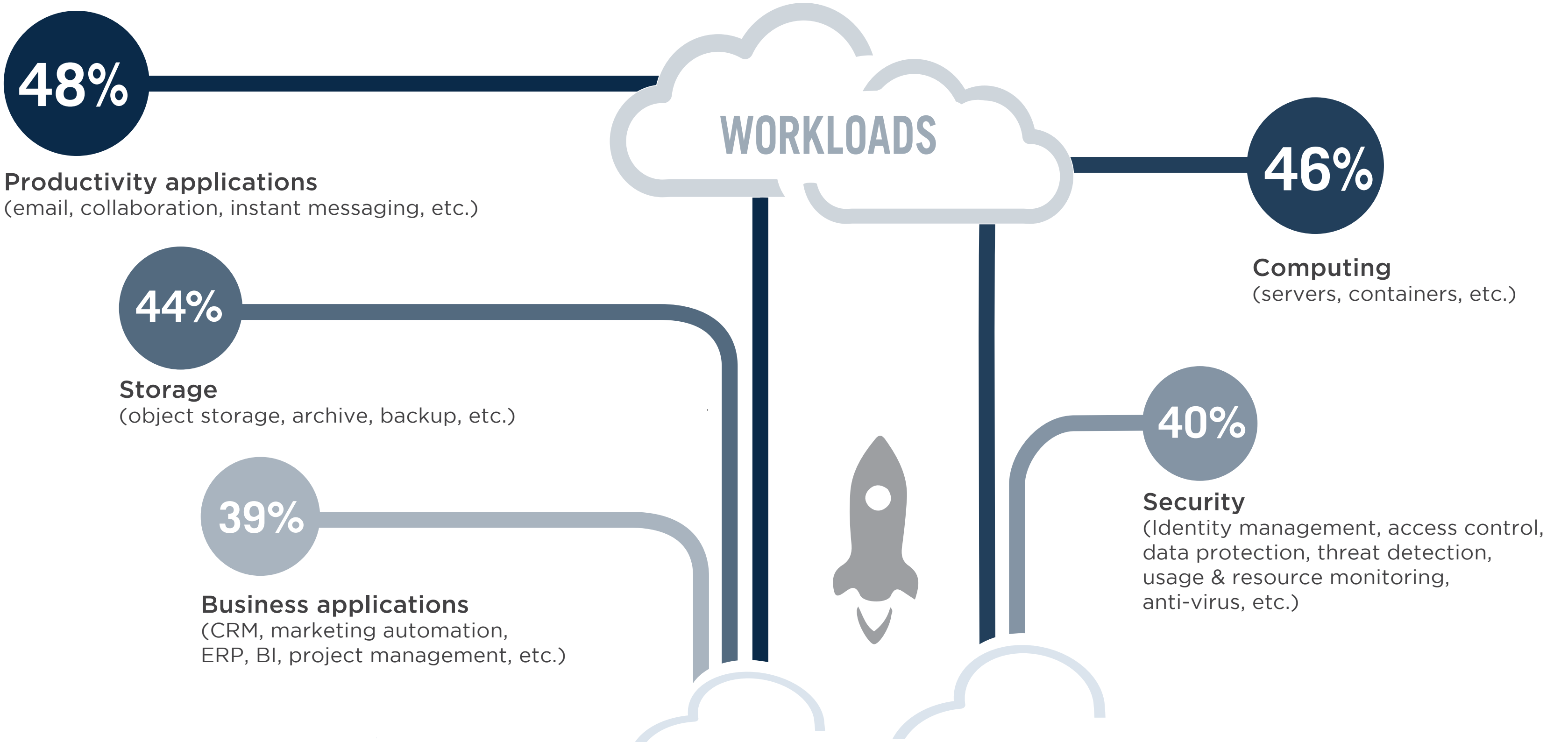


MOST COMMON WORKLOADS

As organizations become more comfortable using cloud services, more are considering cloud for broader categories of services beyond email and sales force automation. These include mission-critical and production-grade applications.

The top three cloud services and workloads that organizations are deploying are productivity applications (48 percent), computing (46 percent) and storage (44 percent).

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



48%
Productivity applications
(email, collaboration, instant messaging, etc.)

46%
Computing
(servers, containers, etc.)

44%
Storage
(object storage, archive, backup, etc.)

40%
Security
(Identity management, access control, data protection, threat detection, usage & resource monitoring, anti-virus, etc.)

39%
Business applications
(CRM, marketing automation, ERP, BI, project management, etc.)

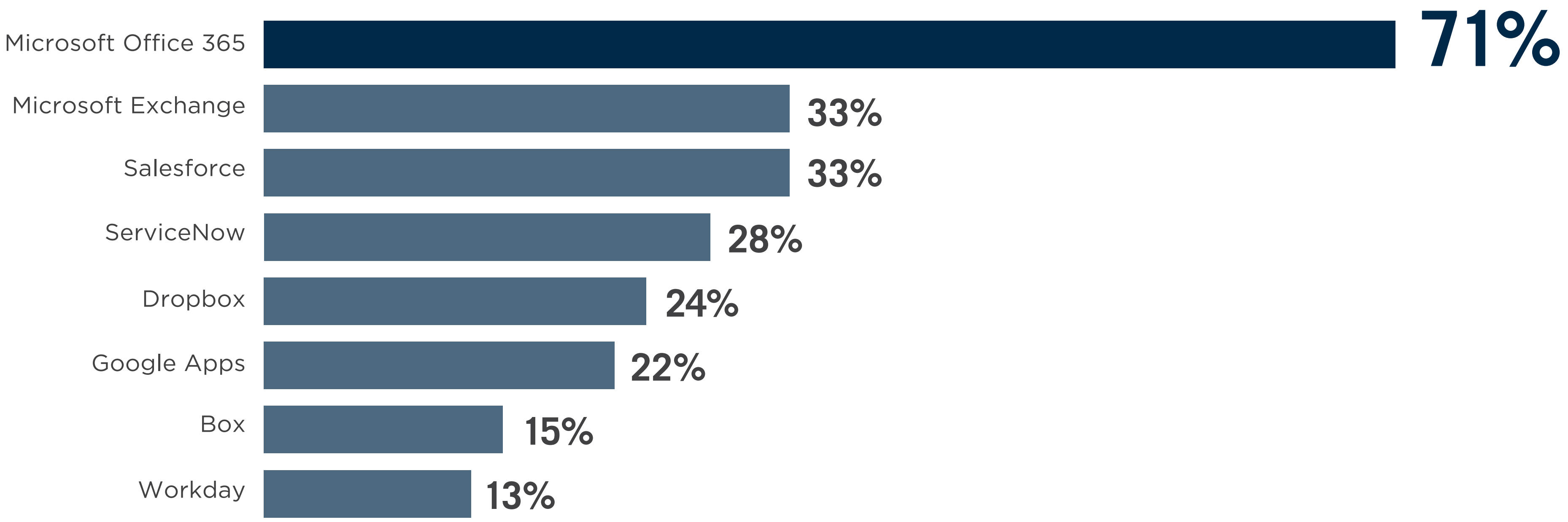
Database (relational, NoSQL, caching, etc.) 37% | Virtualization 37% | Developer/Testing Applications 37% | Networking (virtual private cloud, DNS, etc.) 34% | IT Operations Applications (administration, backup, provisioning monitoring, etc.) 31% | Operating System 29% | Middleware 17% | Runtime 10% | Not sure/other 22%

MOST POPULAR CLOUD APPS

Software as a Service (SaaS) has become the de facto delivery model for organizations to consume many core business applications, replacing traditional on-premises applications. These business applications include email, collaboration, customer relationship management, human resources, marketing automation, business intelligence, storage and many more.

In this year's survey, a majority of respondents deploy Microsoft's productivity suite, Office 365 (71 percent), followed by Microsoft's online email service, Microsoft Exchange (33 percent). Rounding out the top five most popular SaaS apps are Salesforce (33 percent), ServiceNow (28 percent) and Dropbox (24 percent).

Which of the following cloud SaaS services are currently deployed in your organization?



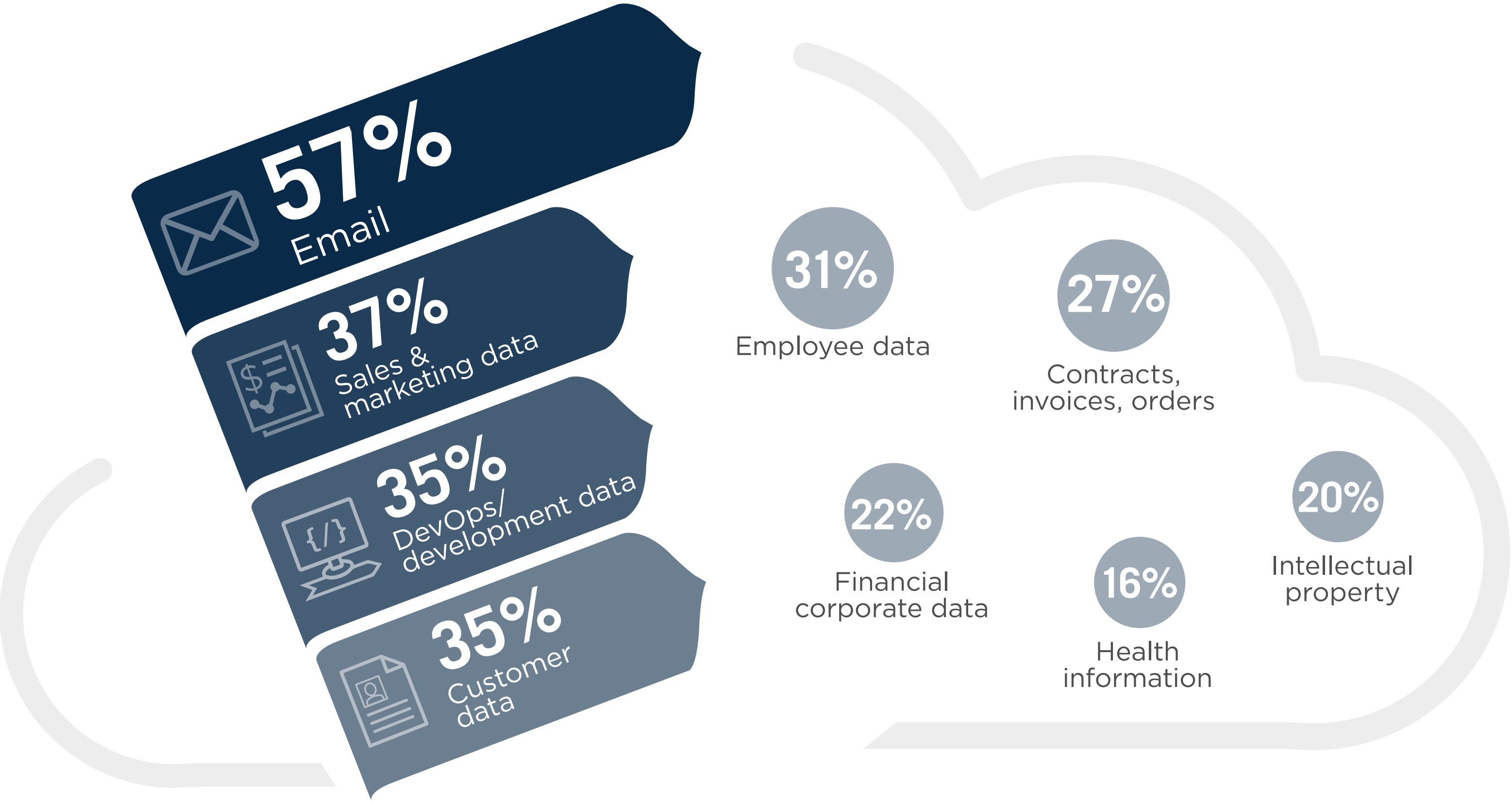
SAP HANA 7% | SAP SuccessFactors 5% | SAP Hybris 2% | Not sure/other 19%

DATA IN THE CLOUD

It's no surprise that for a third year in a row, email is the most common information stored in the cloud (57 percent), a 13 point increase over last year's survey. Notably, a reversal in trend this year, an increasing number of organizations indicate they are storing more of their intellectual property information in the cloud.

This re-enforces our findings that organizations are more comfortable with investing and moving their business-critical applications and data to the cloud. Sales and marketing data (37 percent) jumped from fourth place to second place this year, and tied for third place are DevOps and customer data at 35 percent.

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



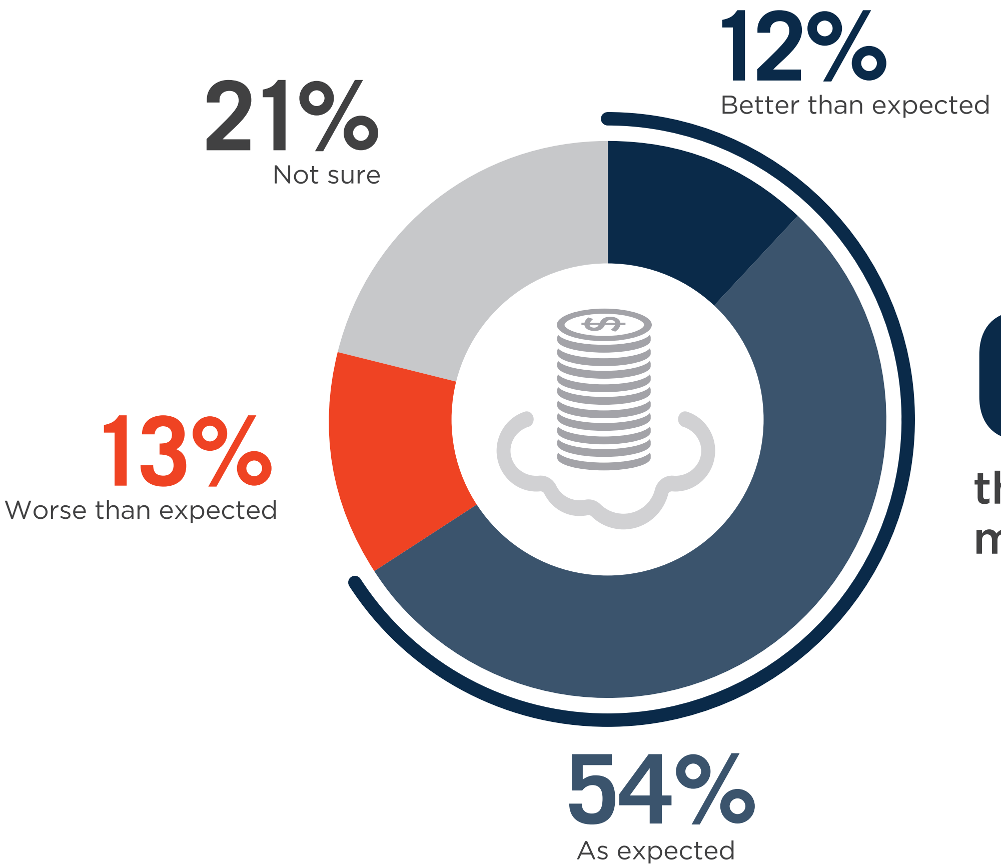
Not sure/other 24%

CLOUD BENEFITS VS. EXPECTATIONS

How does the reality of cloud computing hold up against the promise of reduced cost, increased agility, accelerated time-to-market or improved uptime?

Sixty-six percent of the IT professionals surveyed said their cloud investments are meeting or exceeding expectations. Notably, about one out of five respondents (21 percent) were unsure if the cloud had delivered on the promised benefits to the organization.

How has cloud computing delivered on the promised benefits for your organization?



66%

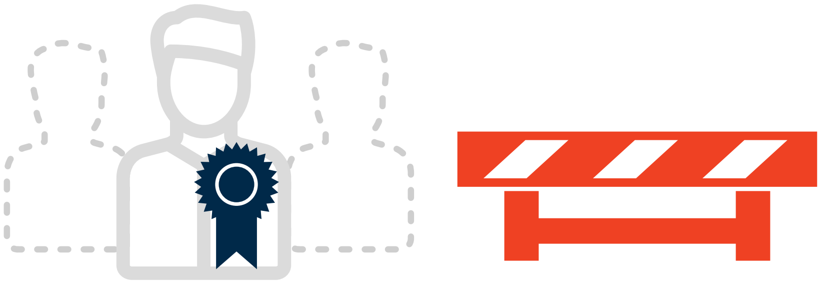
think their cloud investments are meeting or exceeding expectations

BARRIERS TO CLOUD ADOPTION

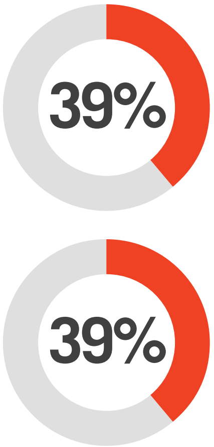
It’s important to recognize that with all of the benefits, cloud is not without its challenges. Lack of qualified staff or expertise tops the list as the primary barrier to cloud adoption (42 percent), moving up one spot from second place last year. Tied for second place this year are general security risks and integration with existing IT environments at 39 percent.

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

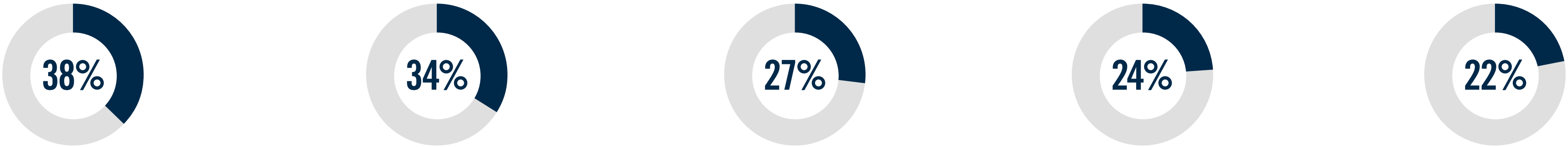


42% Lack of staff resources or expertise



39% General security risks

39% Integration with existing IT environment



38% Data security, loss & leakage risks

34% Legal & regulatory compliance

27% Loss of control

24% Internal resistance and inertia

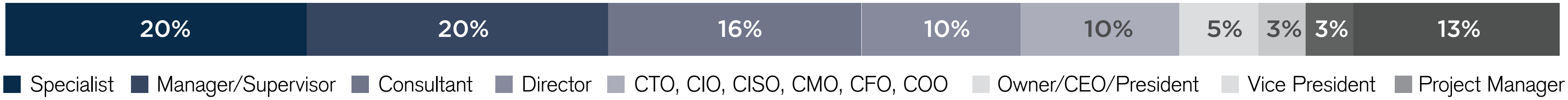
22% Fear of vendor lock-in

Lack of maturity of cloud service models 21% | Complexity managing cloud deployment 20% | Lack of transparency and visibility 19% | Lack of management buy-in 17% | Lack of budget 15% | Cost/lack of ROI 14% | Billing & tracking issues 12% | Performance of apps in the cloud 11% | Dissatisfaction with cloud service offerings/performance/pricing 10% | Lack of customizability 10% | Lack of support by cloud provider 7% | Availability 4% | Not sure/other 15%

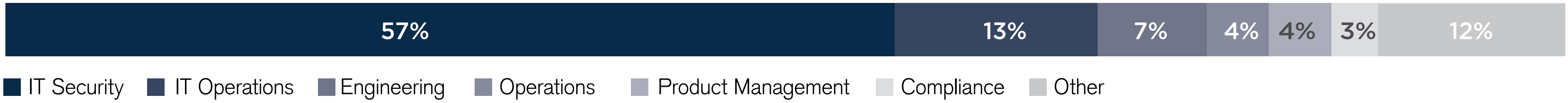
METHODOLOGY & DEMOGRAPHICS

The 2018 Cloud Security Report is based on the results of a comprehensive online survey of over 570 cybersecurity and IT professionals to gain deeper insight into the state of cloud adoption and security challenges, trends and best practices. The respondents range from security analysts and IT managers to CISOs, reflecting a representative cross section of organizations of varying sizes across different industries.

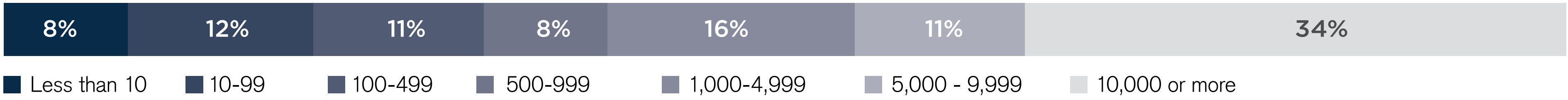
JOB LEVEL



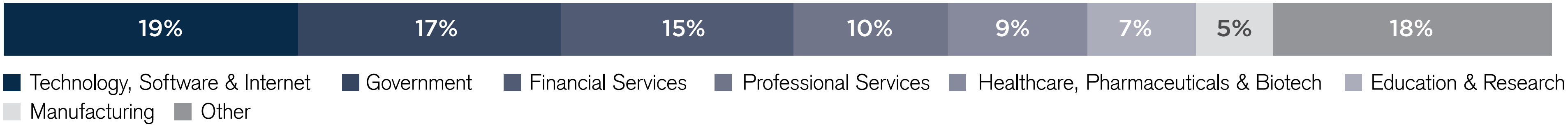
DEPARTMENT



COMPANY SIZE



INDUSTRY



COMPANY OVERVIEW

ABOUT US

SECURONIX
Security Analytics. Delivered.

Securonix | www.securonix.com

Securonix radically transforms enterprise security with actionable intelligence. Our purpose-built security analytics platforms mine, enrich, analyze, score and visualize data into actionable intelligence on the highest risk threats to organizations. Using signature-less anomaly detection techniques, Securonix detects data security, insider threat and fraud attacks automatically and accurately.

RESOURCES

Securonix offers several resource channels to keep you up to date on the latest developments in cyber security. Our cyber security subject matter experts as well as the Securonix Threat Research Labs team regularly publishes thought leadership content on emerging security threats, major breaches, security and compliance best practices.

- **Securonix BrightTALK Channel** – Our webinar channel provides CISOs, SOC analysts, incident responders, compliance professionals and other cyber security professionals the knowledge to make the right security investments and decisions. Our channel features webinars on topics for CISOs, front-line analysts and everyone in between.

  https://www.securonix.com/webinars/

- **Securonix Whitepapers** – For in depth technical papers, policy documents and deep dive collateral for specific topics make sure to visit the Securonix whitepaper library. These papers are published by our development, implementation and field teams and include real-world scenarios, use cases and customer stories.

  https://www.securonix.com/category/resources/white-papers/

- **Securonix Blog** – Check out our blog for articles on a wide range of cyber security and compliance topics, including technical commentary on key trends, news related to behavior analytics, insider threats, ransomware, social engineering, incident response, threat hunting, and more.

  https://www.securonix.com/blog/

SECURONIX
Security Analytics. Delivered.

0418