CLOUD SECURITY

TABLE OF CONTENTS

CLOUD SECURITY SPOTLIGHT REPORT

OVERVIEW

Cloud adoption is increasing quickly as organizations are looking to reduce IT cost, increase agility and better support business functions. However, security of data and systems in the cloud remains a key issue and critical barrier to faster adoption of cloud services.

This report is the result of comprehensive research in cooperation with the 250,000+ member Information Security Community on LinkedIn to explore the specific drivers and risk factors of cloud infrastructure, how organizations are using the cloud, whether the promise of the cloud is living up to the hype, and how organizations are responding to the security threats in these environments.

In this report you will learn how your peers are approaching security in the era of cloud infrastructure and gain valuable benchmark data to gauge how your own organization stacks up.

Also many thanks to our sponsors for supporting this exciting project: AlertLogic, AlienVault, Bitglass, CloudPassage, Palerra, and Redspin.

Thanks to everyone who participated in this survey.

We hope you will enjoy this report.

Holger Schulze

Holger Schulze
Group Founder
Information Security
Community on LinkedIn

✉ hhschulze@gmail.com

LinkedIn Group Partner

Information Security

The 5 Major Trends in Cloud Security

1 Security is still the biggest perceived barrier to further cloud adoption. Nine out of ten organizations are very or moderately concerned about public cloud security.

2 The dominant cloud security concerns involve unauthorized access, hijacking of accounts, and malicious insiders. Almost 80% of managers are concerned about personal cloud storage services operated by employees or visitors.

3 The most popular method to close the cloud security gap is the ability to set and enforce consistent cloud security policies. Encryption for data at rest and in motion top the list of most effective security controls for data protection in the cloud.

4 Is cloud computing delivering on the hype? Yes on flexibility, availability and cost reductions. But security and compliance remain the biggest concerns.

5 Despite SaaS providers making massive investments in security, 36% of respondents believe that major cloud apps such as Salesforce and Office 365 are less secure than on-premise applications.

CLOUD ADOPTION TRENDS

71% of respondents are either in planning stages, actively implementing or in production cloud environments.

71%
use cloud or plan to use

17%	17%	11%	17%	26%	12%
No plans to deploy	Planning to deploy	Trial / pilot phase	Currently implementing cloud	Currently deployed / in production	Not sure Other
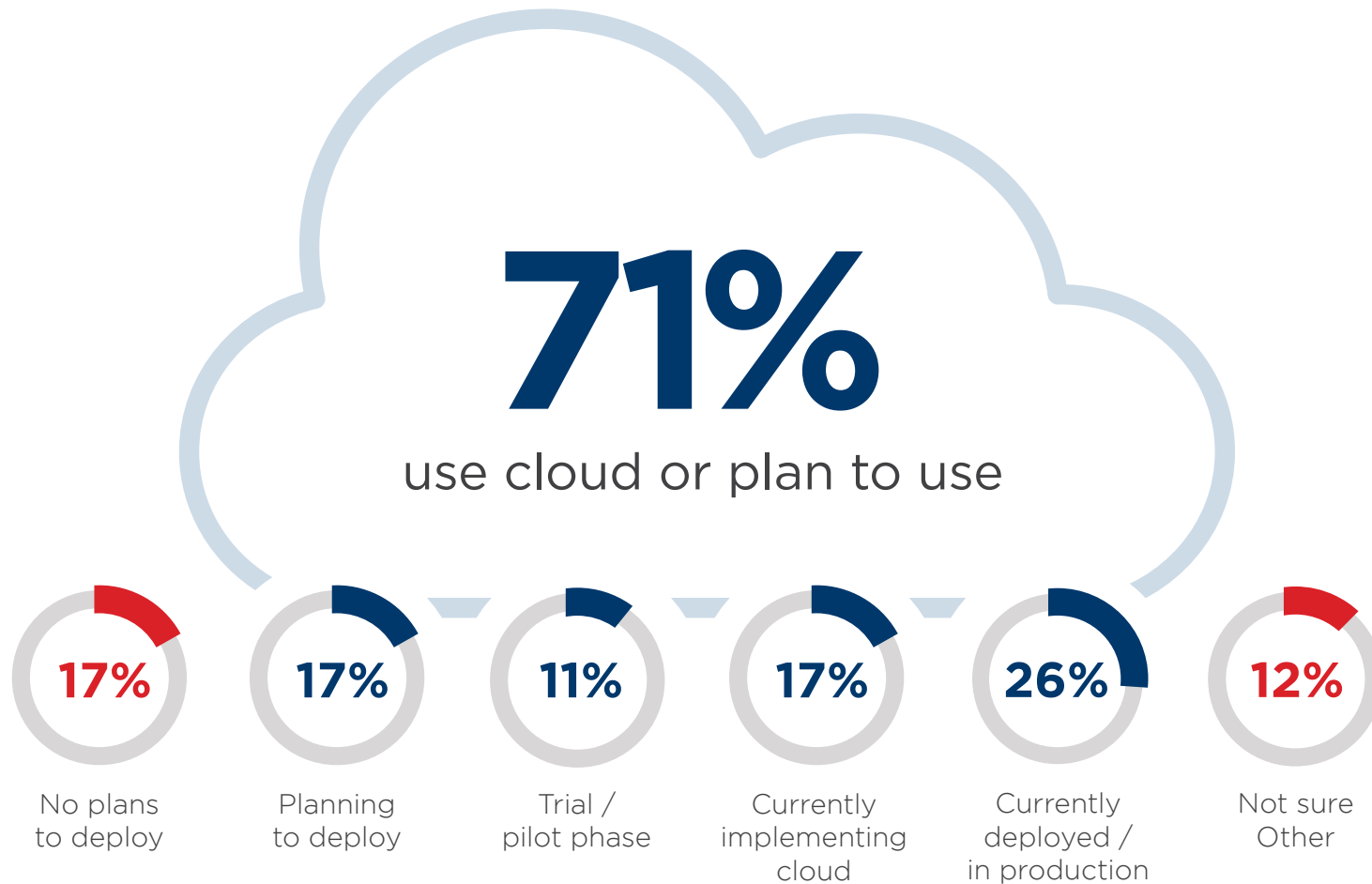
Q: What is the overall status of your organization's cloud adoption?

This question reveals a typical technology adoption pattern where 37% of respondents characterize themselves as moderate to heavy users of public cloud services. Over 77% of organizations surveyed already have at least some investment in public cloud services.

77%
are investing in public clouds

Category	Percentage
Heavy	10%
Moderate	27%
Light	40%
None	13%
Other / Not sure	10%
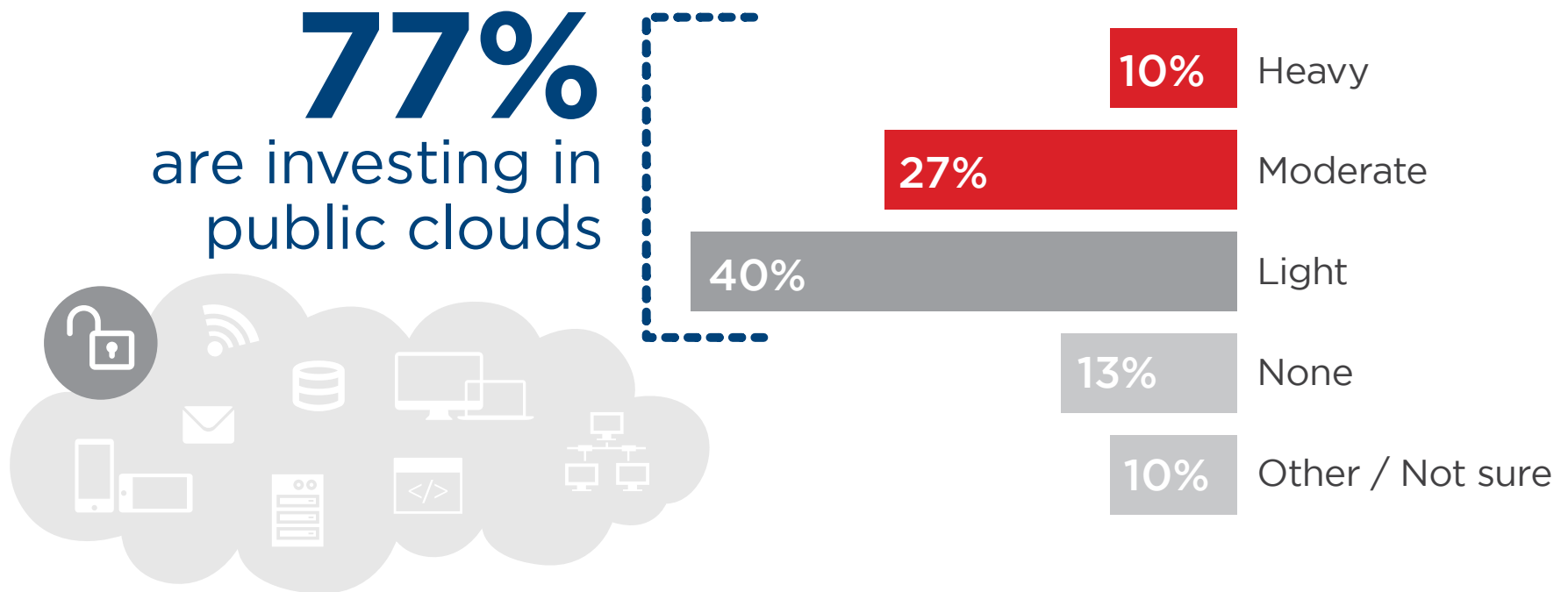
Q: What best describes your organization's use of public cloud computing?

Hybrid cloud deployments are most common with 7 out of 10 respondents using both private and public clouds in their organization.

71%
Hybrid
public & private cloud

12%
public cloud

17%
private cloud
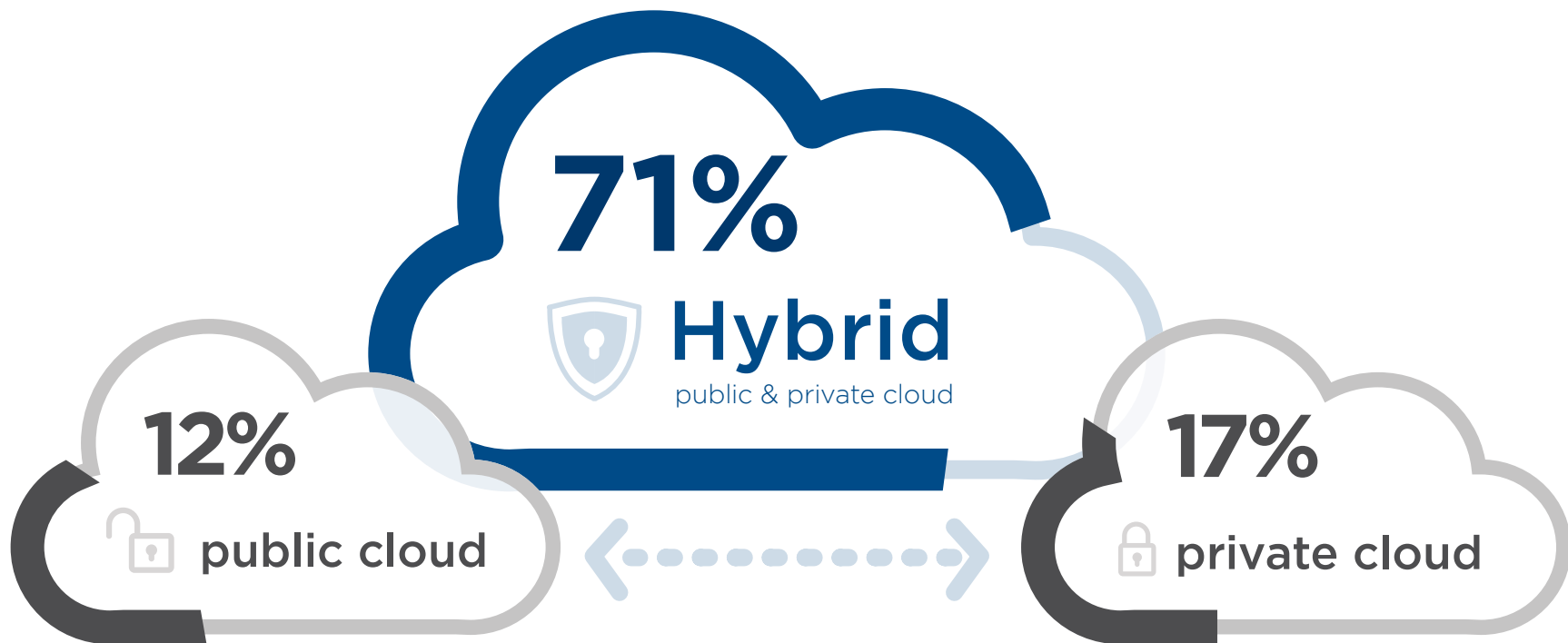
Q: What cloud deployment model is your organization using?

CLOUD SERVICE DELIVERY & PROVIDERS

The vast majority of respondents (60%) uses SaaS models, followed by IaaS (47%) and PaaS (33%) as their cloud service delivery model.

Amazon AWS is the big fish in the cloud infrastructure services pond, used by over a third of respondents. Google and Microsoft Azure follow with 25% and 22% respectively.

cloud service delivery models

SaaS
60%

PaaS
33%

IaaS
47%

31%

amazon web services™

25%

Google Cloud Platform

Windows Azure

22%
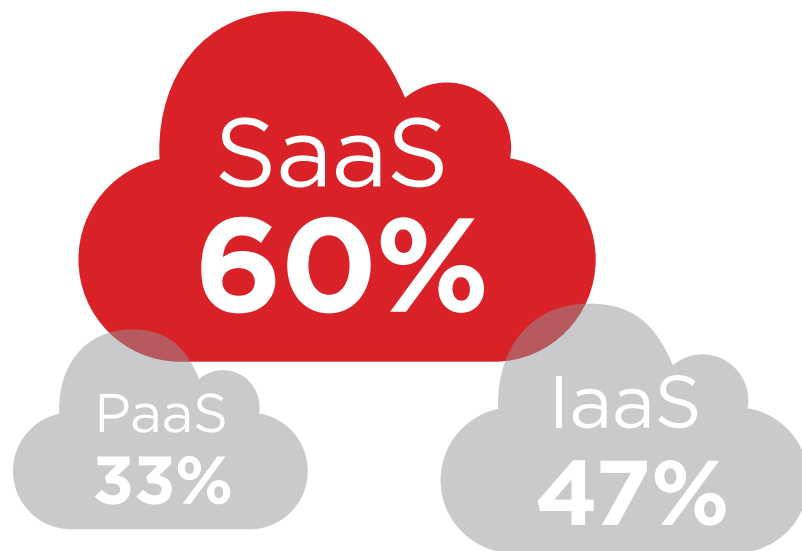
Q: What cloud service delivery model(s) is your organization using?
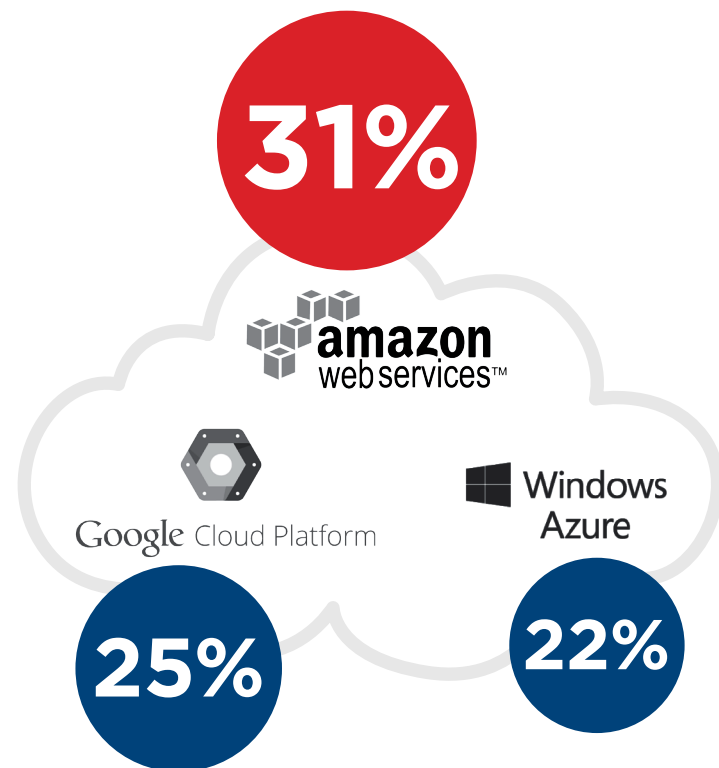
Q: What public cloud provider(s) do you currently use?

The most popular cloud workloads deployed by companies are storage (45%), computing (42%) and business applications (40%).

POPULAR CLOUD WORKLOADS

STORAGE **45%**

COMPUTING **42%**

BUSINESS APPLICATIONS **40%**

33% Networking

33% Virtualization
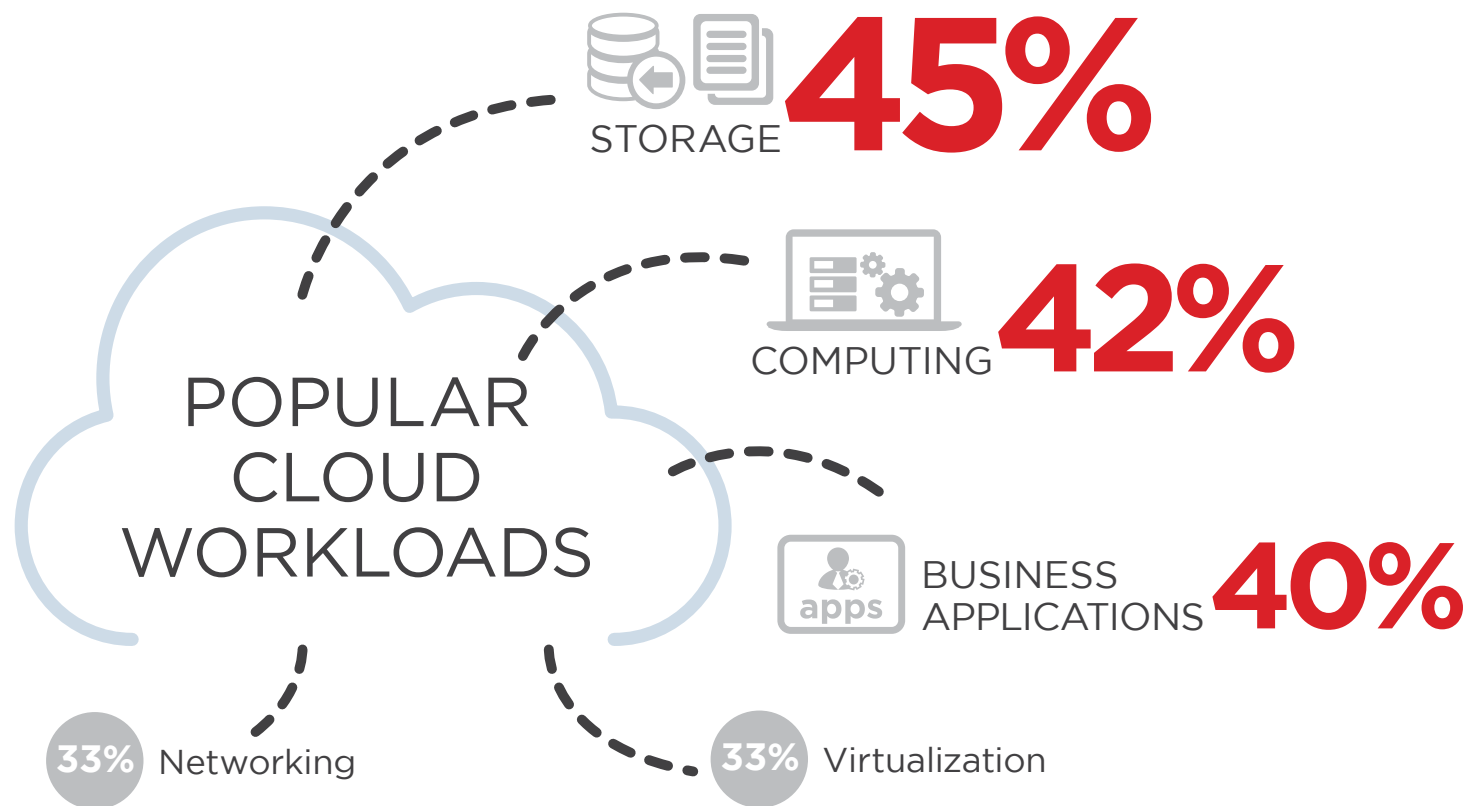
Q: What services & workloads is your organization deploying in the cloud?

MOST POPULAR CLOUD APPS

Web apps	**43%**
Collaboration & communication apps	**39%**
Sales & marketing apps	**30%**
Productivity	**29%**
IT Operations	**26%**

Web applications (43%), collaboration & communication apps (39%), and sales & marketing apps (30%) are the most common apps deployed in cloud environments.

Application development / testing 24% |
Disaster recovery / storage / archiving 23% |
HR 22% | Business intelligence / analytics 20% |
Content management 18% | Custom business applications 18% | Finance & accounting 18% |
Supply chain management 9% | Not Sure / Other 19% |

Q: What types of business applications is your organization deploying in the cloud?

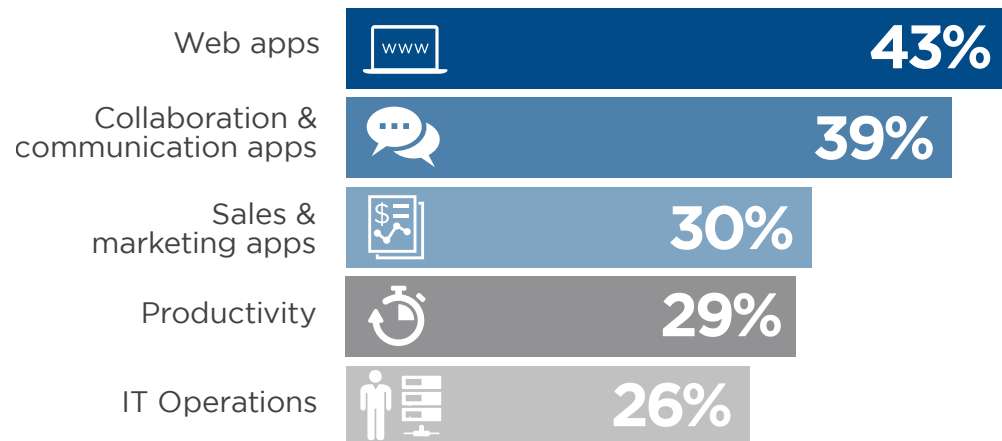## MOST POPULAR CLOUD APPS

Salesforce is leading the way in existing deployments (22%), but Office 365 is making significant headway – currently at 16% deployment among our respondents but it is the cloud service of most future interest (29%). On the File Sharing & Sync side, Dropbox (13%) has a commanding lead over Box (6%) in current deployments but Box is catching up in future interest.

CURRENTLY DEPLOYED		FUTURE DEPLOYMENT
22%	Salesforce	15%
16%	Microsoft Office 365	29%
16%	Google Apps	13%
16%	Microsoft Exchange	13%
13%	Dropbox	4%
7%	Service Now	10%
6%	Box	8%
3%	Workday	8%

Q: Which of the following cloud applications are deployed or will be deployed in your organization?

Email is the most frequently stored corporate information in the cloud (45%), followed by sales & marketing data (42%), intellectual property (38%) and customer data (31%). Few organizations store sensitive financial data (19%) or employee healthcare data (8%) in the cloud.

INFORMATION
STORED IN THE CLOUD

45% Email

42% Sales & Marketing data

38% Intellectual property

31% Customer data

19% Sensitive financial data

8% Employee healthcare data
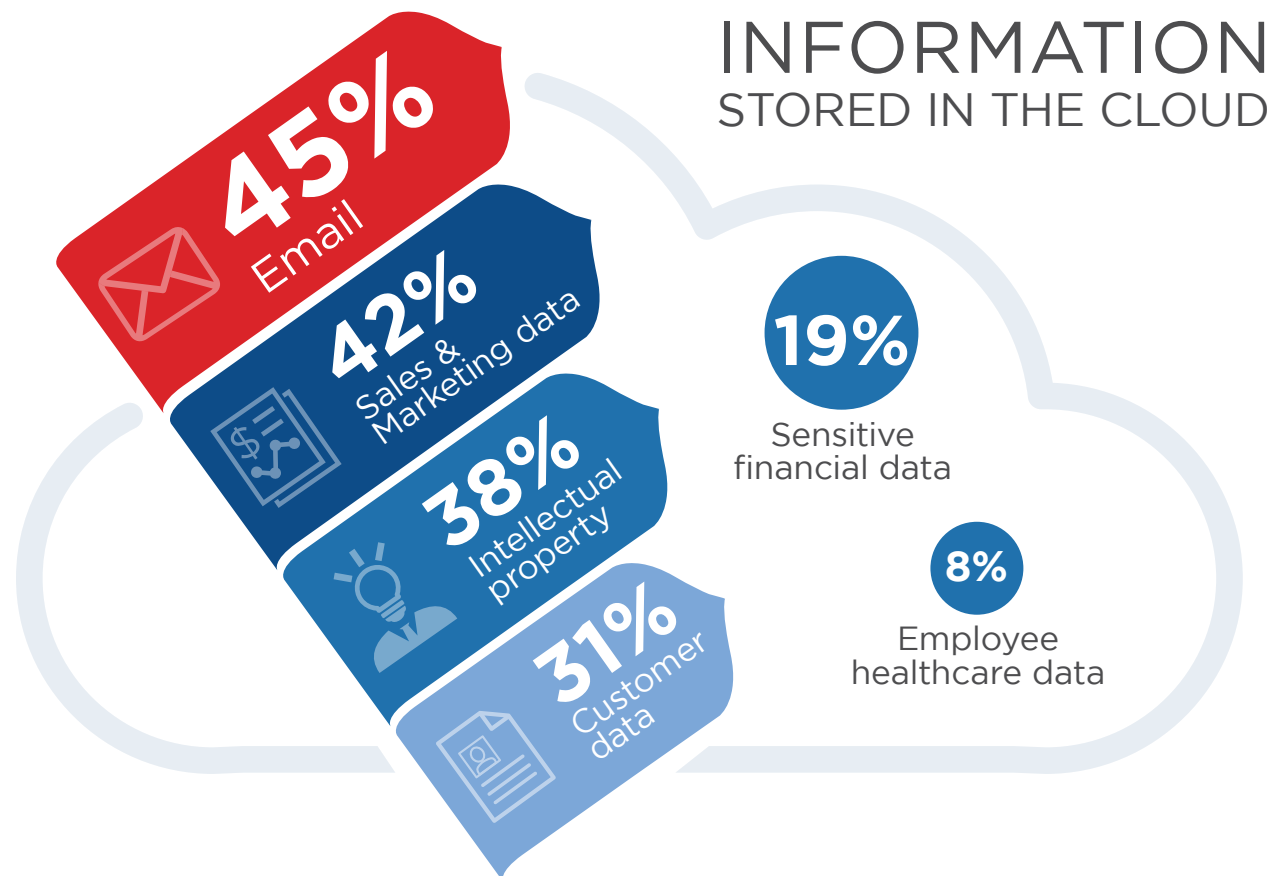
Q: What types of corporate information do you store in the cloud?

There has been much hype around the benefits of moving to the cloud. We dug deeper to uncover the truth - cloud is delivering on its promise of flexibility (51%), availability (50%) and much talked about cost reductions (48%).

Where is cloud falling short? Security (22%) and regulatory compliance (9%).

51% flexibility

50% availability

48% cost reductions

Cloud Benefits

22% security

9% compliance perceptions

EXPERIENCED CLOUD BENEFITS

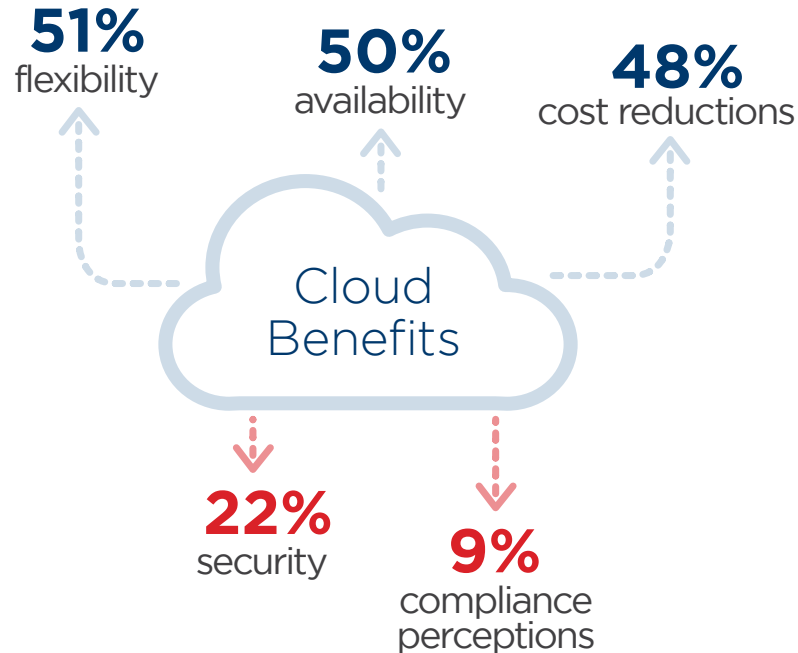|	
Gained more flexible capacity / scalability	51%
Improved availability	50%
Reduced cost	48%
Improved business continuity	46%
Increased agility	45%

Increased efficiency 41% | Moved expenses from fixed CAPEX (purchase) to variable OPEX (rental / subscription) 38% | Accelerated deployment and provisioning 38% | Increased employee productivity 31% | Increased geographic reach 28% | Accelerated timetomarket 28% | Reduced complexity 27% | Improved performance 27% | Align cost model with usage 26% | Improved security 22% | Improved regulatory compliance 9% | Not Sure / Other 3% | None 1%

Q: What benefits have you received from your cloud deployment?

CLOUD SECURITY RISKS

An overwhelming majority of 90% of organizations are very or moderately concerned about public cloud security. Today, security is the single biggest factor holding back faster adoption of cloud computing.

47%

5%

5%

43%
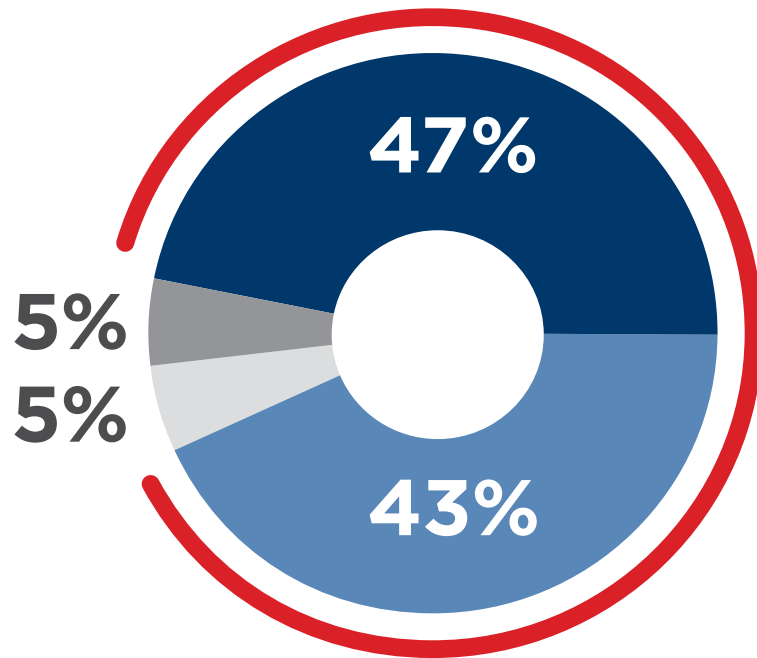
90%
organizations have security concerns

- Very concerned
- Moderately concerned
- Not at all concerned
- Not sure

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

It's clear that IT teams have security top of mind. General security concerns (45%), data loss & leakage risks (41%), and loss of control (31%) continue to top the list of barriers holding back further cloud adoption.

Cloud Adoption Barriers

#1
45%
General security concerns

#2
41%
Data loss & leakage risks

#3
31%
Loss of control

Legal & regulatory compliance 29% | Integration with existing IT environment 29% | Lack of maturity of cloud service models 21% | Internal resistance and inertia 19% | Lack of transparency and visibility 19% | Fear of vendor lock-in 19% 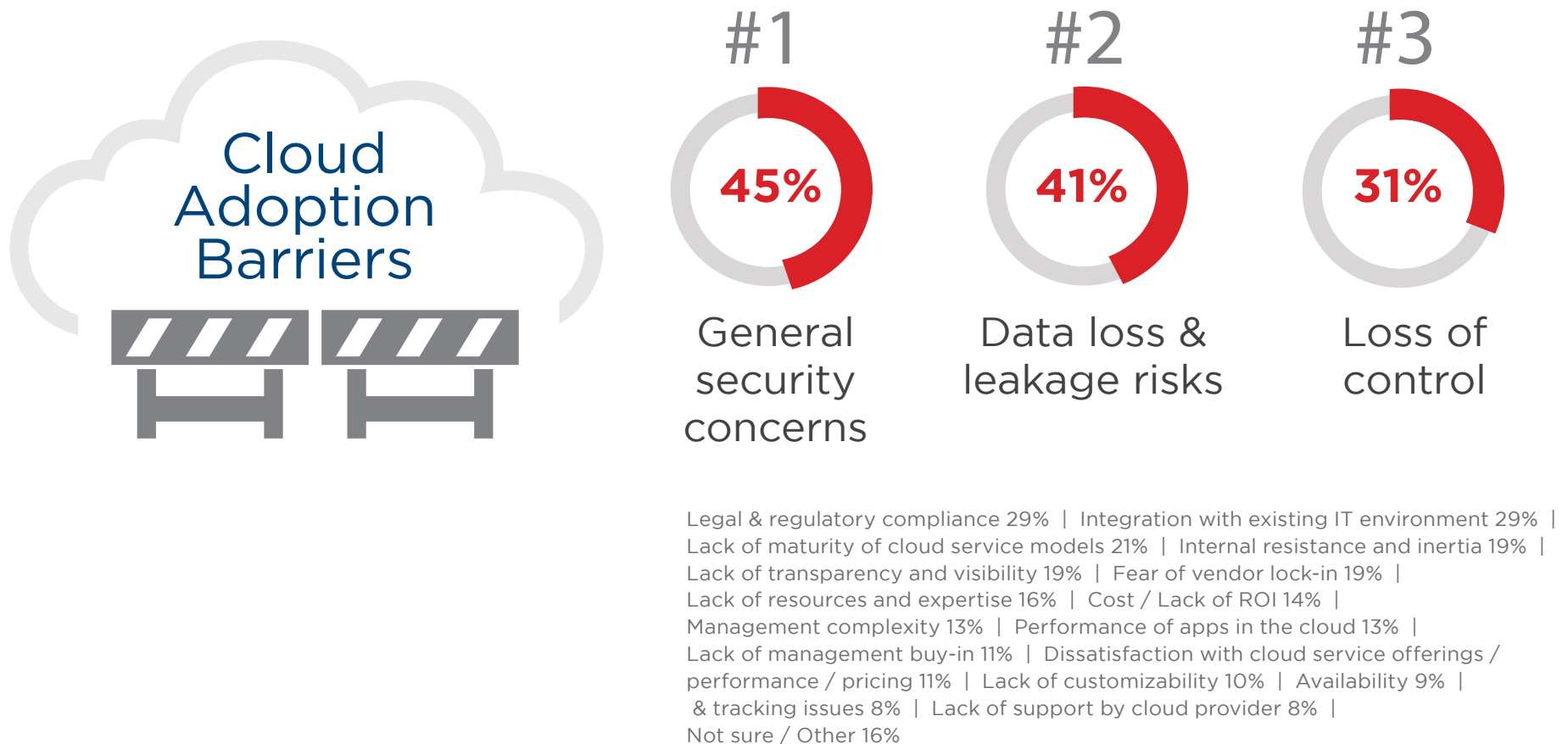| Lack of resources and expertise 16% | Cost / Lack of ROI 14% | Management complexity 13% | Performance of apps in the cloud 13% | Lack of management buy-in 11% | Dissatisfaction with cloud service offerings / performance / pricing 11% | Lack of customizability 10% | Availability 9% | & tracking issues 8% | Lack of support by cloud provider 8% | Not sure / Other 16%

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

SECURITY THREATS IN PUBLIC CLOUDS

The biggest cloud security concerns include unauthorized access (63%) through misuse of employee credentials and improper access controls, hijacking of accounts (61%), and malicious insiders (43%). Malware, denial of service attacks, and other direct attacks against the cloud provider rank lower on the list of concerns.
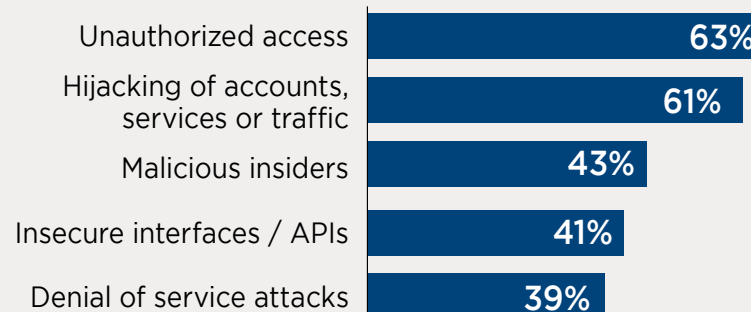
#1 63% Unauthorized access

#2 61% Hijacking of accounts

#3 43% Malicious insiders

BIGGEST SECURITY THREATS

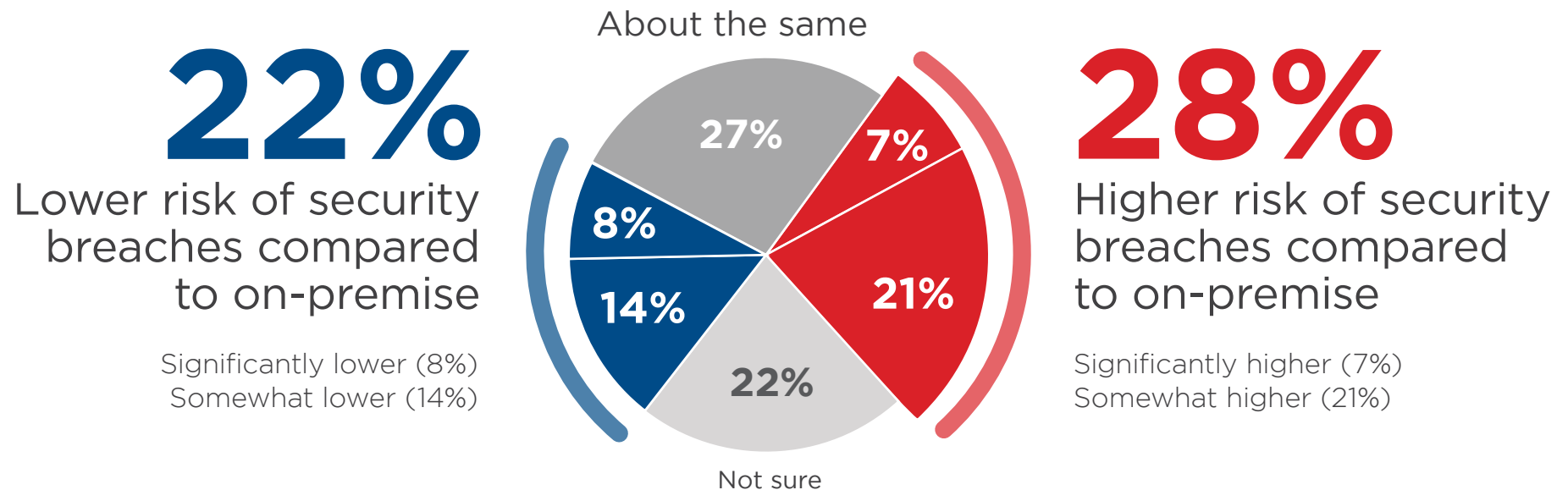|	
Unauthorized access	63%
Hijacking of accounts, services or traffic	61%
Malicious insiders	43%
Insecure interfaces / APIs	41%
Denial of service attacks	39%
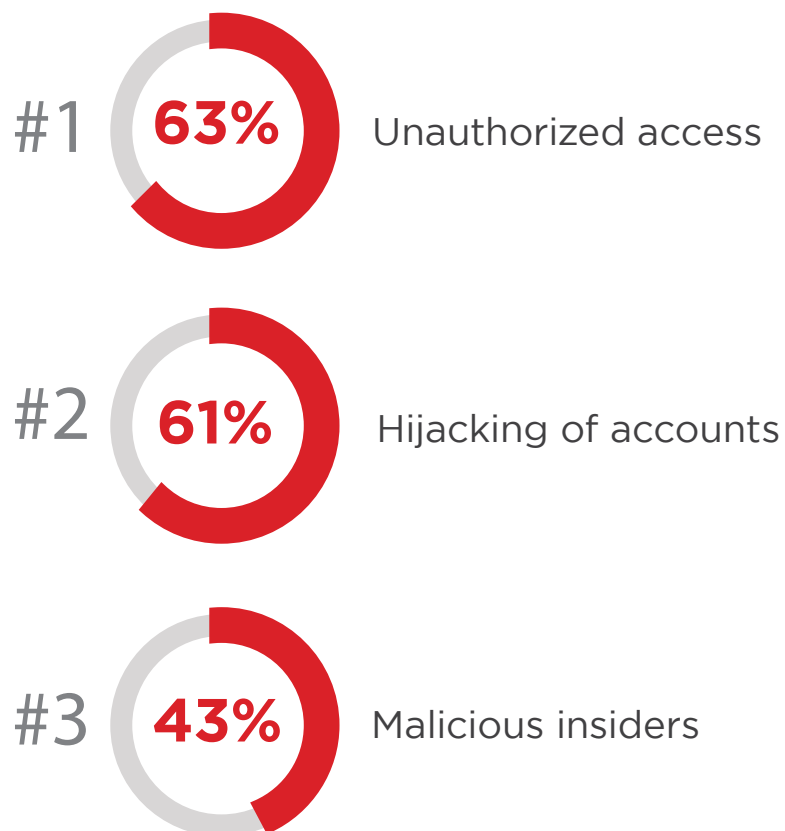
Malware injection 33% | Abuse of cloud services 33% | Shared memory attacks 24% | Theft of service 23% | Cross VM side channel attacks 22% | Lost mobile devices 18% | Natural disasters 7%

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

About one third of enterprises have experienced more security breaches with the public cloud than with on-premise applications. Only 22% say the number of cloud security breaches is lower.

About the same

22%

Lower risk of security breaches compared to on-premise

Significantly lower (8%)
Somewhat lower (14%)

27%

7%

8%

21%

14%

22%

28%

Higher risk of security breaches compared to on-premise

Significantly higher (7%)
Somewhat higher (21%)

Not sure

Q: How does the number of security breaches you experienced in a public cloud compare to your traditional IT environment?

SECURITY OF PUBLIC CLOUD APPS

Despite SaaS providers' significant investments in security, 36% of respondents believe that major cloud apps such as Salesforce and Office 365 are less secure than on-premise applications. Only 12 % believe these apps are more secure.

ARE PUBLIC CLOUD APPS SECURE?

12% More secure than our internal apps

36% Less secure than our internal apps

28% About the same

13% Not sure

11% We don't use any public cloud apps
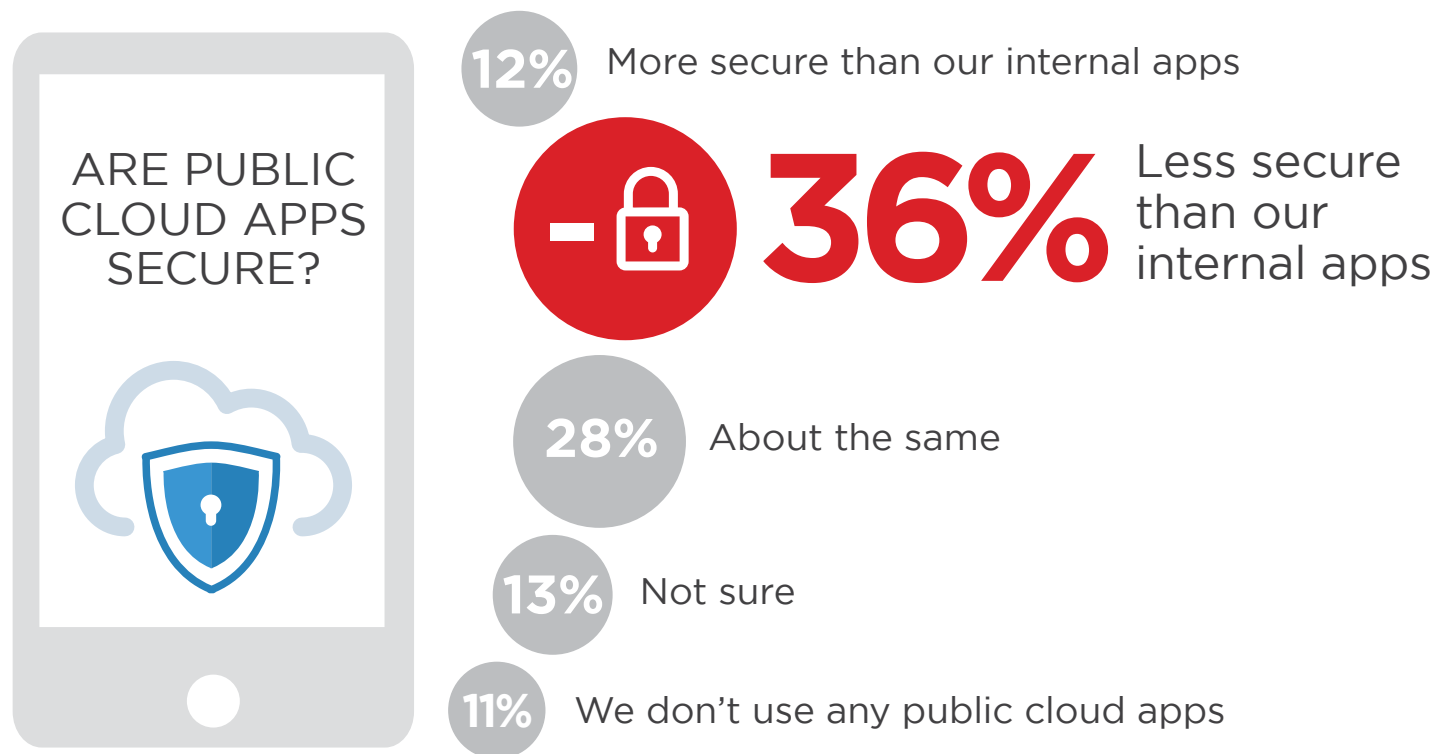
Q: Do you believe well-known public cloud apps like Salesforce and Office 365 are more or less secure than your internally hosted applications?

PERSONAL STORAGE CONCERNS

Almost 80% of managers are concerned about personal cloud storage services operated by employees or visitors, and the risk they pose regarding data privacy and leakage. This underscores the need for better visibility into data leaving the network.

78% | Yes
12% | No
11% | Not sure
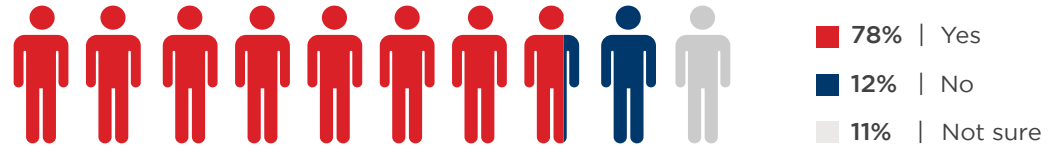
Q: Is management concerned about data security and privacy of personal cloud storage services?

Employee access to personal cloud storage services

7%

14%

36%

- Yes
- No
- We don't have a policy
- Not sure
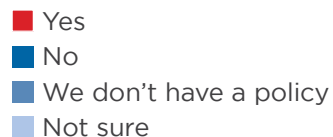
43% of respondents confirm that employees are allowed to access personal storage services from the corporate network.

Q: Are employees allowed to access personal cloud storage services from the company's network?

CLOUD SECURITY SOLUTIONS

KEY FACTORS FOR CLOUD SECURITY
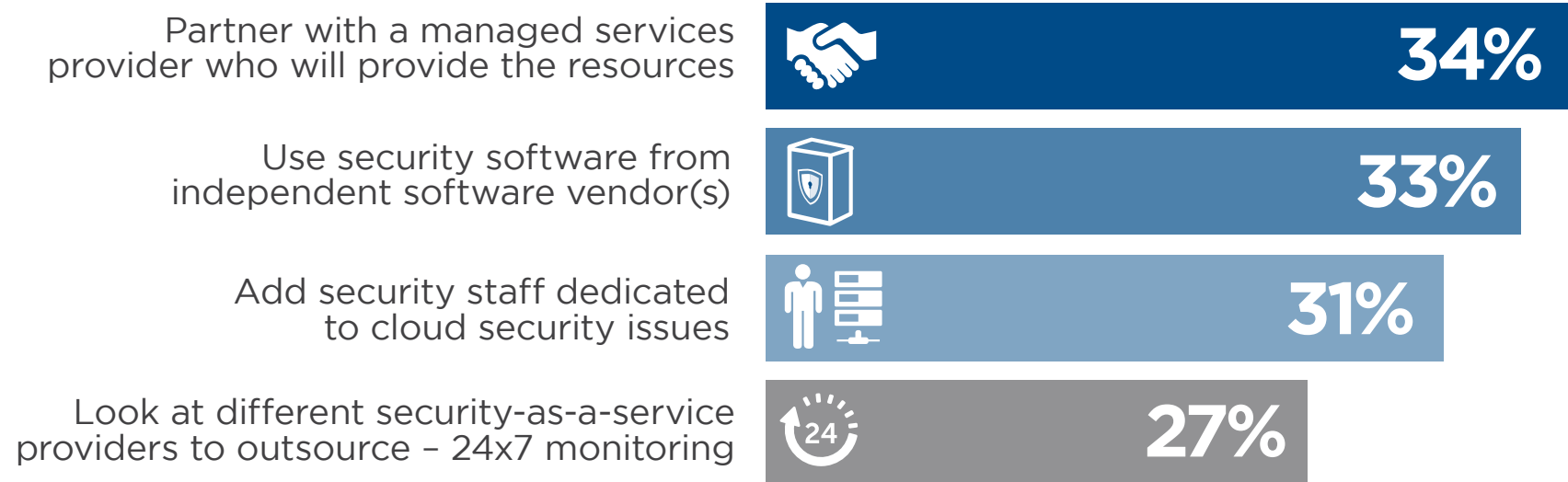
Consistent security across IT infrastructures (60%) and continuous protection (58%) are the most important factors for protecting cloud environments.

60% Consistent security with other IT infrastructure

58% Continuous protection

26% Affordability

7% No new security resources required
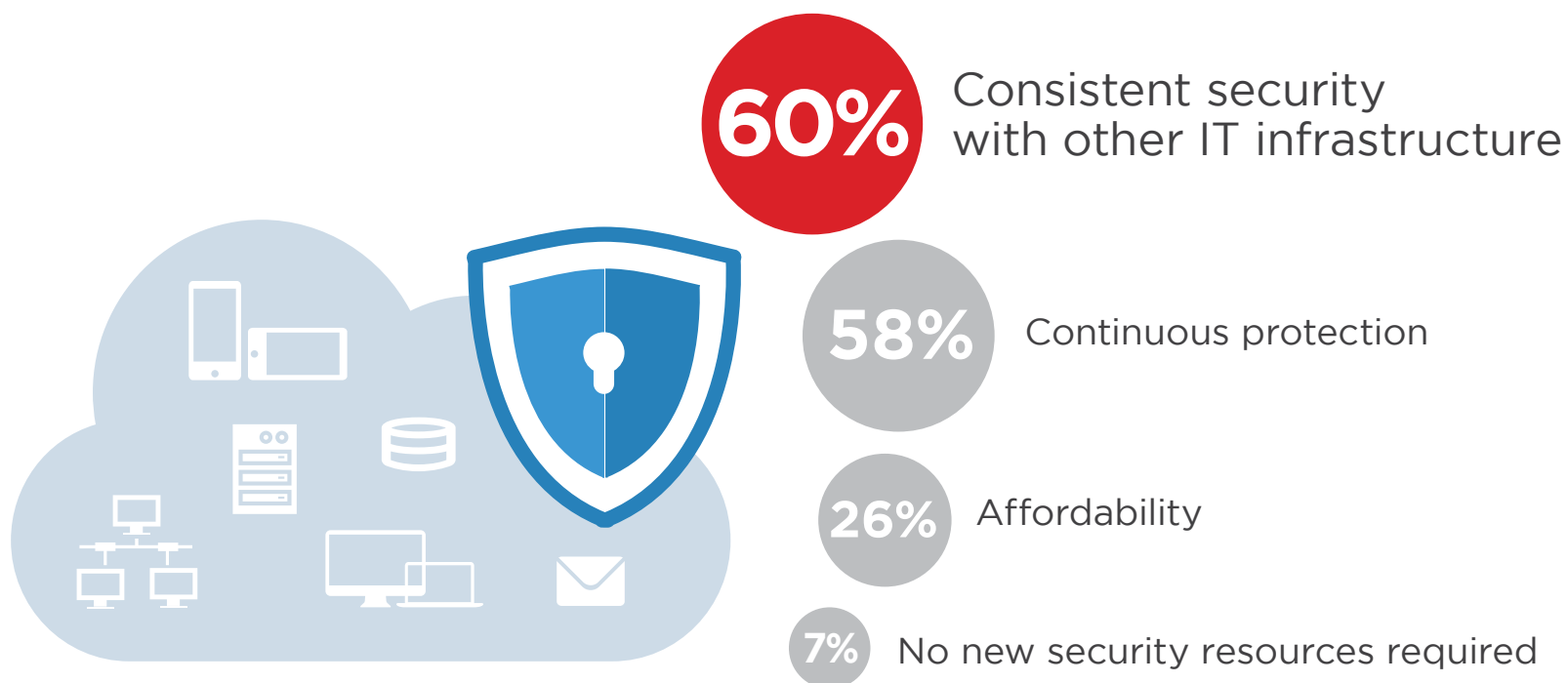
Q: What is the most important factor for protecting your cloud infrastructure?

SECURITY CHOICES

To address companies' security needs when moving to the cloud, partnering with managed service providers ranks highest (34%), followed by using security software (33%), and adding IT staff to deal with cloud security issues (31%).

Choice	Percentage
Partner with a managed services provider who will provide the resources	34%
Use security software from independent software vendor(s)	33%
Add security staff dedicated to cloud security issues	31%
Look at different security-as-a-service providers to outsource – 24x7 monitoring	27%

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

The most popular method to close the cloud security gap is the ability to set and enforce consistent cloud security policies (50%).

#1 50%
Setting and enforcing Security policies across clouds

45% #2
APIs for reporting, auditing and alerting on security events

#3 41%
Effective mapping of security controls for internally hosted applications to the cloud infrastructure

39% #4
Isolation / protection of virtual machines

#5 38%
Ability to compare security levels across cloud providers

35% #6
Highintegrity infrastructure

#7 33%
Ability to create data boundaries
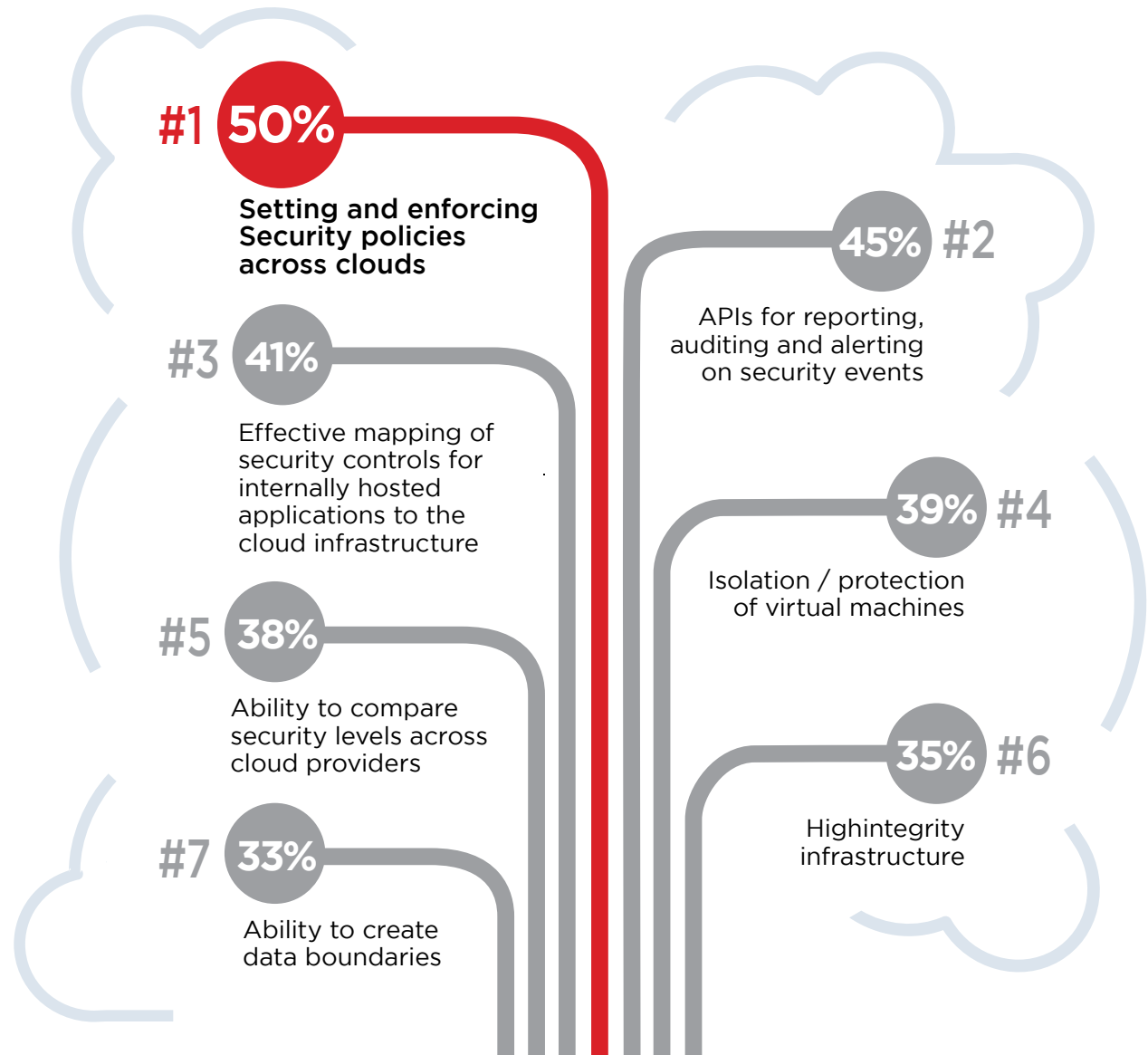
Q: Which of the following would most increase your confidence in adopting public clouds?

Encryption of data at rest (65%) and in motion (57%) tops the list of most effective security controls for data protection in the cloud. This is followed by access control (48%), intrusion detection and prevention (IDP) (48%), and security training & awareness (45%).

Encryption is most effective for data protection

Category	Percentage
Data encryption	65%
Network encryption	57%
Access control	48%
Intrusion detection & prevention	48%
Security training	45%
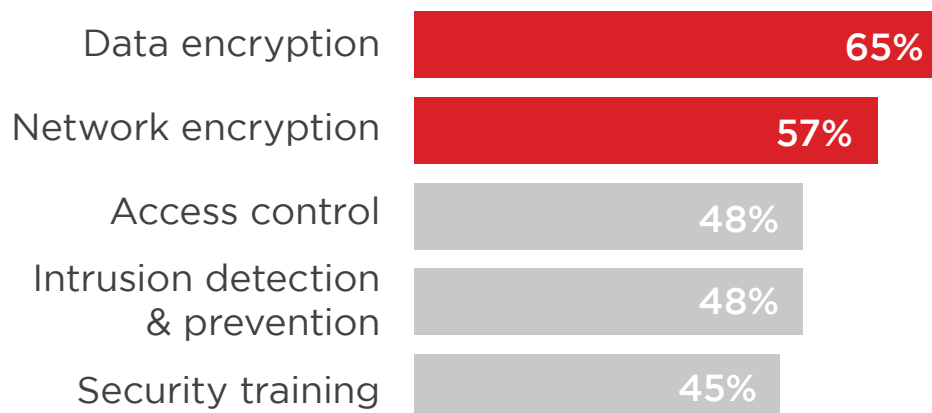
Data leakage prevention 41% | Firewalls / NAC 40% |
Log management and analytics 39% Network monitoring 36% |
Endpoint security controls 36% | Antivirus / Antimalware 36% |
Single sign-on/ user authentication 36% | Patch management 30% |
Employee usage monitoring 28% | Mobile device management (MDM) 27% |
Database scanning and monitoring 22% | Cyber forensics 21% |
Content filtering 21% | Not sure / Other 12%

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

PERIMETER SECURITY FALLS SHORT

68% of respondents say that perimeter-based security is not the whole answer to securing cloud infrastructure. The increasing frequency and success of attacks bypassing the network perimeter (and the fact that corporate data is increasingly residing outside of the perimeter) underscores the need for additional layers of defense.

15%

51%

18%

17%

68%
say perimeter-based security is not the whole answer to cloud security

- Effective
- Somewhat effective
- Ineffective
- Not sure
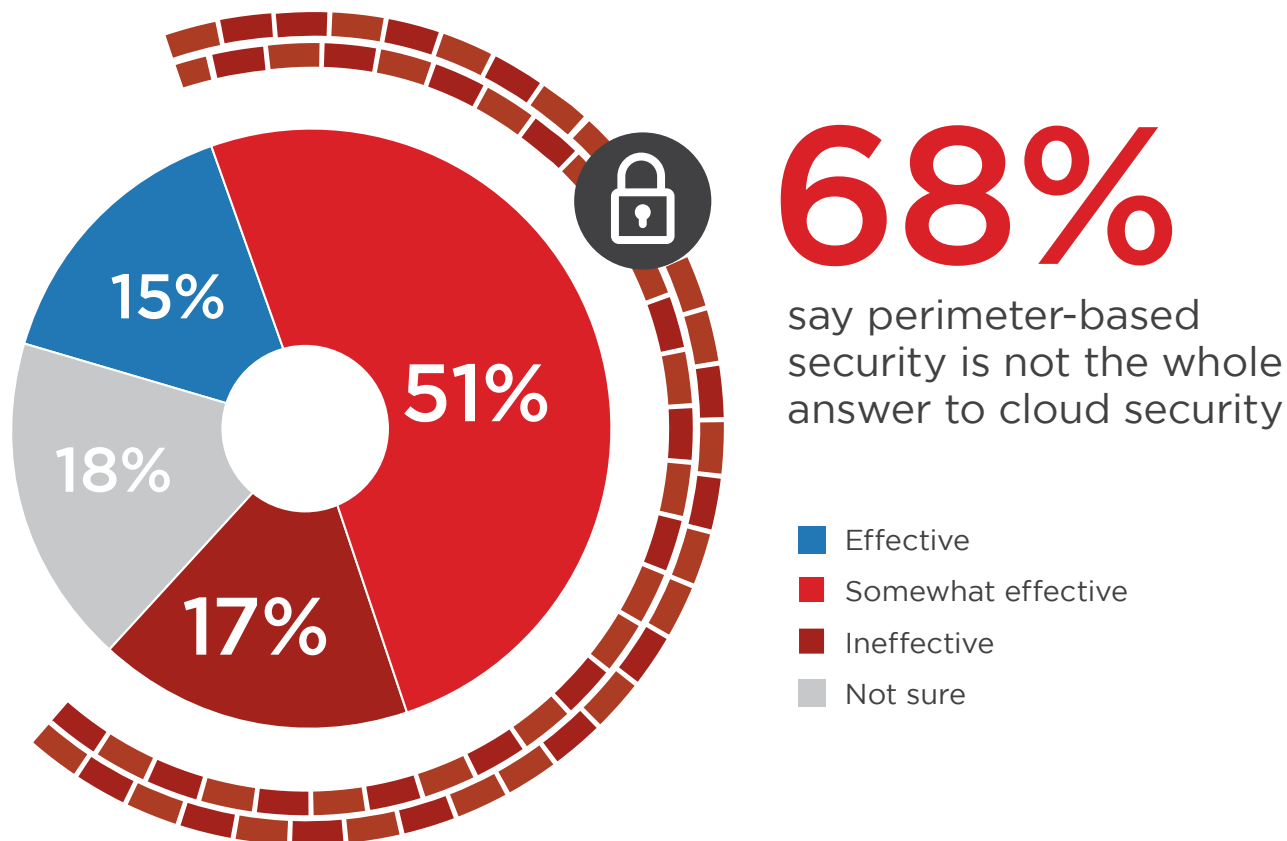
Q: How effective are perimeter-based security models in public or private clouds?

65% of respondents say that protecting the workload is at least somewhat effective. This finding confirms the shift from focusing on attack prevention and perimeter security toward defense in depth and advanced data protection methods such as encryption.

18%

47%

27%

8%

65%

say that protecting the workload is effective or somewhat effective

- Effective
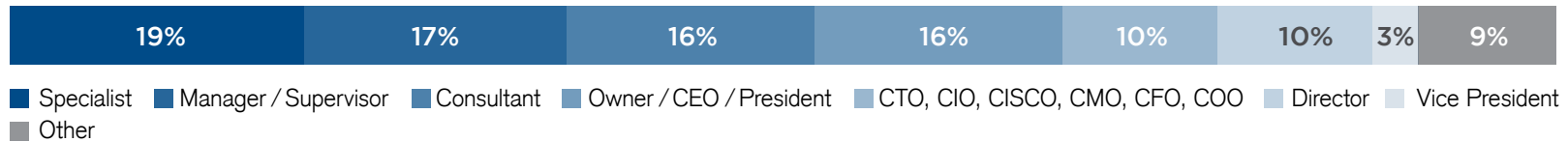- Somewhat effective
- Ineffective
- Not sure
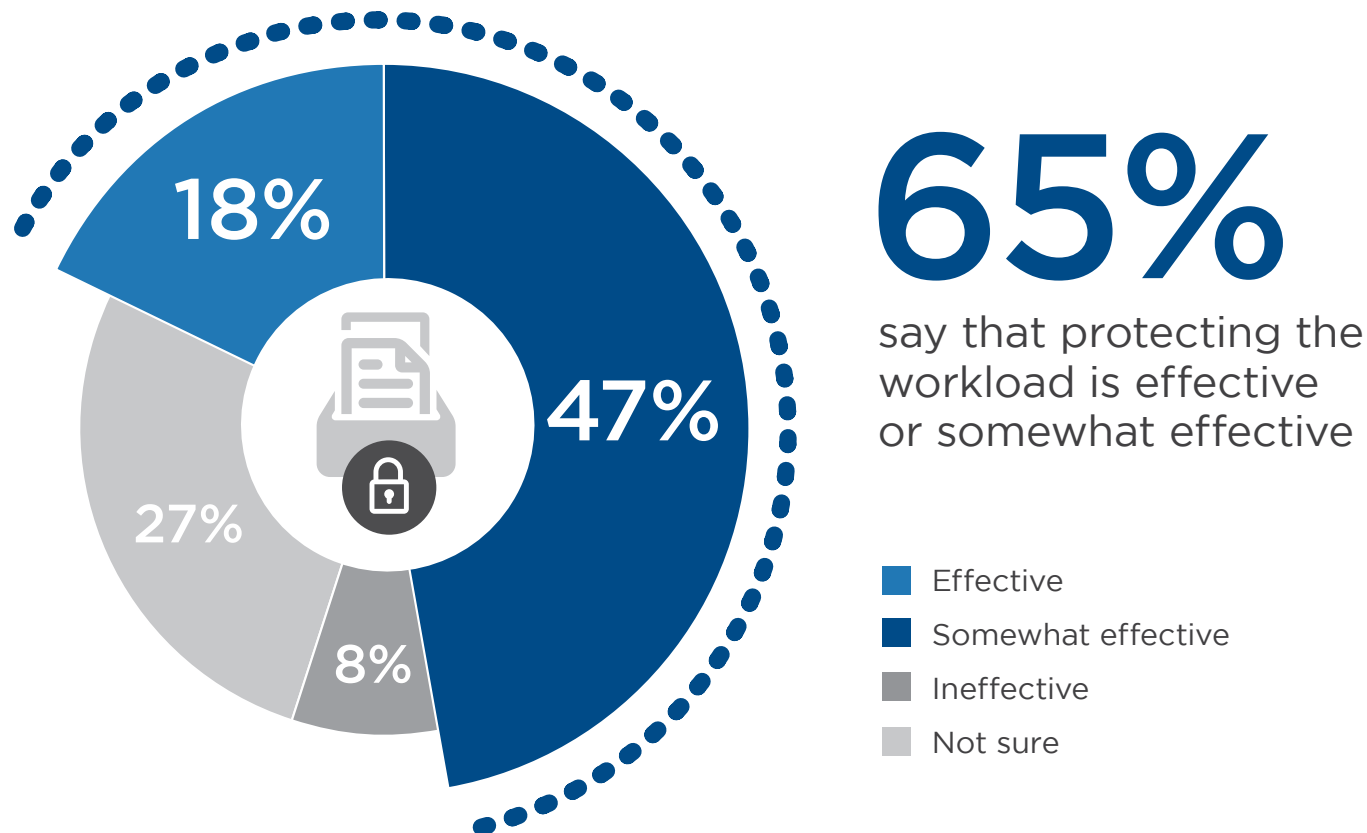
Q: Is moving security from the perimeter to the workload an effective model for private or public cloud implementations?
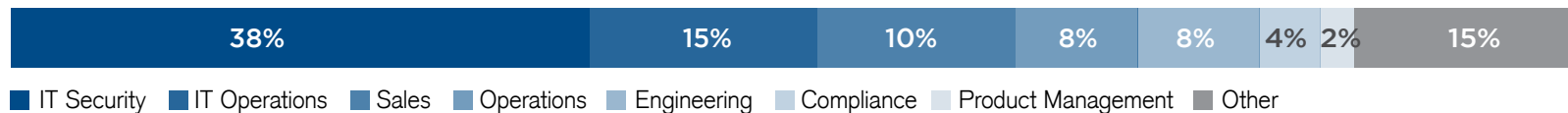
METHODOLOGY & DEMOGRAPHICS

The Cloud Security Spotlight Report is based on the results of a comprehensive survey of 1,010 professionals across a broad cross-section of organizations about their adoption of cloud computing and security related concerns and practices.

The 1,010 respondents range from technical executives to managers and practitioners, and they represent organizations of varying sizes across many industries. Their answers provide a comprehensive perspective on the state of cloud security today.
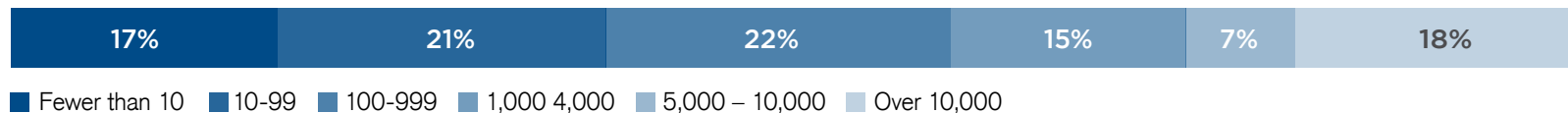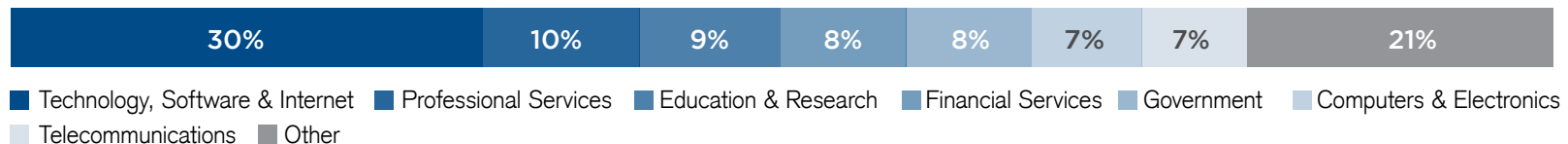
CAREER LEVEL

19%	17%	16%	16%	10%	10%	3%	9%

■ Specialist ■ Manager / Supervisor ■ Consultant ■ Owner / CEO / President ■ CTO, CIO, CISCO, CMO, CFO, COO ■ Director ■ Vice President
■ Other

DEPARTMENT

38%	15%	10%	8%	8%	4%	2%	15%

■ IT Security ■ IT Operations ■ Sales ■ Operations ■ Engineering ■ Compliance ■ Product Management ■ Other

COMPANY SIZE

17%	21%	22%	15%	7%	18%

■ Fewer than 10 ■ 10-99 ■ 100-999 ■ 1,000 4,000 ■ 5,000 – 10,000 ■ Over 10,000

INDUSTRY

30%	10%	9%	8%	8%	7%	7%	21%

■ Technology, Software & Internet ■ Professional Services ■ Education & Research ■ Financial Services ■ Government ■ Computers & Electronics
■ Telecommunications ■ Other

AlertLogic | www.alertlogic.com

Alert Logic, the leader in security and compliance solutions for the cloud, provides Security-as-a-Service for on-premises, cloud, and hybrid infrastructures, delivering deep security insight and continuous protection for customers at a lower cost than traditional security solutions. Alert Logic partners with the leading cloud platforms and hosting providers to protect over 3,000 organizations worldwide. Our patented platform stores petabytes of data, analyzes over 400 million events and identifies over 50,000 security incidents each month. Alert Logic, founded in 2002, is headquartered in Houston, Texas, with offices in Seattle, Dallas, Cardiff, Belfast and London.

AlienVault | www.AlienVault.com

AlienVault™ is the champion of mid-size organizations that lack sufficient staff, security expertise, technology or budget to defend against modern threats. Our Unified Security Management™ (USM) platform provides all of the essential security controls required for complete security visibility, and is designed to enable any IT or security practitioner to benefit from results on day one. Powered by the latest AlienVault Labs Threat Intelligence and the Open Threat Exchange™—the world's largest crowd-sourced threat intelligence exchange—AlienVault USM delivers a unified, simple and affordable solution for threat detection and compliance management. Follow us on Twitter @AlienVault.

Bitglass | www.bitglass.com

In a world of cloud applications and mobile devices, IT must secure corporate data that resides on third-party servers and travels over third-party networks to employee-owned mobile devices. Existing security technologies are not suited to solving this task, since they were developed to secure the corporate network perimeter. Bitglass is a Cloud Access Security Broker that delivers innovative technologies that transcend the network perimeter to deliver total data protection for the enterprise - in the cloud, on mobile devices and anywhere on the Internet. Founded in 2013 by industry veterans with a proven track record of innovation, Bitglass is based in Silicon Valley and backed by venture capital from NEA and Norwest.

SPONSORS

CloudPassage | www.cloudpassage.com

CloudPassage Halo® is the world's leading agile security platform that empowers our customers to take full advantage of cloud infrastructure with the confidence that their critical business assets are protected. Halo delivers a comprehensive set of continuous security and compliance functions right where it counts — at the workload. Our platform orchestrates security on-demand, at any scale and works in any cloud or virtual infrastructure (private, public, hybrid or virtual data center). Leading enterprises like Citrix, Salesforce.com and Adobe use CloudPassage today to enhance their security and compliance posture, while at the same time enabling business agility.

Palerra | www.palerra.com

Palerra designed LORIC™ to provide continuous compliance, threat visibility, and automated incident response for an organization's entire cloud footprint (SaaS, PaaS, and IaaS) in a single platform. It automates all steps of the security lifecycle to enable organizations to keep pace with the rapidly increasing volume of cloud usage as well as the velocity of change in the threat landscape. LORIC does so without any hardware or software, and does not impact the native user experience for cloud usage. Today enterprises across financial services, consumer hospitality, hi-technology and more use LORIC from Palerra, to secure their Cloud footprint.

Redspin | www.redspin.com

Redspin has provided HIPAA Security Risk Analysis services to 135+ hospitals, nearly 1000 clinics, and several large business associates. Staffed by expert security engineers and compliance consultants, Redspin helps safeguard confidential information and protect critical IT infrastructure. The company offers penetration testing, continuous vulnerability assessments, web application security audits, internal security and compliance reviews, mobile device security assessments, social engineering, and security awareness training. Through in-depth analysis and business acumen, Redspin has become a trusted security advisor to the healthcare industry, as well as banking and financial services, retail, energy, technology, and hospitality.

Interested in joining the next security research report?

Contact Holger Schulze to learn more.

✉ hhschulze@gmail.com

Linked **in** Group Partner

Information

Security