

# Navigating a Cloudy Sky

Practical Guidance and the State of Cloud Security



## Table of Contents

|           |  |           |  |
|-----------|--|-----------|--|
| <b>3</b>  | <b>Preface</b>   | <b>12</b> | <b>Dealing with Obstacles</b>  |
| <b>4</b>  | <b>Key Survey Findings</b>   | <b>12</b> | Data theft   |
| <b>5</b>  | <b>Introduction</b>  | <b>13</b> | The looming uncertainty of GDPR  |
| <b>6</b>  | <b>Setting a Course</b>  | <b>13</b> | Concerns and the reality of security incidents for IaaS                |
| <b>6</b>  | Combination of public and private cloud is the most popular architecture             | <b>15</b> | Concerns and the reality of security incidents for SaaS                |
| <b>8</b>  | Security is working to catch up with the use of containers and serverless computing. | <b>16</b> | Concerns and the reality of security incidents for private cloud       |
| <b>9</b>  | IaaS workloads have many roles   | <b>18</b> | Learning to live with Shadow IT  |
| <b>9</b>  | Lifting and Shifting to the cloud versus cloud-native applications                   | <b>19</b> | Malware from cloud apps  |
| <b>9</b>  | Cloud-first is the strategy of most organizations                                    | <b>19</b> | <b>Adjusting the speed</b>   |
| <b>10</b> | Sensitive data stored in the public cloud  | <b>20</b> | Skills shortage is decreasing  |
| <b>11</b> | Benefits of the cloud still outweigh the risks                                       | <b>21</b> | Going faster and safer   |
|           |  | <b>21</b> | Effects of cloud first   |
|           |  | <b>22</b> | Usage of DevOps and DevSecOps  |
|           |  | <b>23</b> | <b>The Takeaway: Accelerate business through secure cloud adoption</b> |
|           |  | <b>24</b> | <b>Appendix: Methodology and Demographics</b>                          |

### Preface

We are moving to the cloud. That has been the recurring message not only in previous publications but actually for a number of years in most industry studies. I remember in our first study on cloud adoption we were told from respondents that they intend to move 80% of their infrastructure to the cloud within 16 months. In the results for this year's study we are seeing a clear delineation between organizations that plan to speed up cloud adoption and those that wish to be more circumspect. Indeed the reduction in cloud-first strategies this year appears to be a clear indicator, with the average number of professionals reporting a cloud-first approach dropping to 65%, down from 82% one year ago.




To put this into perspective, organizations with a cloud-first strategy plan to migrate 80% of their IT budget to the cloud in 12 months, compared to 18 months for those without. Often, geography is cited as the key differentiator regarding cloud adoption. Whilst stereotypes like this are a useful talking point, a broad range of organizations across the globe have indeed invested in developing strategies to address the challenges of migrating to third party cloud providers. Even the realization of risk in the cloud does not appear to discourage adoption. For example 56% of professionals surveyed had tracked a malware infection back to a cloud application, up from 52% in 2016. Despite the risks, the impending march continues. In fact not only will it continue, but usage will almost certainly increase. A safer approach is being taken with security in mind and budget growth to match.

This year's study demonstrates that there are firms ramping up cloud adoption and increasing investment to manage the risks, and conversely a larger number of organizations (compared to last year) that are taking a more cautious approach. I use the words a 'cautious approach' but their competitors might perceive them as instead, 'being left behind'.

Raj Samani, McAfee Chief Scientist

[Twitter@Raj\\_Samani](https://twitter.com/Raj_Samani)

### Key Survey Findings<sup>1</sup>

-  **97%** Of organizations use cloud services (public, private, or a combination of both), up from 93% one year ago.
-  **65%** Have a cloud-first strategy, down from 82% one year ago.
-  **83%** Store sensitive data in the public cloud.
-  **69%** Trust the public cloud to keep their sensitive data secure.
-  **1 in 4** Have experienced data theft from the public cloud. (found for both Software-as-a-Service and Infrastructure-as-a-Service).
-  **1 in 5** Have experienced an advanced attack against their public cloud infrastructure.
-  **40%** Of IT leaders are slowing cloud adoption due to a shortage of cybersecurity skills.
-  **2x** More likely to have a strategy for securing containers and serverless computing when a DevSecOps function is present.
-  **27%** Of IT security budgets on average are allocated to cloud security—estimated to reach 37% in 12 months.
-  **<10%** Of organizations on average anticipate decreasing cloud investment as a result of the European Union's General Data Protection Regulation (GDPR).

<sup>1</sup>See Appendix for details of the survey methodology and demographics



## Introduction

Poor visibility is one of the greatest challenges to a navigator, preventing them from ever leaving their familiar and well-charted environment unless they can learn to rely on their instruments and expertise. Across all industries—computing, storage, and asset protection are transitioning to the cloud, making it difficult for IT practitioners to confidently see what is ahead. This uncertainty and lack of visibility to new environments is causing some executives to move slowly or stick to their known paths, while others move boldly ahead, trusting their instruments and expertise to help them navigate an increasingly cloudy sky.

Cloud services are nearly ubiquitous, with 97% of worldwide IT professionals surveyed using some type of cloud functions in their organization, up from 93% just one year ago. To gather more insight, we asked about the different types of cloud services these organizations are using, the nature of their operational processes, and issues they have actually experienced. Prominently, 1 in 4 organizations who use Infrastructure-as-a-Service (IaaS) or Software-as-a-Service (SaaS) have had data stolen, and 1 in 5 have experienced an advanced attack against their public cloud infrastructure. Security is a fundamental part of cloud operations, so we also inquired about security budget plans and assessed the impact of various adoption strategies on security spending. Finally, as organizations prepare for the European Union's General Data Protection Regulation

(GDPR), we surveyed information security executives on the adjustments and expected impacts to future cloud adoption in light of this new law.

The overall objectives of this research are to categorize uses of cloud services today, identify near-term investments, measure how quickly change will occur, and outline methods for dealing with critical privacy and security obstacles. Providing practical guidance for our readers is a primary objective for this year's report. 1,400 IT decision makers were surveyed around the world, and for additional insight we interviewed several C-level executives in-depth to add their personal perspective to the findings.

Connect With Us





### Setting a Course

Getting to your destination requires knowing where you are, where you want to go, and what obstacles are between those two locations. Almost all organizations are well into cloud adoption now. The average number of self-reported public cloud services in use has increased slightly in the past year, from 29 to 31 services per organization. The number of services in use grows steadily with organization size, from 25 services reported on average in firms with up to 1,000 employees, to 40 services on average in enterprises with more than 5,000 employees. The highest cloud service users are organizations in Japan and the United States, or those in the financial services industry. The lowest are in the United Kingdom, or in government and education organizations.

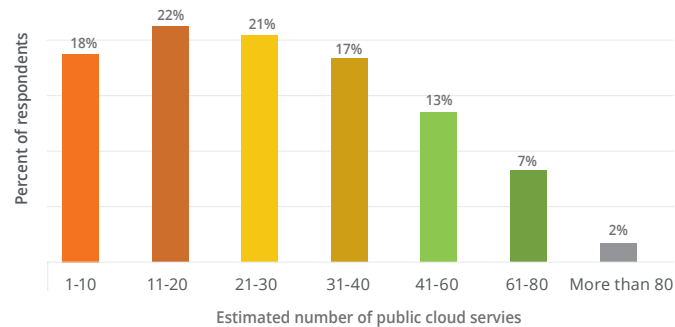


Figure 1. Please estimate how many public cloud services (IaaS, SaaS or PaaS) are currently in use by your organization.

### Combination of public and private cloud is the most popular architecture

Survey respondents were asked which of three types of cloud architecture were in use at their organization, and could choose only one option:

- Private only (single-tenant cloud)
- Public only (SaaS, IaaS, or PaaS)
- Hybrid (combination of public and private cloud)

## REPORT

Respondents were then asked what types of cloud services they were using, and could choose one or more of the three options:

- Software-as-a-Service (SaaS) e.g. Salesforce, Box, Office 365
- Infrastructure-as-a-Service (IaaS) e.g. Amazon Web Services, Microsoft Azure
- Platform-as-a-Service (PaaS) e.g. Google App Engine, Red Hat OpenShift, Force.com, AWS PaaS, Azure PaaS

The dramatic shift away from private-only to a hybrid architecture that began in 2015 appears to be stabilizing, with 59% of respondents now reporting that they are using a hybrid model, up from 57% in 2016. While private-only usage is relatively similar across all organization sizes, hybrid usage grows steadily with organization size, from 54% in organizations up to 1,000 employees, to 65% in larger enterprises with over 5,000 employees. Public-only drops from 23% to just 13% respectively.

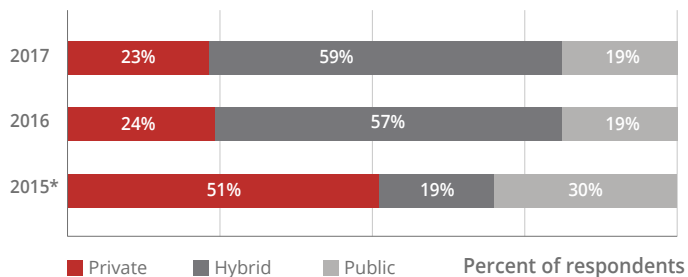


Figure 2. Which type of cloud architecture is your organization currently using? (grouped by year).

\*In 2015 this question was worded slightly differently, as 'What percent of your cloud deployment is made up of the following?', with SaaS-only respondents omitted.

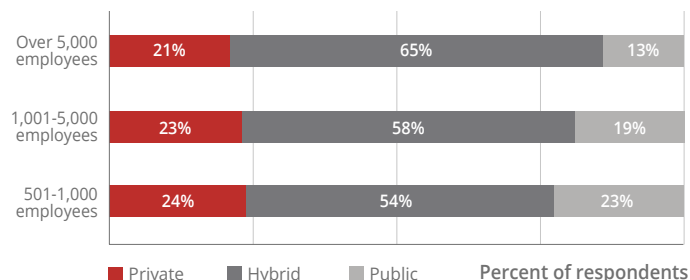


Figure 3. Which type of cloud architecture is your organization currently using? (grouped by organization size).

By industry, private-only usage was highest in governments, hybrid highest in telecoms, and public-only highest in manufacturing and education. It is not surprising that governments continue to be the most reliant on private cloud. In addition to the regulatory and cross-border concerns of sensitive data storage, procurement and budgetary issues impact cloud adoption for those public institutions. Many governments have restrictions on multi-year service contracts, forcing them into sometimes undesirable yearly-renewal options. It is also easier to justify spending to support an asset, such as physical server hardware, than operating expenses such as cloud services in the yearly government budgeting process.

The manufacturing industry is an interesting case, made up of a mix of long-term industrial control systems, sometimes still running a legacy version of Windows, and sophisticated logistics and customer interfaces. It is not surprising to see this industry at the high end of public-cloud service adoption, as their success is often based on multinational supply-chains and detailed electronic interactions with their customers and suppliers.

## REPORT

During an interview with the Chief Information Security Officer (CISO) of a large entertainment company, it came to light that they have moved completely to the public-cloud out of necessity, starting in 2013 with the objective of no longer operating a data center. Cloud services enable the project-to-project flexibility required by their business model. They use a variety of service types, driven by the needs of the project, the department, and requirements of their partners.

The Chief Technology Officer (CTO) of a health products company said that they were operating a hybrid cloud environment, what he referred to as “cloud appropriate”. While much of their operation is cloud-based, the decision to go cloud or not is based on the specific needs of the application and data.



### Security is working to catch up with the use of containers and serverless computing.

Containers (e.g. Docker and Lynx) and serverless computing options have grown rapidly in popularity over the past few years, with around 80% of those surveyed using or experimenting with them. However, only 66% have a strategy to apply security to containers, and similarly only 65% have a strategy to apply security to serverless computing. This is a significant lapse in security coverage, which most respondents recognize, as most of those without a security strategy are planning to develop one in the coming year. Departments outside of IT are the least prepared to secure containers and serverless.

Assessing the shared responsibility model laid out by cloud providers, the available native controls, and the interconnectivity to production workloads and data stores can help build a foundation for secure container and serverless initiatives.

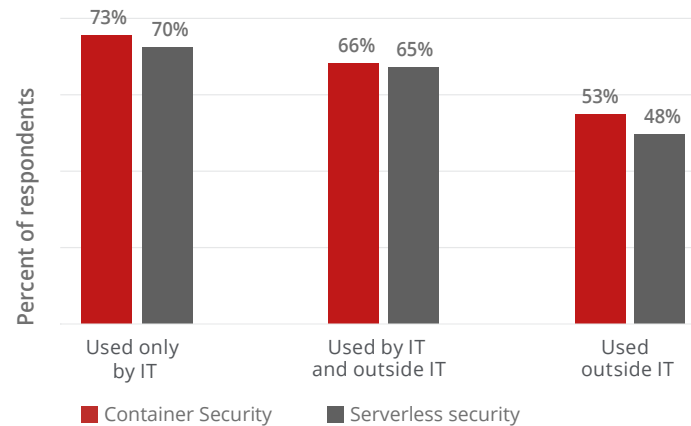


Figure 4. Does your organization have a strategy for applying security to containers? Serverless computing? (grouped by department ownership).





**IaaS workloads have many roles**

The types of workloads that organizations are running in their IaaS instances are quite broad. More than half of respondents are running general business applications, cloud native applications, e-business sites, and mission-critical enterprise applications. In addition, just under half are running development environments, and a third have their Internet of Things applications in IaaS. Most are running between three and four different types of workloads.

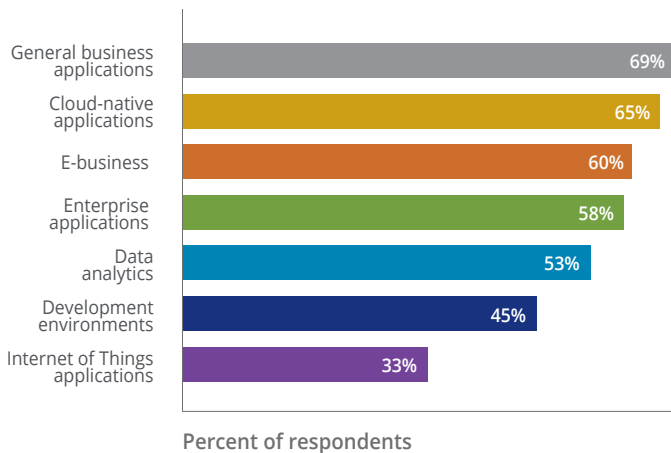


Figure 5. What types of workloads are you running in IaaS cloud services (e.g. Amazon Web Services, Microsoft Azure etc.)?

**Lifting and Shifting to the cloud versus cloud-native applications**

There are two main tactics for IaaS adoption: developing cloud-native applications or transferring existing on-premises workloads to the cloud, which is often referred to as lift and shift. Overall, just under half (46%) are pursuing a mix of both tactics, while 37% are just working to lift and shift from on-premise to the cloud. Only 17% are trying a purely cloud-native approach.

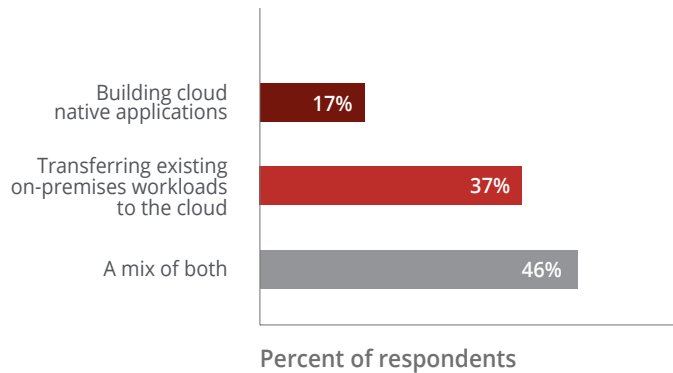


Figure 6. What is your organization’s primary approach to using IaaS?

**Cloud-first is the strategy of most organizations**

Heading directly for the cloud is still the strategy for the majority of organizations worldwide, although the average number of professionals reporting a cloud-first approach dropped to 65% in 2017, down from 82% in 2016. This change appears to be rooted in maturity, and a result of finding the best fit for the organization after a period of experimentation.

Compared to organizations without a cloud-first strategy, those who state they have a cloud-first strategy

## REPORT

are using more cloud services, are twice as likely to have tracked a malware incident back to content pulled from a cloud application such as Dropbox or Office 365, and more likely to have experienced every one of the IaaS and SaaS issues that were asked about (more on this below). Even so, these respondents still believe that public cloud is safer than private cloud. It would appear that the more they know, the more confident IT professionals are that cloud-first is the course they want to be on.

Shared security responsibility models are likely a strong contributor to this confidence. The CISO of a large entertainment company summarized his sentiment towards shared responsibility with cloud providers as “our breach is their breach, and their breach is our breach.” Both parties have a stake in keeping cloud assets secure.

### Sensitive data stored in the public cloud

The majority of organizations store some or all of their sensitive data in the public cloud, with only 16% stating that no sensitive data is stored in the cloud, percentages that have been stable over the past year. Healthcare and engineering organizations are the most likely to have at least some data in the public cloud, at more than 90%, while insurance and utilities companies are the least likely, at just over 70%. By country, public cloud storage was lowest in European countries and Japan.

The types of data stored run the full range of sensitive and confidential information. Personal customer information is by far the most common, reported by 61% of organizations. Around 40% of respondents

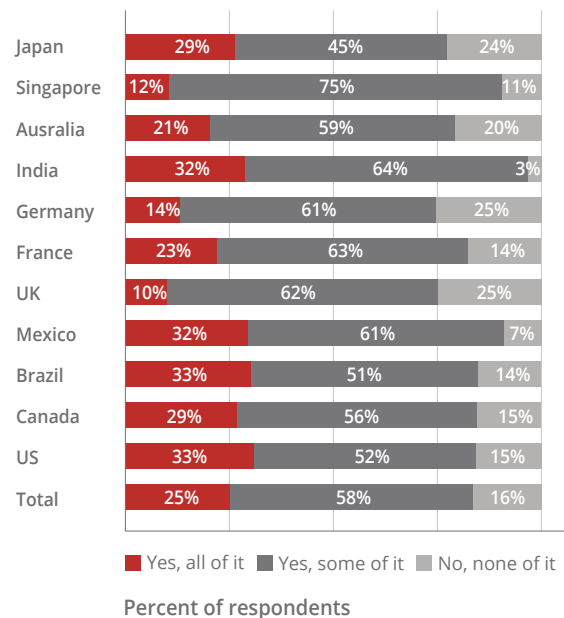


Figure 7. Does your organization's public cloud service store your organization's sensitive data?

also store one or more of internal documentation, payment card information, personal staff data, or government identification data. Finally, about 30% keep intellectual property, healthcare records, competitive intelligence, and network passwords in the cloud. Managing the risk of storing sensitive data in the cloud means ensuring that the organization first and foremost has visibility to it, both at rest and in motion. A focus on fundamental governance and technological steps, such as requiring departments and personnel to participate in asset identification, classification, and accountability helps build visibility. Data Loss Prevention integration with cloud providers, including the use of Cloud Access Security Brokers, manual or automated

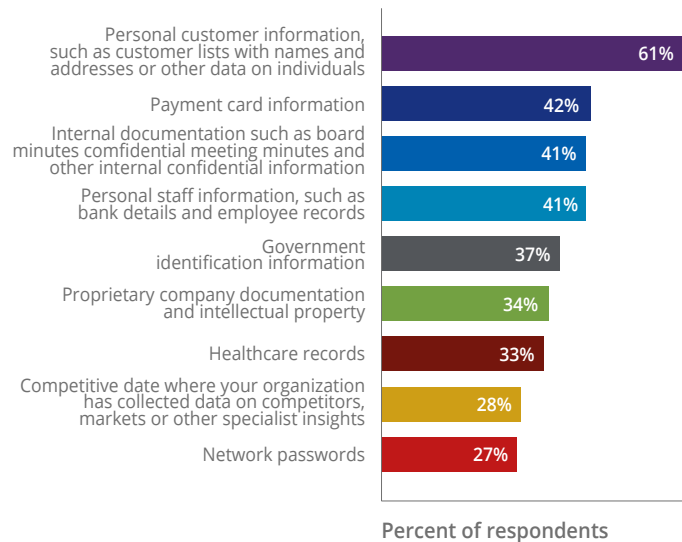


Figure 8. What type of sensitive data is stored in your organization's public cloud services?

data classification, and other technology steps will help reduce the risk of sensitive information flows to and through cloud services.

One of the C-level executives interviewed for this report stated that their biggest threat is from insiders, whether intentional or accidental. They manage this by restricting sensitive data to only managed devices, use behavioral analytics to monitor activity, and have plans in place to react quickly in the event of a breach in the cloud.

Another executive interviewed explained that they have a mature data governance model that reduces third-party access to cloud data. Their ordering and delivery is direct to the consumer, so sensitive and confidential

personal information is not seen by sales consultants or other intermediaries, significantly reducing the risk of intentional or accidental disclosure.

**Benefits of the cloud still outweigh the risks**

More than 90% of respondents trust the cloud more now than they did last year, even after a wide range of publicized security incidents. This may be the result of organizations thinking differently about cloud security, and realizing the benefits of shared security responsibility. Cloud customers don't have less responsibility now that their data is in the cloud, but instead there is a logical division of roles, with cloud providers covering security of the cloud, and customers handling what they put in the cloud. In this model, the deeper skillsets, funding, and workforce of the cloud service provider are complemented by the customer's detailed knowledge of their users and dataset. Continued investment by cloud service providers in native security and third-party integration for commercial security technologies is improving the ability for both parties to uphold their responsibility.

As public cloud services become ubiquitous, IT professionals are coming to accept their benefits as commonplace. Lower total costs of ownership, visibility of the organization's data, and use of a proven technology are overall considered to be more likely realized through public cloud than private cloud. Respondents were near equally split on whether public or private clouds provide better safety for the organization's data. Protection from intrusions and



breaches and the ability to maintain identity and access control were the benefits that respondents felt had the most advantage in the private cloud.

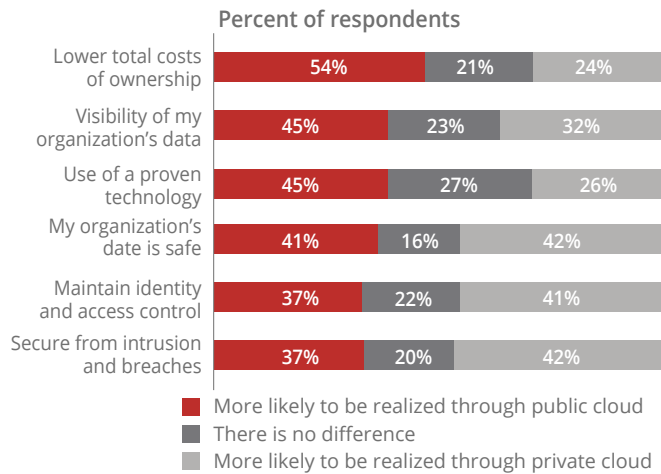


Figure 9. Which benefits are more likely to be realized through public cloud or private cloud?

### Dealing with Obstacles

Once you know where you want to go, the next step is identifying and navigating around any obstacles in the path to the cloud, such as data theft, changing regulations, and shadow IT. At the center of these issues is a difference of opinions on whether the top priority should be greater visibility or greater control.

### Data theft

Theft of data from cloud infrastructure or applications is predictably the number one concern of surveyed IT professionals, and with good reason. More than 25% of IaaS and SaaS users have experienced data theft from their hosted infrastructure or applications. This appears to be at least partially related to the shortage of security skills, as only around 10% of the small group of IT leaders not reporting a skills shortage experienced data theft from IaaS or SaaS.

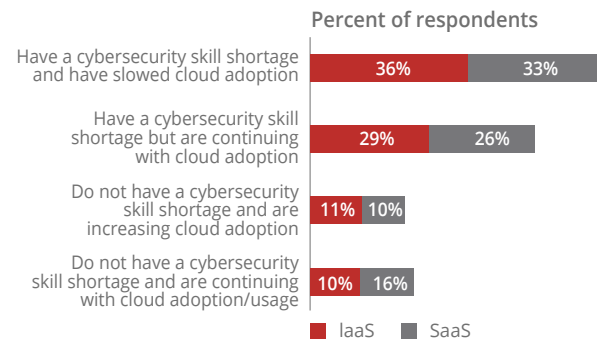


Figure 10. Has your organization experienced theft of data from cloud infrastructure (IaaS) by malicious actor? From a cloud application (SaaS)? (grouped by status of skills shortage).

### The looming uncertainty of GDPR

The enforcement date of the European Union’s General Data Protection Regulation (GDPR) in May 2018 is affecting cloud users around the world. In our 2017 study [Beyond the General Data Protection Regulation \(GDPR\)](#), we found that more than 80% of organizations are expecting help from their cloud service providers to achieve regulatory compliance. Yet in our study here, only half of the respondents stated that all of their cloud providers have a plan in place for GDPR compliance. Not surprising, the organizations that are more confident in the ability of their cloud providers are more likely to have plans to increase their overall cloud investments in the coming year, while those less confident plan to keep their investments at the current level. Fewer than 10% on average anticipate decreasing their cloud investments as a result of GDPR.

A striking correlation between the two studies came out of this analysis. In [Beyond the General Data Protection Regulation \(GDPR\)](#), it was found that the reaction to GDPR and other political or regulatory changes is resulting in a reduction of overall spending per organization of \$85,000 USD– yet as shown here, many still anticipate increasing investment in the cloud.

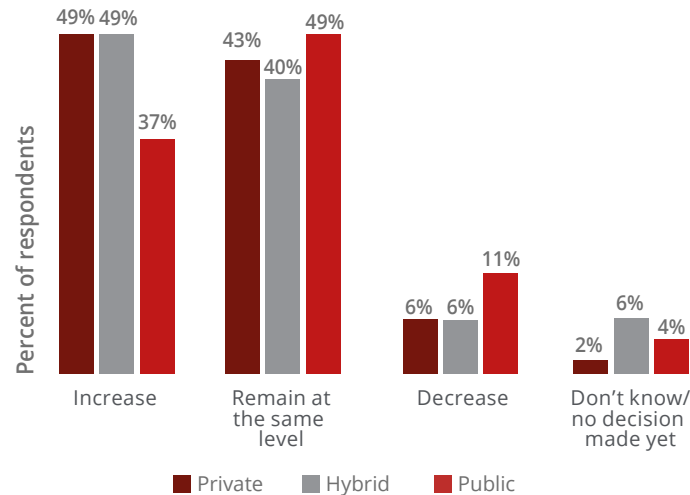


Figure 11. With the upcoming European Union General Data Protection Regulation (GDPR) in May 2018, do you anticipate increased or decreased investment in public, private, and hybrid cloud? (grouped by cloud architecture).

### Concerns and the reality of security incidents for IaaS

IT professionals are experiencing a variety of security threats and issues with IaaS, ranging from regulatory compliance to data theft, which can be roughly grouped into three categories: lack of visibility, insufficient controls, and cyber threats and attacks. Underlying all of this is the fact that more than a quarter of the respondents have a shortage of skilled staff to secure their cloud infrastructure.

## REPORT

Visibility issues lead the list by a slim margin, whether it is users creating cloud workloads outside of IT, lack of visibility into what data is in the cloud, or the inability to monitor cloud workloads. Being unable to see what is going on makes it difficult to secure the cloud, regardless of the level of controls available.

Control issues were a very close second for the surveyed group. Incomplete control over sensitive data and inconsistent security controls were the two most reported. As one of our interviewed CTOs put it, “why create visibility if you are not going to do something about it? Nobody looks at what people are doing in the cloud and then moves on with their day. They use that information to spark further investigation and potentially implement some type of control.”

Cyber threats and attacks may be the third group, but more than a quarter of the organizations surveyed experienced at least one of these. Actual data theft leads this group, whether by a malicious outsider or insider. Advanced attacks against cloud infrastructure were reported by 1 in 5, and denial of service attacks by 1 in 7.

As a result of these experiences, this year’s concerns have shifted. Last year’s top two concerns, inconsistent security controls and lack of skills, have fallen in importance, replaced by concerns about data theft and

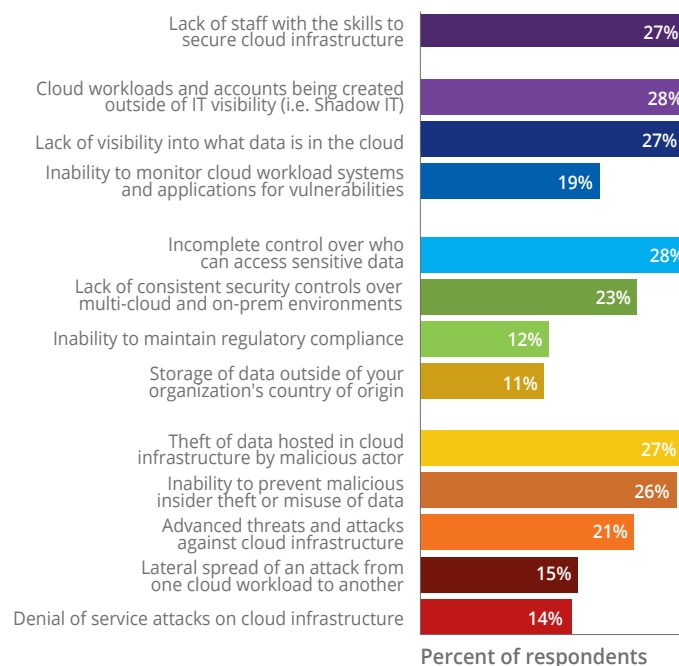


Figure 12. Has your organization experienced any of the below issues when it comes to using IaaS?

lack of visibility, and followed by shadow IT. In general, concerns about visibility into IaaS usage rank higher than control concerns.

**Top concerns about using IaaS, ranked first:**

1. Theft of data hosted in cloud infrastructure by malicious actor
2. Lack of visibility into what data is in the cloud
3. Cloud workloads and accounts being created outside of IT visibility (i.e. shadow IT)
4. Advanced threats and attacks against cloud infrastructure
5. Incomplete control over who can access sensitive data
6. Inability to prevent malicious insider theft or misuse of data
7. Lack of consistent security controls over multi-cloud and on-premise environments
8. Lack of staff with the skills to secure cloud infrastructure

To protect themselves, organizations should consider the recent evolution in attacks that extend beyond data as the center of IaaS risk. Malicious actors are conducting hostile takeovers of compute resources to mine cryptocurrency, and also re-using those resources as an attack vector against other elements of the enterprise infrastructure and third-parties.

Assessing the ability to prevent theft and control access are important initiatives when building out infrastructure in the cloud. Determining who can enter data into the cloud, tracking resource modifications to identify abnormal behaviors, securing and hardening orchestration tools, and adding network analysis of both north-south and east-west traffic as a potential signal of

compromise are all quickly becoming standard measures in protecting cloud infrastructure deployments at scale.

**Concerns and the reality of security incidents for SaaS**

SaaS users are experiencing a similar range of security threats and issues as IaaS users. Lack of visibility leads by a wider margin in SaaS than IaaS, with almost one third of organizations having difficulty getting a clear picture of what data is in their cloud applications. Poor visibility of data in transit and shadow IT are also significant concerns.

For incidents related to control, incomplete control over sensitive data was number one, which is not surprising if the organization is having difficulty seeing what data is

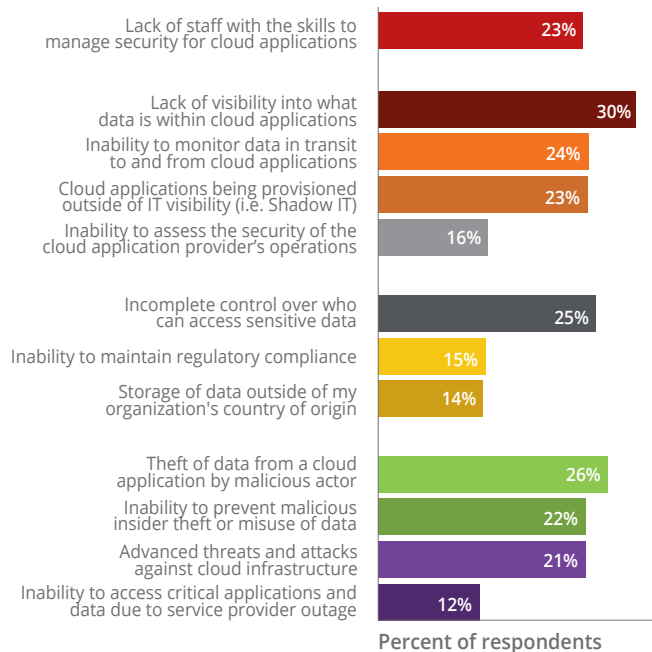


Figure 13. Has your organization experienced any of the below issues when it comes to using SaaS?

## REPORT

in the cloud. Maintaining regulatory compliance and data being stored outside the country of origin complete the control list, but at a higher percentage than IaaS users. Again, it is difficult to control what you cannot see.

Cyber threats and attacks are almost as prevalent in SaaS services, with more than a quarter of respondents experiencing some significant issue. Theft by a malicious actor or insider leads the list, followed by advanced threats against the application. Just over 10% of organizations using SaaS experienced a service outage that left them unable to access their critical data.

SaaS users, perhaps because of the many publicized threats and thefts, now rank data theft, followed by advanced threats directed at the cloud provider, as their top concerns. Like IaaS, visibility concerns outranked control concerns for SaaS.

### Top concerns about using SaaS, ranked first:

1. Theft of data from a cloud application by malicious actor
2. Advanced threats and attacks against the cloud application provider
3. Inability to monitor data in transit to and from cloud applications
4. Lack of visibility into what data is within cloud applications
5. Cloud applications being provisioned outside of IT visibility (i.e. shadow IT)
6. Incomplete control over who can access sensitive data

7. Inability to prevent malicious insider theft or misuse of data
8. Lack of staff with the skills to manage security for cloud applications

Issues experienced with SaaS applications are naturally centered around data and access, as most shared security responsibility models leave those two as the sole responsibility for SaaS customers. It is every organization's responsibility to understand what data they put in the cloud, who can access it, and what level of protection they (and the cloud provider to a certain extent) have applied.

It is also important to consider the role of the SaaS provider as a potential access point to the organization's data and processes. Recent developments in 2017, such as the rise of XcodeGhost and GoldenEye ransomware, emphasize that attackers recognize the value of software and cloud providers as a vector to attack larger assets and are increasing their focus on this potential vulnerability. Enhanced scrutiny of provider security programs, setting the expectation to have predictable third-party auditing with shared reports, and insisting on breach reporting terms can all complement technology solutions in protecting the organization.

### Concerns and the reality of security incidents for private cloud

Private cloud experiences and security issues are quite different from those of IaaS or SaaS. A higher percentage of this group are reporting a shortage of security skills, an issue exacerbated by the top two challenges of lacking consistent security controls over traditional and



## REPORT

virtual infrastructures, and the increasing complexity of private cloud infrastructure. This ongoing problem is probably the leading reason why organizations are shifting away from private clouds, to take advantage of the larger pool of skilled staff and economies of scale held by cloud service providers.

Like IaaS and SaaS users, visibility is an important issue, in this case incomplete visibility over the security of their software-defined network. Actual data theft is slightly lower overall than for public cloud users, but is skewed by organization size, with smaller organizations experiencing just as much theft from private cloud as from public cloud. Interestingly, respondents were only

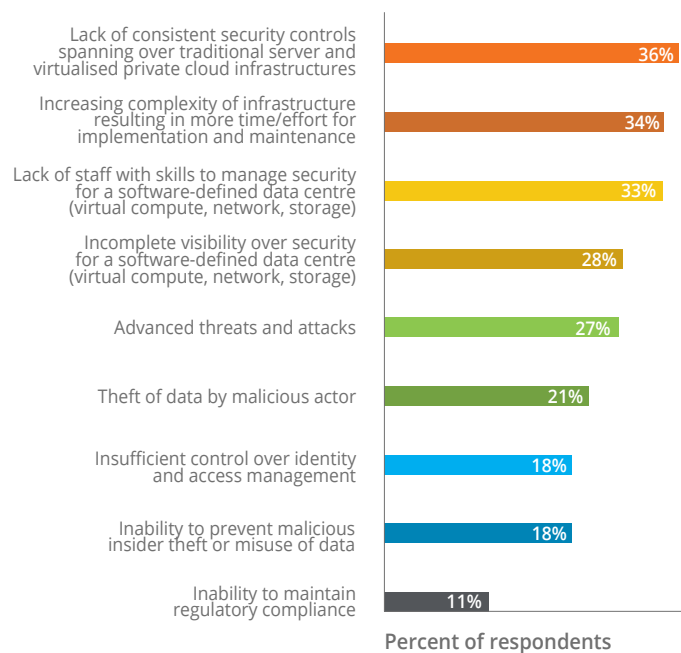


Figure 14. Has your organization experienced any of the below issues when it comes to using private cloud?

slightly less likely to struggle with regulatory compliance in private cloud environments than public cloud. This year's concerns match very closely with last year's. Private cloud operators are most concerned about infrastructure complexity, advanced threats, and the lack of consistent controls. These concerns, combined with the ongoing skills shortage, support the continued trend towards hybrid cloud architectures.

### Top concerns with private cloud, ranked first:

1. Increasing complexity of infrastructure resulting in more time/effort for implementation and maintenance
2. Advanced threats and attacks
3. Lack of consistent security controls spanning over traditional server and virtualized private cloud infrastructures
4. Lack of staff with skills to manage security for a software-defined data center (virtual compute, network, storage)
5. Incomplete visibility over security for a software-defined data center (virtual compute, network, storage)
6. Theft of data by malicious actor
7. Inability to prevent malicious insider theft or misuse of data
8. Insufficient control over identity and access management

The fine-tuned control available in private cloud environments should be a factor in the decision-making process to allocate resources to the public vs private cloud. Additional levels of control and supplemental

## REPORT

protection can compensate for the limitations of private-cloud deployments and may contribute to a practical transition from monolithic server-based datacenters.

At the same time, organizations should consider that maintaining fine-tuned control creates complexity, at least beyond what the public cloud has developed into, where cloud providers take on much of the effort to maintain infrastructure themselves. Reducing complexity through abstraction of controls which unify public and private cloud platforms above and across physical, virtual, and hybrid environments can help simplify security management.

### Learning to live with Shadow IT

On average, IT professionals think that about 35% of cloud services are commissioned by departments outside of IT, down from 40% last year. Unfortunately, visibility of those shadow IT services is also decreasing, from 47% to 43%. However, concern about the effects of shadow IT on the organization's ability to keep cloud services safe and secure also decreased, from 66% to 62% of respondents. Interestingly, visibility of shadow IT increases in relation to the percentage of cloud services created outside of IT, i.e. the more services created outside of IT, the more visibility IT has of them. It would appear that allowing or encouraging lines of business to use the cloud services that they need also encourages them to openly communicate with IT about their cloud use instead of trying to hide it.

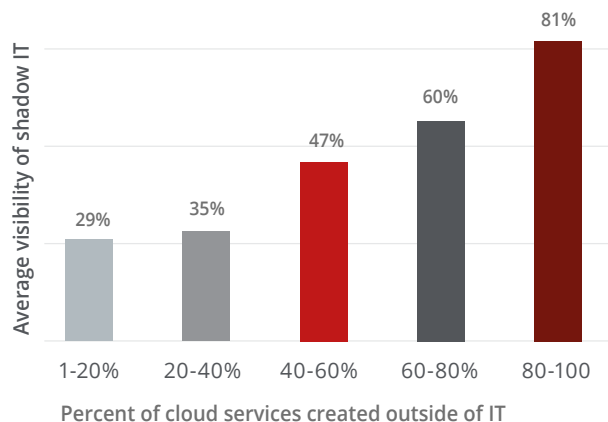


Figure 15. What percentage of the total number of public cloud services in use at your organization are commissioned by departments other than your IT department and without the direct involvement of the IT department i.e. shadow IT? (ranked by average visibility of shadow IT).

Our entertainment industry CISO provided an illustrative perspective on shadow IT that is quite flexible. Their organization has a set of corporate-sanctioned cloud services available, but do not block other services, as they feel employees will just go around them. The CISO looks at why they are doing something different. It could be a need specific to that department, requirements or recommendations from another studio or artist, or something new and better. The objective is to embrace the users' needs and help them find the right tools, finding a balance between creative timeframes and the protection of the intellectual property.

Another executive generally agreed with this approach, emphasizing the need to avoid an adversarial relationship between IT and the rest of the organization. Their team views shadow IT users as their trend and discovery system, rewarding them for finding new, useful

## REPORT

apps. The IT team then takes on the responsibility to manage, pay for, and make the application use more secure. This is done within a risk/reward framework, so that high-risk activities are still discouraged.

Effectively monitoring shadow IT usage requires a mix of tools, primarily next-generation firewalls, database activity monitoring, web gateways, and cloud access security brokers (CASBs). Organizations with a cloud-first strategy are more than twice as likely to rank CASB as their first priority for monitoring shadow IT activity.

Securing shadow IT is a task requiring multiple methods. The leading methods are:

- Data loss prevention (DLP) and encryption
- Identity and access management
- Regular audits of apps in use and assessments of potential risks
- Blocking access to the unauthorized cloud service
- Migrating the shadow IT to an approved and similar service

Conceptually, a complete view over shadow IT is the ultimate solution. The ease with which un-managed devices can create accounts in the cloud and share data with an unsanctioned service makes unification of data domains and full control nearly impossible. Consider a combination of financial oversight, departmental outreach, and technology solutions to establish comprehensive governance over shadow IT.

### Malware from cloud apps

Malware continues to be a concern for all types of organizations, and 56% of professionals surveyed said they had tracked a malware infection back to a cloud

application, up from 52% in 2016. When asked how the malware was delivered to the organization, just over a quarter of the respondents said that their cloud malware infections were caused by phishing, followed closely by emails from a known sender, drive-by downloads, and downloads by existing malware.

### Adjusting the Speed

Speed is dependent on two major factors, the capabilities of the vessel and the capabilities of the crew. Or, how fast can it go, and how well can you see and steer? While almost all organizations are well into the cloud, the ultimate destination does not appear to be getting closer. When asked how many months they anticipate it will take for their IT infrastructure to be 80% cloud, the average response is 14 months, one month less than last year. However, those with a cloud-first strategy think this target will be achieved in 12 months, compared to 18 months for those without.

Data center virtualization is progressing faster, with an average of 17 months remaining until full transformation to a software-defined data center is complete, down from 27 months last year. Cloud-first organizations are in the lead again, with only 14 months to go and 61% virtualization of their servers, compared to 23 months and 50% virtualization for those without a cloud-first strategy. Last year, the largest organizations were running well behind smaller ones in their virtualization efforts, but they have caught up in the past year. There is now little difference between virtualization levels and expected transformation times by the size of the organization.

## REPORT

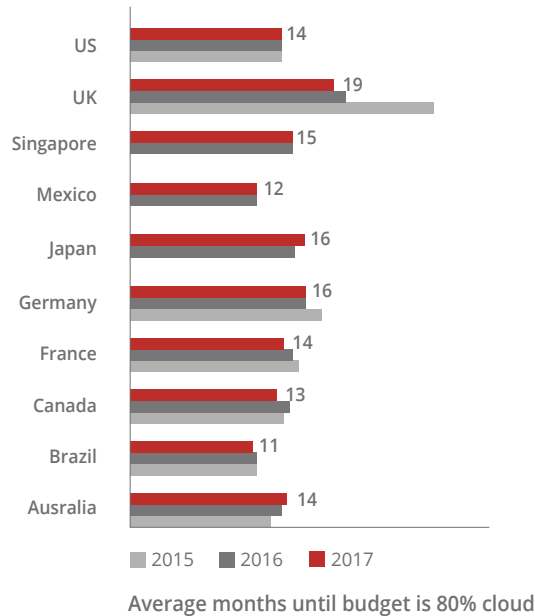


Figure 16. Months until IT budget is 80% cloud.

### Skills shortage is decreasing

The shortage of cybersecurity skills related to cloud adoption appears to be decreasing, as those reporting no skill shortage increased from 15 percent to 24 percent this year. Of those still reporting a skills shortage, only 40% have slowed their cloud adoption as a result, compared to 49% last year. Very interesting to note that those with a cloud-first strategy are almost twice as likely to have slowed adoption than those without such a strategy. Private-only cloud operators are more likely to be experiencing skills shortages, and more likely to have slowed their adoption, which helps to explain the continued shift to hybrid cloud. The highest skills shortages were reported in Asia-Pacific countries

and telecom and software firms, and the lowest reported in Japan and manufacturing and utilities firms. It is notable that by industry, cloud adoption rates are highest in those reporting the highest skills shortages.

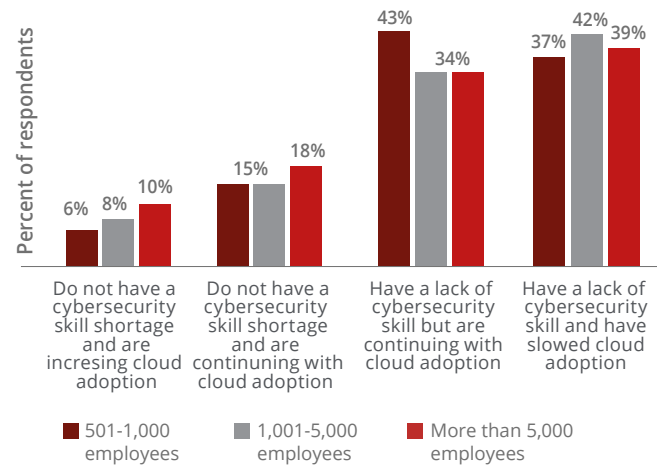


Figure 17. Is a shortage of cybersecurity skills affecting your organization's usage of cloud computing? (grouped by employee count).

Those facing a skills shortage and prioritizing cloud adoption may benefit from testing cloud deployment automation, multi-provider administration tools, and unified workload security platforms to reduce the number of technologies deployed to protect cloud environments. Legacy approaches to choosing point providers, as many organizations have done on-premises, may extend skill challenges to the cloud. Organizations should consider new cloud infrastructures as an opportunity to fundamentally change the protection strategy to accommodate available skills, speed of deployment, and orchestration needs.

## REPORT

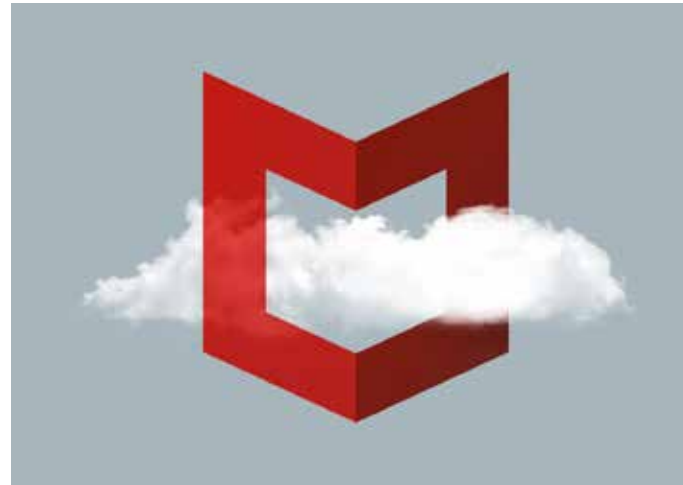
One CTO we interviewed agreed that there was not enough seasoned security talent to go around. They are partnering with consultants, managed service providers, and their cloud providers to augment and magnify in-house capabilities.

### Going faster and safer

Since almost all organizations are using cloud services and are planning to increase their usage level, what steps can they take to get to their chosen destination quickly and securely? Currently, 27% of IT security budgets on average are dedicated to cloud security, anticipated to grow to 37% in 12 months. Having a cloud-first strategy contributes to higher security spend and has a strong effect on the speed of cloud transformation.

### Effects of cloud first

Comparing the operational practices of groups with and without a cloud-first strategy identifies some significant differences. It is important to remember that even those organizations without a cloud-first strategy are operating a substantial number of cloud services. However, the cloud-first group are more than twice as likely to have a DevOps process, and almost seven times as likely to have a DevSecOps process, both of which have been shown to have a positive impact on data and application security.



While the cloud-first group reports a higher incidence of shadow IT, they also have higher visibility of shadow IT. The critical philosophical difference between the two groups appears to be the benefits of greater control versus greater visibility. For both IaaS and SaaS concerns, cloud-first proponents ranked issues relating to visibility higher, while control issues were ranked higher by those not following this approach. The cloud-first group were significantly more likely to have strategies for applying security to their container and serverless functions. Not surprising, cloud-first respondents also had a 25% higher budget for cloud security.

#### DevOps:

A line of business or application team directly operating cloud assets and deploying new application versions or changes independent of formal IT involvement, often using an iterative development or deployment method. The objective is to more rapidly deliver high-quality applications.

#### DevSecOps:

Building on DevOps, the application team also incorporates security into their group, instead of relying on a separate, post-development security verification team. The objective is to incorporate security into every aspect of the lifecycle, resulting in more secure applications with fewer vulnerabilities.

### Usage of DevOps and DevSecOps

Speaking of DevOps, this integrated approach to application development and IT operations has a proven effect on deployment times, code stability, and downtime recovery. Yet only 49% of the surveyed organizations are currently running their cloud environments using a DevOps approach. 77% of those with a DevOps approach have integrated security into this function, often referred to as DevSecOps. DevOps does not appear to be related to organization size, or industry, with the exception of software and technology firms, where 60% are using DevOps. Japan, Germany, and Australia are the lowest DevOps practitioners, at around 35%. DevOps and DevSecOps appear to have a positive effect on security practices, with these organizations twice as likely to have security strategies for containers and serverless computing, as well as operating a unified security solution across their clouds.

One CTO underlined the positive effects that DevSecOps has had on the quality of their code. Before this process was implemented, teams were not conducting regular or complete code inspections. They simply trusted the work of their engineers. Now with security directly involved in code deployment, regular testing and inspection does occur, reducing errors that could result in a breach or vulnerability.

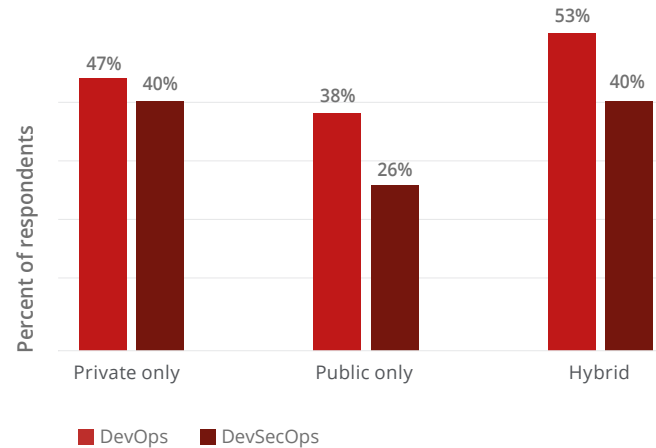


Figure 18. Percent of organizations running DevOps or DevSecOps. Note: DevSecOps respondents are a subset of DevOps respondents (grouped by cloud architecture).

### The Takeaway: Accelerate Business Through Secure Cloud Adoption

Poor visibility has a bigger impact on navigation than any single control or capability. After all, you cannot steer around what you cannot see. The leading adopters of cloud services understand this axiom and are integrating cloud visibility into their IT operations to accelerate business. Better cloud visibility enables an organization to adopt transformative cloud applications sooner, respond more quickly to security threats, and reap the cost savings that virtualization provides.

These visibility-driven organizations are most likely using a full range of cloud services, so that they can choose the best fit for each business need. Whether or not they have a cloud-first strategy, they have a security strategy for containers and serverless functions, operate a hybrid architecture, have greater visibility of shadow IT, and take direct responsibility for the security of their cloud data. They want to see as much as possible, and then make decisions about the optimal approach, ranging from whether data and access require additional controls, employees need more training and security awareness, or which services and applications are necessary.

Your organization is using cloud services, even if they are not your primary strategy. From a security perspective, there are three best practices identified in this research that all organizations should be actively working towards:

#### 1. DevSecOps processes.

DevOps and DevSecOps have repeatedly been demonstrated to improve code quality, reduce exploits and vulnerabilities, while increasing the

speed of application development and feature deployment. Integrating development, QA, and security processes within the business unit or application team, instead of relying on a stand-alone security verification team, is crucial to operating at the speed today's business environment demands.

#### 2. Deployment automation and management tools.

Even the most experienced security professionals find it difficult to keep up with the volume and pace of cloud deployments on their own. Automation can augment human advantages with machine advantages, creating a fundamental component of modern IT operations. Deployment automation and management tools, such as Chef, Puppet, or Ansible are examples which can be used in both public and private cloud environments.

#### 3. Unified security solution with centralized management across all services and providers.

Multiple cloud provider management tools make it too easy to for something to slip through. A unified management solution with an open integration fabric reduces complexity by bringing multiple clouds together and streamlining workflows.

Finally, when trade-off decisions have to be made, better visibility should be the number one priority, not greater control. It is better to be able to see everything in the cloud, than to attempt to control an incomplete portion of it.

## REPORT

### Appendix: Methodology and Demographics

In Q4 2017, McAfee surveyed 1,400 IT professionals for its annual Cloud Adoption and Security research study. Respondents were drawn from a general market panel of IT and Technical Operations decision makers, selected to represent a diverse set of countries, industries, and organization sizes. Quotas were set to obtain a representative sample of enterprise and commercial organizations in each country, with a particular focus on the financial services and healthcare sectors. Fieldwork was conducted from October to December 2017, and the results offer a detailed understanding of the current state and future plans for cloud adoption and security.

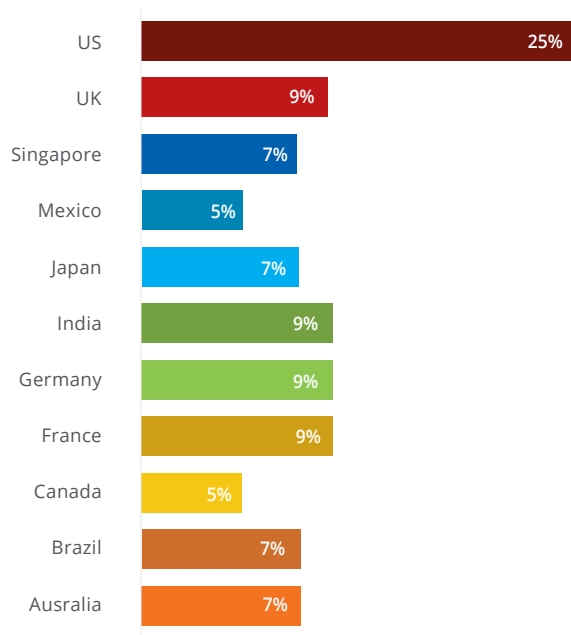


Figure 19. Respondents by country

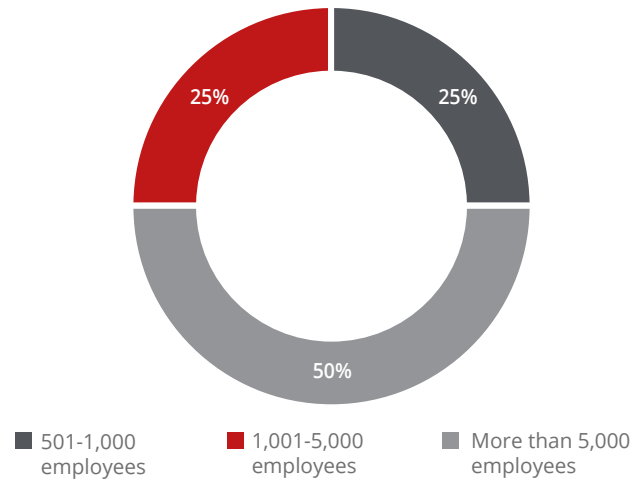


Figure 20. Respondents by organization size



# REPORT

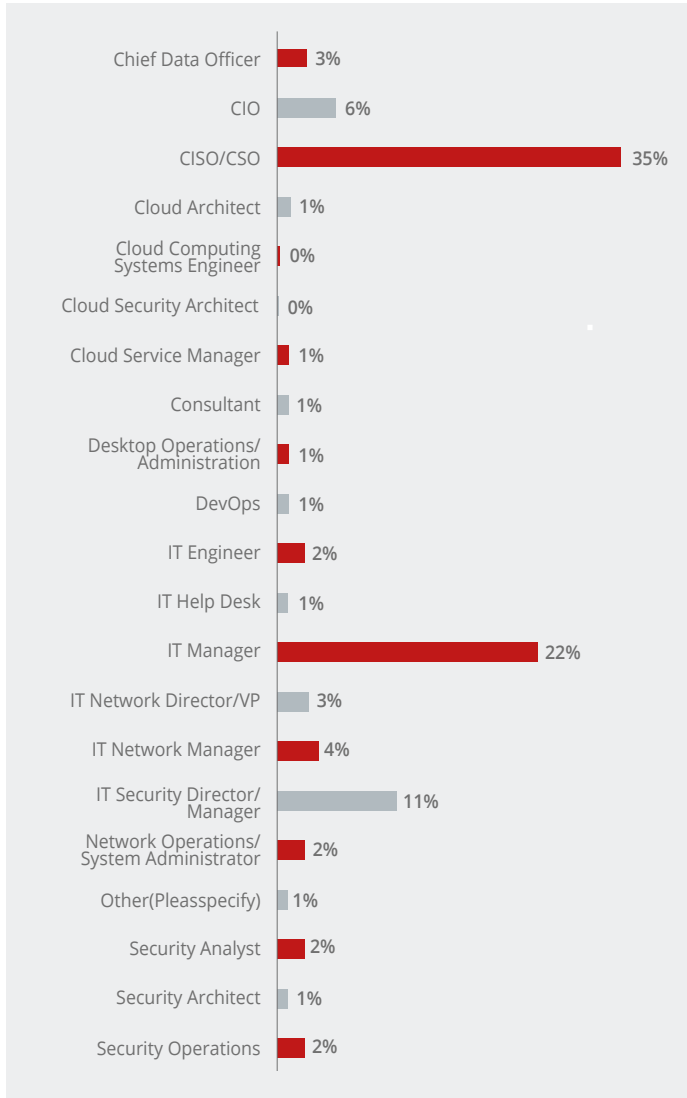


Figure 21. Respondents by job title

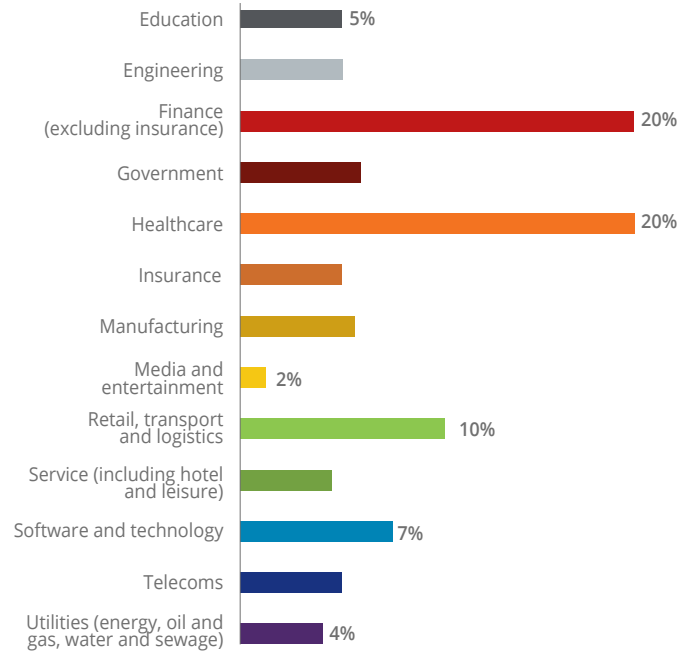


Figure 22. Respondents by industry

## About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

[www.mcafee.com](http://www.mcafee.com).



2821 Mission College Blvd.  
Santa Clara, CA 95054  
888.847.8766  
[www.mcafee.com](http://www.mcafee.com)

McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2018 McAfee, LLC. 3872\_0418