REPORT

McAfee
Together is power.

Building Trust in a Cloudy Sky

The state of cloud adoption and security

Table of Contents

Foreword

I am pleased to provide a foreword to McAfee's survey and research paper, "Building Trust in a Cloudy Sky". This report contains a rich set of findings of the progress towards cloud adoption by a diverse global audience and the key security considerations in play. Reading this document will greatly aid practitioners in taking a data-driven approach towards securely migrating to cloud computing and I encourage security professionals to carefully review these findings and share broadly with management and other key stakeholders outside of the security organization.

This report clearly resonates with the anecdotal information I have received in my travels representing the Cloud Security Alliance this past year. Cloud computing is maturing and broad-based adoption is occurring. This maturity is not manifesting itself by a period of stasis, but is instead highly dynamic. New technologies and market entrants abound, and just as importantly, key players are exiting the cloud markets. The one constant in all of this is the clear responsibility of cloud users to understand their role in assuring that cloud computing is as secure as it can be and needs to be. Proper cloud security education and tools are every organization's bulwark against the evolving threat vectors in cloud.

I expect that we will see several important milestones in cloud computing in 2017. Microservices such as containers and APIs will gain significant traction as important means to enhance the value of virtual machines. DevSecOps will become a mainstream information security topic. Several strategic regulatory bodies will announce new guidelines that will in effect ease the path to adoption of cloud computing for providers and customers. Information security professionals should prepare themselves for this next wave of cloud adoption. Understanding the current cloud security benchmarks articulated in this survey provides a fantastic way to continue your journey.

Jim Reavis
jreavis@cloudsecurityalliance.org
CEO, Cloud Security Alliance

Preface

Cloud First. Two simple words, but the approach is now well and truly ensconced into the architecture of many organizations across the world. In our survey from 2015 there were some remarkable findings, none more so than the average of 16 months the surveyed IT organizations believed it would take before 80% of their IT budget was devoted to cloud solutions. Our initial assumption when designing the survey, that there was a gap between intent and implementation and that the transformation to cloud would take several years, was proven inaccurate. The desire to migrate quickly towards cloud computing appears to be on the agenda for most organizations. This year the average time before respondents thought their IT budgets would be 80% cloud-based was 15 months, indicating that Cloud First for many companies is progressing and remains the objective.

We can still see some dark clouds on the horizon. It is evident from our survey that the lack of cybersecurity skills is having an impact on cloud adoption for organizations of all sizes. Previous concerns about the lack of trust in public clouds seem to be dissipating compared to the responses in 2015, with more practical considerations becoming the biggest concerns today. Senior management also appear to be more understanding of the risks involved in storing sensitive data with third-party providers.

Perhaps one of the reasons that a Cloud First approach is moving ahead is that incidents are decreasing. Yet again more practical issues dominate the landscape, such as interoperability, the lack of transparency of data movement, and public cloud operations. In one year, the IT professionals surveyed have moved away from the feeling the cloud is untrustworthy, to a better understanding of the benefits that it can bring. What is equally encouraging is IT departments have made progress, not only in terms of articulating the risk up the management chain, but also across the company. Public cloud benefits are being realized, with the cost of outsourcing compared to hosting internally acting as the key motivator.

As we move forward into a world where cloud computing is almost ubiquitous, we are faced with practical issues that could slow adoption. These issues need to be addressed, and research efforts such as those conducted by the Cloud Security Alliance can aid organizations looking for best practices. Remarkable progress has been made within the past 12 months, and the cloud and security industries are now moving into a new phase of work to be done.

Raj Samani
@Raj_Samani
Chief Technology Officer, EMEA, McAfee

Building Trust in a Cloudy Sky

The state of cloud adoption and security

Introduction

There does not appear to be any question that cloud services have been accepted as a viable IT option for organizations. More than 90% of the over 2,000 cloud security professionals surveyed stated that they were using some type of cloud service in their organization, and many are now operating under a Cloud First strategy.

Clouds come in a variety of shapes and sizes, and while they are definitely saving money and enabling greater flexibility, the change in technologies is straining some IT resources. Investigating the impact of the security skills shortage on cloud adoption is a priority for this year's report. We also asked more details this year about operating architecture, types of services in use, and ongoing concerns. The overall objectives of this research are to identify the types of cloud architectures and services currently in use, understand organizational security concerns and how to address them, and investigate the nature of Shadow IT and the impact it has on an organization's adoption of cloud services.

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

- Software-as-a-Service (SaaS) e.g. Salesforce, Dropbox, DocuSign
- 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

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

- Private only
- Hybrid, or a combination of public and private
- Public only

Perhaps most important to the success of cloud services is the rapidly improving perception of public clouds as a secure place to store sensitive data. Trust in public clouds as a safe place to work and store sensitive data continues to increase, and most senior management now appear to have a reasonable understanding of the risks involved. Most organizations are now operating a hybrid private/public architecture, and are reducing and consolidating their cloud services, mostly with top tier providers.

93%
of organizations **utilize cloud services** in some form

49%
of respondents had **slowed their cloud adoption** due to a lack of cybersecurity skills

74%
of organizations reported **storing some or all of their sensitive data** in public clouds

52%
likelihood of getting a **malware infection from a cloud app**

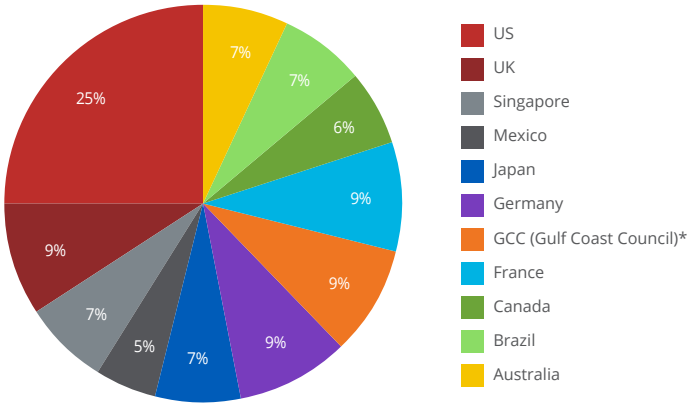
65%
of IT professionals believe that **Shadow Cloud is interfering** with their ability to keep the cloud safe and secure

73%
will move to a fully **software-defined data center** within two years

In the face of the security skills shortage, half of the organizations in this survey have slowed their cloud adoption plans, possibly causing an increase in Shadow IT services. Increasingly, IT departments are working with users to find and secure acceptable solutions, instead of just blocking them. While good news for those users and departments, this is increasing the burden on security teams. Organizations with a Cloud First strategy are finding this easier, as they turn to integrated or unified security solutions to improve their visibility and reduce their response time to detect, protect, and correct threats to the organization's data.

Methodology & Demographics

In September 2016 McAfee surveyed over 2,000 professionals for its annual cloud security research study. The 2,009 respondents were drawn from a third-party database of IT and technical decision makers to represent a diverse set of countries, industries, and organization sizes, with a particular focus on the financial services and healthcare sectors. After screening out those who were not using cloud services or not directly involved in decision making for cloud security initiatives, 1,400 senior technical professionals completed the study. The results offer a detailed understanding of the current state of cloud adoption and security.



*Gulf Coast Council comprises Saudi Arabia and United Arab Emirates

Figure 1. Respondents by country

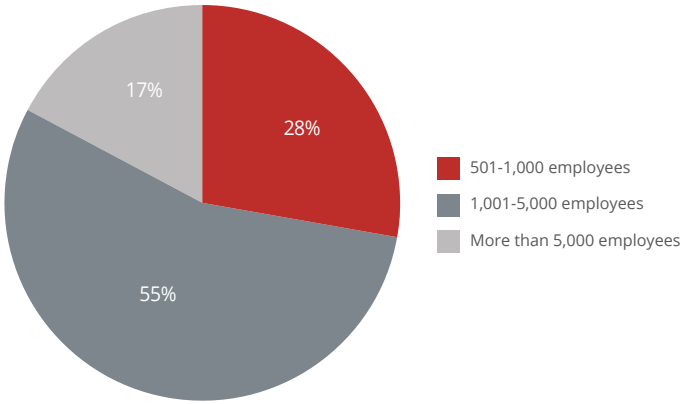


Figure 2. Respondents by organization size

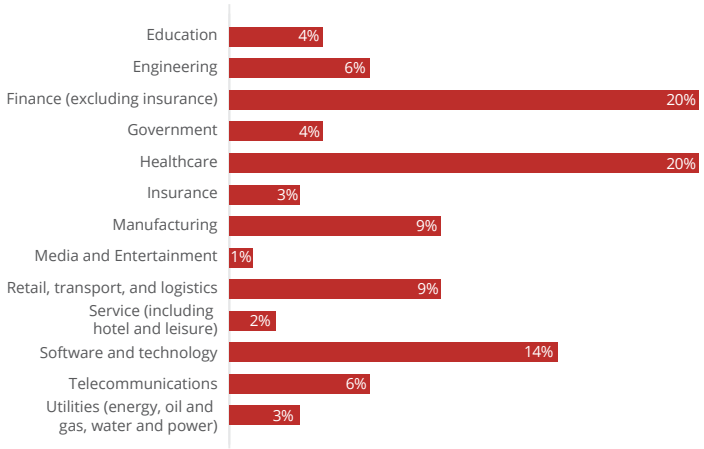


Figure 3. Respondents by industry

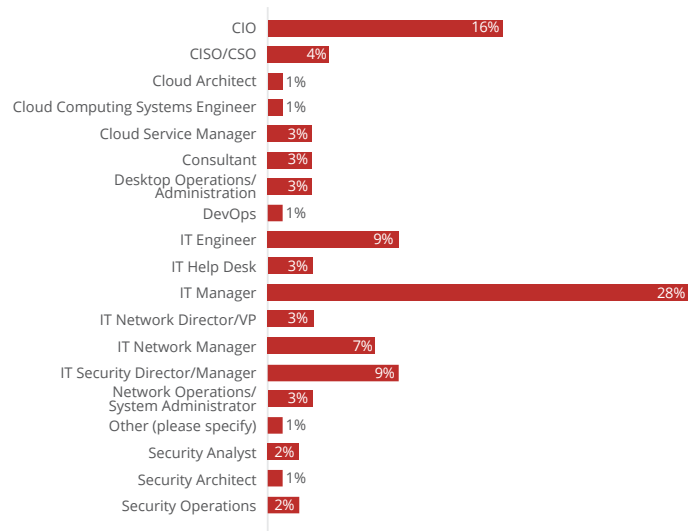


Figure 4. Respondents by job title

Research Findings

Cloud architecture shifting from private to hybrid

The past year saw a dramatic shift in cloud architecture, from private-only or public-only to predominantly hybrid. Utilization of private-only was significantly reduced, from 51% last year to just 24% this year. Public-only architectures also recorded a big drop, from 30% to just 19%. Part of this is likely due to this year's higher percentage of respondent organizations with 1,000 or more employees compared to last year; small and medium businesses are more likely to use SaaS applications.

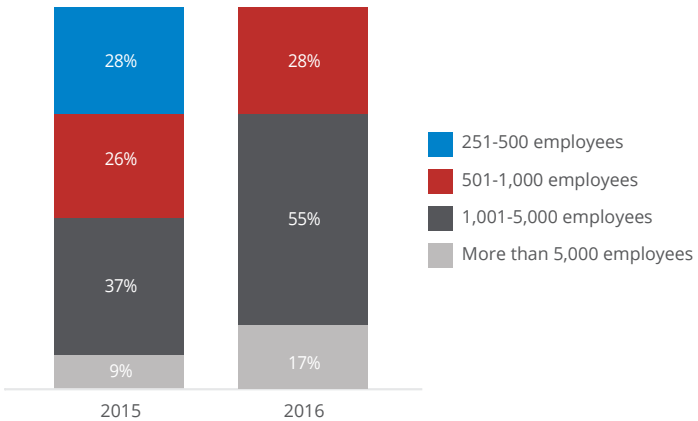


Figure 5. Respondents by organization size, by year

The majority (57%) are running a hybrid public/private architecture, up dramatically from last year's 19%. This shift to hybrid architecture was accompanied by a significant decrease in the average number of cloud

services in use, which dropped from 43 in 2015, to just 29 in 2016, as organizations appear to be consolidating their cloud applications and services. Overall, 93% of those surveyed are operating some type of cloud services in their organization.

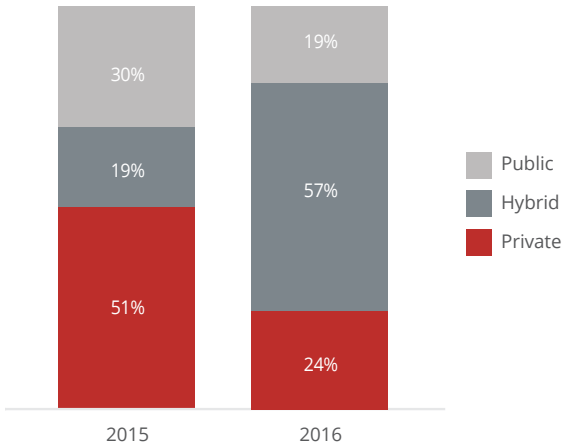


Figure 6. Which type of cloud architecture is your organization currently using? (grouped by year)

According to the survey data, cloud usage was lowest in Japan, with 23% stating they were not using any cloud services. This does not appear to be a trust issue, as the Japanese respondents were not any less trustful of public cloud than the average. It appears to most likely be due to security workforce issues, as the most common concern about using cloud services in Japan was the skills required by IT security staff.

By industry, utilization of cloud services was lowest in government (27%) and education (19%). This appears to be related to trust and control issues in both industries. Governments were least likely to consider their data safe within the public cloud. Educational institutions were least likely to think that the public cloud is secure from hackers. Both industries were concerned about their ability to maintain identity and access control.

By industry, use of private-only cloud was highest in engineering (30%), primarily due to compliance concerns, and government (29%) organizations, due to trust and control issues, as mentioned above. Purely private cloud infrastructures were lowest in services companies (16%), due to concerns over IT security skills, and media organizations (17%), who had issues with insufficient visibility of their security posture.

Public-only usage was highest in services companies (28%). Pure public cloud usage was lowest in insurance (9%) and retail (12%). Retailers, not surprisingly in their price-competitive industry, were primarily concerned about costs. The top concern of insurance companies was compliance, specifically the location of cloud service providers' data centers and data stores outside of the country of operations.

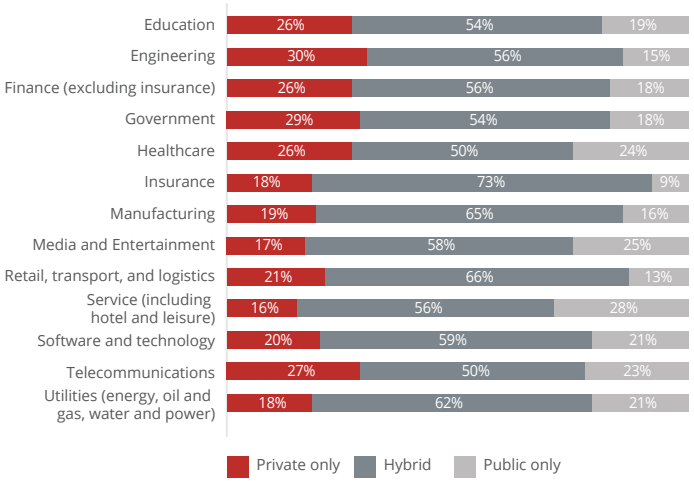


Figure 7. Which type of cloud architecture is your organization currently using? (grouped by industry)

Private-only cloud usage remained highest in the Gulf Coast Council (Saudi Arabia and United Arab Emirates) (30%) and Mexico (28%). Gulf Coast organizations were much more concerned about public cloud costs and the ability of cloud service providers to meet SLAs than average. Mexican organizations were also concerned about meeting SLAs, but their top concern was protecting sensitive data as it moves to and from the cloud, well above the rest of the group (54% vs 34%). Japan had the lowest usage of private clouds, at just 7%, once again due to higher than average concerns about staff security skills.

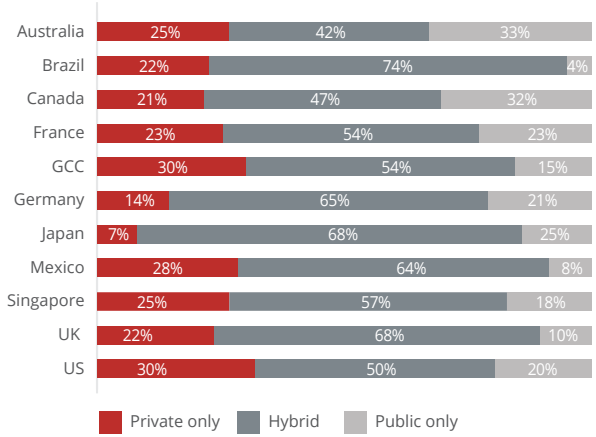


Figure 8. Which type of cloud architecture is your organization currently using? (grouped by country)

Public-only usage remained highest in Australia (33%) and Canada (32%). Australians were primarily concerned about the challenges of having consistent security controls integrated across both traditional and virtualized infrastructures. Canadians were primarily concerned about maintaining compliance across hybrid services. Pure public cloud usage was lowest in Brazil (4%), Mexico (8%), and the UK (10%). Brazilians have the highest usage of hybrid architectures, at 74%. Mexican organizations are high private cloud users, as mentioned above. In the UK, low public cloud usage appears to be predominantly a trust issue, as they reported the lowest opinions of the public cloud's abilities to maintain identity and access control, and to keep their organization's data safe and secure from hackers.

Cloud First strategies affecting IT budgets

More than 80% of the organizations surveyed stated that they are now following a Cloud First strategy, where priority is given to applications that can be purchased as a service or deployed in the cloud over requiring hardware and physical servers and systems to be deployed in the data center. Those with a Cloud First strategy believe that their IT budgets will be 80% cloud services in less than 12 months, while those without such a strategy think it will be closer to 20 months.

The rate of cloud investment and adoption continues to be significant, but overall organizations do not seem to be getting much closer to the point where 80% of their IT budget will be comprised of cloud services. Comparing last year's responses, the average number of months until they think this will happen dropped from 16 months to 15 months, indicating last year's respondents were overly-optimistic. The cloud skeptics in the UK reported the most significant year-over-year change, from 28 months to 21 months, showing that their comfort with cloud is improving, but leaving them still the laggards in this study. The Germans, ranking among last year's skeptics at 18 months, are much closer to this year's average, reporting that they think this shift to predominantly cloud will take 16 months. The Australians now think their cloud migration will take a little longer, from 11 to 13 months. Perhaps most notable, the percentage of IT professionals who stated that they do not think their IT budget will ever be 80% cloud was cut by half, from 12% in 2015 to just 6% in 2016.

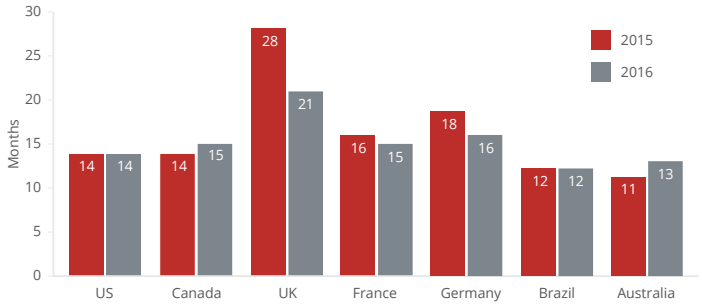


Figure 9. Average number of months respondents believe it will be until 80% of their organization's IT budget will be comprised of cloud computing services, grouped by country (comparing only countries which were included in both the 2015 and 2016 studies).

Perceived benefits of public cloud surpassing private cloud

There appears to be an improving perception of public clouds. Overall, respondents see public cloud as more likely to deliver the key benefits stated below over private cloud. The majority believe that a public cloud is more likely to deliver lower total costs (59%), provide better visibility of their data (54%), and keep their data safe (51%). Our respondents indicated they believe data in public clouds is as secure from hackers as it is in their private cloud.

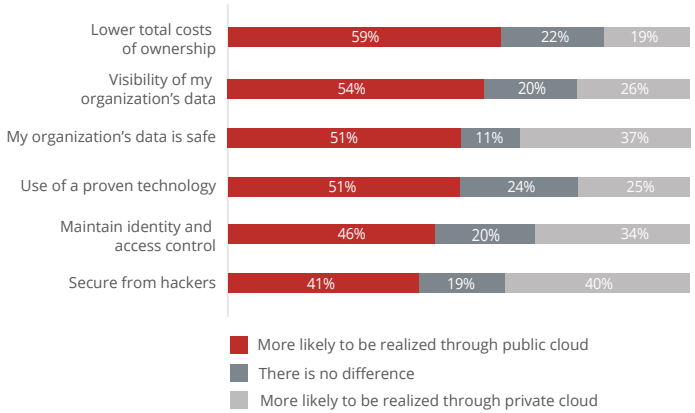


Figure 10. In your opinion, which of the below benefits are more likely to be realized through public cloud and which are more likely to be realized through private cloud for your organization?

Skills shortages affecting cloud adoption

The ongoing shortage of security skills is continuing to affect cloud deployments. Almost half of the organizations report that the lack of cybersecurity skills has slowed adoption or usage of cloud services, possibly contributing to the increase in Shadow IT activities. Another 36% report that they are experiencing a scarcity but are continuing with their cloud activities regardless. Only 15% state that they do not have a skills shortage.

By country, the skills shortage is worst in Japan, Mexico, and the Gulf Coast Council, and also in engineering and telecommunications firms. Engineering firms are most likely to have slowed their cloud adoption plans due to the lack of security skills, with more than 60% reporting this.

The largest organizations are least likely to have a shortage, and as a result are also least likely to have slowed their cloud adoption plans.

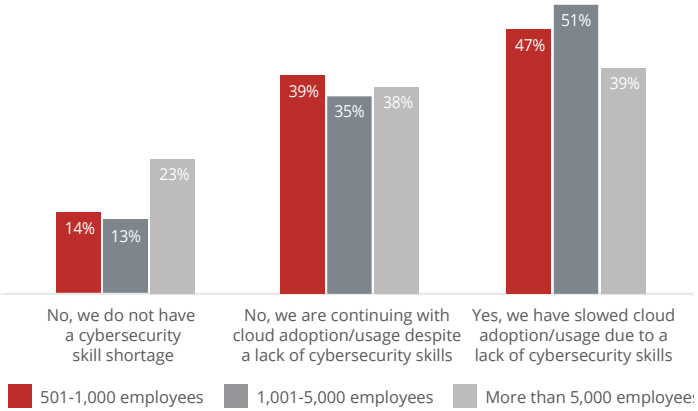


Figure 11. Is a shortage of cybersecurity skills affecting your organization's usage of cloud computing? (grouped by organization size)

Sensitive data moving to the public cloud

A strong indicator for the improving perception of public clouds is an organization's willingness to store sensitive or confidential data there. Almost 85% of professionals surveyed report they store some or all of their sensitive data in the public cloud. Almost a quarter (23%) completely trust it to keep their data secure, a strong increase from 13% in 2015. In addition, the total of those who distrust public clouds dropped from 50% to 29%.

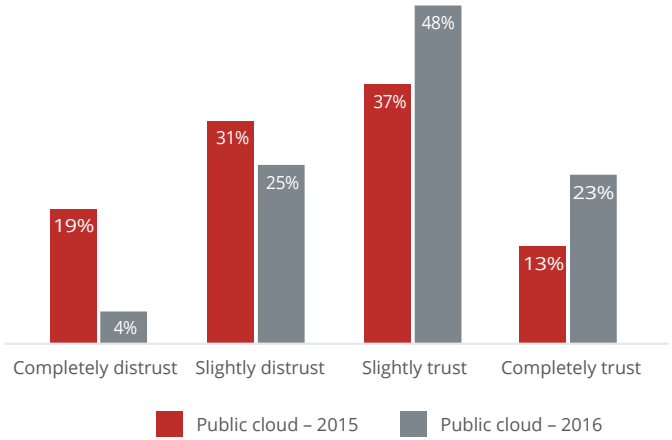


Figure 12. To what extent do you trust the following to keep your organizations' sensitive data secure?

This increase in trust appears to be encouraging organizations to store more sensitive data in public clouds, with 25% overall storing all of their sensitive data in the cloud, and 59% storing some of it. Only 16% are storing no sensitive data in public clouds, lowest in Canada (5%) and highest in France (28%), Australia (27%), and the UK (26%).

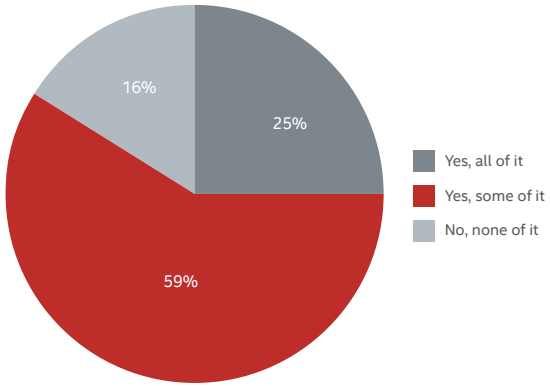


Figure 13. Does your organization's public cloud service store your organization's sensitive data?

The most common type of data stored in the cloud is personal customer information. This appears to be influenced by online business models. Industries with a high proportion of online transactions are the most likely to store their customer data in the public cloud, such as utilities (79%), services (73%), insurance (65%), and finance (64%). Government organizations were more likely to keep staff information (66%) than customer information (59%) in the cloud. Media and entertainment companies, not surprisingly, were most likely to keep proprietary and internal company information in the public cloud, which encompasses their product and service offerings such as music, videos, and other content.

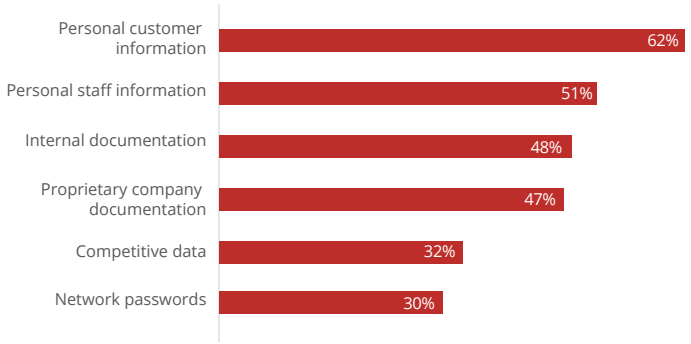


Figure 14. What type of sensitive data is stored in your organization's public cloud services?

Integrated security better at securing sensitive data

Storing sensitive data in the cloud changes the risks and responsibilities of the security team, potentially requiring them to work with a diverse set of tools across the different cloud platforms. Security vendors are responding to this increasingly popular operating model with higher levels of integration between tools and across multiple vendors. Security operations now have the option to purchase tools that are partially or fully integrated across their private and public cloud services, or a unified security solution that provides single-pane-of-glass views. The improvements in visibility and response times that result from higher levels of integration appear to significantly increase the security team's confidence and willingness of organizations to store sensitive data in the public cloud. The greater the integration of an organization's security solution across multiple cloud environments, the more likely they are to store some or all of their sensitive data in a public cloud service.

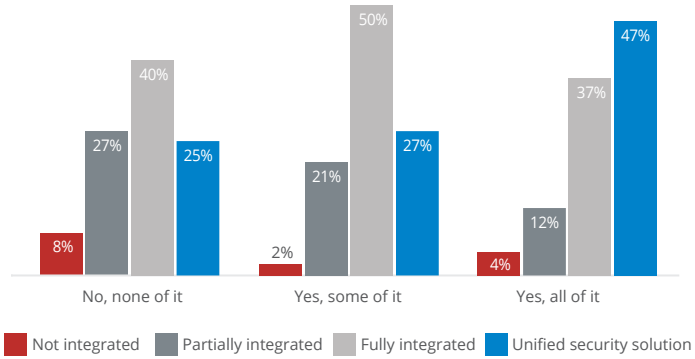


Figure 15. Does your organization's public cloud service store your organization's sensitive data? (split by level of integration of security solutions)

Senior management more understanding of the risks and rewards

Senior management also understand the risks of public clouds more, with 86% mostly or totally understanding the risks that come from storing sensitive data in the public cloud, up from 80% last year.

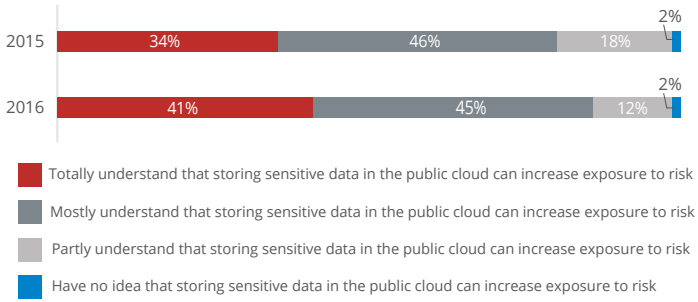


Figure 16. Do you think your organization's senior management/ executives understand the increased exposure to risk that comes from storing sensitive data in the public cloud?

CIOs and other C-level executives involved in the study were more likely to be following a Cloud First strategy, and expected their budgets to be 80% cloud-based within the next 12 months. These senior executives were also aware of the security skills shortage, and the affect it was having on their cloud adoption rate. To help alleviate the workforce challenges, they were more likely to be operating an integrated or unified security solution, and had DevSecOps functions as part of central IT. Organizations with higher C-level involvement were most likely operating a hybrid architecture encompassing multiple types of services. In these organizations, a greater proportion were storing some types of sensitive data in the public cloud, and there was a much higher level of intention to increase investments in all types of public cloud services.

Usage of PaaS growing faster than SaaS or IaaS

Cloud services are available in three primary options: software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS), and organizations can use any combination of these, in both private and public variants.

The shift to a hybrid public/private architecture has been accompanied by a strong increase in organizations adding PaaS to their mix of cloud services. Overall, PaaS is now in use by 40% of organizations surveyed, up from 21% last year. PaaS usage and hybrid architecture are strongly related, with more than half of those running a hybrid architecture also using PaaS as part of their cloud services. This year's investment plans are 66% SaaS, 64% IaaS, and 59% PaaS, which is consistent with their relative usage rankings.

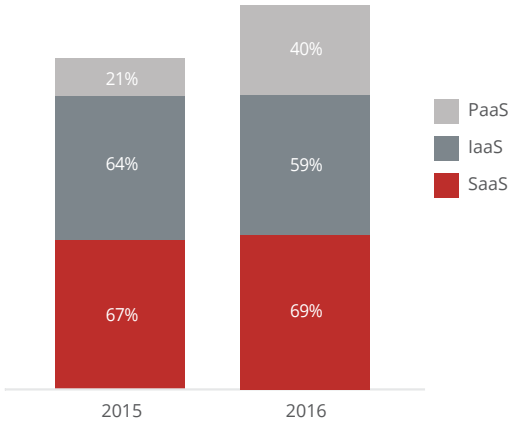


Figure 17. Which cloud services is your organization currently using? (grouped by year)

Greater than 50% chance of getting malware from a SaaS application

More than half of the professionals surveyed report that they have tracked malware incidents to a SaaS application. SaaS applications have added a new threat vector for malware to enter networks and systems.

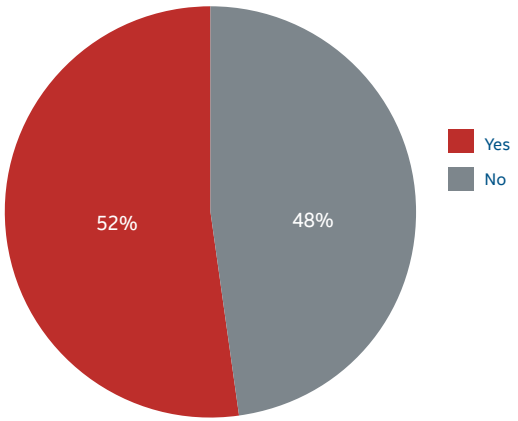


Figure 18. Have you ever definitively tracked a malware incident back to content pulled from a cloud (SaaS) application such as Dropbox, Office 365, etc.?

Issues and concerns with cloud service providers

Organizations continue to experience issues related to data loss with their cloud service providers. While the incidence of actual breaches declined a small amount, unauthorized access to data or services was cut in half, to just 10%, and credential theft also dropped, from 13% to 10%. This could be related to the reduction in the overall number of cloud applications and services in use. Organizations are consolidating their usage, especially with the top tier service providers, which are gaining market share at the expense of smaller service providers. The top tier providers, such as Amazon, Microsoft, Google, and Salesforce, have been improving their security posture and expanding their security resources, increasing the differences between them and smaller cloud service providers.

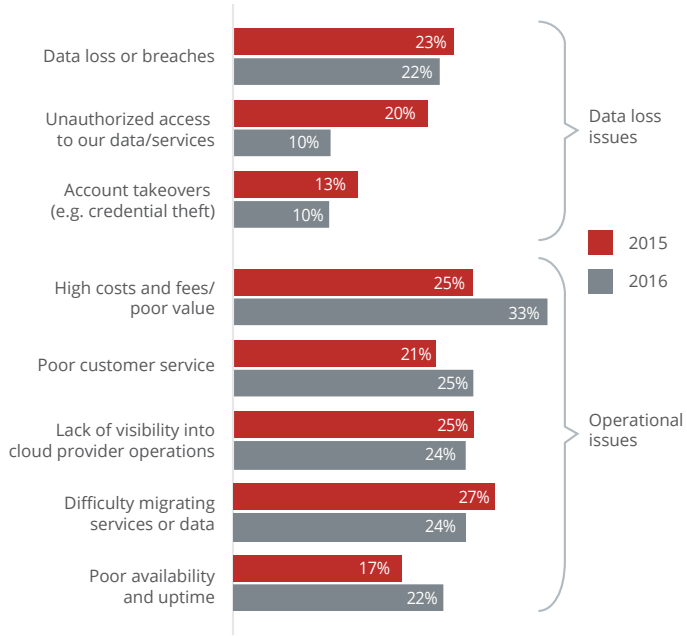


Figure 19. Has your organization experienced any of the following issues with cloud service providers?

High costs/poor value is now the number one operational issue that IT professionals have experienced with their cloud providers in the past year, and poor customer service is number two. Compare this to last year, when difficulty migrating services or data, which is now in fourth place, was the top issue. Lack of visibility into cloud provider operations is now the top technical issue, although it has not changed much over the past year. Poor availability and uptime has moved up into the top five, increasing from 17% last year to 22% this year.

Data in transit top concern for SaaS

With increasing trust comes a change in the types of concerns IT professionals have with their cloud services. Historically, a breach or other type of data loss has been the top concern with public cloud services, whether SaaS or IaaS. This year, the top concerns for public cloud services were around operational issues rather than blanket fears of data loss.

SaaS users were most concerned about protecting sensitive data moving to and from the cloud, understandable given that half have experienced a malware infection from SaaS applications and a quarter have suffered a data breach. The second most common concern of SaaS users was cost, reinforcing how mature these services are becoming. Security operations concerns were similar to those using other types of clouds, including data compliance, advanced threats, and identity management. Ability to meet service level agreements and departmental Shadow IT cloud use rounded out the list.

1.	Protecting sensitive data as it moves to and from the cloud
2.	Cost
3.	Maintaining data compliance
4.	Advanced targeted attacks and/or advanced persistent threats
5.	Skills required by your IT security staff
6.	Identity and access management
7.	Ability of SaaS provider to meet service levels/SLAs for performance and availability
8.	Departments commissioning SaaS applications without involving IT dept. i.e. Shadow IT

Figure 20. Top concerns about using SaaS, ranked list

Integrated security top concern for IaaS

IaaS users' top concern this year was integrated and consistent security controls, followed closely by concern about staff security skills. As organizations adopt Amazon, Google, or Microsoft infrastructure services, their security teams are having to adapt to the new shared responsibility model. Working with multiple services makes it more difficult to ensure that policies are configured and enforced consistently across multiple environments. Security concerns do not appear until fifth on the list, which may imply responders were slightly more comfortable with IaaS provider's security operations than general operational issues.

Operational concerns about the provider included inability to meet SLAs and the location of data centers. Top security operations concerns were: maintaining compliance, identity and access management, and dealing with advanced threats.

1.	Having consistent security controls that provide integrated security with central management across all cloud (private and public) and traditional data center infrastructure
2.	Skills required by your IT security staff
3.	Maintaining compliance
4.	Ability of the cloud provider to meet service levels/SLAs for performance and availability
5.	Unauthorized access to sensitive data from other cloud tenants in a multitenant environment
6.	Identity and access management
7.	Advanced Targeted Attacks and/or Advanced Persistent Threats
8.	Location of the cloud service providers' data centers and data stores outside of my country

Figure 21. Top concerns about using IaaS, ranked list

Actions to increase public cloud adoption

Addressing concerns and increasing public cloud adoption requires some additional work, from both cloud service providers and security vendors. Reducing the cost is the number one action that providers can take to increase adoption. However, the next four are related to protecting data in the cloud and in transit and controlling user access. Cloud providers and security vendors must work together to address these critical issues:

- Enhancing the ability to protect data in motion and within cloud applications
- Providing greater assurance that data remains under the owner's control
- Enabling stricter access and identity management
- Delivering greater transparency

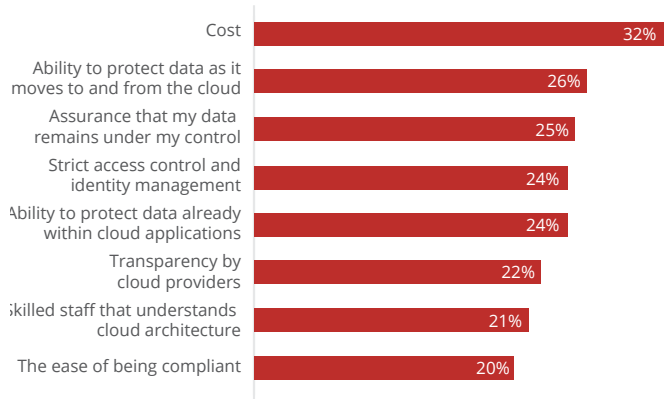


Figure 22. Which of the following would increase public cloud adoption within your organization?

The growing nemesis of Shadow IT

An IT organization that is slow to deploy solutions can inadvertently encourage other departments to commission their own services. It can also lead to a disjointed security environment, creating more work for the security team.

Whatever is driving Shadow IT, whether it is the mainstream acceptance of public cloud services or slowed adoption by IT due the shortage of security skills, almost 40% of cloud services in use in an organization today are commissioned without the involvement of the IT department. This is not necessarily a bad thing, if IT and security operations have sufficient visibility to keep the applications, data, and the organization safe and secure.

Unfortunately, visibility of these Shadow IT services has dropped from about 50% last year to just under 47% this year. This is not a very large drop, but it does affect the security posture of the organization. More than 65% of IT professionals think this lack of visibility is impairing their ability to keep the cloud safe and secure, up from 58% last year.

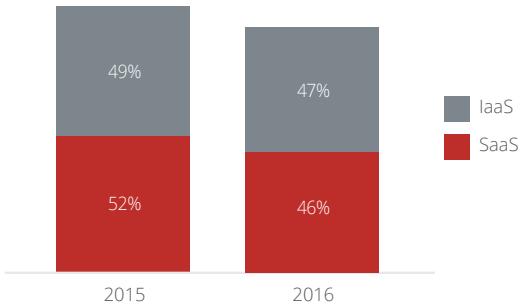


Figure 23. What percentage of public cloud services commissioned by departments without the direct involvement of the IT department do you believe you have visibility over?

How IT is finding Shadow IT

There are significant changes in the actions which IT is taking to monitor and manage the use of Shadow IT services. IT departments appear to be moving towards more active methods of monitoring and employing technology in an effort to gain better visibility. Next-generation firewalls have replaced database activity monitoring as the most likely method being used this year, increasing from 41% to 49%. Utilization of web gateways increased from 37% to 41%, and use of cloud access security brokers (CASBs) increased slightly from 32% to 33%. At the same time, more passive methods of detecting Shadow IT activity, such as working with finance, checking license usages, or word or mouth, dropped significantly. Overall, only 1% of organizations are not monitoring Shadow IT usage, down from 5% last year.

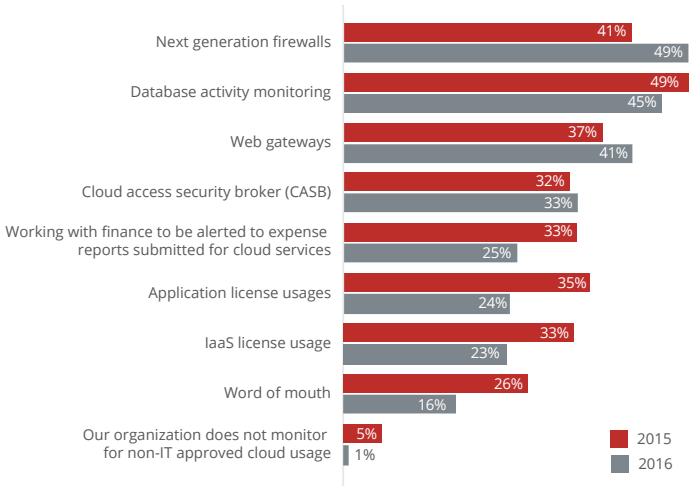


Figure 24. How does the IT department monitor non-IT approved cloud usage? (grouped by year)

How IT is securing Shadow IT

IT departments are taking a variety of steps to secure shadow services in use. Blocking access to unauthorized services is the top choice, but only 27% of organizations are taking this action. Most appear to be striving to support the department's choice of service with measures such as identity and access management, DLP and encryption, or working with the users to find an acceptable solution. Interesting to note, while 22% have experienced a data breach with their cloud services, only 24% are using DLP and encryption to protect the data, with almost no correlation between the two.

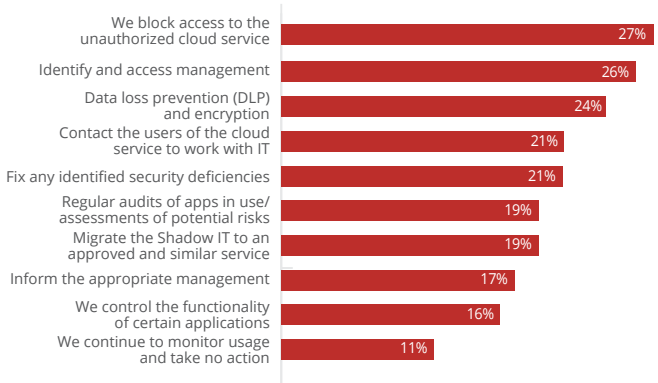


Figure 25. Once Shadow IT is discovered in your organization how does the IT department secure the cloud service?

Data center infrastructure shifting to true private cloud

In order to move to a hybrid private/public cloud architecture, the data center has to evolve to a highly-virtualized, cloud-based infrastructure. Very few organizations are there yet, with only 4% reporting a fully software-defined data center (SDDC). However, the majority (73%) expect to complete their transformation to SDDC within 24 months, while 20% expect it to be complete within 5 years. Only 7% indicate that they never plan to fully transform to SDDC. The shift is happening slowest at the largest organizations, with 10% of those stating no plans to fully transform, and 29% expecting it to take up to five years. Government (19%) and utilities (14%) are the leaders of the "No, never" group, and government (33%), education (31%), and services (33%) leaders of the "within 5 years" group. These responses are all arguably due to concerns about the scarcity of skilled IT staff to implement and maintain their private cloud. The telecommunications industry ranked the scarcity of IT staff skills similarly high, yet they are leading the transformation to SDDC.

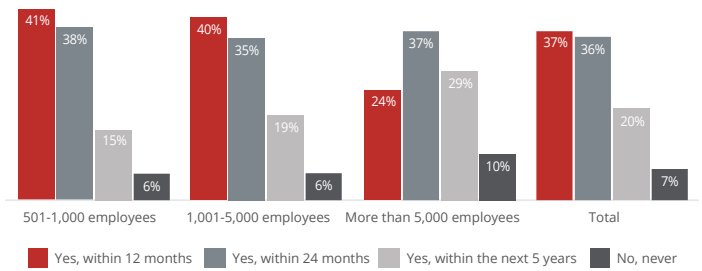


Figure 26. Does your organization plan on having its data center fully transformed into a software-defined data center ? (grouped by organization size)

Currently an average of 52% of an organization's data center servers are now virtualized.

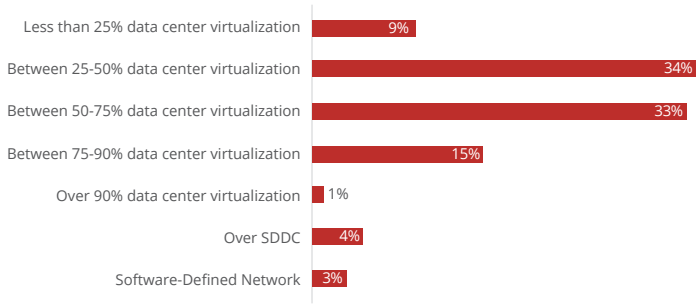


Figure 27. Which of the following statements most closely describes the current architecture of your private cloud?

This transformation to cloud services is transforming other aspects of the organization as well. Containers, the younger and smaller siblings of virtual machines and the next step in granular resource allocation, are growing very quickly. More than 80% stated that they are now using containers—36 % using them just inside IT, 18% just outside IT, and 29% both inside and outside of the IT department. Containers tend to be used in higher quantities per host than virtual machines, but last for a small fraction of the time, making them more challenging to protect.

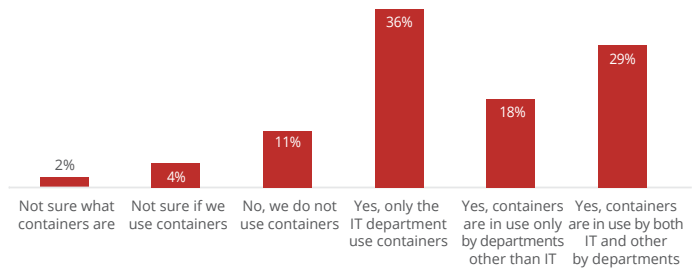


Figure 28. Does your organization use containers (e.g. Docker or Lynx)?

Unauthorized access top concern about private clouds

Private cloud users listed unauthorized access to sensitive data as their top concern, with concern about staff security skills a very close second. The time and effort involved in implementation and maintenance also made the list. The majority of the concerns are related to security operations, including maintaining compliance, identity and access management, dealing with advanced threats, insufficient visibility, and consistent controls. New virtualization technologies, such as containers, are putting additional pressure on the IT departments' resources and skill sets.

1.	Unauthorized access of sensitive data in the private cloud
2.	Skills of IT staff for implementation and maintenance
3.	Maintaining compliance
4.	Identity and access management
5.	Advanced targeted attacks or advanced persistent threats
6.	Visibility of security posture
7.	Having consistent security controls that are integrated across both traditional and virtualized infrastructures
8.	The time/effort for implementation and maintenance

Figure 29. Top concerns about using private cloud, ranked list

DevSecOps improving efficiency of security teams

DevSecOps is a growing organizational option intended to help distribute security throughout the organization. DevSecOps functions are now found in 45% of organizations using cloud services, with 49% planning to introduce this function in the future. Only 6% of the IT professionals surveyed stated that they have no plans to introduce a DevSecOps function.

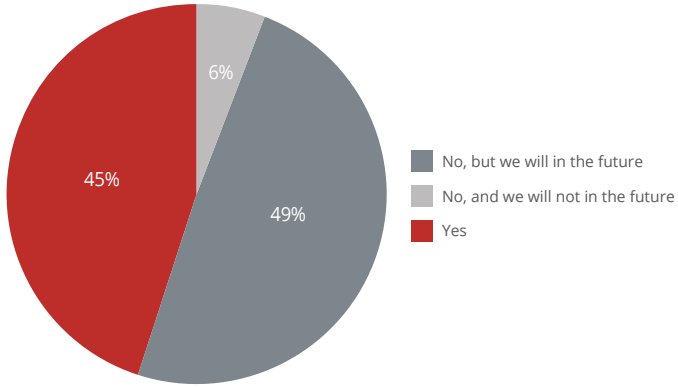


Figure 30. Do you have a DevSecOps function in your organization?

DevSecOps is most likely to be part of Central IT (71%), with placement of it in Engineering (15%) or Technical Operations (14%) far less likely.

Conclusions

Clouds are here to stay. Businesses are trusting them with a wide range of applications and data, much of it sensitive or business critical. Data goes to where it is needed, most effective, and most efficient, and security needs to be there in advance to quickly detect threats, protect the organization, and correct attempts to compromise the data.

Clouds today encompass a large variety of architecture and operating models. There is no one right model, and organizations are choosing the services and architecture that best fits their needs. The cost and resource savings are real, and the offerings are maturing rapidly, allowing organizations to move onto specific operational issues that are important to their business.

Security concerns about clouds are maturing, moving from vague and generic fears about breaches to more detailed issues about protecting data at rest and in transit, consistently configuring and enforcing security policies, and controlling identity and access. Unfortunately, the scarcity of security skills is also real, and is an issue for most organizations, regardless of industry, country, or size. Increased use of public cloud services may help alleviate the impact of the security skills shortage, as organizations leverage the broad and deep security talent pools that are present in most major cloud providers.

Recommendations

The pressures of speed, efficiency, and cost will push more applications and data outside the trusted network and into a service provider's clouds, where those benefits can be realized. The growth of cloud services and movement of sensitive data between private and public clouds means that those services will become increasingly valuable as targets of attack. As enterprises cloud-enable their operations, gaps in control, visibility, identity, and security are the most likely paths to data breaches. Integrated or unified security solutions are a strong defense against these threats, giving security operations visibility across the cloud services in use and which data sets are permitted to traverse them.

Attackers will most likely look for the lowest hanging fruit between an organization's data center or private cloud, its partnership extranets, hybrid clouds shared between organizations, or in the data or applications hosted by a public cloud provider. Credentials and authentication systems will continue to be the most vulnerable point of attack, according to the **McAfee Labs 2017 Threat Predictions Report**, so cybercriminals will work hard to steal credentials, especially administrator credentials because those can provide the broadest access. Organizations should make sure that they are following best practices for cloud credentials, including distinct passwords and multi-factor authentication to mitigate this risk.

Security technologies such as DLP, encryption, and CASB provide essential identification and protection for an organization's data and cloud services, but are still vastly underutilized. These tools increase visibility, enable discovery of Shadow IT, assist with classifying data based on the value to the organization, and provide automatic protection, such as encryption, of sensitive data at rest and in motion within a private data center or among cloud environments. As an organization looks to add DLP, CASB, and other emerging tools in its security defenses, it must make sure they are integrated with its threat intelligence, policy controls, and security operations to get the most benefit to its security posture with the least expenditure of costly trained labor.

Many organizations using multiple IaaS providers are concerned about consistent visibility and controls. The ideal security model should have functionally equivalent controls across all environments, so that when workloads are provisioned, the question of which provider they are provisioned on is not an

issue. Organizations should look for specialty security solutions that provide an equivalent control layer across all providers. These solutions enable brokering of workload provisioning across multiple clouds, while delivering the confidence and assurance that security policy and enforcement are consistent, regardless of location.

Organizations should identify whether there are compliance or regulatory challenges precluding the use of hybrid or public clouds, or what the additional costs of using them would be. If the costs for securing data and applications in the cloud are lower, they should consider adopting a Cloud First strategy to align with the mission of their business partners, both internal and external to the organization. This strategy not only encourages the organization to adopt applications and services that are likely to save money and increase flexibility, it also puts security operations in front of the shift, instead of reacting to it.

Fundamentally, the use of cloud computing allows an organization to focus on its core strengths and outsource the work to a third party that has the necessary skills in an evolving world. However, as many organizations have realized, while it is possible to outsource the work, it is not possible to outsource the risk. Subsequently, due diligence in the use of third party services will be essential in the event that a security breach involving a third party occurs. The role of the internal security department may evolve to become less technical and more as an oversight function against third parties, but their role and importance has never been so critical.

Statements expressed herein are based upon McAfee's 2016 cloud survey results. For more details on the survey, contact ***Public Relations at McAfee.***

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the 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.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com