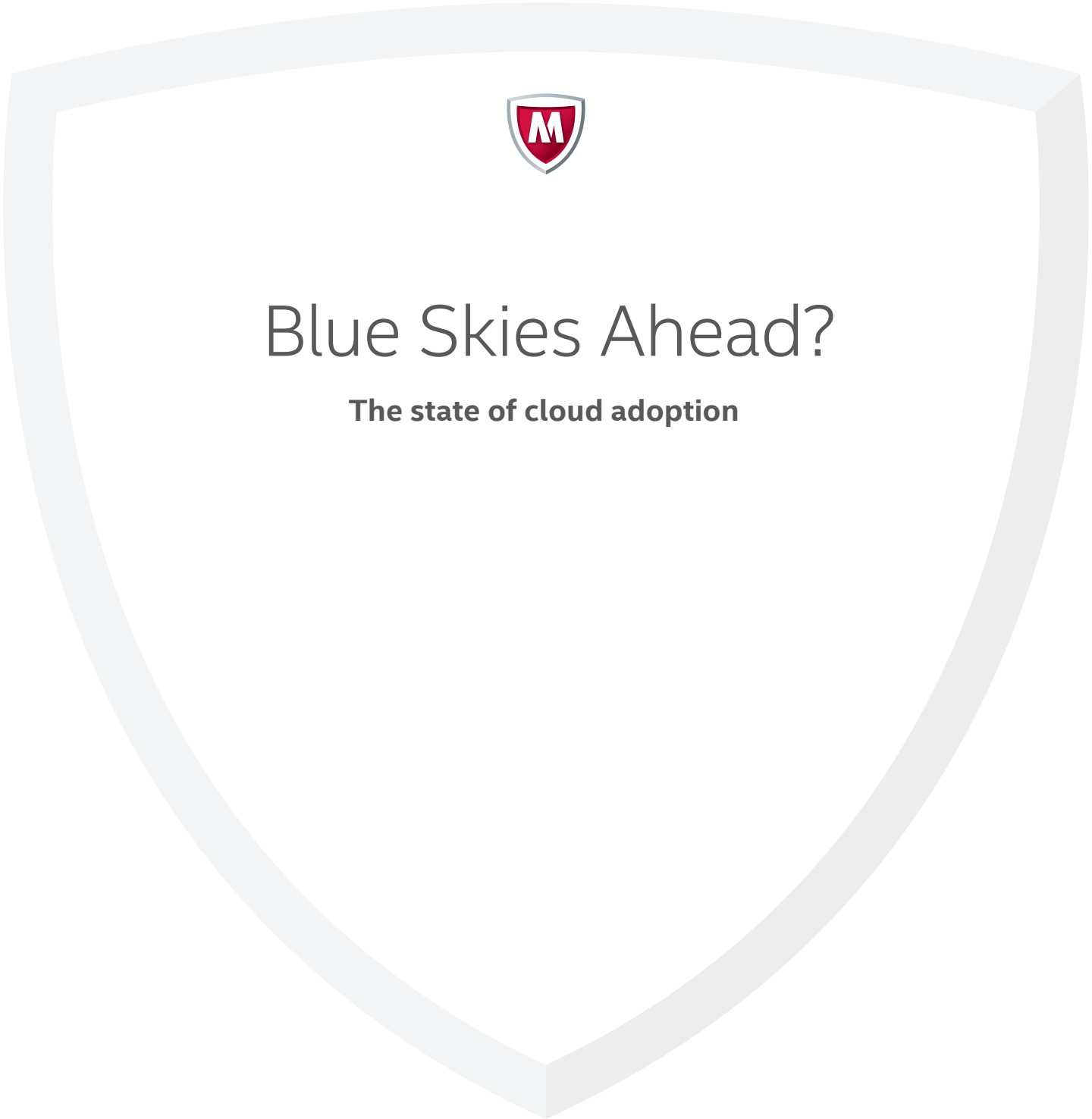
Report



Blue Skies Ahead?

The state of cloud adoption

intel Security

Table of Contents

We thank the 1,200 core survey respondents for their participation and these top executives for sharing their expertise and viewpoints for this report:

- Brent Conran, Vice President and Chief Information Security Officer, Intel
- Brian Dye, Corporate Vice President, Intel Security
- Dimitra Liveri, Network and Information Security Officer, European Network and Information Security Agency (ENISA)
- Vanessa Pegueros, Chief Information Security Officer, DocuSign, Inc.
- Jim Reavis, Chief Executive Officer, Cloud Security Alliance
- Dave Shackleford, SANS analyst and Chief Executive Officer, Voodoo Security
- Timothy Youngblood, Chief Information Security Officer, Kimberly-Clark

A Cloud for Every Season? It's a Question of Trust.

Almost everyone who turns on an electronic device is consuming cloud computing in some way. Whether it's for home automation or for revenue-generating business applications, we all rely on Amazon Web Services, Microsoft Azure, other cloud providers that maintain availability of such services. As we consider the evolution and future of cloud computing, our use of this computing platform will grow, and the impact of our dependency on the cloud will have tremendous ramifications for each and every one of us—consumers and businesses. According to our survey, in the next 12 to 18 months, most of enterprise IT's budget will be spent on public cloud resources. Some people refer to this as a tipping point in IT.

Let's consider the implications of this transition. First, the skills of technology professionals working in these companies will have to evolve significantly. Second, the level of trust in the cloud will have to improve—and, with that, the additional visibility we all require to achieve this level of trust.

While the cloud is a reality today, the future brings an expanding scope of its capabilities—it will not be surprising to see critical infrastructure applications and services moving to the cloud. Indeed, as we begin to speculate about what the enterprise data center of the future looks like, it could possibly be that Cloud First will be the default deployment for applications, with the exception being (only if it makes sense) to host on premises.

With the appropriate security in place, the power of cloud computing can be harnessed to support new applications and advanced business tools to grow productivity. However, as you will read from our study, enterprises continue to struggle with issues of trust and security.

As our reliance on such computing platforms grows, we have an opportunity to raise the level of trust in alignment with the expectations of enterprises and consumers. The Cloud Security Alliance, a volunteer-led organization and a leader in technical research, extends an invitation to organizations and their constituents to participate in and lead this transformational change.

—Raj Samani, EMEA Chief Technology Officer, Intel Security
—Jim Reavis, Chief Executive Officer, Cloud Security Alliance

Introduction

As business requirements drive enterprises rapidly towards cloud computing and beyond small-scale projects and pilots, what are the key trends and issues they will need to address? How can businesses reap the benefits of the cloud without compromising security and control?

In an eight-country survey, we asked 1,200 IT decision-makers with responsibility for cloud security in their organizations about their plans for cloud adoption, their biggest challenges, and their investment priorities over the coming year.

In this report, we look at enterprise cloud adoption trends and how they differ across Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Security-as-a-Service, and also public, private, or hybrid cloud. We also look at how organizations in more regulated industry sectors are trying to overcome compliance issues related to the adoption of cloud computing.

We will explore the myth and reality of the biggest cloud security issues facing enterprises and look at the effectiveness of investments in cloud security technologies, including encryption, data loss prevention, and more.

We will also examine how enterprises are tackling the challenge of shadow IT-procured cloud while enabling employees and departments to get access to the services they need with the necessary security in place to protect corporate information. In this report, we will also assess board-level awareness of cloud security risks.

Enterprise IT Ramps Up Cloud Investment

"We've gone well beyond the early adopters—those who are testing and piloting cloud—to the full-scale adoption of a variety of different types of cloud. Across the board we are seeing a real recognition that this is the future of IT, moving compute to a utility."

—Jim Reavis, CEO, Cloud Security Alliance

Consumers already live their life in the cloud and use it on a daily basis to accomplish tasks, like uploading photos to accessing email to backing up data. Our survey shows we are now at a similar inflection point where cloud computing will become a dominant technology focus for enterprise IT.

While rising cloud investment and adoption by enterprises might not be such a big surprise, what is significant is the rapid pace at which this is now happening. Our survey reveals a game-changing shift for enterprise IT, with the vast majority of organizations' IT budgets being spent on cloud services in less than a year and a half—and even faster than that in some countries (Figure 1.). Survey respondents said they expect 80% of their organization's IT budget to be dedicated to cloud computing services in 16 months' time. Organizations in Brazil and Australia expect to hit this 80% mark within a year.

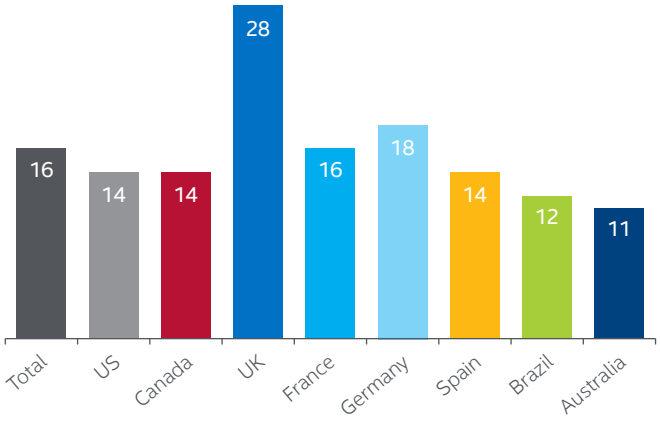


Figure 1. Average number of months until 80% of the respondent organization's IT budget will be comprised of cloud computing services, split by country.

"Our business partners are leveraging the dynamic nature of the cloud, the improved speed, increased collaboration, the elasticity of services—which all make the cloud attractive—and they are taking steps to increase that because it's to your detriment if you don't. As security professionals, we have to be engaged and show how security can be the foundation."

—Timothy Youngblood, CISO, Kimberly-Clark

The migration to cloud services cited by our survey respondents will be to both private and public cloud deployments. According to our survey, private cloud is currently the most dominant cloud model in the enterprise, with 51% of their cloud deployment comprised of private cloud. Public cloud makes up 30%, and hybrid cloud accounts for 19% of enterprise cloud deployments. When we look at how many months it will take until 80% of an organization's IT budget will be allocated to cloud computing services, the timeframe for the private cloud shrinks to just 15 months.

We can see evidence that the adoption of cloud services is at the tipping point. Organizations are using an average of 43 cloud services now—although it's worth noting some significant regional variations (Figure 2). The UK, for example, is the slowest in terms of cloud adoption (an average of just 29 cloud services per organization), while Brazilian enterprises are among the highest adopters of cloud services (55 cloud services per organization).

"We have a philosophy of 'cloud first' at DocuSign, and we are seeing many of our customers across industries following the same approach. It's a longer conversation with companies in highly regulated industries, like financial services and healthcare. The IT organizations at these companies are in a very difficult position because their regulators are requiring that they prove that all the necessary security measures are in place prior to implementation. They feel an incredible pressure to take the time to prove this to the regulators, but at the same time their businesses are pushing them to get more efficient and more nimble—and do it all faster."

—Vanessa Pegueros, CISO, DocuSign, Inc.

"Be aware of what information is appropriate to store in the cloud and what isn't. If there's information that is valuable to the company, then it should probably stay within the boundaries of the company's domain and stay in a private cloud."

—Eric Knapp, Global Director of Cybersecurity, Honeywell

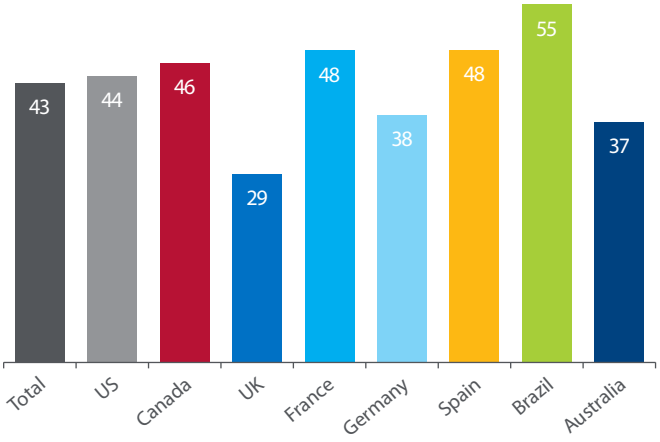


Figure 2. The average number of cloud services organizations are currently using, categorized by country.

Of course, there will also be differences in the rate of adoption of different types of cloud platforms—public, private, and hybrid or managed, as well as SaaS, IaaS, and PaaS. Anecdotally, there is also evidence that adoption varies from sector to sector. In highly regulated sectors, such as financial services, there is still some caution about moving to the cloud, and the government and the public sector also lag behind.

When we look at cloud adoption trends, it's easy to fall into the trap of talking about just SaaS. In fact, our survey reveals that the majority of organizations are planning on investing in all cloud service models, but (perhaps surprisingly) the highest percentage (81%) is actually for IaaS, compared to only 60% for SaaS (Figure 3). This is closely followed by Security-as-a-Service (79%), and even planned investment in PaaS (69%) is higher than SaaS.

That is backed up by the SANS report, which also shows that IaaS will be the largest area of growth for enterprise cloud deployments in the next year.

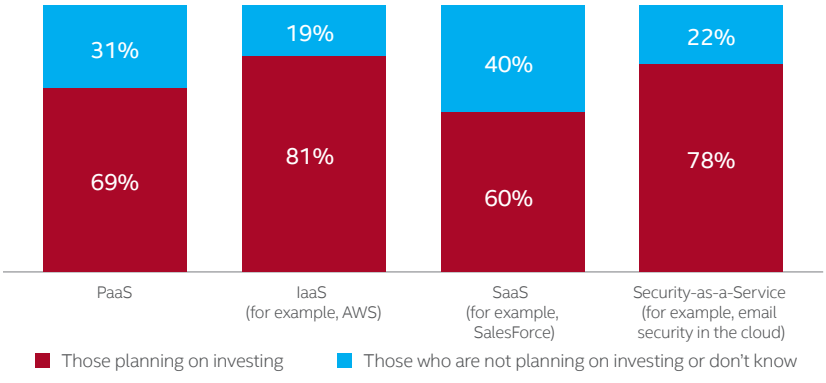


Figure 3. Which cloud deployments does your organization plan to invest in?

"The visibility into how the cloud service provider operates and what's happening really inhibits some of the risk analysis and the risk management decisions. A lot of regulations were made pre-cloud, with the assumption that an enterprise has full control over the compute technology and that, with cloud, they no longer do."

—Jim Reavis, CEO, Cloud Security Alliance

"We do see concerns over data breaches. It often ends up being an attack on the credentials of the user who has legitimate access to the cloud service—and the information gets exfiltrated in that way."

—Jim Reavis, CEO, Cloud Security Alliance

Security and Compliance: The Need for Better Visibility

What are the implications of this increased cloud adoption for enterprise security? We may see additional important and sensitive data hosted in the cloud. Some 40% of respondents to the SANS survey, **Orchestrating Security in the Cloud**, say they process or store sensitive data in the cloud.[1] The most common types of data stored in the cloud are business intelligence (52%), financial accounting (52%), employee records (48%) and customers' personal information (40%). Of greatest concern are the 13% of organizations that said they do not know whether they have sensitive data in the cloud. Many security experts believe that figure is actually much higher, particularly among larger enterprises. One reason for that is that some organizations do not want to admit they don't know, while others with operations and business units spread across the globe actually do not know if they are exposed in this way.

Maintaining compliance in the cloud is the biggest concern, across all types of cloud deployment, according to 72% of SANS survey respondents. The real challenge here is around visibility, with more than half (58%) of SANS survey respondents citing the lack of visibility into a cloud provider's operations as their biggest issue.

Dark Clouds Ahead? Threats for the Twenty-First Century

Our survey suggests it is time for a re-evaluation of what the real cloud threats are, with evidence of a gap between perception and reality.

In most countries the main concern around using SaaS is data security incidents—as cited by more than one in five respondents (22%). Data breaches are also the top concern for IaaS and private clouds. There are some regional differences—most notably in Australia, where downtime is actually the top concern.

But what is the reality?

When quizzed further, less than a quarter (23%) of enterprises said they actually experienced data loss or breaches with their cloud service providers, and only one in five had someone gain unauthorized access to data or services. The SANS survey shows an even lower level of cloud data breaches, with just 9% of respondents experiencing an incident in either public clouds or with their SaaS or private cloud applications.

The most common incidents and issues that respondents had with cloud services were actually migrating services and data, high costs, and poor value or lack of visibility into the cloud provider's operations (Figure 4).

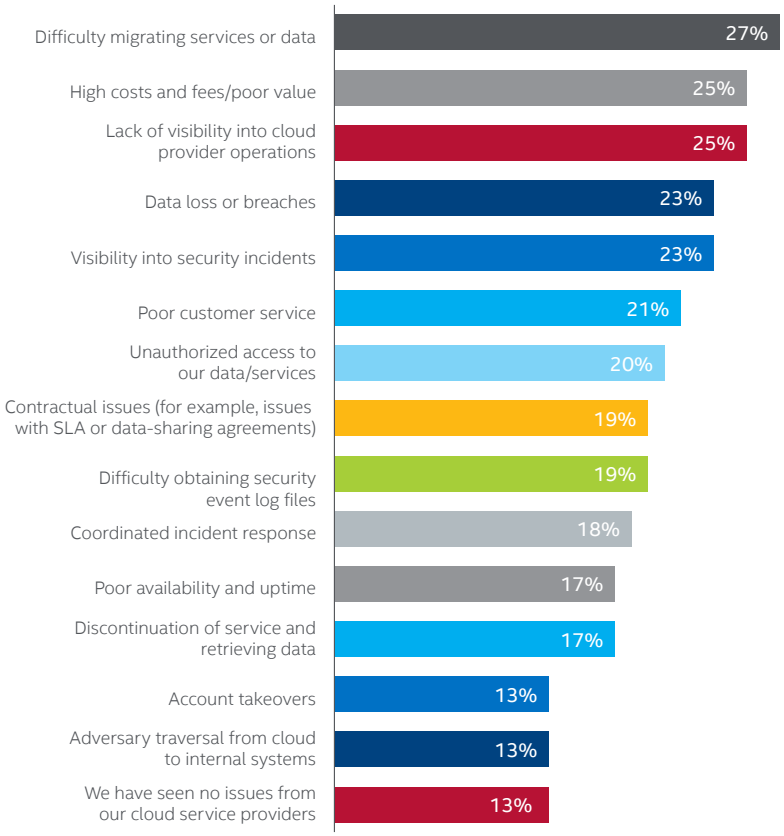


Figure 4. With regard to cloud security, what issues has your organization had with cloud service providers?

"Enterprises need to embed security into DevOps and the two most critical elements are continuous monitoring and change detection."

—Dave Shackleford, SANS Analyst and CEO, Voodoo Security

When we look at specific security threats to the cloud identified by respondents, malware and botnets are the top issue for private cloud deployments (33%), while denial-of-service attacks are perceived as the main threat for public clouds (36%).

Other cloud security risks potentially arise through the rapid scaling up or down of services, though this is more of an availability and business continuity issue that enterprises need to plan for. Another key feature of cloud adoption is the rise of DevOps—the increasingly rapid cycles of application development, testing, and deployment. Embedding robust security into that continuous development environment is vital for keeping track of those rapid changes and being alerted to any potential security risks associated with them.

Clearly we shouldn't jump to the conclusion based on survey results that cloud data breaches are not a serious security threat or that they never happen. We should consider the possibility of under-reporting of data breaches when they are not disclosed to law enforcement agencies or regulators. And, of course, when cloud data breaches do occur, the consequences are often significant. While the gap between cloud security threat perception and reality does need to be closed to some extent, the survey suggests that investment and planning around mitigating high-profile breach risks needs to be balanced with some of the more common day-to-day threats for enterprise systems and data in the cloud. These include migration problems, poor customer service, and contractual issues, as well as specific security threats such as denial-of-service, malware, and hacking of accounts.

Cloud Security and Risk: The C-Suite Blind Spot

"Boards and C-suite executives are broadly recognizing that cloud security is a critical element of any business and must be taken seriously."

—Vanessa Pegueros, CISO, DocuSign, Inc.

Our survey shows a high level of involvement in cloud security decision-making by senior management—not just the IT director, CIO, and CISO, but frequently the CEO and CFO as well. However, does senior management fully understand the security risks?

When it comes to public clouds, there appears to be a perturbing gap in board-level awareness of the security implications of storing sensitive data in the public cloud. (See Figure 5.) Only 34% of respondents feel senior management in their organization fully understands the implications, while one in five says C-level executives have no idea or only partly understand those risks. There is an even more pronounced gap in the UK, where just 15% believe senior management in their organization totally understands the risks of storing data in the public cloud. Contrast that with Brazil (49%) and Australia (47%), where awareness is far higher among board members.

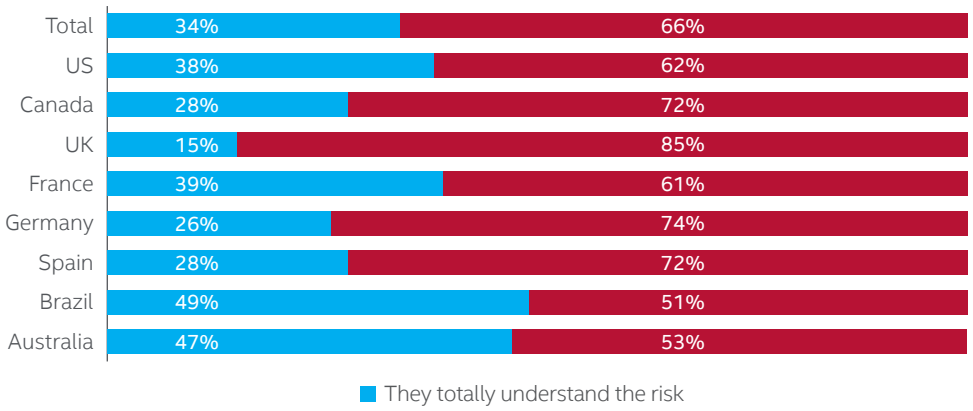


Figure 5. Do you think your senior management/executives understand the security implications of storing sensitive data in the public cloud?

While high-profile data breaches and the financial and reputational consequences have made data security a top-of-mind concern for many CEOs and the C-suite, our survey suggests there is still a need for more education to raise awareness and understanding of risks associated with storing sensitive data in the cloud

"Education is power. We have a very intensive security awareness program, focusing on educating all our employees on the value of information. It's what I call our 'human firewall'."

—Timothy Youngblood, CISO, Kimberly-Clark

Shadow IT: Risk or Opportunity?

A majority of respondents to our survey say shadow IT has a negative impact on their organization's ability to keep cloud services safe and secure, with 10% indicating that it leaves their organizations exposed to significant risk.

Securing shadow IT continues to be a major challenge: 52% of the lines of business still expect IT to secure their unauthorized department-sourced cloud services. In addition, nearly a quarter of survey respondents (23%) say that these departments source their own security without the help of IT.

Visibility over departmental shadow IT is generally greater for SaaS than IaaS. However, in all instances, at least a fifth of respondents do not know whether shadow IT is occurring in every department across their organizations. Levels of shadow IT are highest in sales, R&D, and marketing departments. The biggest question mark hangs over the legal department. Some 37% of our respondents can't tell if that department is procuring cloud without the knowledge of the IT department.

"Shadow IT is the new IT. The old model has gone away. The more we fight it, the more we deflect focus on working to secure it. We need to accept that shadow IT is today's reality and focus our energy towards managing it securely."

—Vanessa Pegueros, CISO, DocuSign, Inc.

"People are just trying to get their job done. If we can't provide it, they are going to go get it somewhere else. IT and the CIO have to be the broker and embrace cloud and SaaS services."

—Brent Conran, VP and CISO, Intel

How are organizations tackling shadow IT? The most common methods are

- Database activity monitoring (49%).
- Next-generation firewalls (41%).
- Web gateways (37%).

Another tactic is to work with the finance department to be alerted to expense reports submitted for cloud services.

There is a notable divide in how to deal with shadow IT when it is discovered. Almost half of respondents (46%) block access, whereas 37% migrate the shadow IT to an approved service.

Is Trust in Cloud Growing?

At first glance, the headline figures from our survey show a relatively low level of trust in cloud computing compared to on-premises or internally hosted IT. Not surprisingly, the public cloud is the least trusted model (Figure 6).

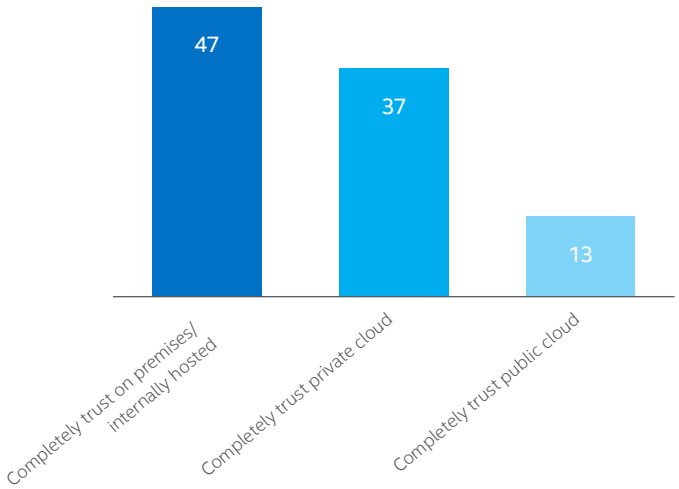


Figure 6. "To what extent would you trust the following to keep your organization's sensitive data secure?"

More significantly, the bigger picture shows an overall growing level of trust in cloud computing over the past year—77% of enterprises say their organization trusts cloud computing more now than they did a year ago (Figure 7).

"We have a new era coming for the cloud providers. We are in a transitional period, but I think these new regulatory provisions will help investment and trust so we should feel more comfortable with cloud services."

—Dimitra Liveri, Networks and Information Security Officer, European Network and Information Security Agency (ENISA)

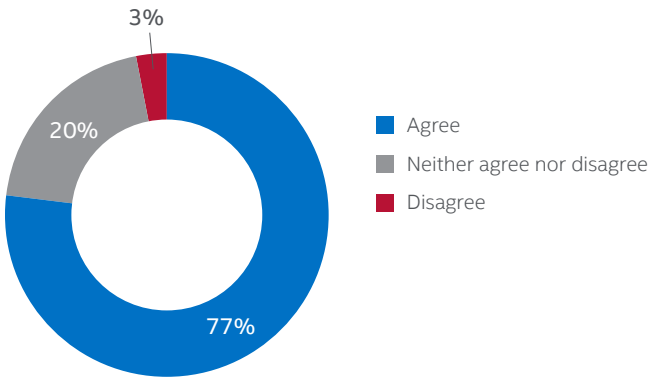


Figure 7. Those who agree with the statement "My organization trusts cloud computing more now than it did 12 months ago."

With two significant regulations awaiting a vote by the European Commission, 2016 promises to be a big year for European cloud providers and users. The regulations are the EU General Data Protection Regulation and the Network Information Security Directive. Will these help to bolster trust in cloud security? The experts believe they will.

"The first starting point for enterprise security in public cloud is asking: what are the responsibility boundaries? What are you, as an enterprise, able to fully control versus what the cloud provider is obligated to manage? And you need to evaluate the controls across the full security spectrum including data security, identity management, and policy application. There will be things you just can't control anymore, especially at the network level."

—Dave Shackleford, SANS Analyst and CEO, Voodoo Security

Cloud Security Investment Priorities

Security investment priorities vary across the different types of cloud deployments. Enterprises are using an average of three security solutions to protect their SaaS applications. The most common is file encryption (60%), followed by email security (55%).

For IaaS, organizations are using an average of four security solutions. Most common are firewalls (70%) and encryption (62%). Private cloud also has an average of four security solutions, with firewalls being the most common (67%).

The top four areas of Security-as-a-Service that organizations plan to invest in are the same ones they are already investing in: email protection, web protection, anti-malware, and application firewall (Figure 8). This trend indicates that enterprises are planning to improve and expand the cloud-based security services they already have in place.

The SANS survey also highlights some key areas for cloud security investment over the next 18 months. These include vulnerability scanning, multifactor authentication, data loss prevention, log management, intrusion detection systems (IDS) and intrusion prevention systems (IPS), security information and event management (SIEM), and cloud access broker services (CASBs).

According to the Gartner report, *Market Guide for Cloud Access Security Brokers*, CASBs, in particular, are a high-growth area. Gartner predicts that, "by 2020, 85% of large enterprises will use a cloud access security broker product for their cloud services, which is up from fewer than 5% today".[2] Our survey backs this up. Despite the fact that CASBs are a relatively new service, 36% of organizations are using such services to protect their SaaS applications, and 32% use these services to monitor shadow IT-procured cloud implementations. Nearly a quarter (24%) of enterprises also plan to invest in a CASB-as-a-Service in the future.

"Understanding what's happening in your cloud environment—for example between the user base and Salesforce—is really critical, and the tools that allow us to manage that more securely are something I'll be looking at more. We also need tools that help automate processes, such as incident response and allow us to do more with what we currently have."

—Vanessa Pegueros, CISO, DocuSign, Inc.

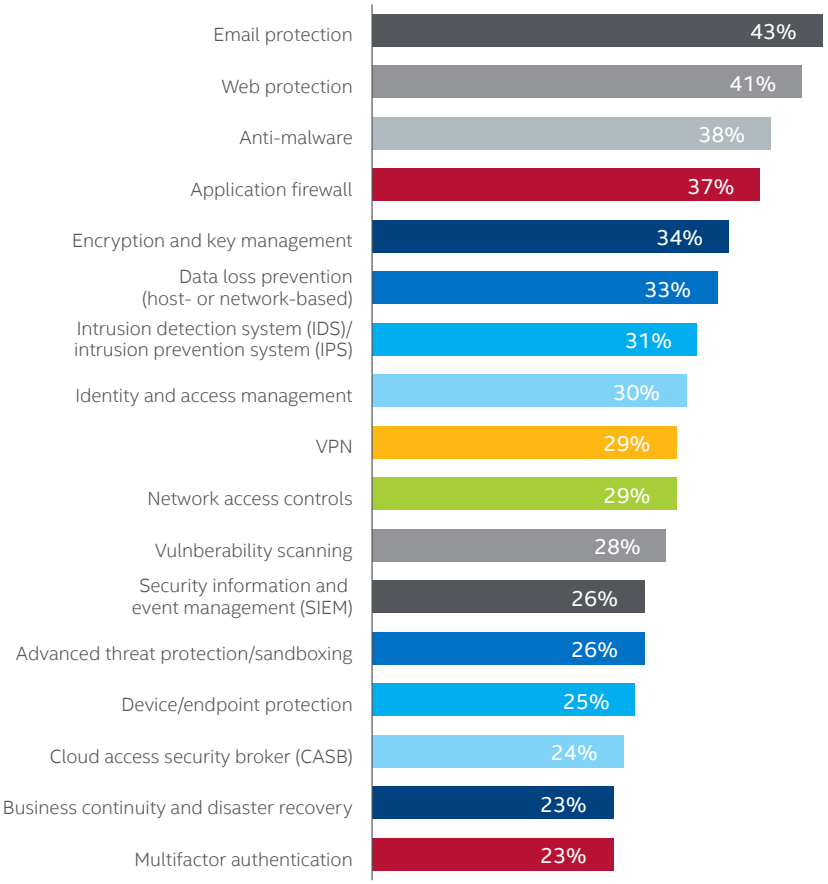


Figure 8. Which areas of Security-as-a-Service does your organization plan to invest in?

Of those organizations using a public cloud service, slightly more than a third (34%) say they have a unified solution with full integration and central management across their hybrid cloud and on-premises systems. So there is room for improvement here.

Summary

Cloud adoption in the enterprise is rapidly approaching a tipping point, with organizations stating that 80% of their IT budget will be taken up by cloud in 16 months or less.

There are many persuasive incentives driving businesses towards the cloud, including greater agility, more rapid innovation, and cost efficiencies. However, with such a vast variety of cloud deployment options, there are inherent security challenges. Since the cloud is or will be the repository of so much vital corporate data, organizations should consider the following:

- Security controls and compliance are shared responsibilities between enterprises and cloud service providers. Ask your service provider about their security controls, and make sure reporting is included in your service level agreement (SLA). However, it is essential for the enterprise to secure what is under their control in the cloud—be it data, applications, or workloads—and to build this into their cloud architecture plans.

"Even though you've outsourced and you are using the cloud, you've not outsourced your responsibility. You don't get to say 'Hey, that was Amazon.'"

—Brent Conran, VP and CISO, Intel

- Key areas for cloud security investment include data encryption, identity and access management, data loss prevention, and email protection. Increasingly, organizations are also investing in Security-as-a-Service and in other services that help orchestrate security across multiple providers and environments, most notably CASBs.
- While shadow IT cloud deployments remain a challenge, as they can potentially expose company data to greater risk, IT organizations should be working with business units to find a more secure way to enable users to implement their own cloud deployments. IT can regain control and visibility by being the broker and redirecting business users to more secure cloud service alternatives.
- While many boards are increasingly involved in cloud security decision-making, there is evidence of a worrisome gap in their awareness and understanding of those risks. More education is needed, as is more involvement of CIOs and CISOs in boardroom discussions with other C-suite executives. The financial fallout and reputational damage suffered by organizations in some recent high-profile data breaches should be an incentive for top executives to make data security—whether internal or in the cloud—a priority.

Methodology

The survey of 1,200 IT decision-makers with responsibility for cloud security in their organizations was conducted by Vanson Bourne in June 2015. Respondents were drawn from Australia, Brazil, Canada, France, Germany, Spain, the UK, and the US and across a range of organizations, from those with 251 to 500 employees to those with more than 5,000 employees.

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. **www.intelsecurity.com**

1. *SANS: Orchestrating Security in the Cloud*, by Dave Shackleford, September 2015 (sponsored by Intel Security)
2. Gartner Report, *Market Guide for Cloud Access Security Brokers*, by Craig Lawson, Neil MacDonald and Brian Lowans, October 22, 2015

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

Intel and the Intel and McAfee logos are trademarks of Intel Corporation or McAfee, Inc. in the US and/or other countries. Other marks and brands may be claimed as the property of others. Copyright © 2016 McAfee, Inc. 62260rpt_cloud_0316_ETMG