The Bi-Directional Cloud Highway:

User Attitudes about Securing Hybrid- and Multi-Cloud Environments

White Paper

Q2-2019

Jeff Wilson
Senior Research Director,
Cybersecurity Technology

IHS Markit Technology | **White Paper**

Contents

Introduction

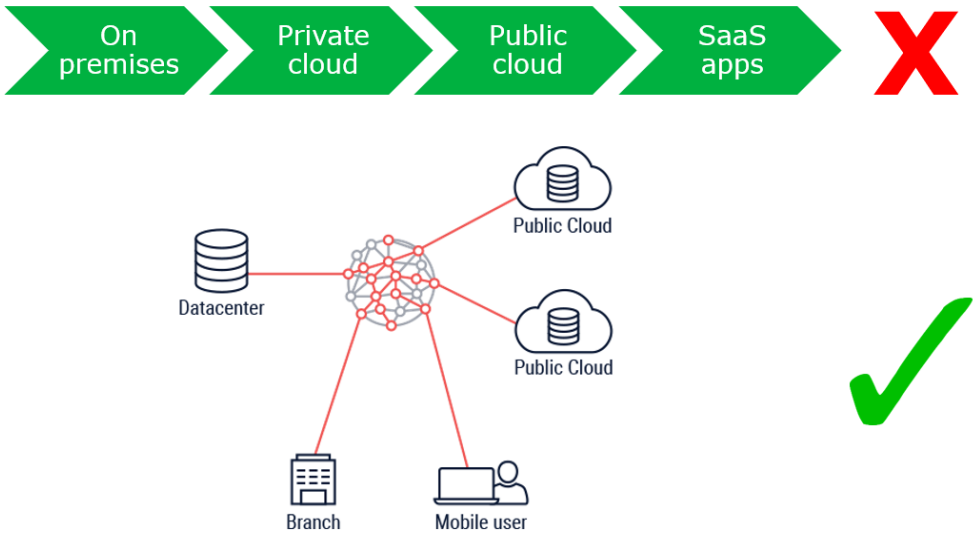
Since the birth of business computing, many profound, new technologies have shifted the way organizations operate day to day, but the development of the cloud over the last 15 years is among the most significant convergences of computing and communications technologies ever. Organizations of all types are taking a serious look at how they can leverage moving infrastructure, applications, and data into the cloud to improve their business; it's unavoidable because the potential benefits are revolutionary. Along with those benefits come significant challenges that impact the processes and technologies required to manage and secure IT infrastructure in the cloud.

To get a sense of the current thinking about the cloud and cloud security, we surveyed 350 enterprises (1,000+ employees in the US, 500+ in all other regions), and we present the highlights of those results, some of which run counter to past technology adoption trends and basic intuition about how cloud and cloud security adoption might play out.

When new technologies emerge, there is usually a clear path from left to right: the left side is the old way (worse), the right side is the new way (better), and everyone is moving from the old to the new. In the early days of the cloud, many assumed deployment would follow this pattern and that the cloud would be the best choice for all IT infrastructure. This could be the case over the very long term, but for the time being, infrastructure, applications, and data will move back and forth from on-premises to private/public cloud infrastructure based on a variety of circumstances and opportunities.

Organizations are just beginning to understand where and how it is appropriate to use the cloud. There are many anecdotal examples of enterprises moving applications into the cloud and then back out for reasons including time- or event-driven applications, mergers and acquisitions, new security concerns, poor performance in the cloud, shifting regulations, changes in deployment cost or pricing, development of new applications, and changes in underlying technology. This is the reality that many companies live in—the dynamic multi-cloud. The goal of this survey is to dig some concrete trends out of these anecdotal examples.

Exhibit 1 The dynamic multi-cloud

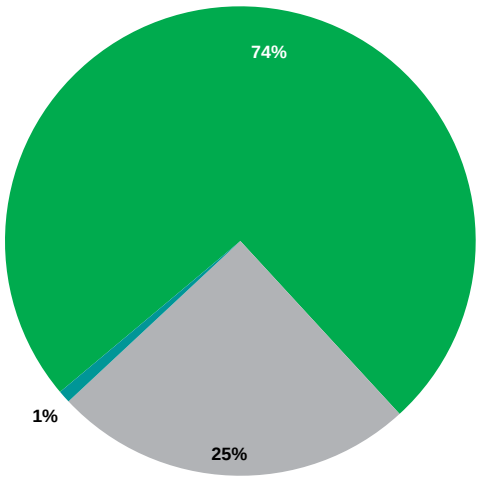


Source: IHS Markit

By now, most companies have tested the cloud and have even made significant investments in using cloud technology in production environments. so it's a good time to step back and talk to architects of IT infrastructure and strategy (C- and VP-level IT, cloud, and IT security professionals) at a large pool of companies worldwide to see how they are taking advantage of the cloud and what security challenges they face as a result.

The first interesting finding is the growing sense that the dynamic multi-cloud reflects reality. Of the 350 companies we surveyed, 74% had moved an application into the cloud and then moved it back into their own infrastructure. This doesn't mean they've reversed all their cloud deployments, just that there are cases for bi-directional movement. Companies deploying in the cloud and the technology providers that help them with infrastructure, management, and security should consider this is a basic condition and need to build products and services with this bi-directional movement in mind.

Exhibit 2 Moving applications back from the cloud



n=350
Source: IHS Markit
© 2019 IHS Markit

Even major cloud providers are acknowledging the reality of dynamic multi-cloud. In December of 2018, AWS announced it would make cloud hardware platforms that companies could use for on-premises deployments. This announcement confirms that there are cases where applications need to stay on premises (or move back) while still allowing customers to take advantage of the AWS platform. Microsoft has a similar offering with Azure stack although it requires customers to purchase hardware from partners. The point in both cases is the same: hybrid is here to stay, and applications and infrastructure will continue dynamic movement from on premises to the public cloud.

We then asked respondents about the factors driving them to move applications back into their own infrastructure. The top two responses, each selected by 52% of respondents, were performance and security. Performance issues will likely improve over time as cloud infrastructure improves. Companies that leverage the cloud will increasingly use cloud infrastructure opportunistically, switching vendors to take advantage of higher performance or better cost. Security is a more vexing problem because many companies don't even have a good handle on who should bear the burden of ensuring proper security in the cloud (which will be discussed in more detail later), much less a strong end-to-end vision of what technologies are required to secure their cloud deployments.

Forty percent of respondents noted that in some cases the cloud deployments they moved back into their own infrastructure were "planned temporary" deployments. Temporary infrastructure set up during the inevitable IT transition associated with a merger or acquisition is a great example of planned temporary cloud deployments, but there are many more. Regulatory issues came up for 21% percent of respondents; this is an example of how the "dynamic" part of the dynamic multi-cloud may not always be in your control.

Every application is a new cloud reality

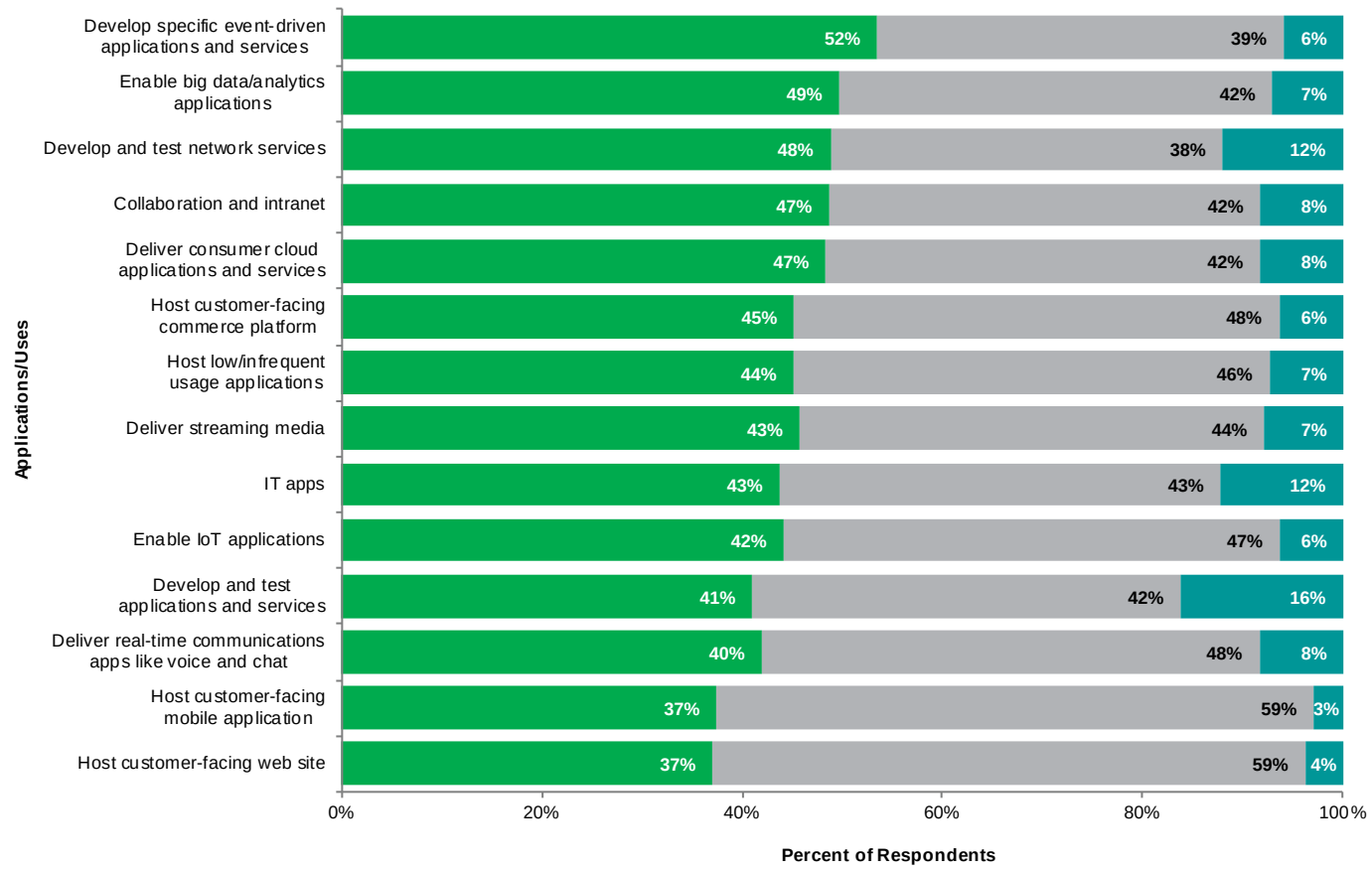
Whether you're talking to the cloud providers, the companies buying cloud infrastructure, or the companies supplying the necessary technologies to make a cloud deployment work, one topic that comes up over and over is that there is no single, clear picture of what the most common applications and uses of cloud infrastructure are. Once you get past some basic cloud truths (that most companies are moving to Office365 or that Salesforce is pervasive) there are infinite ways to use the cloud, and companies are exploring all of them.

Although this flexibility is one of the long-term strengths of cloud architecture, it makes it difficult to tease out trends that everyone needs to understand in order to speed up deployment, make cloud applications and infrastructure manageable, and—most importantly—secure cloud deployments. The shared nature of cloud infrastructure ensures that no one really gets a complete picture of what is happening on it.

To get a better sense of how respondents are using the cloud, we presented them with a list of common applications and uses for cloud infrastructure and asked which they were using. For the ones they were using, we asked what role the cloud played: full replacement or full-time hybrid deployment, augmenting a primary in-house deployment (for bursting over or disaster recovery), or as an ad hoc/temporary deployment. The basic idea here is that the farther the application is up the list, the more likely it is a "cloud-first" or "cloud-native" deployment.

Asking the question this way generates some interesting insights as there are some less-common uses that bubble up to the top (like event-driven applications/services and service development and testing), as well as applications that really leverage the power of the cloud (like enabling big data/analytics applications). Well understood legacy applications with more history (like customer-facing web sites, IT applications, and communications applications) fall farther down the list. When companies go cloud first, it's often to explore new ways of using technology. For more established applications, they leverage the cloud opportunistically to enhance an in-house deployment by providing redundancy or additional capacity.

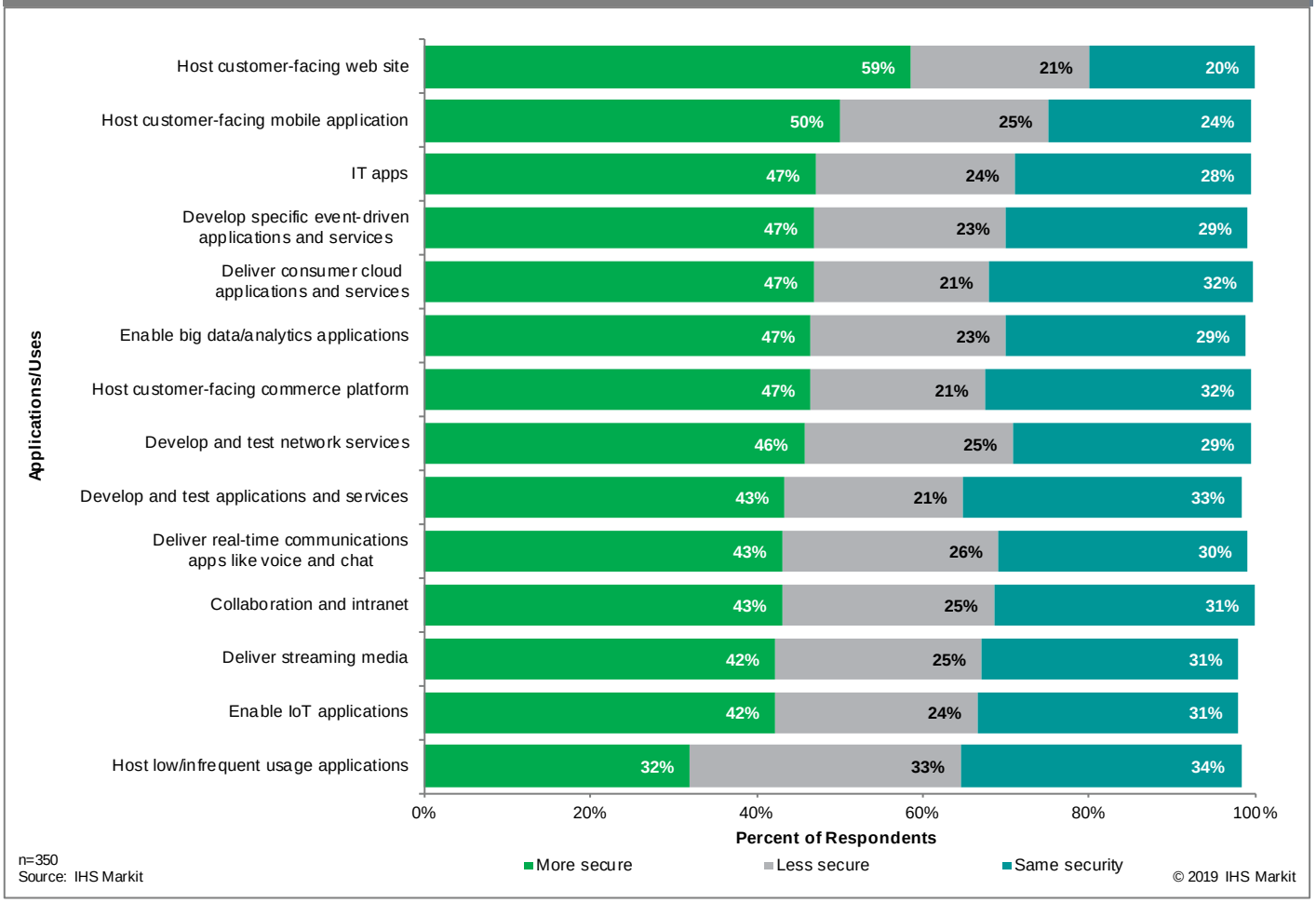
Exhibit 3 Which applications/uses are closest to “cloud first”?



n=350
Source: IHS Markit

So far, we've looked at questions that deal with cloud deployment, but the pervasive narrative is that security concerns are the key issue when companies hesitate with cloud deployments. We asked respondents (who are a mix of IT, cloud, and security focused professionals) to talk about their perceptions of security in the cloud for each application/use: were they more secure in the cloud, less secure, or roughly the same?

Exhibit 4 Perception of security in the cloud by application/use



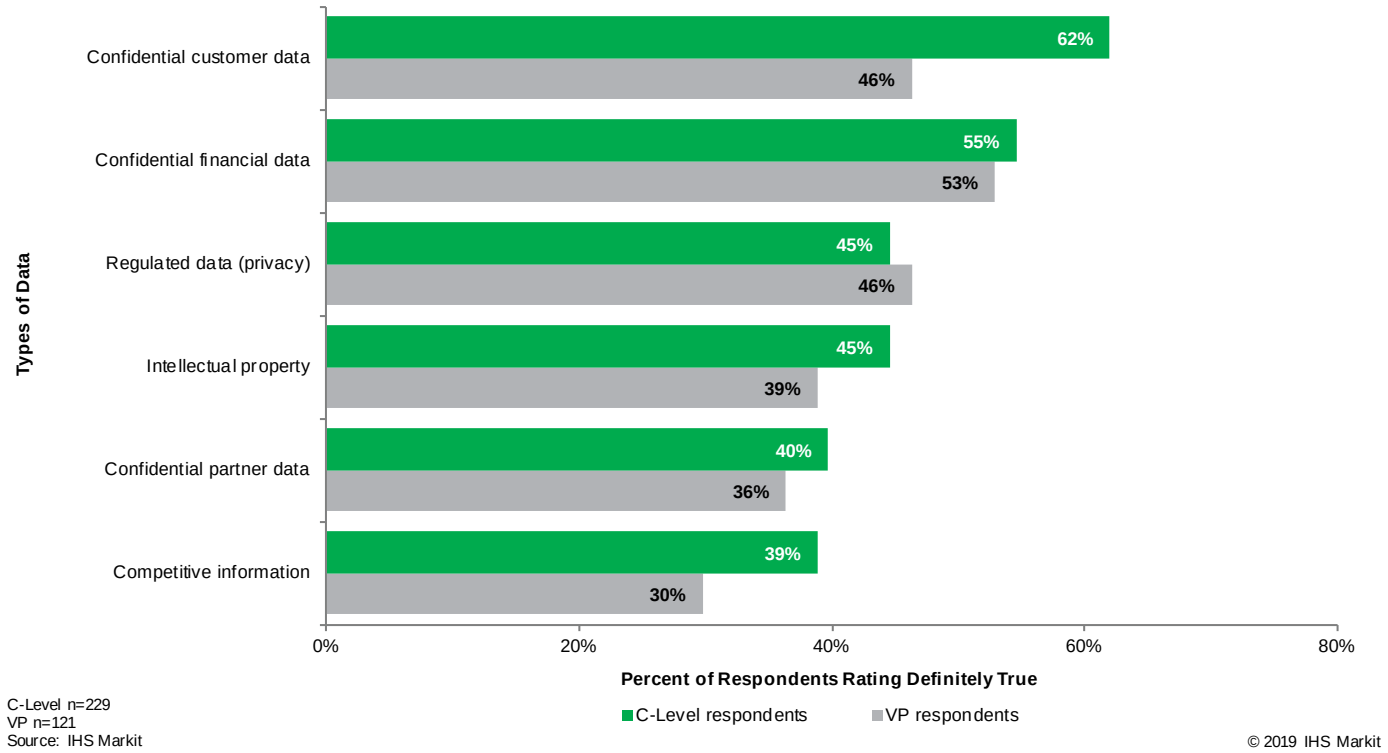
Here the chart flips in roughly the opposite order of the last question, with the more established and well-understood uses generally leaning toward "more secure in the cloud" and the fringe cases (the ones that more often fit the "cloud first" profile) perceived as less secure in the cloud. To some degree, this is because the security models for those well-understood legacy applications (for both on premises and in the cloud) are better understood, more widely deployed, and more mature.

The base issue, though, creates problems for implementation (assuming those applications and uses are indeed less secure in the cloud) because the applications and uses respondents want to go "all in" on in the cloud will likely require more time and money investment on the security front to meet security goals. If these fringe cases aren't seen as business critical, can the investment in security for them be justified, or will these cloud projects be left behind? There's no single answer because every use case is different, but it's an interesting way to frame understanding of cloud security for the various applications you may be considering.

The power dilemma: Business priorities and technology realities

This dilemma manifests in many ways, perhaps most powerfully in the constant tug of business priorities versus technology realities, a concept that is at the heart of most successful (and stalled) cloud deployments. One way to look at this dilemma is to separate the data roughly by title: the C-level executives (CEO, CIO, CISO, CTO) who responded to the survey and the VP-level executives (VP of IT, VP of IT Security, VP of Cloud). Even though all our respondents were high level, the VP-level executives generally have a better window into the difficulties of implementation and operations than their C-level counterparts. With that in mind, we'll look at one question where the difference in the responses between C-level and VP-level were significant on one key item. We asked respondents their thoughts on storing specific types of sensitive information in the cloud, and although VP- and C-level respondents agreed on most items, a much higher percentage of C-level respondents would "definitely" store customer data in the cloud.

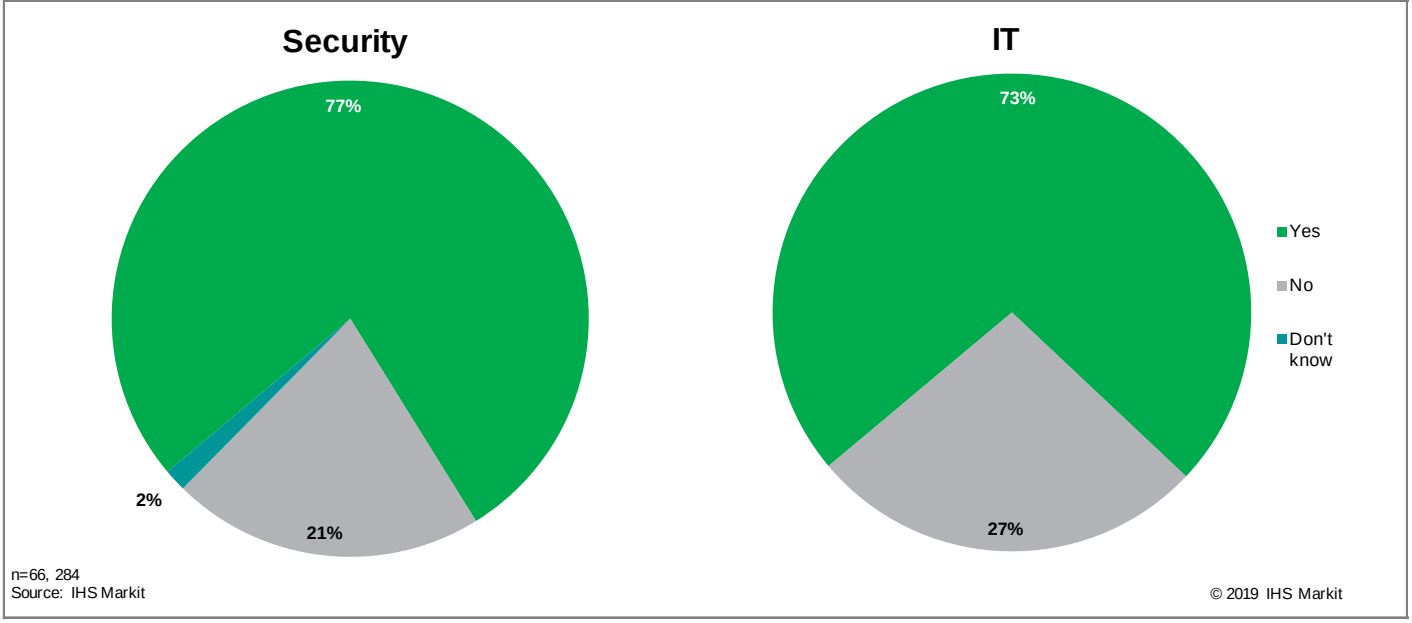
Exhibit 5 Storing data in the cloud: VP-level versus C-level



Many factors influence this answer (such as industry and regulations), but in cases where storing in the cloud doesn't violate regulations, why is there a difference between the two groups? In most cases, it's because there is a business mandate to store that data in the cloud for reasons outside of security (chosen technology partner, chosen application for ERP or CRM, a need to make customer information available to third parties, etc.). These mandates are typically developed at the C-level and then handed down to the implementors to figure out. The issue for the VP-level respondents is that they may not want to store customer data in the cloud, but they may not have a choice in the matter, which is why they lean on their cloud and security technology partners to deliver technology that helps combat their trepidation.

Another way to separate the respondent group is to pull all respondents who had a security-focused title of any level (CISO, VP of security) into one group ("security" in the chart below) and leave everyone else in a second group (labelled "IT"). Following our line of questioning around security concerns, we asked respondents if they had ever moved applications or infrastructure into the cloud despite specific security concerns with the deployment. 77% of security respondents said yes compared to 73% of IT respondents. The result is high for both groups, but the security teams deploying despite concerns will likely be paying close attention to those deployments.

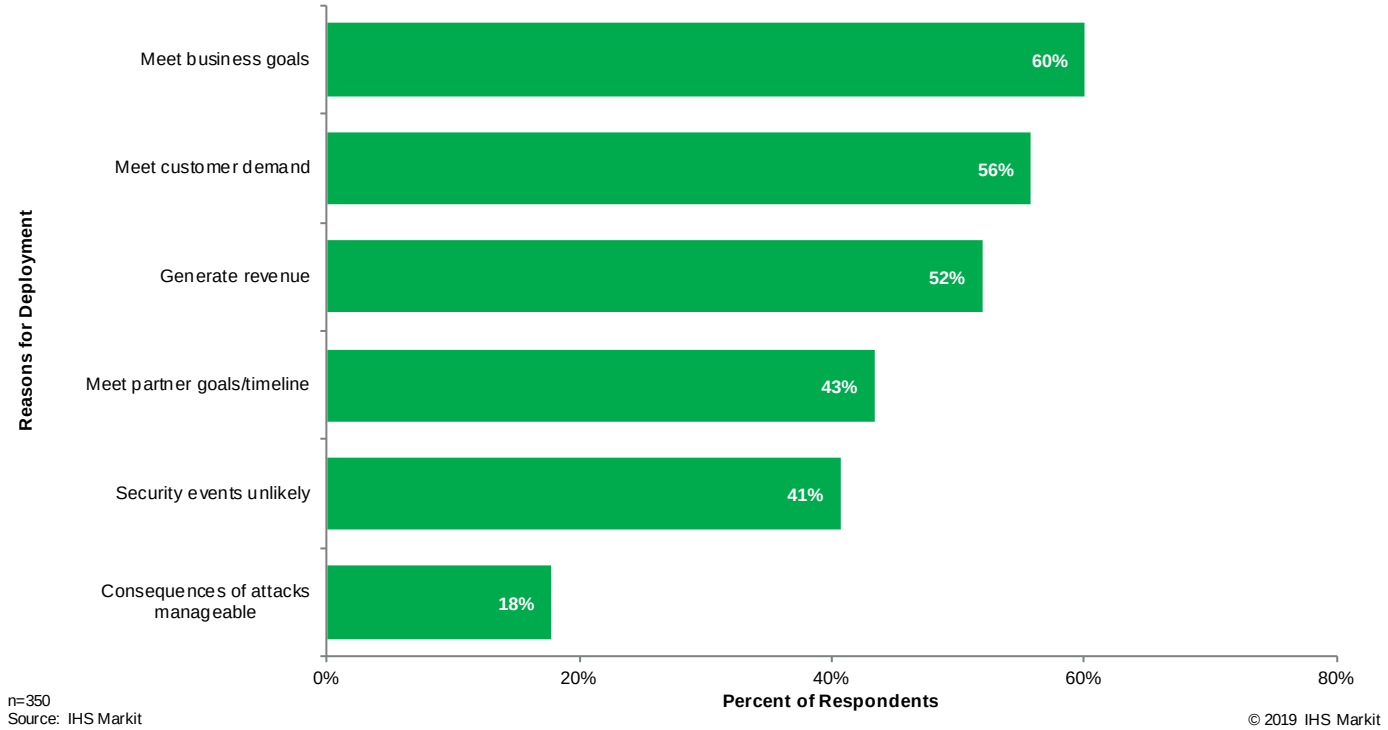
Exhibit 6 Move to cloud despite security concerns: Security versus IT respondents



The notion that access nearly always trumps security was true in private infrastructure, and it does not appear to be changing in this transition to the cloud. We asked a follow-on question to understand what causes deployments to move forward despite the concerns. The top three responses indicate that these risky cloud deployments *support key business goals*, help *meet customer demand*, or directly *generate revenue*. Most IT infrastructure exists to support these goals, and the rapid adoption of the cloud indicates that the cloud is doing an excellent job overall.

Respondents don't believe that they won't be breached (only 41% said they move forward with the deployment because security events are unlikely), and they understand a breach in the cloud will come with significant consequences (only 18% move forward because they think the aftermath of an event will be manageable). They simply must deploy in the cloud to meet business goals and hope they can sort out security along the way before anything significant happens.

Exhibit 7 What drives the move when concerns exist?



In both cases (C-level versus VP-level and security versus the world), the simple reality is that cloud implementors and security teams must contend with applications destined for the cloud, and they will have an increasingly short window to figure out what technology they already have in place to manage the deployment and what they will need to build (in a DevOps world), buy from technology partners, or lean on their cloud service providers for.

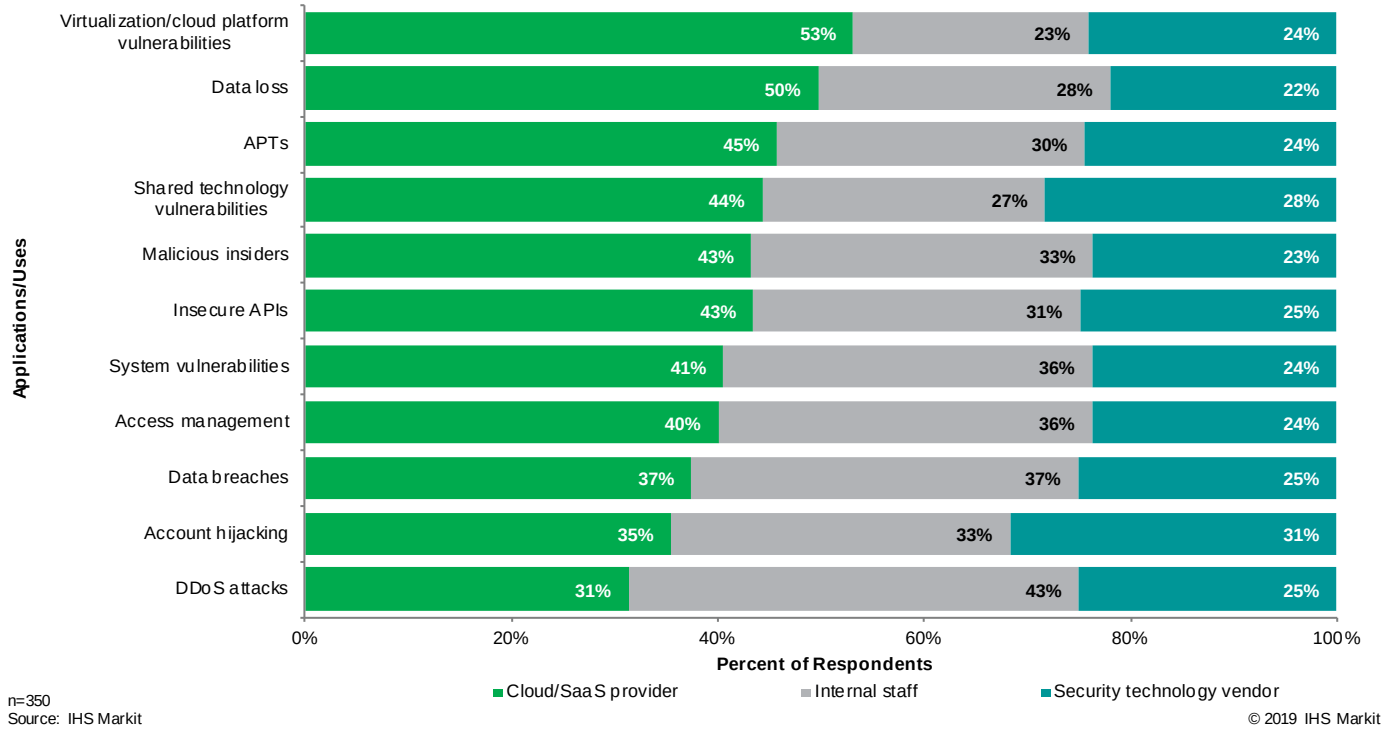
The responsibility conundrum: Balancing internal and external roles

There are a wide range of security solutions available for all types of cloud deployments. Any trip to a cybersecurity-focused trade show will reveal that "cloud security" is every security technology company's number-one priority. If any of these respondents were to go to AWS or Azure tomorrow to carve out a bit of space for an ad hoc application or to test a new application or service, the list of security vendors that are check-box add-ons through the cloud's marketplace is exhaustive. The cloud providers themselves offer a range of security solutions (built into their platforms or added on), and many of the cloud management platforms, hypervisors, orchestration tools, and other bits of cloud infrastructure have various levels of security available.

Successful cloud deployments rely on a network of vendors, partners, and infrastructure providers, but who do respondents think is truly responsible when there is a vulnerability or security event in their cloud deployment? The answer is no one and everyone. In the best-case scenario where it is clear who should be responsible (such as a vulnerability in the virtualization/cloud platform), only about half of respondents pin the blame where it truly belongs: on the company who built the vulnerable platform (like VMware or AWS). This is a cynical response, built on long experience working with flawed technology riddled with vulnerabilities for which IT and security teams accept responsibility in most cases where they own the data and applications running on top of the vulnerable platform.

There's a bit of learning that needs to happen as a higher percentage of respondents are looking to their cloud provider to be responsible for higher layer threats (like APTs) when cloud providers are more likely to excel at infrastructure protection (DDoS attacks), but the understanding of each entity's abilities, and ultimately strengths, when it comes to responding to security events in the cloud will build over time.

Exhibit 8 Who is primarily responsible in different attack scenarios

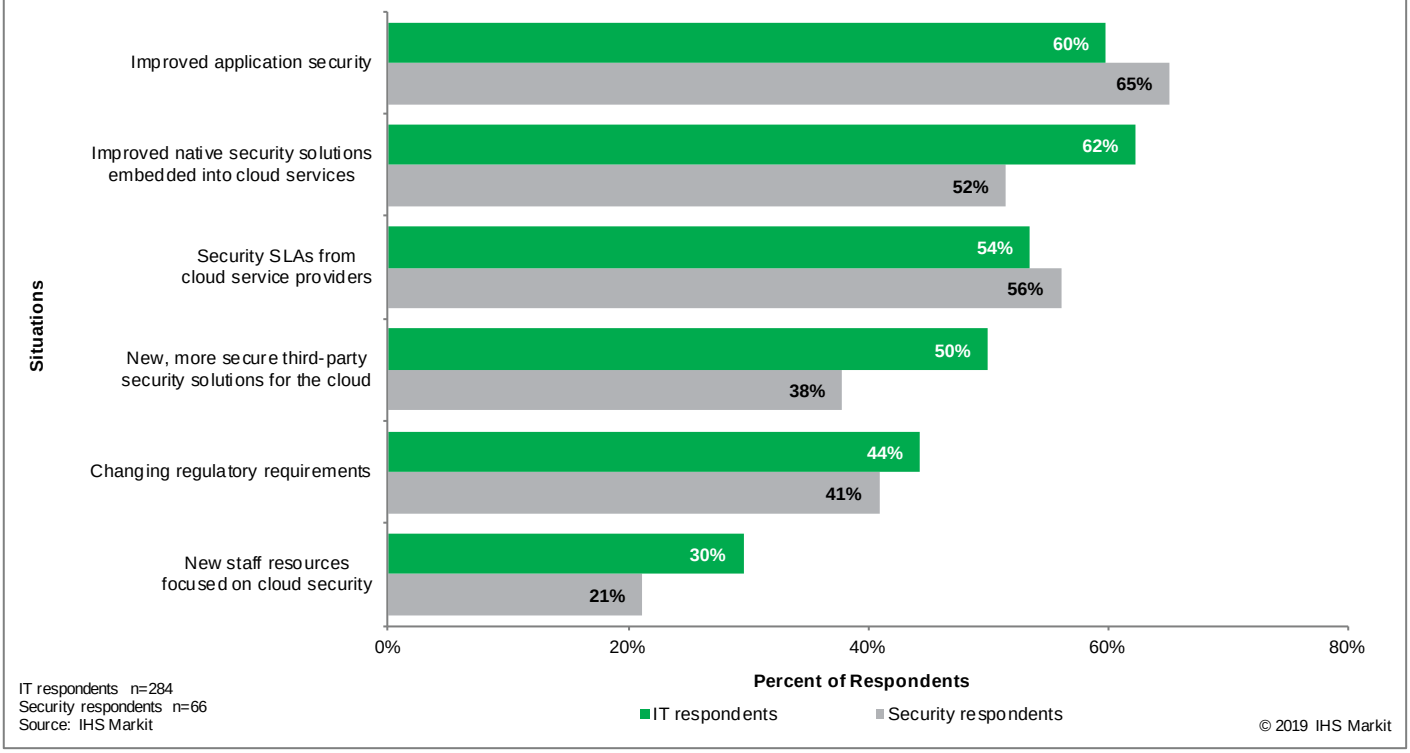


n=350
Source: IHS Markit

We believe the best course of action is to build a playbook for security events in the cloud that plots actions and responsibilities for all parties involved and then to ultimately digitize that playbook and use technology to orchestrate responses between all parties. Whichever pieces of the response that can be automated should be—the truth is the cloud is shared infrastructure, and when it comes to security events there will always be shared responsibility.

We looked at one final question splitting the data by the security respondents and IT. The question was simple: for assets/data that you refuse to store in the cloud, what would cause you to reconsider? The difference is stark: security respondents in most cases feel like they understand what should and shouldn't go into the cloud, and they're relatively unmoved by improvements and changes. The non-security respondents are open to reconsidering, largely because they're more likely to feel the weight of the need to "meet business goals," which is the wedge that will be used when these security practitioners are forced to move another block of data into the cloud that they think shouldn't be there.

Exhibit 9 What would cause you to reconsider the cloud: Security versus IT



Conclusion: Plotting the course for a secure cloud

The cloud is starting to feel like the end of the list that starts with “death and taxes”: inevitable. Technology staff at most companies around the globe are using, evaluating, or developing multiple cloud applications. As inevitable as the cloud is, it’s not simple to understand; the cloud supports infinite applications and infinite deployment models running on shared semi-public infrastructure. Successfully navigating secure cloud deployments requires the right planning, staff, partners, and support from your organization, but based on the results of this survey and our experience analyzing cloud security solutions, here are a few things that can help smooth the ride toward the dynamic multi-cloud:

- Plan for change—to truly take advantage of the best of the cloud, make sure the tools and technologies you use for infrastructure are mobile; they should work in multiple public cloud environments, in private clouds, and on premises.
- Take a look at all the cloud projects you have completed or are in progress and see where they fall on the spectrum of “cloud first” versus “cloud supported;” it will likely help organize your thinking around security models for those applications that can be scaled and repeated.
- Make a clear plan for each use case that lays out how security responsibility will be shared among your DevOps staff, your IT/security staff, the cloud provider, your security technology partners, and anyone else involved.
- Look continuously at what functionality (particularly security) is being embedded into parts of the cloud technology chain (the cloud provider’s platform, orchestration tools, your existing security products); security features are often used as a way to differentiate and keep customers loyal, and you can use this to continuously bolster the security of your cloud deployments.
- Work to ease the natural tension between different groups within your organization; cloud deployments require the most coordination between executives, business units, and IT and security staff of all levels, who must understand that “meeting business goals” means different things to different people.
- Take concerns about security that anyone on your staff has seriously, but try to foster a culture of curiosity around the cloud and cloud deployments. Remember that all supporting cloud technologies (and security especially) are changing and advancing rapidly and should be reexamined constantly to see if a “no because of security concerns” can change to a “yes.”

Demographics and Survey Overview

Using a panel of qualified IT decision-makers, we conducted a web survey in March 2019 with 350 organizations around the globe. To qualify, respondents must be C- or VP-level decision-makers responsible for managing or planning cloud and cloud security products and/or services at their organizations; 65% of respondents were C-level (CIO, CSO, CTO, CISO), and 35% were VP-level (VP of IT, VP of Cloud Architecture, VP of IT Security). Respondents must also have detailed knowledge of and purchase decision influence for their organizations' cloud and cloud security products or services. The table below details our sample:

Exhibit 10 Respondent demographics

Country	Number of Respondents	Company Size
United States	105	1,000 and up
England	35	500 and up
France	35	500 and up
Germany	35	500 and up
Australia	35	500 and up
Hong Kong	35	500 and up
New Zealand	35	500 and up
Singapore	35	500 and up
Category	35	500 and up

Source: IHS Markit

For this survey, we focus on companies' use of the cloud to deliver applications, data, and infrastructure to their users, customers, or partners using the four primary cloud service models:

- IaaS: Infrastructure as a service delivers data center (DC) facilities, servers, network, storage, database, network applications (layer 4–7), and management
- CaaS: Cloud as a service provides a bundled application execution environment; includes servers, network, storage, management, and orchestration; this service is purchased as a bundle and pricing is based on usage
- PaaS: Platform as a service provides an application development and execution environment; includes application middleware (web servers, database management systems), servers, network, storage, management, and orchestration platforms; this service is purchased as a bundle and pricing is based on usage
- SaaS: Software as a service provides a complete application with a pay-per-use pricing model

This report, which looks at end-user attitudes toward cloud and cloud security deployment, was produced as custom research at the request of Fortinet. IHS Markit is exclusively responsible for this report and all of the analysis and content contained herein. The analysis and metrics developed during the course of this research represent the independent views of IHS Markit and Jeff Wilson, Senior Research Director, Cybersecurity Technology.

Contacts

Jeff Wilson
Senior Research Director, Cybersecurity
Technology
+1 408.583.3337
Jeff.Wilson@ihsmarkit.com

IHS Markit Customer Care:

CustomerCare@ihsmarkit.com
Americas: +1 800 IHS CARE (+1 800 447 2273)
Europe, Middle East, and Africa: +44 (0) 1344 328 300
Asia and the Pacific Rim: +604 291 3600

IHS Markit