REPORT REPRINT

Moving to the cloud: What are the speed bumps?

WILLIAM FELLOWS, CARL BROOKS

29 DEC 2016

While 451 Research data finds that 'cloud first' is becoming the 'new normal' for many organizations, significant challenges remain for organizations making this shift, especially those in regulated industries.

451 Research®

Cloud computing is causing a rethink and gradual change with regard to how IT is consumed. Enterprises are getting started with cloud and as-a-service deployments wherever possible instead of starting new datacenter builds or developing infrastructure services that offer no differentiated value. Enterprises are increasing their use of third-party vendors to host business services, using private and public tenant options to complement or replace on-premises systems rather than source hardware and software themselves. Many organizations are using multiple cloud services; indeed, 'Amazon +1' is gaining use as an operating principle for CIOs evaluating services to meet different workload needs and to support fiduciary responsibility. While AWS may have become the lingua franca for public cloud, all-in refers to the operating model of cloud, not going all-in on a single vendor.

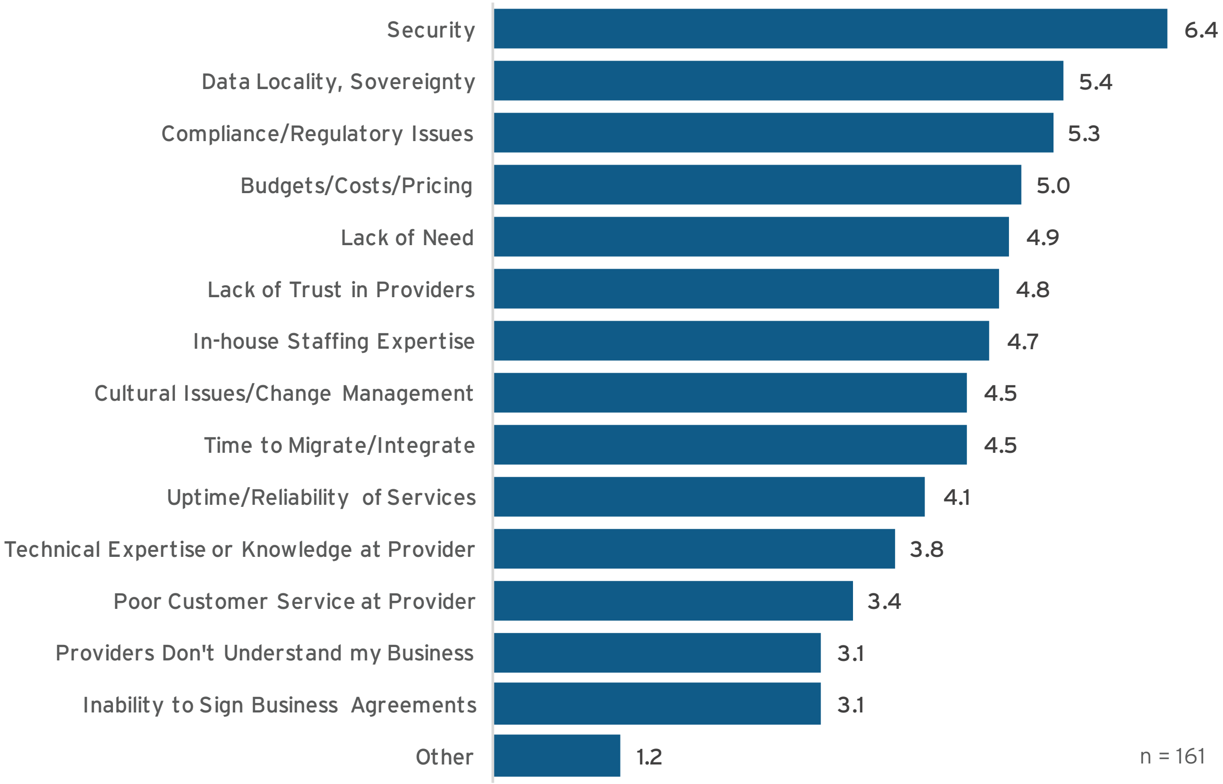
At its most fundamental, cloud is a consumption-based service-delivery model with a retail-model discipline. It is being used to align business and technology to create new products, support change to meet new market demands and become agile – at speed. The experience of cloud users is 'build faster, run better at lower cost.' At the same time, the change required, plus the complexity and confusion in moving to cloud, represents the biggest IT opportunity in decades.

Atop the list of key concerns and inhibitors for using cloud among noncloud enterprise end users surveyed by 451 Research's Voice of the Enterprise service is security (Figure 1). We believe security has moved back to the top of CIO priority lists for their organizations, displacing agility and flexibility.

Figure 1: Impact of Inhibitors

Source: 451 Research, Voice of the Enterprise: Cloud Computing Q4 2015

Pleast rate how much of an impact the following have on inhibiting your organization's use of cloud computing. Please use a 0-10 scale where '0' is "No Impact" and '10' is "Significant Impact"

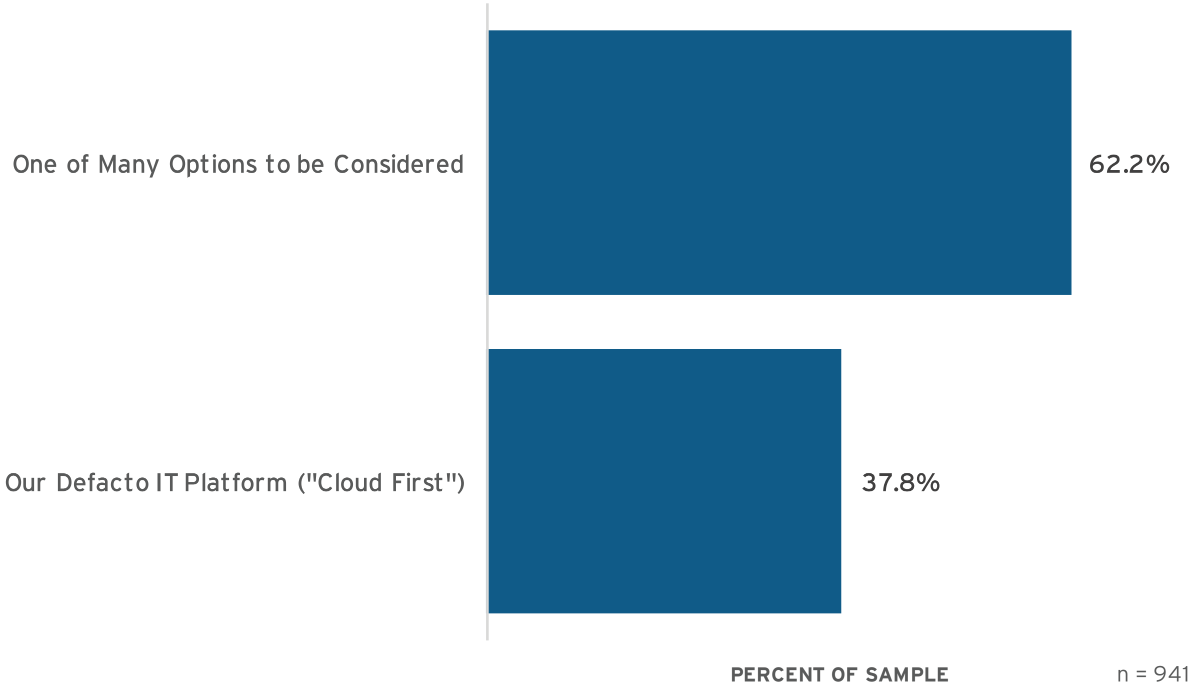


THE 451 TAKE

While 451 Research data finds that 'cloud first' is becoming the 'new normal' for many organizations (Figure 2), significant challenges remain for organizations making this shift, especially those in regulated industries. There are inhibitors that have an impact on an organization's ability to adopt cloud in the first place. Then there are the 'speed bumps' that slow the ability to move through the phases of adoption – from virtualized noncloud to self-service, automated service delivery and orchestration; from T&D and new application deployment to application modernization and migration of existing applications; or from departments and projects to organization-wide rollout. This report examines some of the key issues, arguments and best practices.

Figure 2: "Cloud First" Frequency

Source: 451 Research, Voice of the Enterprise: Cloud, Workloads and Key Projects 2016



SECURITY

Security is concerned with the physical IT assets, the availability of services, data governance and protection, and more. For enterprise organizations gathered at 451 Research's Cloud Executive Summits this year, data protection was the overarching security challenge, and can be summarized as 'the Dropbox problem' writ large. 'What kind of control will I have when my data leaves the firewall, and how confident can I be that public cloud providers support the level of security that I get on my private cloud?'

PUBLIC CLOUD SECURITY

Public clouds like AWS and Azure are secure by default because they have a vested business interest in being as durable as possible. Thanks both to geographic distribution and scale of operations, as well as the nature of doing business with millions of customers at once, they must operate at a level that starts with a security posture that rules out as much inconsistency and variability in outcome as possible, including a crystal-clear demarcation between customer responsibilities and provider responsibilities. They have large pools of skilled experts that identify, contain and eradicate security threats. They provide incident response and malware protection, and are acting upon the experience of performing analysis through security intelligence systems powered by massive compute resources and data sets. Moreover, because they are so massive and automated, they have a range of deployment models and disaster-recovery profiles that can be selected – hot, warm and cold. They are embedding foundational security intelligence into their as-a-service operations, protecting their own infrastructure, and alerting customers to potential hazards and attacks. Moreover, they are designed for the kind of failure that results from all of the above. 'Expect failure to happen,' has been the mantra of AWS CTO Werner Vogels as the design point for cloud infrastructure and applications.

AWS, Azure and Google (and others) have never lost a significant amount of customer data because they tell users that they are only responsible for providing the platform, not for holding their users' hands. In other words, 'I can screw up my own stuff on AWS, but AWS won't.'

If AWS didn't make the best possible choices about securing the underlying platform, it would fail to gather new business at the rate it does; it would simply fail by natural economic consequences. Contrast this with a private cloud, where security is a design choice weighed in balance with other considerations in the overall investment, and it's far more likely that corners will be cut or inexperience will win out, and the opportunity to be battle tested will be measured in one or two intrusions or exploits instead of millions upon millions of rebuffed attacks. As an analogy, there is one door in my house with a lock and key fitted to it, and I have the key, as well as a few others; in a hotel, every single door has a lock and key, and the hotel management is the only entity that can give out those keys and demand their return.

That said, it cannot be emphasized enough that the demarcation of responsibility is the great differentiator between public and private. AWS and Azure are far more secure and robust as platforms than almost anything an enterprise can build by default. However, there is a shared security model in place at the hyperscalers that nevertheless puts demands on end users. The portion of this responsibility from AWS and Azure does not go beyond securing the infrastructure itself. End users are obligated to integrate security measures on their own to protect applications and workloads. Moreover, the fact is that users of these platforms can still fail quite handily by running insecure applications or making poor management choices. Public cloud providers make their living by removing uncertainty from infrastructure – not from people.

Perhaps more than in any other previous IT era, the world of consumption-based, on-demand as-a-service approaches demands strict security protocols. Organizations that are operating in this environment will require comprehensive, proactive and adaptive threat protection embedded into the fabric of the businesses. However, companies will have different risk profiles – the result of being in a particular industry or geography, or simply culture. They will reflect whatever legacy, organizational, or institutionalized policy or behavior is extant, and there are different options in the market to meet different needs. This ultimately is gating their use (or not) of public cloud.

BRIDGING THE OLD WORLD AND THE NEW

Most companies are not cloud-native, but as a result of the shift to cloud, they have one foot in the old world of IT and one in the new-style as-a-service world. As a result, they are facing challenges in bridging what are essentially two operating models. Traditional IT policies, institutional knowledge and written documents that are typically the canon of old-style IT operations don't lend themselves to automation and real-time behavior. Moreover, we have learned that 'paving the cow paths' – applying new technology without changing the process – doesn't work.

Cloud requires users to move from hard-wired, top-down 'waterfall' approaches to automated, agile operations to support continuous development, delivery and integration; from allocated budgets to consumption-based services; from transactional license purchases to transformational relationships; and from product-driven to service-driven approaches. In short, they have to shift from the world of ITIL to the world of agile.

Companies that want to do cloud must embrace DevOps. This is the process; it is here that applications and infrastructure are abstracted in such a way that it becomes possible to deliver continuous improvement – with automation and self-service – at speed. Removing barriers to scaling applications can allow product and marketing teams to take calculated risks and reach new markets before opportunities are lost. It's widely held that organizations must be willing to disrupt their own business models, processes and especially cultures in order to make this change. A clash of cultures between developers and IT operations is inevitable in this. The essence of the shift means embracing failure as a cultural competency. This 'culture of failure' allows continuous experimentation, to learn quickly what works and what doesn't without wasting a lot of money and time. Failure, then, can bring rewards too.

Advisory and planning tools will be required to help answer the questions about which apps should move to the cloud, which cloud to use and what the cost will be. Enterprises want a verifiable and rapid ROI. This is why consumption planning, optimization, measurement and chargeback – providing multi-level cost visibility across all projects and providers – is becoming a precondition for launching a cloud initiative, and will be crucial when using multiple cloud services.

Services that help users match IT business needs to the right cloud service, balancing performance and cost (what we call 'best execution venue strategies'), will be essential. The ability to find, select and use those services – with control – is the desired state.

There is an increasing buyer appetite to improve the automation of service delivery in order to improve end-user satisfaction without having to grow IT staffing levels, which supports this shift. The ultimate goal for the IT department is to continue maximizing its reduction in operational expenditure while minimizing business impact. As IT becomes more like a broker of services, the role of IT is changing within, and staffing (who can bridge the old world and the new) will be a significant issue, both in acquisition of new talent and retention of the existing workforce.

451 Advisors' work with enterprises shows that centers of excellence can help drive change here. Furthermore, organizations that find cross-functional opportunities will be able to stimulate organization-wide collaborative change. Working collaboratively with external providers that can help augment internal expertise (and skills gaps) should be a consideration when evaluating suppliers.

AVOIDING VENDOR LOCK-IN

Avoiding vendor lock-in is a business imperative, not an option. If only for fiduciary responsibility, organizations are adopting multiple cloud services. This is especially true for large enterprises, which are now spending millions of dollars a year on cloud services, where cloud spending has become a visible line item on the balance sheet and the CIO/CFO – fearing lock-in – is asking whether this cloud is providing best value, what other options are available and at what cost.

Lock-in is also about control. Self-service access to and provisioning of services based on role should be a precondition, and while many vendors talk about offering a 'single pane of glass,' the danger is that it can too easily become a 'single glass of pain.' This is why modular approaches that enable customers to use multiple tools (and their own where necessary) will be key to success.

A cloud management platform enables organizations to find, access, and manage public, private and hybrid cloud resources, and is a way to help address the challenges of moving to cloud. The greater the number of functions available to the user as part of the CMP, the better it can navigate this shift to cloud. It can provide a range of functions, from aggregation, integration, fulfillment and delivery to handling more complex things, such as dependencies, resource constraints and consumption optimization, as well as taking the sting out of contract complexity and vendor management. It can support a mix of old-style and new-style IT services and the use of planned and unplanned options. A CMP enables users to make data-driven decisions in the selection of cloud applications and services. This includes (but is not limited to) cost, compliance, utility, governance and auditability. The point is that rules are applied to every application; as a result, users will be able to begin to move from compliance in selecting multiple individual services to risk assessment in selecting federated services to meet a requirement.