Perception or Reality?

The Truth About Cloud
Adoption Concerns

High performance. Delivered.

CONTENTS

Executive Summary

Cloud technology is pervasive and is here to stay. According to independent analyst firm Forrester Research, Inc., 79% of technology and business decision-makers identify upgrading or replacing their legacy systems to cloud technology in 2015 as a priority.[1] Accenture's 2015 Enterprise Cloud Report echoes this statistic, revealing that 82% of organizations worldwide identify cloud technology as a key part of their IT strategy and 75% are already implementing or using at least one cloud application.[2] As adoption continues to grow, those organizations who don't make the move will become less competitive.

Given the numerous benefits that organizations report from adopting cloud technology, with improved collaboration, efficiency, engagement, innovation and intelligence topping the list,[3] moving more systems to the cloud is quite compelling. But if the improvements are so significant, why haven't more organizations made the move already?

A 2014 study from IDG Enterprise uncovered numerous disconnects from an IT senior management perspective that are holding back cloud-based infrastructure and applications from greater adoption. These disconnects include concerns about security (61%), integration (46%), the ability of cloud computing solutions to meet enterprise and/or industry standards (27%), information governance (35%) and difficulty measuring ROI/determining the accurate economic value of cloud solutions (30%), among others.[4]

As IDG Enterprise's data reveals, there are indeed numerous challenges that exist when it comes to adopting cloud technology. However, in many cases, organizations make out these challenges to be much more significant than they truly are. With the proper advice and strategy, you can overcome these challenges and successfully adopt cloud solutions across the enterprise.

This paper will present the common viewpoints around five cloud challenges – security, system, organizational, cost and legal and compliance challenges – and use data and real-life examples to dispel many of the myths that these viewpoints contain.

Security Concerns

According to the Accenture 2015 Enterprise Cloud Report, 59% of organizations agree or strongly agree that security concerns have prevented one or more business functions from adopting cloud technology.[5] Similarly, a Forrester survey finds that 60% of respondents were very concerned or concerned about security and protection against cybercrime.[6]

The truth? Your approach to security actually shouldn't be that different in the cloud versus on premise. At the end of the day, security comes down to your organization's policies and plans, and that's the same whether you're looking at SaaS or on premise environments. In fact, if you really want to dig into it, SaaS solutions typically offer more security than their on premise counterparts because cloud providers have more resources to invest in security than individual organizations.

Let's take a step back: Of course security is a concern. We see stories in the news all the time about data breaches that compromise personally-identifiable information (PII) and other sensitive corporate data. But the question here isn't if security is an issue, it's if security is a cloud-specific issue. And the answer is no, it's not a cloud-specific issue.

Security is an issue because many organizations have overlooked this area and failed to make the appropriate investments to secure their environments. A major component of this investment is developing and enforcing best practice security policies. In many cases, organizations relegate security policies to a group of employees who develop rules for one-off projects. However, this means there is no overarching policy in place for security, which is a problem, as adopting a robust and comprehensive policy is key to mitigating risks in this area. The fact that 46% of technology decision-makers who have experienced data breaches reported that they occurred due to internal incidents within the organization in 2014 as reported by Forrester[7] only confirms the importance of a robust and comprehensive security policy.

Once you have this type of policy in place, you can then extend it to your cloud environment. For example, you should use your security policy as an assessment point when you evaluate new applications. Doing so can help you ensure that what the SaaS provider offers meets or exceeds the requirements of your security policy, which should be clearly spelled out. If they do, you have mitigated the security risk and done what you can to secure your data, including PII and proprietary information. In fact, as more and more organizations realize that internal policies have a heavy influence on security, concerns in this area are beginning to trend downward.[8]

If you've mitigated the security risk from your end by implementing a robust, overarching policy and assessing new applications in light of this policy, how can cloud solutions actually provide you with tighter security than their on premise counterparts? It's absolutely critical for major cloud providers like Amazon, HP, Microsoft and Salesforce to invest heavily in securing their applications and client data, since this is one of their core competencies. As a result, they can dedicate more resources to security than a small or even mid-size IT organization ever could to secure on premise applications, as doing so would be extremely cost prohibitive for these smaller groups.

System Concerns

Perceived system challenges, including the ability to integrate with other applications (53%), the potential issue that SaaS can financially lock the organization into staying with one vendor (47%), application performance (46%), inability to customize solutions (38%) and technical immaturity of technology (34%), are all SaaS concerns according to research from Forrester.[9]

There are several critical factors, including integration issues, interoperability and evolving standards, system availability, complete dependence on a cloud provider and lack of functionality to meet business needs, that fall under this challenge. Let's break down the reality by each of these factors.

Integration
Designing, building and maintaining integrations between disparate systems, both internal and external, has always been a challenge for IT. In fact, Forrester forecasts that US businesses and government organizations will reach $138 billion on system integration services in 2015, accounting for 7.2% of total tech consulting and system integration services purchases.[10]

Organizations pay such high attention to ensuring proper integration because doing so is critically important to the flow of information. However, a significant number of organizations don't have a comprehensive, enterprise-wide strategy for system integration. Most often, as these organizations deploy new applications, IT will build point-to-point integrations as needed, leading to a messy web of integrations. This messy integration landscape then requires heavy overhead costs from a maintenance and resource perspective and turns performance and latency into major challenges.

The key here is to take a meaningful look at what integrations your organization needs and adopt a more holistic strategy based on these needs. IT should ask: Will there be data-centric integrations, business process-based integrations or both? Answering questions like these will help bring everything together from an integration perspective.

As is the case with security, integration is not a cloud-specific challenge. Rather, it's a challenge for all applications, both cloud and on premise. And, once again like security, the cloud actually provides an advantage here. In this case, it's because SaaS providers typically have very structured approaches for how to integrate into their systems and offer adapters (both native and third party) that allow you to integrate with relative ease.

In sum, integration is no more challenging in the cloud than it is on premise. In fact, thanks to the resources made available by SaaS providers, there's even the potential for integration to become *less challenging* in the cloud.

Interoperability and Evolving Standards
There's no two ways about it: Interoperability is definitely a challenge and constantly evolving standards are a cause for concern. However, as the market matures, standards are being established. Given that the world of cloud applications is still relatively new, organizations must take very careful consideration as they consider whether to push the limit and use bleeding edge technology

(which, by it's nature, evolves constantly) like Google or to use more proprietary software like Azure.

These decisions should be based on the overall IT landscape of your organization. If your current IT infrastructure includes heavy investments in a specific technology like Microsoft or Siebel, adopting a complementary cloud technology like Azure might make the most sense. Meanwhile, if your infrastructure is less proprietary, adopting a solution like Google might be your best course of action.

While interoperability and evolving standard concerns are not specific only to SaaS, they are very relevant to this area. As a result, this should be categorized as a true cloud challenge.

System Availability/Business Continuity and Complete Dependence on a Cloud Provider

This factor does pose a risk, but the amount of risk all comes down to analysis. In this area, the responsibility falls on the organization to analyze what applications make good candidates for moving to the cloud. There's no one-size-fits-all approach for cloud migration and adoption, which means you must examine each and every application in your stack to answer questions like what is the true return on investment for moving this application to the cloud and how complex will the migration be.

While this application stack evaluation should be unique to each organization, there are certain types of applications that are more cloud-ready across the board than others. For example, the Accenture Enterprise Cloud Report discovered that among business applications, CRM and Human Resources Information Systems are already in the cloud for 36% and 27% of organizations, respectively, and among IT applications, email, office productivity and IT service/operations management are already in the cloud for 44%, 25% and 24% of organizations, respectively.[11] Additionally, these same applications all top the list to move to the cloud in 2015.[12]

Another important point to keep in mind here is that leading cloud providers are running services for thousands of customers, which means they do have high redundancy and failover plans that allow them to maintain high system availability.

On the other hand, the fact that complete dependence on a cloud provider is a challenge is more of a perception than a reality. Yes, the cloud does create some dependency on a provider, but this dependence eliminates many of the challenges that comes with maintaining and upgrading on premise systems.

Most importantly, just like with any other application provider, you can control your dependence by selecting the right provider for your needs, establishing clear SLAs and having the proper skills in-house that align closely with that of your cloud provider. As a result, proper evaluation is critical in this regard.

So, while system availability and dependence can be challenges, you can mitigate any risks by doing your due diligence when it comes to evaluating your application stack and potential cloud providers.

Lack of Functionality to Meet Business Needs

The cloud's lack of functionality to meet business needs is a genuine risk, but it falls into the same camp as security: The risk is more or less the same as it is with any on premise application. The one twist in the cloud is that some SaaS applications don't allow for customization. Leading cloud application providers do build their solutions around best practice processes though, so you should consider adopting these solutions out-of-the-box to the maximum extent possible and try to keep any customizations to the bare minimum.

In general, the key here is to perform a very detailed analysis upfront before you adopt any new application. During this analysis, you need to determine which business processes are essential for any given system and map those processes to native functionalities provided by the application.

Going through this type of detailed gap-fit analysis from a process perspective before you adopt any new application (SaaS or otherwise) or infrastructure environment can help mitigate the risk that a new technology will lack the proper functionality to meet your business needs.

Organizational Concerns

Recent research from IDG Enterprise and Forrester Research reveals that 11% of business leaders and 10% of employees are not receptive to cloud computing solutions (IDG Enterprise)[13] and that 44% of organizations consider a lack of control over upgrades/release cycles a concern (Forrester Research).[14]

As this data makes clear, there still exists a general resistance to and fear of adopting cloud solutions. Although technically this resistance and fear is not a myth because it does actually exist, you can often address and overcome these feelings with proper knowledge and training. Understanding the root cause of any resistance and/or fear and then developing a specific plan to address those feelings is critical for overcoming this challenge.

For example, a lot of resistance to adopting cloud applications exists because people have misconstrued perceptions. Many people in the IT world fear that adopting cloud technology will put them out of a job because their skills will no longer be relevant. Similarly, many organizations resist moving to the cloud because they don't have the necessary skills in-house to support those applications. This is a real challenge, as 53% of organizations agree or strongly agree that their IT teams are not educated or skilled in cloud technology.[15]

While it is true that skillset requirements are different in the cloud than they are on premise, the necessary cloud skillset isn't all that difficult to acquire. For IT people who already have a foundation in programming languages, picking up the necessary skills won't be as difficult today as it was even five years ago. Still, there's no doubt that making this change will be a challenge, but proper training can go a long way in helping mitigate it.

Additionally, many organizations are choosing to simplify this transition by augmenting their own internal IT teams with support from an external partner. According to the Accenture Enterprise Cloud Report, 45% of organizations rely on a mix of internal and external IT staff, with managed services (52%), software/application

development (33%) and IT consulting (33%) ranking as the top three outsourced responsibilities.[16]

Another common root cause of resistance to cloud adoption is the fear that IT will lose control of critical apps and data. Accenture finds that this is a concern for 30% of organizations worldwide.[17] However, this fear is more of a perception than it is a reality because even when your data is hosted in a cloud application, you still own that data. It's your data and it's up to your organization to ensure its security by creating and enforcing a robust security policy and by confirming that your SaaS provider has the proper SLA in place. Despite common views to the contrary, putting your data in the cloud is not akin to leaving it in a black hole.

You can mitigate this fear about losing control of data and technology by thoroughly evaluating SaaS providers and their SLAs, having proper data and security policies in place and assessing your application stack to determine what makes sense to move to the cloud and what makes sense to keep on premise.

Finally, many cases of resistance to going cloud stem from general unawareness about what the cloud is and the benefits it offers. The best way to mitigate this resistance is to educate the organization by demonstrating the value of the cloud. For instance, you can use real-life use cases to reveal how cloud solutions can increase productivity, decrease costs, make your IT environment more robust or even give your business a competitive edge. Once again, the key is to address the root cause of these fears.

Cost Concerns

According to a 2015 report from Forrester Research, 47% of survey respondents are concerned or very concerned about the cost of adopting SaaS technology. Interestingly, the same report reveals that 38% of respondents feel that pricing is unclear or complicated in the cloud.[18]

When it comes to cost in the cloud, there are three main areas viewed as challenges. Let's take a look at each area individually.

Transition and Implementation Costs
The fact that transition and implementation cost challenges are unique to the cloud is complete perception. Once again, this is an example of a challenge that's the same in the cloud as it is on premise.

Whether you're looking at SaaS, PaaS or IaaS, you need to treat the implementation just like you would any other IT project. This means you need to develop a proper project management structure, adopt best practices and work with a realistic budget. Yes, there is a cost, but it's a cost that should be built in to the project as it would be for any other implementation. In most cases, cloud implementation costs will be akin to what they would be for similar kinds of systems on premise. If anything, though, the costs could be less because there's a lot that you can use without having to install other applications or do complex configurations. Nevertheless, proper project management still needs to be in place.

Recurring vs. One-Time Investment (CAPEX vs. OPEX)
Yes, the cost structure in the cloud is different than it is on premise.

But different doesn't necessarily mean challenging. It just means something new for which your organization must prepare.

Even though the on premise model requires a larger one-time investment, there are still recurring costs since these solutions require support, patches and upgrades. These maintenance fees can cost as much as 20-25% of the initial licensing cost,[19] not to mention the cost of staffing support resources in house.

Meanwhile, the SaaS model doesn't have the large capital expenditure. Instead, once you get the application implemented and running, you're simply left with the recurring subscription cost. All those "hidden" costs that come with the on premise model – maintenance, upgrades, etc. – disappear in the cloud.

The key to mitigating this challenges is to first recognize that the cost model will change in the cloud and to then build a proper business case based on that updated cost model.

Lack of Effective ROI and Potentially Escalating Costs
The idea that the cloud lacks an effective ROI is nothing more than perception. It all comes down to whether or not your organization built a solid business case for cloud adoption. To build this business case, you need to evaluate your business processes to determine where the cloud application can deliver improvements like increased efficiency and agility. If you consider all of the necessary factors in this business case, you can then calculate a proper ROI.

There are many third party advisory practices that exist in the cloud space who can help your organization conduct this type of assessment in order to build a solid business case for moving to the cloud and develop a proper ROI based on that information.

Legal and Compliance Concerns

Both Accenture and Forrester find that nearly half of organizations have legal and compliance concerns about cloud computing. Accenture's data reveals that 48% of organizations agree or strongly agree that concerns in this area have inhibited them from evaluating cloud technology,[20] while Forrester's research discovers that 44% of survey respondents consider compliance with local laws and concerns about access by foreign agencies a potential issue of adopting SaaS technology.[21] Along similar lines, IDG Enterprise reports that 27% of organizations consider the ability of cloud solutions to meet specific enterprise and/or industry standards a significant barrier to cloud adoption.[22]

These concerns can create misconceptions that may lead to organizations making uninformed decisions about cloud technology. For regulated organizations that operate under the purview of a regulator, cloud misconceptions such as *"the regulator forbids cloud adoption," "cloud data is offshored"* or *"cloud data is insecure"* are common and can have a material impact on organizations' acceptance and adoption of cloud technology.

Regulators do not typically prohibit the use of cloud technology, however they do tend to specify complex standards and guidelines that organizations must address. Regulators are also typically concerned about data security and residency, although these

requirements are readily addressed since leading cloud vendors operate sophisticated data centers, architectures and protocols that offer (typically) higher levels of security than what's available on premise. Furthermore, many leading cloud vendors offer in-country data centers to ensure that data is retained on-shore. And when vendors only offer offshore data centres, your organization can typically address regulator data residency standards through a combination of augmented solution architectures that leverage specialized technology, governance and regulatory oversight.

As has proven true for many of these challenges, legal and compliance issues aren't cloud-specific. Meeting these requirements will pose challenges, but those challenges will exist whether you're looking at cloud or on premise applications. In some cases, meeting these requirements can be a bit more challenging in the cloud though because some cloud applications are more difficult to modify. If this modification is a concern, it simply needs to become a factor as you evaluate SaaS applications and providers and review your application stacks to determine what makes sense to move to the cloud and what makes sense to keep on premise.

Another important factor to consider as you evaluate solutions – cloud and on premise alike – in light of legal and compliance is that these requirements differ based on region. For example, requirements in the US are significantly different than they are in France, and the French requirements are different than they are in Germany and so on. If you're rolling out an application globally, you must consider the ability to localize the solution based on these different requirements. Regardless, you should factor the following general guidelines into your approach:

1. Create a cloud risk management strategy to manage the relevant risk types you've identified and then have your board endorse this strategy.
2. Engage with any regulators early on regarding your intent to move to the cloud and share your approach with them.
3. Share your risk concerns with your cloud vendors and hold them to the same standards and diligence as the regulator will hold you.
4. Manage your risks through ongoing measurement of the performance of your cloud vendors relative to your identified risks.
5. Ensure your IT governance framework contains a cloud strategy and appropriate risk management measures that are in alignment with your regulators' standards and guidelines.

Conclusion

Despite the fact that these perceptions are widely held by organizations and individuals across all industries and geographies, the truth remains that properly preparing for cloud adoption can mitigate most of these concerns. This preparation includes activities like educating the organization on the value of cloud technology, evaluating your application stack to make the best possible decision about what to move to the cloud, developing a sound business case for adopting a SaaS solution, adhering to an established security policy and procedures, diligently assessing potential cloud providers and their solution offerings and SLAs, creating a project plan for implementation and deploying a comprehensive security policy.

Furthermore, it's important to recognize that many of these challenges, including those around security, integration, implementation costs and legal and compliance requirements, are not cloud-specific challenges. These challenges are real, but they are as true for cloud applications as they are for on premise applications.

Given this reality, knowledge and preparation should eliminate most, if not all, barriers to cloud adoption, thereby allowing your organization to take advantage of the many benefits these next generation solutions have to offer.

Resources

1 Gownder, J.P. with Christopher Voce, David K. Johnson and Andrew Hewitt. "How To Budget For Workforce And Customer-Facing Technology In 2015 And Beyond." Forrester Research, Inc. January 5, 2015.

2 "Enterprise Cloud Report." Cloud Sherpas. April 2015.

3 "Enterprise Cloud Report." Cloud Sherpas. April 2015.

4 Columbus, Louis. "Cloud Computing Adoption Continues Accelerating In The Enterprise." Forbes.com. November 22, 2014.

5 "Enterprise Cloud Report." Cloud Sherpas. April 2015.

6 Hamerman, Paul D. and Herbert, Liz with Chris Andrews and Arelai Ephraim. "Application Adoption Trends 2015: The SaaS Boom Continues As Businesses Demand Agility." Forrester Research, Inc. April 24, 2015.

7 Shey, Heidi and Mak, Kelly with Stephanie Balaouras and Josh Blackborow. "Understand The State Of Network Security: 2014 to 2015." Forrester Research, Inc. December 22, 2014.

8 Goulart, Karen. "Cloud security risks still an issue for CIOs, but change is in the air." SearchCIO. June 20, 2013.

9 Hamerman, Paul D. and Herbert, Liz with Chris Andrews and Arelai Ephraim. "Application Adoption Trends 2015: The SaaS Boom Continues As Businesses Demand Agility." Forrester Research, Inc. April 24, 2015.

10 Bartels, Andrew with Peter Burris and Amanda LeClair. "US Tech Market Outlook For 2015 And 2016: The BT Agenda Powers Steady Expansion." Forrester Research, Inc. June 29, 2015.

11 "Enterprise Cloud Report." Cloud Sherpas. April 2015.

12 "Enterprise Cloud Report." Cloud Sherpas. April 2015.

13 Columbus, Louis. "Cloud Computing Adoption Continues Accelerating In The Enterprise." Forbes.com. November 22, 2014.

14 Hamerman, Paul D. and Herbert, Liz with Chris Andrews and Arelai Ephraim. "Application Adoption Trends 2015: The SaaS Boom Continues As Businesses Demand Agility." Forrester Research, Inc. April 24, 2015.

15 "Enterprise Cloud Report." Cloud Sherpas. April 2015.

16 "Enterprise Cloud Report." Cloud Sherpas. April 2015.

17 "Enterprise Cloud Report." Cloud Sherpas. April 2015.

18 Hamerman, Paul D. and Herbert, Liz with Chris Andrews and Arelai Ephraim. "Application Adoption Trends 2015: The SaaS Boom Continues As Businesses Demand Agility." Forrester Research, Inc. April 24, 2015.

19 Mitchell, Robert L. "Buried in software licensing." Computerworld. August 12, 2013.

20 "Enterprise Cloud Report." Cloud Sherpas. April 2015.

21 Hamerman, Paul D. and Herbert, Liz with Chris Andrews and Arelai Ephraim. "Application Adoption Trends 2015: The SaaS Boom Continues As Businesses Demand Agility." Forrester Research, Inc. April 24, 2015.

22 Columbus, Louis. "Cloud Computing Adoption Continues Accelerating In The Enterprise." Forbes.com. November 22, 2014.

Contact

For more information, call 888-260-7660.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 373,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.