G00292047

Predicts 2016: Cloud Computing to Drive Digital Business

Published: 8 December 2015

Analyst(s): David Mitchell Smith, Ed Anderson, Yefim V. Natis, Jay Heiser, Thomas J. Bittman, Douglas Toombs, David W. Cearley, Jeffrey Mann, Neville Cannon, Gregor Petri

As its technologies and processes mature, the cloud is being increasingly relied on as a vehicle for agile, scalable and elastic solutions. To build competitive advantage and cut costs, CIOs and other IT leaders need to constantly adapt their strategies to leverage cloud capabilities.

Key Findings

- Hybrid will be the most common usage of the cloud — but this requires the public cloud to be part of the overall strategy.
- The defensive stance that dominated the large software vendor strategies toward the cloud has been replaced in recent years with a cloud-first approach. Today, most vendor technology innovation is cloud-centric, with the stated intent of retrofitting the technology to on-premises.
- Failure to put the people and processes in place to consistently leverage the security advantages of cloud computing can easily create workloads that are less secure than those created by traditional computing practices, resulting in unnecessary compliance incidents and data losses.
- As more applications move to public cloud environments, confidence in their use will increase. The ecosystems required to support mission-critical enterprise use cases will expand, reinforcing the viability of public cloud services as a destination for mission-critical workloads.

Recommendations

IT leaders should:

- Revisit your organization's assumptions if it avoids the cloud on principle, as cloud deployments become more widespread and their benefits clearer.
- Give preference to vendors that are strategically investing in cloud computing models and attributes.

- Design on-premises architectures with off-premises interoperability in mind when possible — in terms of governance, integration and migration.
- Consider public cloud services as a destination for mission-critical applications, performing a thorough evaluation of its merits.

Table of Contents

Strategic Planning Assumptions..... 2
Analysis..... 2
What You Need to Know..... 3
Strategic Planning Assumptions..... 3
A Look Back..... 11
Gartner Recommended Reading..... 13

Strategic Planning Assumptions

By 2020, a corporate "no-cloud" policy will be as rare as a "no-Internet" policy is today.

By 2019, over 30% of the 100 largest vendors' new software investments will have shifted from cloud-first to cloud-only.

By 2018, 50% of the applications running in public cloud environments will be considered mission-critical by the organizations that use them.

By 2020, more compute power will have been sold by IaaS and PaaS cloud providers than sold and deployed into enterprise data centers.

Through 2020, 95% of cloud security failures will be the customer's fault.

Analysis

Cloud computing continues to mature and increasingly dominate IT and business conversations worldwide. Hype remains high and adoption is increasing (see "Hype Cycle for Cloud Computing, 2015"). Across the landscape of cloud computing, however, technologies, services and inconsistently used terms can create confusion (see "The Top 10 Cloud Myths"). Cloud vendors and users alike make outlandish and misleading claims about cloud capabilities ("cloudwashing"), which can add to this confusion.

There are many examples of organizations that have recognized the benefits and avoided the pitfalls of cloud computing. Understanding the broad landscape of cloud service offerings and technologies, as well as the cloud computing terminology, is critical for organizations looking to exploit the real benefits of cloud computing (stated as business outcomes).

What You Need to Know

Our cloud computing predictions for 2016 are focused on some of the bigger-picture strategic issues surrounding the topic and the implications for CIOs and cloud strategists. Cloud computing is a broad topic and has the potential to affect all aspects of IT.

Conventional wisdom, longstanding biases and news stories continue to sway views on a daily basis, but the trend toward cloud acceptance is unmistakable. Excitement around the potential to accelerate digital business permeates the market. As this continues, the role of the cloud as a carrier or vehicle for digital business is becoming paramount.

Note that in this document, use of the term "cloud" refers to the public cloud. If private or hybrid cloud is meant, this will be specified.

Strategic Planning Assumptions

Strategic Planning Assumption: By 2020, a corporate "no-cloud" policy will be as rare as a "no-Internet" policy is today.

Analysis by: Jeffrey Mann, David Mitchell Smith

Key Findings:

While adoption of cloud computing continues to grow, skepticism remains in some organizations. Some even claim to have a generalized "no-cloud" policy. IT planners most commonly cite concerns about security, privacy protection, compliance, vendor lock-in and confidence in their organizations' abilities to provide equal or superior service at an equal or lower cost to justify these positions.

Aside from the fact that many organizations with a no-cloud policy actually have some under-the-radar or unavoidable cloud usage, Gartner believes that this position will become increasingly untenable. Many mainstream software vendors have already adopted a "cloud-first" policy, meaning they now consider cloud as the first option when implementing a new application. Many are moving to "cloud-only" for their newest and most innovative products. Cloud will increasingly be the default option for software deployment. The same is true for custom software, which increasingly is designed for some variation of public or private cloud.

Gartner believes that by 2020, a general no-cloud policy will be extremely rare — about as rare as a "no-Internet" policy is now. There are some organizations in 2015 that block Internet access to all of their employees; not many, but they exist due to concerns about employees wasting time on frivolous websites, or due to extreme security concerns such as in military installations or nuclear plant control rooms. However, it is safe to say that the vast majority of organizations would find it unthinkable to do business without some level of Internet access today, even if just for email. By 2020, the same will be true for cloud deployments — it will be largely unthinkable to eschew cloud deployments as a matter of policy. This prediction does not mean that there will be no on-premises deployments and everything will be cloud-based; the concerns mentioned above will remain valid in

some cases. However, we feel that the extreme of having nothing cloud-based will largely disappear.

Market Implications:

- Hybrid will be the most common usage of the cloud — but this will require public cloud to be part of the overall strategy.
- Most new capabilities will be delivered from the cloud.
- Technology providers will increasingly be able to assume that their customers will be able to consume cloud capabilities.

Recommendations:

- Revisit your organization's assumptions if it avoids the cloud on principle, as cloud deployments become more widespread and their benefits clearer.
- Plan on ways to accept cloud usage as a fundamental core capability.

Related Research:

"The Key Trends in PaaS, 2015"

"Cloud Office Questions Begin the Shift From 'If' to 'When'"

"Cloud Adoption Trends Highlight Buyer Preferences and Provider Opportunities"

"When IT Leaders Should Select Private Over Public Cloud Services"

Strategic Planning Assumption: By 2019, over 30% of the 100 largest vendors' new software investments will have shifted from cloud-first to cloud-only.

Analysis by: Yefim V. Natis

Key Findings:

- The defensive stance that dominated the large software vendor strategies toward the cloud has been replaced in recent years with a cloud-first approach. Today, most vendor technology innovation is cloud-centric, with the stated intent of retrofitting the technology to on-premises.
- Visionary technology providers recognize that managing both the software and service offerings of the same technology is cumbersome and expensive. They tend to offer private technology variants in the form of hosted private (also referred to as managed or dedicated) or managed local services. IT vendors will increasingly look to manage a single code base and thus gain efficiency and agility in innovation.

- A cloud environment is not a transposition of an on-premises data center "to the sky." Essential cloud attributes such as Web-scale, agility, quality of service, security and manageability demand a changed architecture.
- Some cloud-native technology capabilities are not as applicable or necessary on-premises. More importantly, some can only be delivered in the cloud context, such as massive scalability. Increasingly, vendors are shifting their sales strategies to attract customers to their cloud offerings at the expense of the licensed software.
- The now well-established stance of cloud-first in software design and planning is gradually being augmented or replaced by cloud-only. This applies also to private and hybrid cloud scenarios.

Market Implications:

- More-leading-edge IT capabilities will be available only in the cloud, forcing reluctant organizations closer to cloud adoption. While some applications and data will remain locked on-premises in older technologies, more new solutions will be cloud-based, thus further increasing demand for integration infrastructure.
- The dilemma of where to allocate available IT budgets between on-premises and cloud resources will become more common and more critical.
- Roadmaps for current precloud systems will rise to a greater challenge. The need to choose between a direct shift without change, modernization and gradual replacement with cloud-native solutions will become common and more acute.
- As delivery shifts more to the cloud, most IT organizations will have to reorganize to reflect the business realities of cloud computing: agility, continuous change, competing with cloud providers for some initiatives, and prevalence of influence over control with regard to IT's relationship with lines of business.

Recommendations:

- Build expertise (in skills and technology) in cloud computing architecture, best practices and organizational alignment.
- Give preference to vendors that are strategically investing in cloud computing models and attributes.
- Direct more of your IT budget to cloud-native initiatives, as appropriate.
- Continue to invest in integration infrastructure, as the long-term cloud adoption process will increase the demand for interoperability and integration.

Related Research:

"The Key Trends in PaaS, 2015"

"Software License Providers Will Exploit Their Captive Licensees in Order to Move Them to SaaS"

"Gartner on the State of PaaS: Recent Research"

Strategic Planning Assumption: By 2018, 50% of the applications running in public cloud environments will be considered mission-critical by the organizations that use them.

Analysis by: Ed Anderson, Neville Cannon

Key Findings:

Cloud adoption continues at a rapid pace. While some organizations are still figuring out where the cloud really fits in their overall IT strategy, most organizations — approximately 58% — are well down the path of using cloud services to support some aspect of their business.

Gartner's 2014 cloud adoption study showed that, of the applications running in cloud environments as of July 2014, 28% of IaaS and PaaS usage was deemed mission-critical. Those same organizations indicated that 37% of SaaS usage was considered mission-critical.

Gartner's 2015 cloud adoption study shows a 300% increase in the number of organizations making investments in cloud services, including IaaS, PaaS and SaaS. Of organizations using cloud services today, 88% indicate a cloud-first strategy. Furthermore, organizations are pursuing strategies because of the multidimensional value of cloud services, including values such as organizational agility, IT scalability, cost benefits, innovation and business growth, which are equally cited as core benefits.

We have observed that cloud services are increasingly being used to replace or extend legacy systems or some of their components. Predominantly, this is undertaken by public cloud SaaS. Such use now accounts for 23% of IT spending on software, and is expected to grow to 34% by 2019. Similarly, IaaS is expected to grow from approximately 7% to 11% of spending on infrastructure capacity.

The adoption of public cloud services as a mainstream component of enterprise IT means more and more production workloads are shifting to public cloud environments. Most of these applications are either new applications or traditional applications that have been rewritten to run on a cloud platform.

Market Implications:

The use of cloud services continues to grow across all use cases, from infrastructure through middleware to application software. The IT marketplace has answered the question of whether or not cloud services have a role to play in mainstream enterprise computing — already, 37% of organizations using the public cloud state that they are using it for mission-critical services. The question is now how much, how soon? The adoption of core cloud service applications such as CRM and office productivity (including email) has demonstrated the capabilities of cloud services to meet mission-critical requirements. Likewise, ERP components such as human capital management, finance and accounting, and supply chain management are showing increased levels

of investment today. According to Gartner studies on cloud adoption, spending on public-cloud-based, vertical-specific applications is expected to significantly increase through 2017, further highlighting the growing confidence in their use for mission-critical systems. For example, we also predict that at least 25% of new core financial application deployments in large enterprises will be public cloud SaaS (see "Predicts 2016: Financial Management Applications").

As more applications move to public cloud environments, confidence in their use will increase. The ecosystems required to support mission-critical enterprise use cases will expand, as we've seen with leading cloud infrastructure and application environments. These factors will reinforce the viability of public cloud services as a destination for mission-critical workloads.

Recommendations:

- IT leaders should consider public cloud services as a destination for mission-critical applications, although this should not alleviate the responsibility of performing a thorough evaluation of the merits of public cloud for a given application workload.
- Cloud service providers must deliver secure and reliable cloud service offerings to remain competitive. End-user organizations will increasingly look to cloud platforms as a destination for production and mission-critical applications. To remain competitive, cloud service providers must demonstrate capabilities to support applications with mission-critical requirements.
- Service providers should build complementary consulting, implementation and managed service offerings to assist clients moving mission-critical workloads to public cloud environments. This will require service practices that thoroughly assess the suitability of public cloud environments for mission-critical applications, in addition to any additional services required to support the mission-critical requirements of the application.

Related Research

"Hype Cycle for Cloud Computing, 2015"

"Three Factors Will Continue to Impact Enterprise Cloud Playbooks"

"Critical Capabilities for Public Cloud Infrastructure as a Service, Worldwide"

"Forecast Overview: Public Cloud Services, Worldwide, 2014 Update"

Strategic Planning Assumption: By 2020, more compute power will have been sold by IaaS and PaaS cloud providers than sold and deployed into enterprise data centers.

Analysis by: Thomas J. Bittman

Key Findings:

The IaaS compute market has been growing more than 40% in revenue per year since 2011, and is projected to continue to grow more than 25% per year through 2019. As of 2014, 20% of all virtual

machines (VMs) were delivered by IaaS cloud providers, up from 3% in 2011. The total number of VMs is expected to continue to grow at least 20% per year through 2019 — but the growth of off-premises IaaS VMs is expected to take up the majority of that growth. By 2019, the majority of VMs will be delivered by IaaS providers. The current forecast shows that revenue from compute IaaS and PaaS will be only 13% less than the revenue for all servers worldwide. By 2020, the revenue for compute IaaS and PaaS will exceed $55 billion — and likely pass the revenue for servers.

Market Implications:

In 2011, when IaaS virtualization accounted for only 3% of VMs, infrastructure architecture decisions were based heavily on an enterprise's virtualization vendor. Expanding the virtualization architecture to build a software-defined data center was very appealing. However, with the growth of both bimodal computing (different applications with different supporting architectures and operational models) and cloud provider offerings, software-defined enterprise data centers have become less centrally important than building a strong multiprovider management capability. Most enterprises — unless very small — will continue to have an on-premises (or hosted) data center capability. But with most compute power moving to IaaS providers, enterprises and vendors need to focus on managing and leveraging the hybrid combination of on-premises, off-premises, cloud and noncloud architectures, with a focus on managing cloud-delivered capacity efficiently and effectively.

Recommendations:

- Invest in skills and technologies to ensure efficient and effective use of infrastructure both on- and off-premises — enterprise use of third-party infrastructure servers won't replace data center infrastructures, but it does need to be governed well.
- Design on-premises architectures with off-premises interoperability in mind when possible — in terms of governance, integration and migration.
- Manage your heterogeneity: Find the right balance between a different architecture for every workload and a single architecture for every workload. Create a process for workload placement as well as guidelines and standards for application development, so that experiments and pilot projects don't determine your standards.

Related Research:

"Four Trends Changing Server Virtualization Decisions"

"Forecast: Public Cloud Services, Worldwide, 2013-2019, 3Q15 Update"

"Forecast: Servers, All Countries, 2012-2019, 3Q15 Update"

"Internal Private Cloud Is Not for Most Mainstream Enterprises"

Strategic Planning Assumption: Through 2020, 95% of cloud security failures will be the customer's fault.

Analysis by: Jay Heiser

Key Findings:

- The high levels of concern about cloud service provider security maturity have become counterproductive, distracting from the need to establish the organizational, security and governance processes required to prevent cloud security and compliance mistakes.
- Many enterprises are paying an opportunity cost by allowing unwarranted fears to inhibit their use of public cloud services that are more secure and agile than traditional in-house computing.
- The naive belief that SaaS providers are responsible for their customers' security discourages enterprises from addressing the reality of how their employees use external applications. This leads to misguided leveraging of the power of cloud services, encouraging employees to inappropriately share huge amounts of data with other employees, external parties and sometimes the entire Internet.
- Ad hoc use of the public cloud can lead to workloads that are less secure than those created by traditional computing practices. This can result in compliance incidents and data losses that could easily have been avoided with a more strategic approach, putting people and processes in place to leverage the security advantages of cloud computing.

Market Implications:

Although security concerns remain the most common reason for avoiding the use of public cloud services, public cloud usage is growing at a brisk pace. Enterprises that have come to terms with cloud security are able to make quicker and better decisions on new cloud use cases.

The diffuse and complex nature of cloud computing will continue to ensure significant and growing opportunities for multiple forms of cloud control planes. ID as a service, cloud application security brokers, cloud management platforms and other categories of cloud control provide convenient single consoles and management points. These make it possible to ensure common configurations and policies, as well as monitor and govern user activities across an increasingly complex virtual enterprise of applications based in IaaS, PaaS and SaaS clouds.

Third-party security standards, such as ISO 27001 and SOC2, will become virtually mandatory product features for any enterprise undertaking strategically significant use of a cloud-based service.

Recent history has shown that virtually all public cloud services are highly resistant to attack and, in the majority of circumstances, represent a more secure starting point than traditional in-house implementations. No significant evidence exists to indicate that commercial cloud service providers have performed less securely than end-user organizations themselves; in fact, most available evidence points to the opposite. Only a very small percentage of the security incidents impacting enterprises using the cloud have been due to vulnerabilities that were the provider's fault.

During the next several years, the news media will continue to report a growing number of stories about security failures, but only a few incidents a year will be attributable to poor provider technology or practices on the part of a cloud service provider. Most will involve small providers and impact relatively few customers.

The cloud business model provides huge market incentives for cloud service providers to place a higher priority on security than is typical for end-user organizations. Cloud service providers can afford to hire experienced system and vulnerability managers, and their economies of scale make it practical to provide around-the-clock security monitoring and response. The branded cloud services use custom platforms that enable them to avoid the security vulnerabilities typical of in-house implementations.

This does not mean that organizations should assume that using a cloud service means that whatever they do within that cloud will be secure. The characteristics of the parts of the cloud stack under customer control can make it easy for naive users to adopt poor cloud practices, which can easily result in widespread security or compliance failures.

Most enterprises that have implemented cloud application discovery capabilities — typically provided by a cloud access security broker (CASB) — have discovered that SaaS is being used in ways that expose sensitive data internally and externally. CASB products are also useful in identifying typical customer security vulnerabilities, such as "open shares" — files that can be accessed by anyone on the Internet. The misuse of public cloud services, which inevitably happens if an enterprise does not attempt to exert some control over cloud use, represents an increase in the exposure of sensitive data to people inside and outside the enterprise. Secure and regulatory-compliant use of public clouds requires that enterprises implement new organizational policies, develop new skills and undertake new processes.

Growing recognition of the enterprise's responsibility for the appropriate use of the public cloud is reflected in the growing market for cloud control tools. By 2018, 50% of enterprises with more than 1,000 users will be using products provided by CASBs to monitor and manage their use of SaaS and other forms of public cloud. This will reflect growing recognition that, although public clouds are usually secure, the *secure use* of them requires explicit effort on the part of the customer.

Near-Term Flags:

- By the end of 2016, 40% of enterprises with more than 1,000 employees and 80% of organizations with over 10,000 employees will have policies and practices in place to approve and track the use of SaaS.
- By 2017, the number of enterprises with policies against placing any sensitive data in the public cloud will have dropped to 5%.
- By the end of 2017, 95% of cloud service providers with annual revenue over $500 million will have had at least one formal security evaluation.
- Through the end of 2018, the number of public disclosures of in-house security failures will have grown every year, but only one or two incidents a year will have been attributed to poor cloud service provider technologies or practices.

- By the end of 2018, 50% of enterprises with more than 5,000 users will have deployed products from CASBs to control their use of cloud services.

Recommendations:

CIOs, CISOs and compliance personnel should:

- Develop and follow an enterprise public cloud strategy. An effective strategy includes security and regulatory compliance guidance concerning acceptable and unacceptable uses of public cloud services.
- Implement and enforce policies on cloud ownership and cloud risk acceptance processes.
- Follow a life cycle governance approach to the use of all cloud services and the processes performed within them. While existing operational practices are usually extended to enterprise applications provisioned within IaaS, most enterprises currently fail to focus the same level of attention on the ongoing operational control of SaaS applications.
- Develop expertise in the security and control of each of the cloud models you will be using. The use of IaaS requires knowledge of virtualization security and new techniques for network security. SaaS requires knowledge of provider characteristics and the use of cloud access security broker tools. All forms of public cloud require careful control over identity and access.
- Implement technology control planes to address the complexity of cloud diffusion. Enterprise security, identity, compliance, continuity, sourcing and other IT roles will increasingly use single consoles that enable them to monitor and manage the use of a wide range of externally provisioned services.

Related Research:

"Developing Your SaaS Governance Framework"

"A Public Cloud Risk Model: Accepting Cloud Risk Is OK, Ignoring Cloud Risk Is Tragic"

"Best Practices for Securing Workloads in Amazon Web Services"

"Everything You Know About SaaS Security Is Wrong"

"Hype Cycle for Cloud Security, 2015"

A Look Back

In response to your requests, we are taking a look back at some key predictions from previous years. We have intentionally selected predictions from opposite ends of the scale — one where we were wholly or largely on target, as well as one we missed.

On Target: 2011 Prediction — By 2014, cloud computing experience will be a listed or demanded skill in most hiring decisions for IT software projects.

In 2011, Gartner predicted that by 2014, most organizations — even if they were still somewhat skeptical about "cloud" — would find themselves depending on some cloud-based services for certain business processes, and to be working toward moving additional enterprise applications to the cloud to modernize their data centers. As a result of these changes, Gartner anticipated that IT organizations would find themselves understaffed in terms of personnel with cloud computing skills, and that finding those capabilities would become high priority for most hiring decisions by 2014. This prediction has proved to be largely on target.

By 2014, adoption of cloud computing services was common within at least half of organizations. Gartner's own CIO priorities survey report from 2014 indicated that 25% of organizations had actually made "significant investments" in public cloud — not just test workloads — and that by 2019, half of the CIOs surveyed felt that half of their business might be running on public cloud infrastructure and SaaS (see "Taming the Digital Dragon: The 2014 CIO Agenda"). The same report for 2015 confirms that not only do a majority of businesses find that cloud services are an acceptable option for in-house workloads, but that 10% to 16% actually operate with a cloud-first policy — where new workload must be sourced from cloud services first before taking on additional on-premises infrastructure (see "Flipping to Digital Leadership: The 2015 CIO Agenda").

As a result of this significant shift by enterprises in the last few years, many organizations now lack the skill sets necessary to understand the specific characteristics of cloud-based services: managing cloud-based software services, integration involving cloud-based interfaces, and the use of development tools that leverage cloud services. In order to fill this gap, demand for cloud computing skills has increased significantly among hiring managers. According to major global IT recruiting firms, cloud computing has become the most in-demand skill in 2015.

Missed: 2011 Prediction — By 2015, 50% of Global 1000 enterprises will rely on external cloud computing services for the top 10 revenue-generating processes.

If the above statement had predicted that the top 10 revenue services would be reliant on hybrid cloud services (as opposed to external cloud services), it would have come somewhat closer to the stated percentage. When looking at relying purely on external cloud services for the top 10 revenue-generating processes, we still see very few industries come close to this prediction. Even today, most IT service providers in the Global 1000 still generate the majority of their revenue through traditional means. The same is true in media, oil and gas, and government. Retail — pushed forward by the success of Amazon — is starting to move faster than most.

In 2011, we did correctly point to security concerns regarding external clouds as the major inhibitor, but we expected enterprise to build internal cloud services instead that, by now (after gaining more familiarity and trust in the cloud model), would be deployed externally.

The reality is that for most revenue-generating services, many corporates were simply too slow. Hence the large interest in the implementation of a bimodal IT organization (if the whole enterprise cannot sprint at the required speed, then at least some parts should be able to).

With the emerging introduction of digital propositions, however, we now see several enterprises picking up the challenge with renewed vigor. Companies such as GE, Philips Healthcare and Capital One are not shy of stating their plans and ambitions publicly at the events of leading external cloud

providers. For example, GE recently stated at Amazon Web Services re:Invent that it is on a path to move no less than 60% of its IT workloads to the public cloud.

Acronym Key and Glossary Terms

CRM	customer relationship management
ERP	enterprise resource planning
IaaS	infrastructure as a service
PaaS	platform as a service
SaaS	software as a service

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"The Top 10 Cloud Myths"

"Hype Cycle for Cloud Computing, 2015"

"Agenda Overview for Cloud Computing, 2015"

"Cloud Strategy Cookbook"

Evidence

"Cloud Adoption Trends Highlight Buyer Preferences and Provider Opportunities"

"Taming the Digital Dragon: The 2014 CIO Agenda"

"Flipping to Digital Leadership: The 2015 CIO Agenda"

"Forecast: Public Cloud Services, Worldwide, 2013-2019, 3Q15 Update"

"Forecast: Servers, All Countries, 2012-2019, 3Q15 Update"

More on This Topic

This is part of an in-depth collection of research. See the collection:

- Predicts 2016: Algorithms Take Digital Business to the Next Level

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp