Predictions For 2014: Cloud Computing

Cloud Formally Joins The IT Portfolio — Whether IT Likes It Or Not

by James Staten, Dave Bartoletti, Andras Cser, John Kindervag, Rachel A. Dines, Lauren E. Nelson, and Liz Herbert
with Christopher Voce and Heather Belanger

WHY READ THIS REPORT

As we head into 2014, cloud computing is no longer a "future" but a "now." Investments are up, enterprise use is widespread, and the hybrid cloud model has arrived. While the bulk of cloud acquisition and use continues to be driven by line of business, in 2014, traditional IT departments will stop asking "why cloud?" and instead get busy integrating cloud into the existing portfolio, extending data center infrastructures with elastic cloud technologies, and consuming new bespoke platforms and private cloud solutions to back the moves by DevOps and line of business. As the age of the customer arrives, all the focus shifts to the systems of engagement and the agility in refining these critical customer tools. Cloud technologies and services represent the fastest way for the business to reach new buyers and breathe new life into aging applications. In 2014, cloud leverage will be both traditional and disruptive as the business and IT put cloud to work. In this report, Forrester's cloud watchers weigh in on what they predict will happen in the world of cloud in 2014.

ENTERPRISE IT GETS ON BOARD AND CLOUD TAKES OFF

Last year, we predicted that enterprises would get real about cloud, and the data and Forrester customer inquiries proved us right. The cloud is not only a viable option for a broad range of workloads but has also quickly become the preferred option for reaching new markets and buyers faster and staying ahead of competition. The latest Forrsights surveys show that nearly 50% of business-unit-aligned developers already are or will build apps in the cloud by the end of 2014, 55% of their peers in IT ops consider private cloud a top infrastructure priority, and 31% plan to adopt public cloud infrastructure-as-a-service (IaaS) in the coming year.[1] This year, we'll see cloud developers and infrastructure and operations (I&O) pros tire of the squabbling, turf wars, and shadow IT buying and realize how much more they can accomplish with cloud when they work together. It's time for IT leaders to ask themselves who will deliver the cloud the business wants — and rise to the challenge.[2] The following are our top 10 predictions for cloud in 2014:

1. **SaaS will become the de facto standard for buying new applications.** Software-as-a-service (SaaS) has now overtaken on-premises in categories such as human capital management (HCM), customer relationship management (CRM), and collaboration. Solutions once available in multiple deployment modes are now SaaS only (e.g., Oracle RightNow and SAP Ariba seldom offer on-premises anymore). The holdouts: Large enterprise suites are still not available in a true SaaS mode but are increasingly shifting to at least an application service provider (ASP) model.

   What you should do about it: SaaS buying continues to be fragmented between line-of-business and application silo teams. This piecemeal buying creates challenges — especially with integration, total cost of ownership (TCO), and workflow. To address this, build out an app store service catalog for SaaS (see prediction No. 3) to help business leaders quickly and seamlessly provision these

FORRESTER®

Headquarters
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA, 02140 USA
Tel: +1 617.613.6000 • Fax: +1 617.613.5000 • www.forrester.com

application services with prebuilt integration, conformance to architectural standards, and visibility into use and cost. This central store for SaaS will balance the time-to-value and agility that the business wants with your corporate policies, IT standards, and TCO considerations.

2. **Public cloud will be the default backbone for IoT.** Whether consumer-led with FitBit, Nike FuelBand, and Samsung Gear, or enterprise-led with sensors, medical devices, and transportation, the Internet of Things (IoT) will generate billions of data points in 2014, and aggregating this data and acting on its findings will best be achieved by capturing, analyzing, and responding *from the cloud*. If you want to analyze billions of inputs in real- or near real-time, you won't want to drag the data all the way back to your data center.[3] A longstanding mantra in business intelligence (BI) has been that it's easier to move the compute to the data than the data to the compute. With cloud-based Hadoop and SaaS-based BI solutions proliferating, it's becoming hard to justify bringing this data down to analyze it.

   What you should do about it: Start getting familiar with Internet storage and BI solutions, especially the coupling of these within the same cloud platform environment.[4] On Amazon Web Services (AWS), this means Redshift, S3, and Elastic MapReduce. On Microsoft Windows Azure, you're looking at Blob Storage, SQL Database, and HD Insight. And on the Google Compute Engine, which just became generally available, look into Cloud Storage, BigQuery, and CloudSQL.

3. **The service catalog will become the strategic cloud entry point.** SaaS applications will become standard portfolio elements, and centralized IT procurement and management processes will rise up to support them. At the heart of these processes will be the service catalog, a place not only to define, advertise, and price the services IT delivers, but the vehicle to empower cloud consumers and IT pros alike through self-service, single sign-on, and centralized delivery. Service catalogs will go beyond the "how" of cloud delivery and engage the business consumer to decide "what" should be delivered and "when." The cloud service catalog is where enterprise governance, cost transparency, and end-to-end value chain management come together.[5]

   What you should do about it: Service portfolio management, the practice of developing, managing, and optimizing a cloud service catalog, is a critical capability to master in 2014 to keep your cloud services relevant, useful, and efficient. Your cloud service catalog is not only where you control cloud but where you *guide* users to the right cloud services for each of their needs. The business will continue to ignore IT operations teams that attempt to block or restrict public cloud adoption, so make sure your catalog is built for the needs of the business first.[6]

4. **Perimeter security will shift outside the perimeter, where it belongs.** The combination of cloud and mobility, predicted and proven in 2013, means there's no longer a perimeter to your business that you can control. Even if you tried to enforce perimeter controls, they would not

be very effective, as so much of the work is shifting outside your perimeter to the public cloud. Additionally, users have so many devices now that you can't enforce device security such as network access control (NAC), as the management overhead is too daunting. The focus needs to shift from protecting the network and the devices to protecting the data. With the network perimeter shrinking and the devices proliferating, your data is the one thing you can control.

What you should do about it: For enterprise clients, this means asking cloud providers and your developers — who will configure virtual networks on cloud platforms — how the network is designed so you can gain assurance that your data isn't just being thrown willy-nilly into a "cloud."[7] The next step is getting familiar with data-centric security tools that work in and outside your walls. For cloud providers, this means using Zero Trust design principles to design the network.[8] Zero Trust networks put the controls close to the data and support multitenancy as well.

5. **Australia will rise to the No. 2 public cloud computing market.** While Europe is certainly the No. 2 market if taken as a whole, Australia, as a country, is quickly taking up public cloud computing services. As with virtualization, smartphones, and other technologies, Australia is a very fast follower once the technology has established its value in the US and Europe, and this is quickly becoming the case for public cloud services. And before you think that it will be China, note that our research shows that its market is still in the virtualization and consolidation phase.

   What you should do about it: If you are an Australian client, look to your peers, as they are likely moving aggressively to embrace SaaS and move systems of engagement applications to the cloud. AWS, Rackspace, Dimension Data, Telstra, and CenturyLink are among the in-country cloud providers, with Microsoft and Google expected to join them in 2014. If you are a multinational looking to see where shadow IT is most rampant, the US is no longer your biggest worry. Look for a Forrester report on this market's cloud use in early 2014.

6. **Cloud-to-cloud continuity will get serious with SaaS.** Disaster recovery (DR) is a leading driver for public cloud use, but mostly by enterprises looking to improve the resiliency of mid- to low-end apps and for smaller companies putting their entire recovery strategy in the cloud.[9] But in 2014, cloud-based DR will go cloud-to-cloud.[10] The first phase will unfurl in the next year with cloud-to-cloud backups for mainstream SaaS offerings. In the SaaS market, enterprises struggle to restore data with steep recovery fees (or, in some cases, total lack of service) by their SaaS vendors. A new market of backup solutions is rising to meet this need with early solutions from Backupify and Spanning. These offerings automate the protection of critical data that is stored with SaaS providers, so organizations can recover this data if it is accidentally or maliciously deleted.

What you should do about it: Dig into your SaaS provider's policies to understand the support provided under your current contract. Make no assumptions around the ability or willingness of your provider to restore data, especially if the fault lies with you. If you're not covered, or minimal recovery is slow and expensive (some vendors charge up to $10,000 in fees to attempt a data recovery that may take several weeks), look to build out your disaster recovery and business continuity plans using some of the new SaaS backup services. Solutions on the market today cover the most popular SaaS offerings, but new vendors are continuously added.

7. **Chef and Puppet will usurp commercial automation solutions.** With the rise of public cloud platforms, these open source configuration automation solutions already dominate on GitHub, driven by developers and developer-focused IT operations (DevOps) teams alike.[11] In 2014, we predict that more new server workloads will be scripted, documented, and replicated automatically by these tools than by BMC, CA Technologies, HP, IBM, and other proprietary automation solutions combined, putting the fortunes for these tools at risk. Open source server configuration automation is quickly becoming the de facto cloud *service* automation approach and will dominate the management of elastic cloud workloads.

   What you should do about it: Reach out to and engage with your public-cloud-savvy development teams to learn how they are collaborating with their peers in IT to deliver new cloud services at the breakneck speeds required to stay competitive. They'll tell you how to break down the walls separating traditional development and IT ops teams and how to leverage the new class of automation tools designed for continuous delivery in the cloud. Think you need an army of IT pros to manage thousands of cloud servers? Think again. Today's open source automation tools let you put the principles of DevOps to work, whatever the size of your cloud.[12]

8. **Bring-your-own-encryption will dominate the security discussion in 2014.** One of the top trending inquiry topics hitting our cloud and security analysts lately are about cloud encryption gateways for AWS and salesforce.com. You can thank the US NSA for popularizing this trend. Clients are asking for recommendations on offerings that encrypt data before it hits the cloud service and lets the enterprise control the keys. Encryption covers a multitude of sins, and by encrypting the data before it hits the cloud, companies effectively strip the toxicity (and the liability) from the data. There is increased interest in using technology from companies like CipherCloud, AlephCloud Systems, PerspecSys, Skyhigh Networks, HighCloud Security, and Vaultive to encrypt corporate in-line data *before* it goes to the cloud. Also, look for larger vendors such as HP, Cisco, VMware, and IBM to acquire some of these intriguing startups in 2014.

   What you should about it: If you have toxic data that needs to be stored in the cloud, encrypt it with a cloud encryption gateway before it goes to your cloud provider. Don't rely on the cloud provider's native encryption solution, as the cloud provider holds the key. You want to control your data and mitigate the chance that the cloud provider will abuse your keys and data.

9. **Cloud security will expand to be much more centralized and automated.** If you're resisting the cloud because of security concerns, you're running out of excuses. The leading public cloud providers have made strong gains in security and compliance, and there are few workloads completely off-limits for public cloud anymore. At the same time, securing private clouds has become safer, more reliable, and easier to control through advanced management tools like HyTrust. We'll see cloud security vendors like CloudPassage, JumpCloud, and Illumio letting you articulate cloud security requirements in executable automation of business policies. Enterprises will achieve better security this way than on their own.

   What you should do about it: Assess your entire cloud portfolio's security needs to see how you can streamline and automate security setup. Since cloudbursting and rightsizing your cloud environment is a de facto requirement, look at automation of security setup during the Puppet or Chef initial configuration and setup phase and during the operations of the deployment using centralized security automation vendors. Providing easily usable interfaces and application programming interfaces (APIs) for security information and event management (SIEM), network security, identity and access management (IAM), and data protection will be the deciding factor in determining the success of SaaS use.

10. **Enhanced virtualization and private cloud will become separate initiatives.** Private cloud is the go-to term to describe everything above basic virtualization — regardless of whether it meets the basic private cloud requirements.[13] In 2013, Forrester saw four types of private cloud initiatives.[14] The most common was enhanced virtualization, which does not satisfy the growing cloud expectations of the business. But this initiative is important to the maturation and efficiency of IT ops and should be done because it improves deployment consistency and agility from two weeks to two days. As a result, in 2014, the enhanced virtualization initiative will be separated from the effort to build a private cloud.

    What you should do about it: Embrace the value of enhanced virtualization without discrediting your private cloud efforts that more closely match DevOps expectations. Making these separate initiatives will let you better align system of record and system of engagement deployments to environments that better suit their needs, evolutionary paths, and timelines. Recognize that the need to provide a private cloud that mirrors the public cloud is a project that must move forward faster than what's likely plausible within your existing virtualized environment.

SUPPLEMENTAL MATERIAL

Methodology

Forrester's Forrsights Hardware Survey, Q3 2013, was fielded to 2,306 IT executives and technology decision-makers located in Canada, France, Germany, the UK, and the US from SMB and enterprise companies with two or more employees. This survey is part of Forrester's Forrsights for Business Technology and was fielded from June 2013 to August 2013. ResearchNow fielded this survey online

on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates. We have provided exact sample sizes in this report on a question-by-question basis.

Each calendar year, Forrester's Forrsights for Business Technology fields business-to-business technology studies in more than 17 countries spanning North America, Latin America, Europe, and developed and emerging Asia. For quality control, we carefully screen respondents according to job title and function. Forrester's Forrsights for Business Technology ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of IT products and services. Additionally, we set quotas for company size (number of employees) and industry as a means of controlling the data distribution and establishing alignment with IT spend calculated by Forrester analysts. Forrsights uses only superior data sources and advanced data cleaning techniques to ensure the highest data quality.

We have illustrated only a portion of survey results in this document. To inquire about receiving full data results for an additional fee, please contact Forrsights@forrester.com or your Forrester account manager.

ENDNOTES

[1] Source: Forrsights Hardware Survey, Q3 2013.

[2] The future enterprise IT infrastructure is a hybrid mix of public and private clouds, but who will manage this new IT portfolio? Today, cloud developers are often doing it themselves out of necessity, but they should be focused on coding and testing. Infrastructure and operations professionals have the operations management skills, but they have not yet earned the right to take over cloud management. To build your cloud management practice in 2014, see the July 30, 2013, "Cloud Management In A Hybrid Cloud World" report.

[3] The carpeted parts of the business — marketing, sales, IT, and service desk — led the empowerment era. These business units harnessed the power of social networking, smartphones, and cloud computing to increase their efficiencies and provide better services to their customers. Not to be left behind, the concrete areas, such as manufacturing sites, hospitals, warehouses, farms, and substations, have recently jumped on the bandwagon with the IoT. See the October 15, 2013, "A Tsunami Of Empowerment Will Hit Your Network With The Internet Of Things" report.

[4] The Forrester Wave™ of public cloud platforms looks at what storage and BI options each of the leading clouds provide. See the June 14, 2013, "The Forrester Wave™: Enterprise Public Cloud Platforms, Q2 2013" report.

[5] IT organizations must now focus on the support, delivery, and operations of services rather than IT technologies. To do this you must have a service catalog. But most service catalogs today simply describe the capabilities and available services that IT offers to the business. Forrester recommends that IT infrastructure and operations leaders evolve their service catalog into a strategic control point for the business to enable visibility, agility, and control. Without one, your business will struggle. See the June 12, 2013, "Master The Service Catalog Solution Landscape In 2013" report.

6   In the age of the customer, only customer-obsessed IT organizations will survive the disruption. Tech
    management must prove itself by moving forward with two agendas: cloud IT (building critical infrastructure
    within the company) and cloud business technology (BT) — technology, systems, and processes to win, serve,
    and retain customers. Read about the four key imperatives that should guide your BT evolution. See the
    October 10, 2013, "Technology Management In The Age Of The Customer" report.

7   Trust is the fundamental problem in information security today. With a higher trust model, I&O managers
    can deploy networks that are easier to build and maintain; I&O can even make them more efficient, more
    compliant, and more cost-effective. Visibility gives security professionals insight into what is actually
    going on in their network and the ability to verify access and inspect behavior on the network. For more
    on network security and software-defined networking, see the November 8, 2012, "Workload-Centric
    Infrastructure Ignites Software-Defined Networking" report.

8   Forrester's Zero Trust Model of information security banishes the old security motto of "trust but verify"
    and replaces it with a new motto: "Verify but never trust." When you're trying to protect your organization's
    intellectual property and sensitive data assets, implicit trust assumptions are dangerous because they:
    1) leave your organization vulnerable to so-called "trusted insiders," and 2) become obsolete when the
    environment or technology changes — and in a world defined by continued digital disruption, your
    environment and your technology are always changing. See the September 12, 2013, "Transform Your
    Security Architecture And Operations For The Zero Trust Ecosystem" report.

9   Seventy-eight percent of public cloud adopters and planners identified disaster recovery as a top driver, just
    below lowered total cost (80%) and improved manageability (80%). Source: Forrsights Hardware Survey, Q3
    2013.

10 Cloud-to-cloud disaster recovery is the ability to failover infrastructure from one cloud data center to
    another, either within a single vendor's environment or across multiple vendors. See the March 20, 2012,
    "An Infrastructure And Operations Pro's Guide To Cloud-Based Disaster Recovery Services" report.

11 Rising in popularity just behind these tools are SaltStack and AnsibleWorks. Please visit the AnsibleWorks
    website (http://www.ansibleworks.com) and the SaltStack website (www.saltstack.com) for more
    information.

12 The ultimate mission of both dev and IT ops is to create competitive supremacy for your business. To get
    there using the cloud, you must dramatically improve your speed of execution, staff productivity, and
    service quality. Today's open source automation solutions have grown up in the cloud and will help you get
    there. For more tips to improve your DevOps practice, see the September 3, 2013, "The Seven Habits Of
    Highly Effective DevOps" report.

13 True private clouds include advanced virtualization, standardization and automation, self-service
    access, and resource usage tracking and monitoring. For more, see the May 8, 2013, "Case Study: Waste
    Management Builds A True Private Cloud" report.

14 The four strategies included enhanced virtualization, test/dev cloud, public-cloud-lite, and
    transformational cloud. For more information, see the October 28, 2013, "Four Common Private Cloud
    Strategies" report.