Trends and Impacts: The Changing Landscape of Cloud
Contents

Introduction ...........................................................................................................................................3

Global IT spend: Tablets stumble as cloud continues to make waves ........................................4

Legacy applications and a lack of cash hold back CIO innovation .............................................7

Cloud security and compliance trends in 2015, according to Vormetric’s C.J. Radford ..........9

Factor in the people side of cloud risk management .................................................................13

Governments must realize limits of control on cloud data, encryption ...................................16

What hybrid cloud? It’s hybrid IT ..................................................................................................19

Five takeaways ..................................................................................................................................22

About OpenText and ZDNet ...........................................................................................................23
Introduction

Cloud computing is a technology very much in flux. According to ZDNet’s recent Cloud Priorities survey, nearly 90 percent of respondent companies are using private cloud (in other words, privately hosted) environments, and 40 percent of those have been deployed for more than two years.

Public cloud resources and SaaS tools have been in use for even longer, but despite some companies having years of experience, many others are still not fully clear on how to approach cloud services. For instance, we’re still hearing about “shadow IT” – where business units circumvent IT and sign up for their own cloud-based services, and about risk-averse companies that aren’t willing to trust any data or process to the cloud. The fact is, cloud service providers haven’t done a sufficiently thorough job explaining how their offerings integrate with legacy systems, how they keep client data secure, and how they maintain compliance with relevant industry and government regulations.

It’s clear that one size – or type – of cloud won’t fit all. But many enterprises are finding success by phasing cloud services into their operations judiciously while updating legacy systems to conform with new models, essentially creating a dynamic and hybrid IT environment. They’re taking a long-term view and working incrementally toward it, while keeping security at the top of their priority lists.

According to RightScale’s 2015 State of the Cloud report, 88 percent of companies are using public cloud services, 63 percent are using a private cloud, and 58 percent use both. Even more compelling: 82 percent have a hybrid adoption strategy in place, up from 74 percent in 2014.

In this evolving world, the IT department takes on the dual role of resource administrator and resource broker. RightScale reports that, in 62 percent of respondent companies, the IT team manages most cloud spending. That leaves a sizable minority where cloud spend is out of IT’s hands, but the trend is positive.

This Tech Roundup will prove to be a worthwhile and insightful resource for business readers and IT professionals alike. It’s packed with relevant articles from TechRepublic and ZDNet on the critical issues facing enterprises today: Cloud trends, security, integration, risk management, and more. You will gain actionable insight plus several key takeaways to guide your adoption of cloud technologies. ♦
Global IT spend: Tablets stumble as cloud continues to make waves

By Toby Wolpe

With overall global spending on IT set to climb steadily this year to $3.83tr, enterprise software remains the biggest growth area. But its 5.5 percent projected increase over 2014 conceals considerable upheaval.

Because of intense competition between cloud and traditional on-premises firms, more price cutting and vendor consolidation are expected in 2015 in the enterprise-software segment, which is on course to total $335bn by year end, according to analyst firm Gartner.

“What we’re seeing now is a - I don’t know if it’s a tipping point but certainly an acceleration away from the license and maintenance model towards more of a cloud- and SaaS-based model,” Gartner research vice president Richard Gordon said.

“What that’s doing is really increasing competition. It’s having an impact on pricing and also both within the traditional software space itself and among the cloud providers as well. We’re seeing a little bit of that impact of price competition affecting the growth figure there.”

The major software categories of customer-relationship management, enterprise resource planning, supply-chain management and databases are all being marked by the shift towards the cloud model.

“If you look at something like CRM, on a global basis, we think that by 2020 all the new spending on CRM -

---

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$696bn</td>
<td>3.8%</td>
<td>$732bn</td>
<td>5.1%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$141bn</td>
<td>0.8%</td>
<td>$143bn</td>
<td>1.8%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$317bn</td>
<td>5.8%</td>
<td>$335bn</td>
<td>5.5%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>It services</th>
<th>2014 spending</th>
<th>2014 growth</th>
<th>2015 spending</th>
<th>2015 growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>$956bn</td>
<td>2.7%</td>
<td>$981bn</td>
<td>2.5%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Telecoms services</th>
<th>2014 spending</th>
<th>2014 growth</th>
<th>2015 spending</th>
<th>2015 growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1,626bn</td>
<td>-0.1%</td>
<td>$1,638bn</td>
<td>0.7%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Overall IT</th>
<th>2014 spending</th>
<th>2014 growth</th>
<th>2015 spending</th>
<th>2015 growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>$3,737bn</td>
<td>1.9%</td>
<td>$3,828bn</td>
<td>2.4%</td>
<td></td>
</tr>
</tbody>
</table>

*Worldwide IT spending forecast for January 2015, Gartner Research*
so in other words people who are buying CRM for the first time so it’s not existing spend but new spend in the market - will be using a SaaS-based model. That’s quite a dramatic shift in buying behavior,” Gordon said.

That underlying change is also having an impact on spending in the related sector of IT services, which is projected to grow 2.5 percent in 2015, accounting for spending of $981bn.

“As you move from a new license software model to a cloud model, there’s less opportunity for IT services in terms of things like implementation and system integration and also software support,” Gordon said.

“Spending there gets impacted because obviously if you move to a cloud model, you don’t have a need for those things. So there is some kind of knock-on effect in services.”

The Gartner figure for services growth in 2014 was slightly higher than this year’s projection, at 2.7 percent as opposed to 2.5 percent.

Datacenter systems spending is due to rise marginally from last year, from 0.8 percent growth and $141bn spending in 2014 to 1.8 percent and $143bn this year. However, it’s another area where the cloud is making its presence felt.

“We’re seeing this shift towards the hyperscale datacenter, so away from your traditional enterprise datacenter spending that individual companies would do, towards this service-provider model. We’ve got these large companies providing datacenter services or capability in a cloud-based model,” Gordon said.

“The x86 server is pretty much commoditized and these large Googles and Amazons are moving towards this model where they’re buying white-box servers or doing an OEM model where they’re actually building their own. Obviously that’s impacting the market for the branded servers. Across the market as a whole we’ve got this consolidation of server capability and larger hyperscale datacenters.”

Gartner has increased its projections for growth in enterprise communications apps and network equipment over its previous forecast but downgraded server and external controller-based storage figures.

In the devices market Gordon said mid-range smartphones are being squeezed out, with demand for low-end handsets and very high-end devices driving growth of 5.1 percent, up from 3.8 percent in 2014.

“There is this bifurcation in cell phones where we’re getting a shift towards very low-end handsets and very high-end smartphones. But in devices overall the thing to look at is the tablet, which is actually seeing a bit of a slowdown,” he said.

“The tablet filled a gap in the market between the laptop and the mobile phone. Nowadays, with notebooks
being lighter, thinner and more portable, and also with smartphones having larger screens - the phablet market - there's less need for the traditional tablet.”

Gordon pointed out that the present strength of the US dollar has led Gartner to revise its projections for IT spending downwards. Last year the analyst firm was forecasting overall growth for 2015 of 3.9 percent, as opposed to the new figure 2.4 percent.

“If we take away the exchange rate impact, [this year’s growth is] around 3.8 percent. So we’re losing one and a half points of growth because of exchange rate at the top level,” he said.
Legacy applications and a lack of cash hold back CIO innovation

By Colin Barker

Despite being in the top five technology priorities for government CIOs in 2015, investing in the much-needed modernization of legacy applications "may be a stretch" for many, according to the analysts Gartner.

Around 30 percent of federal and national CIOs say that they have to deal with a decreasing IT budget, compared to only 15 percent of state, local and regional government CIOs who said the same thing.

Why the difference? To start with it is not one difference but many, Gartner points out, as its figures show a strong regional variation. For example, 27 percent of the state, local and regional government CIOs surveyed in the Europe, the Middle East and Africa region indicate their IT budgets are declining, whereas only nine percent of similar CIOs in North America said the same.

“Similarly”, said Gartner, “the issue of declining budgets appears to be particularly acute in all tiers in the Asia/Pacific region.”

While the issue of legacy applications and systems is particularly acute in government it is not confined to that sector, but does create an additional headache for public sector tech chiefs.

“The burden of legacy technologies in government puts innovation on a path of incremental improvement when agility and quick solution delivery is expected,” said Rick Howard, research director at Gartner.

As Howard sees it, IT managers will have to make their infrastructure flip around. “To demonstrate ‘digital now, digital first’ leadership in government”, he said, “CIOs must flip their approach to managing IT from the inside-out perspective of legacy constraints to the outside-in view of citizen experience.”

Legacy First, Digital First, why not Cloud First?

As IT managers know, this has been a long standing complaint of not just governments but of organizations of all kinds who so often complain of IT departments that are out of touch or blind to changing priorities.

According to Gartner’s research, infrastructure and data center technology continue to be the top two priorities of government IT departments. However, Gartner believes that this is changing and that government IT organizations will slowly reduce their role as infrastructure providers and data center operators and will instead serve as a broker of those foundational services.

Gartner seems to think that a simple change in nomenclature would be helpful and IT organizations should
first move from “legacy first” to “digital first” - if they haven’t done that already - and they should then ask, “why not cloud?”

“In the US, this trend is reflected among state CIOs as they consider the advantages of private, public, community and hybrid cloud sourcing strategies,” Gartner said.

“With cost, value and security as top considerations, government CIOs should begin with the assumption that public cloud is the preferred deployment option and then, if necessary, work back from public cloud to the cloud, co-location or on-premises option that provides the best fit for their business environment,” said Howard. ◆
Cloud security and compliance trends in 2015, according to Vormetric’s C.J. Radford

By Brian Taylor

More and more Amazon Web Services (AWS) customers in 2014 could not make their networks as secure as using AWS/S3, explained Vormetric’s VP of Cloud C.J. Radford. This trend will pick up in 2015, with more enterprises using cloud applications in order to defend themselves from the rising tide of cyber threats.

In an email Q&A with TechRepublic, regarding 2015 cloud security trends Radford said he also expects that organizations will “open their coffers” to protect Software as a Service (SaaS) offerings, that more Information as a Service (IaaS) providers will offer encryption and access control services, and that hosted private clouds will exceed the number of in-house private clouds as the preferred environment.

Founded in 2001, Vormetric provides enterprise encryption and key management services to over 1,400 customers, including 17 on the Fortune 25 list. According to Radford, at present the main data security challenges for enterprises is “moving data to the cloud while keeping it safe, encrypted, and secure -- while still managing to retain key ownership -- across the entire cloud stack of infrastructure, platform, and software services.”

In our Q&A Radford also discussed how he would advise CISOs, protecting data at rest, the Vormetric data security solution, and compliance trends.

TechRepublic: With 2015 approaching, what do you consider to be the main data security trends?

C.J. Radford: I can tell you some of what I think we can expect to see on the cloud security side.

In 2014 we saw AWS customers saying they couldn’t make their own networks as secure as using Amazon’s AWS/S3 services. This trend will accelerate in 2015; small and medium business/enterprise usage of cloud applications will accelerate because they are unable to keep pace with the rate of change of attacks and threats, as well as the resulting legal and compliance requirements.

With over 50% of enterprise application spending in 2014 going to SaaS, and with sensitive data a large component of the information used and stored there, organizations will open their coffers to increase spending on protections for SaaS. SaaS providers that offer explicit security controls, as well as additional detail on data locations and written security commitments, will see their business increase at the expense of competitors who lag.

I also believe all serious IaaS and hosting providers will offer an encryption and access control service to customers. As the bar continues to rise for services to earn enterprise business, IaaS and hosting vendors will
offer a baseline and advanced service set to enterprise customers for data protection within their environments.

Lastly, hosted private cloud will take over from in-house private clouds as the majority private cloud environment. As economies of scale, service-level commitments and security visibility and controls become more widely available from cloud providers, enterprises will increasingly favor hosted private cloud environments that offer the best of both worlds. That happens to be the scalability available from public clouds, plus the increased security required for enterprise data protection and operation.

**TechRepublic:** How would you advise a CISO of a mid to large-size organization seeking to boost his or her data security capabilities?

**C.J. Radford:** When thinking about the security posture of mid to large-size organizations, I advise CISOs to think about the data that needs protecting and review what security solutions are being deployed up and down the IT stack in order to protect the data that matters most to the organization.

First, organizations should use “best in class” security solutions across the IT stack. One required adjustment is a need to add focus on protecting data where it is used. The reason for this is that strong perimeter, network, and end point defenses are no longer enough to protect sensitive data. No matter the strength of these traditional defenses, they are subject to compromise by attackers’ present suite of available attacks, mining techniques, and extraction strategies. Add to this the blurring of perimeters caused by cloud and mobile, and it becomes clear IT security strategies and implementations need a strong element of data protection.

Second, ensure that your organization’s internal IT and security policies and procedures are being followed and continuously tested to ensure compliance against those policies.

Finally, have a plan for when a security event happens to limit the negative impact of such event -- don’t get caught off guard because it’s not a question of whether you will have security event, it’s when and how it will occur. Invest in tools that can detect compromises early and have mitigation plans in place to minimize damage.

**TechRepublic:** Why is protection of data at rest critical to an enterprise cloud deployment?

**C.J. Radford:** Data-at-rest protection is absolutely imperative for enterprise cloud deployment, due to the rising tide of data breaches at high profile institutions, multiplying national privacy regulations, and increasingly strict compliance requirements. Enterprises that fall behind on any of these fronts will risk losing business opportunities, or worse.

There are very clear business and economic benefits that come from leveraging cloud environments, but those benefits are moot if enterprises don’t have proper precautions in place. Think about the reputational and financial fallout that occurs following data breaches, or the sticky legal challenges that arise when data residency laws aren’t respected.
TechRepublic: What are the main benefits of the Vormetric data security solution?

C.J. Radford: The Vormetric Data Security platform provides a complete solution across databases, platforms (Linux, Windows, Unix) and operating environments (data centers, big data, and private/public/hybrid cloud).

Our solution makes it simpler and less costly to protect information within databases. The platform allows organizations to deploy quickly in a uniform and repeatable way. Instead of having to use a multitude of point products, enterprises can take a consistent and centralized approach.

Along those lines, administration is also simple and efficient. Vormetric Data Security offers an intuitive web-based interface, application programming interface, and command-line interface. Because database security can be applied quickly and consistently across the organization, IT resources can be employed more efficiently.

And of course, the platform provides capabilities for encrypting data, controlling access, and creating granular security intelligence logs that help organizations quickly meet security and compliance requirements.

TechRepublic: What differentiates Vormetric’s technology in the data security marketplace?

C.J. Radford: Only Vormetric offers a single scalable solution for data-at-rest encryption and access control at the file system and volume level that can easily protect any file, database, or application, anywhere it resides. Competing solutions specialize in either encryption or access control, have limited support for OS platforms, cloud environments, and have limited key management options. Customers utilizing Vormetric receive a) transparent encryption b) fine-grained access controls c) security intelligence and d) broad cloud platform support.

TechRepublic: In enterprise cloud computing, what are the main trends in compliance?

C.J. Radford: Data sovereignty -- the idea that enterprises don’t like their data to leave the four walls of their own country, largely because of strict data residency laws or concerns about who has a legal right to access that data -- often comes up as a big (global) issue for cloud service providers (CSPs) with data centers located in jurisdictions different from those of their customers. Recently, we’ve seen CSPs like Amazon and VMware take the step of opening up database centers in other countries to meet that country’s customers’ needs. I suspect we’ll see more and more CSPs going this route as we usher in the New Year.

There are hundreds of data privacy laws on the books, but our mantra remains the same: enterprises concerned about meeting data residency requirements should encrypt all data-at-rest, and only allow access to data-at-rest from the jurisdiction that it originates from.
TechRepublic: How does the Vormetric solution enable compliance for your customers?

C.J. Radford: We serve over 1,400 customers in 20 countries across a broad range of industries including healthcare, retail, consumer goods, manufacturing, banking, insurance, government, and CSPs -- so it’s safe to say we have our finger on the pulse of compliance! In short, Vormetric Data Security provides a common, extensible implementation infrastructure that supports compliance regimes with protection for data-at-rest. Some of the most common compliance regulations our customers must abide by include HIPAA, Sarbanes-Oxley, and of course, state and national data breach and protection laws.

Top of mind for many of our customers is the Payment Card Industry Data Security Standard’s (PCI DSS) recent update. As of January 1, 2015, all companies that access, store, or transmit cardholder data and personally identifiable information will be required to meet the new 3.0 standard. Knowing how important this is to our customers, we actually issued a white paper about the new rules and how Vormetric Transparent Encryption helps achieve PCI DSS encryption.

Another important regulation is the new cybersecurity framework, or FedRAMP/NIST. Government agencies and CSPs who want to do business with the federal government must meet a baseline security standard. We took a similar approach towards NIST as we did with PCI DSS, and pulled together a white paper that maps Vormetric’s data security capabilities against the updated NIST security controls. ◆
Factor in the people side of cloud risk management

By Judith Myerson

A cloud risk management policy is about mitigating high risks to a lower level of risk. You should follow a four-step process when setting up the policy, taking into account how different users will perceive it (e.g., some users will want more flexibility than what’s in the policy).

How to set up a cloud risk management policy

Step one: Identify the assets

- **A Software as a Service (SaaS) user** is limited to the desktop, laptop, and/or tablet they use to access a SaaS application.

- **A Platform as a Service (PaaS) developer** works with more assets. A PaaS developer uses computers and their tools to develop and manage an application; this person also runs their application on an operating system provided by the service provider.

- **An Infrastructure as a Service (IaaS) specialist** works with network, storage, or compute resources provided by the service provider.

Step two: Assess the risks

You need to assess each asset’s risk and rate them low, medium, or high. It doesn’t matter whether a risk is man-made (e.g., faulty application logic) or a natural disaster (e.g., an earthquake-prone area).

Step three: Implement safeguards

Before implementing a safeguard, you should make sure it would result in mitigating a high risk to a lower risk level. Safeguard examples include a failover mechanism, leap year recognition, and nested firewalls and two-factor authentication (e.g., a strong password plus facial recognition). If a safeguard for an asset does not offer a positive return on investments, you should get insurance for that asset.

Step four: Review assets, risks, and safeguards

You should periodically review assets, risks, and safeguards (usually every three or six months). When you do, you may discover that:

- **New assets have been acquired.** For example, you get the latest tablet model from your organization, and you use it to access a SaaS application. Go back to the first step of identifying assets and start over.

- **New risks have emerged due to changing business requirements of an application you are**
developing with a PaaS. If your inventory doesn’t show any new assets, go back to the second step of assessing the risks. Otherwise, return to the first step and start over.

- New safeguards may need to be implemented. This can happen when a new technology can make a safeguard more efficient for less money or when new risks emerge. It doesn’t matter whether you are a PaaS developer or an IaaS infrastructure specialist. Do the four-step process again.

How different users may perceive the policy

The way a user perceives the benefits of cloud risk management is influenced by:

- the cloud role they undertake;
- the organization they work for; and,
- the controls they are granted by the cloud service provider.

A SaaS user’s perception

At any organization, the only control a SaaS user has is access to a SaaS application from whatever the device they choose -- it doesn’t matter if the application is accounting, human resources, or supply chain tracking. This user doesn’t have control over application development or virtual machines.

A SaaS user is likely to perceive the service provider’s cloud risk management policy as limited, because the provider will not let the user use his or her security tools to scan for SaaS application vulnerabilities.

A PaaS developer’s perception

A PaaS developer can use any security tools they like; therefore, they perceive the provider’s risk management policy as flexible. A PaaS developer controls the entire application life cycle, from concept to deployment, and they can build a security tool to test their safeguards. SaaS users will be happy with any safeguards that would be difficult obstacles for hackers to overcome.

A PaaS developer doesn’t have control over the operating system updates and virtual machines supporting the PaaS platform. The developer will likely be disappointed the provider will not let them implement safeguards for the operating system and virtual machines.

An IaaS network specialist’s perception

An IaaS network specialist can use his or her own security tools in the virtual infrastructure. This specialist likely perceives the provider’s cloud risk management policy as very flexible.
IaaS network specialists have control over the tools they need to safeguard the virtual machines from unplanned downtime. They understand the provider will not let them control its infrastructure of physical servers and networks.

Summary

Your best bet for mitigating or resolving cloud-related security issues is to consider the various people who will be using this policy and how each side might react to how you’re managing risks.
Governments must realize limits of control on cloud data, encryption

By Eileen Yu

Governments need to realize there are limits to how much they should exert control on issues that have global impact, such as cloud data and encryption.

The U.K. government, for instance, proposed a ban on data encryption that prevented digital communication from being monitored and read by law enforcement and intelligence agencies. Prime Minister David Cameron said he would propose new legislation, if he won the next general election, in a move deemed to potentially impact messaging platforms that encrypt their data, including apps such as WhatsApp and Snapchat, as well as Apple’s iMessage and FaceTime.

There are, however, already legislations that allow the government to monitor electronic communications for national security, said Rob Bratby, managing partner of Olswang Asia, where the Singapore-based lawyer advises on issues related telecom, media, and technology in the region.

He noted that the U.K.’s Regulation of Investigatory Powers Act 2000 was designed to enable the government to conduct surveillance, including accessing an individual’s electronic communications, if they followed the correct processes and procedures. It sets the boundaries within which the government can listen to conversations and requires proper approval before it is allowed to do so.

Voicing his disagreement for the proposed encryption ban, which he described as impractical and “not good from a policy perspective”, Bratby told ZDNet in an interview: “If the objective is [to enable] law enforcement to listen to [communications between] the bad guys, blanketing this with a ban is not the best way to achieve the objective.”

“Saying you want to ban encryption [to do that] is wrong... It’s a knee-jerk reaction to what happened in Paris,” he said, referring to last month’s terrorist attack on satirical weekly magazine, Charlie Hebdo, during which 12 people were killed.

Forcing tech companies to hand over data stored in foreign jurisdictions also shouldn’t be any government’s prerogative.

In a much-watched legal case that is still playing out in the U.S., Microsoft was found in contempt of court last September after it refused to hand over foreign data— held in its Dublin, Ireland, data center--to the U.S. government. It was defying orders do so by magistrate judge James Francis.
The New York-based judge had ruled that local search warrants must include customer data stored in servers located outside the U.S., referring to one issued to Microsoft for a customer’s e-mail data stored in its Dublin data center, which houses European citizen data.

Microsoft’s appeal against the ruling is still pending.

Reiterating his point about observing the necessary procedures, Bratby noted that the U.S. government could still access the data if it followed the proper legal processes, including those outlined by foreign jurisdictions.

“In this case, the U.S. government is saying they don’t care. The U.S. needs to be aware that they can’t do that on a global basis and that they aren’t the center of the global economy,” he said, adding that it will negatively impact the U.S. IT industry.

The good news is, elsewhere, the cloud industry is maturing and market players recognize the need to be transparent and for their data centers to be resilient and secure, Bratby noted. The Trans Pacific Partnership (TPP), for instance, includes a financial services chapter that looks at cross-border data flow to enable financial institutions to move data overseas, he said.

In most countries, financial services providers typically are required to store their customer data in the local jurisdiction, preventing them from using cloud services or data centers that host data in different countries.

**Emerging Asian ecosystem, innovation**

Noting the importance of the TPP from a legal perspective, Bratby explained that trade deals between nations often are centered around efforts to standardize local laws, including intellectual property.

In most countries, financial services providers typically are required to store their customer data in the local jurisdiction, preventing them from using cloud services or data centers that host data in different countries.
poured into these markets. Already, market players such as Xiaomi have been launching thinner and cheaper products, he added.

He also expects closed interest groups to grow in popularity, such as SpiceWorks, as well as social networks that provide targeted information for verticals. Wearables will also see wider adoption this year, where the use case is currently centered around health and fitness, he added.

He noted that this interest in healthcare could throw up legal discussions around personal data and privacy, particularly in EU countries where such data is classified sensitive and requires a higher degree of care. Consent for use, for instance, has to be more explicit. ◆
What hybrid cloud? It’s hybrid IT

By Eileen Yu

Hybrid cloud may be garnering increased interest and adoption, but it is already giving way to new terms such as hybrid IT and hybrid enterprise, which industry folks say are the next phase of the cloud evolution.

With increasing maturity and understanding of cloud services through actual deployment, the business IT environment is no longer simply defined as a public, private, or even hybrid cloud model. Instead, it is about managing an infrastructure that can offer agility and scalability, as well as the best platform on which to deliver applications.

“I sense even the term hybrid cloud is approaching a use-by date. If anything, I’m hearing more about hybrid IT,” said Bob Hayward, Singapore’s managing director at KPMG, at the Asia-Pacific Center of Excellence for IT Leaders. “As public clouds, private clouds, and community clouds are adopted, the ‘old’ IT environment is rarely completely replaced.

“As a result, many processes use systems that span cloud of all types, as well as highly virtualized stacks, new software-defined infrastructure, and a legacy traditional IT environment,” Hayward said.

Chris Levanes, CenturyLink’s Asia-Pacific director of cloud and managed hosting, agreed. He noted that hybrid cloud should be seen as a subset of hybrid IT, with a mix of outsourced and in-house IT services, which can comprise datacenter collocation, managed hosting, network, and cloud services.

He added that a managed hybrid IT strategy offers businesses the flexibility and agility to move IT workloads so they can operate a more optimal platform.

“Cloud technologies can be highly beneficial and offer many advantages, such as elasticity and scalability. However, there often are requirements that may drive organizations toward other deployment approaches,” Levanes said, pointing to applications that require exceptional levels of performance, direct access to the underlying hardware, or compliance of regulatory stipulations.

“[These] considerations of bandwidth, data transfer costs, and security can have an impact on a desired solution. Meeting business and IT goals often require more than just a hybrid or public cloud strategy. They require a comprehensive managed hybrid IT strategy,” he said.

This approach would allow businesses to easily expand geographically, and scale to meet fast-changing market trends, such as the Internet of Things (IoT), mobility, and e-commerce, he added.

According to Simon Naylor, ASEAN and Japan vice president of Riverbed Technology, IT innovations are pushing bandwidth demands up by 28 percent each year, through to 2017. Citing statistics from Gartner, he said this increase is due to enterprise adoption of cloud computing, mobile devices, and video.
Naylor added that the increase in bandwidth requirements is in turn driving the growth of hybrid networks. “The hybrid cloud has evolved with the appearance of what we call hybrid enterprise. Now, it’s not just where apps, compute, or storage are hosted, it’s also how they’re accessed and delivered,” he said, adding that the delivery platform is also going hybrid.

He noted that private networks are being coupled with VPNs and public online offerings for different delivery options, with mission-critical applications delivered on more costly private channels while bulk loads such as backup would run on cheaper public networks.

These applications are also being accessed remotely via a multitude of mobile devices, creating increasing complexities for the enterprise in terms of how they manage their IT environment. “It is this combination of private and public assets delivering essential business services that defines the hybrid enterprise,” he said.

Charlie Dai, Forrester’s principal analyst, further noted that hybrid cloud is not simply about running public and private simultaneously, but also about gaining automation for business agility.

“A hybrid IT environment gives organizations the advantage of customizing their infrastructures and solutions to meet their specific data, security and regulatory, scalability, and capacity needs.”

She pointed to the need to operate digital businesses as well as the emergence of IoT and mobility as the main drivers for hybrid cloud deployment.

Dai added that businesses should not view a hybrid model as a way to cut costs.

Levanes said, “A hybrid IT environment gives organizations the advantage of customizing their infrastructures and solutions to meet their specific data, security and regulatory, scalability, and capacity needs.

“It strikes the right balance of on-premises and off-premise compute, networking, and storage resources, and is more relevant to customer requirements of aligning business and IT,” he said.

Rise of the cloud brokers

Hayward urged enterprises to look past concerns about security and data sovereignty, or even the location of datacenters. While there are issues to consider with any cloud service, they should not necessarily lead to the decision to deploy hybrid cloud.

“In reality, hybrid cloud has very little to do with datacenter location or data sovereignty. It is where processes increasingly require functionality that spans multiple cloud services,” he explained. “Everything we do in business is unlikely to be fully available from just one cloud or even just one cloud provider.”

He noted that operating a modern business is complex, and supporting all functions necessary in a process
typically means deploying several clouds from multiple providers across different geographic locations. These would then have to be brokered, integrated, and orchestrated, he said, giving rise to concerns about how this should be managed.

In fact, this increased complexity has led to the emergence of new business models involving cloud brokers and aggregators.

“Many IT services firms see their future as a new form of intermediary to provide that single point of accountability, while they deal with the back end of multiple cloud services,” Hayward explained. “However, many also struggle, since they also provide some of those back-end services and are viewed as having a conflict of interest.”

Naylor further highlighted the need for visibility so the root source of an issue or sluggish performance could be quickly identified and addressed.

He said there are tools and technologies in the market that could track down and isolate the cause of service bottlenecks and outages, so problems could be narrowed down and resolved swiftly.
FIVE TAKEAWAYS

Five points you should take away from this reference guide:

The key to successful cloud deployments is to view the technology as a means to achieve important ends, such as operational efficiency, lower costs, improved customer and employee satisfaction, and headache-free security and compliance.

1. **Look at OpEx, not CapEx.** Purchasing servers is so 2005. Whether your goal is to support mission-critical transactional applications or to provision another hundred mailboxes, cloud should be the first option considered.

2. **Look for security in the cloud, not in house.** Fear, uncertainty, and doubt aside, the leading cloud providers deliver better security than most companies can afford to maintain in house. Look for SaaS and IaaS providers that include encryption, access control, data location, and privately hosted options in their offerings.

3. **Look at users, not policy manuals.** Design cloud access and authentication measures around the individual needs of each user class in your company. Sales reps interact with IT infrastructure differently than developers and analysts. Look at the tools each uses and the data to which each requires access, then build strategies that reflect real workflows, instead of vice-versa.

4. **Look at the world, not the building.** When you’re using cloud services, the IT infrastructure on which your business is running may be located thousands of miles away from headquarters. This creates tremendous opportunity, in terms of resiliency and agility, but it also may bring regulatory complications. You must ensure that your data is encrypted in motion and at rest, but you must also ensure that your security measures don’t run afoul of local rules, either because they’re too strong or not strong enough.

5. **Look at workloads, not servers.** In a well-orchestrated hybrid cloud environment, the needs of a given workload and the policies set by IT and governing bodies determine where and how the information is managed. If it’s considered highly sensitive, you may decide to keep it on premises. If it’s highly variable, it can be run in a flexible, off-premises/cloud environment. These decisions are part of analyzing the business and developing your cloud strategy.
About OpenText

The cloud doesn’t have to be nebulous. OpenText provides transparency into how your information is handled.

More than 65,000 customers rely on OpenText Cloud to drive $6.5 trillion in commerce annually. Unlike others, the OpenText Cloud is designed for enterprise information management solutions and is supported by a global, scalable, and secure infrastructure with data centers around the world.

For more than two decades, OpenText has been providing enterprise-class global applications. OpenText is the leader in Enterprise Information Management, helping customers prepare for a Digital-First World by simplifying, transforming, and accelerating their information needs. Learn more at www.opentext.com/abettercloud

About ZDNet

ZDNet (www.zdnet.com) is where technology means business. The site attracts an enthusiastic and interactive audience of business technology influencers, many of whom visit for the latest coverage and analysis of how technology impacts business. Business leaders and decision makers including CEOs, CIOs and IT professionals at all levels value the site due to its extensive resources, enabling them to make the most out of technology for their business challenges.