



Mobile Goes into the Cloud

Despite research demonstrating that the cloud can be a boon to IT and the business it supports, there's still hesitancy by some to embrace the platform. Data privacy is the biggest concern for IT executives looking to move to the cloud, according to a January 2011 survey by the IT Governance Institute (ITGI). In fact, 49.6 percent of executives surveyed cited security as their number one concern, according to the nonprofit ITGI's report. Cloud isn't the only technology making people nervous, though. Privacy and security are also concerns for those IT executives looking to enable smartphones and tablet usage within their organizations. You'd think then that — with the perceived threats of mobile and the cloud — IT would make sure the two could never come together. However, some experts say that mobile and the cloud may be a match made in IT heaven.

“With the increasing need for IT people to make sure the right people in the right places have the right information, merging cloud and mobile platforms may make perfect sense for many,” said Brad Eskind, principal federal technology leader at Deloitte Consulting. “The power of the cloud gives our government services folks the ability to do so much more than they could in the past, and it adds a level of security to wireless that mitigates the inherent threat that comes along with those devices.”

Consider the biggest problem with mobile: the fact that data resides on the platform itself and can result in data loss if the device goes missing. The cloud can eliminate that problem, storing information and data, which is then accessed when needed. “Virtualizing all your applications and access through a client or Web browser means if the device is lost or stolen, it's just a device without sensitive information on it,” agrees Sascha Segan, lead analyst for mobile devices at PCMag.com. It also makes collaboration easier since data can be shared with multiple people, including employees and constituents, he said. Previously, it was impossible to collaborate using a mobile device.

Making IT Work

Indeed, while a major driver of cloud computing has been a reduction in capital expenses — at least on the

mobile side — the benefits seem to be an increased flexibility for a platform that may be convenient but certainly isn't agile, said Windsor Holden, a principal analyst with Juniper Research. “When you're using the cloud in conjunction with a mobile device, you can extend the solution to employees in the field, allowing them to have access to documents and synch documents to the office,” he said. “It results in a productivity bonus. People don't have to wait to work until they get back in the office, and you're always working from the same data.”

Companies can also use the cloud to enable applications and functionality that can be more difficult to administer and create with a traditional client-server implementation, said Richard Schum, senior industry analyst with research firm INPUT. “The cloud facilitates mobility with unified communications applications, which can be offered as both a component of Infrastructure as a Service (IaaS) or Software as a Service (SaaS),” explains Schum. It also makes it possible to allow almost every employee to work remotely as long as the correct security precautions are in place, he said.

There are some drawbacks to accessing the cloud via a mobile device and network. IT, for example, should make users aware that even with today's ubiquitous mobile networks, they can't assume that they're always going to be connected. This can be a serious problem for anyone who relies on the cloud for his or her productivity applications and data, said PCMag.com's Segan. “Even in the densest city you can hit a dead zone,” he said. “You as an IT person must be thinking about what you can do to make sure your user can still work, which might take some custom development.” One option might be to cache just enough data so a momentary loss of connectivity won't render the device useless, he said.

However, considering the fact that almost three-quarters (72 percent) of agency IT departments say they have already deployed mobility solutions, according to a February 2011 INPUT report, yet only 33 percent of federal executives say they have the tools they need to be productive, it may be time to take the marriage of cloud and mobile seriously. ▲



Tablets Poised to Make an Impact

Law enforcement officers in Jefferson County, Tenn., have them. The General Services Administration is rolling them out. The City of Williamsburg, Va., gave them to its city council and other key staff. The Interior Department has given them to about 1,000 field agents. As these examples demonstrate, tablets are hot right now, and not just in the public sector.

“The form factor of the smartphone is just a little too small. It’s not easy replying to a complicated e-mail or looking at an attachment,” explains Dr. Michael Salsburg, a spokesperson for the Computer Measurement Group, a nonprofit group focused on ensuring the efficiency and scalability of IT service delivery. “A tablet provides a whole lot more space, as well as ease of use, and access to the applications and connectivity that make it a real productivity device.”

So much so that after less than a year on the market, tablets have become big business, according to Oppenheimer & Co. The company in January 2011 predicted that the total shipments of tablet devices will explode from 15.1 million units this year to more than 115 million by 2014, topping \$55 billion in sales. The numbers are not surprising given the exponential growth of Apple’s iPad, which nearly hit the 7.5 million unit mark between the time it debuted in April 2010 and the end of the third quarter of 2010. The growth will come from Apple’s device as well as from new tablets from Dell, HP, Motorola and Research In Motion, the company behind the ever-popular BlackBerry device. The most surprising part: More than a quarter of the devices will be purchased by the enterprise, according to a Deloitte Consulting report.

“If you think about the movement, what’s driving apps to mobile platforms, you see how tablets can be used in the field when coupled with cloud services,” said Brad Eskind, principal federal technology leader at Deloitte. “Some things like grants management or data or predictive analytics are easily handled on a tablet.” The reasons are

simple. Today’s tablets have dual-core processors, which provide the computing power to handle advanced, processor-hungry applications. In addition, tablets ship with touch screens, the ability to connect to a network via Wi-Fi or wireless carrier, and an already well-established software development base so custom applications can be built quickly and cheaply.

“Tablets are basically filling a lot of niche requirements,” agrees Richard Schum, senior industry analyst at INPUT, who said that tablets, at least in the foreseeable future, will be a complement to more traditional computing devices. For instance, Schum recently interviewed law enforcement officials who were looking for a device to use in the field for fingerprinting and photo identification. Tablets worked well, said Schum, because of their form factor and the fact that customized applications were easily created. In effect, they allowed the law enforcement agents to do their jobs more effectively and efficiently, two elements that will come into play as new devices such as Research In Motion’s tablet entry, the PlayBook, is introduced this year.

And then there’s the cloud connection. The tablets play well in the cloud since they can act as not-so-dumb terminals, offloading storage and data, which helps boost end-user security. “Tablets have solid state memory, but not nearly as much as you’d find on a laptop hard drive, so when you attach it to the cloud, the possibilities become unlimited,” said Schum.

And we’re only seeing a small portion of what tablets will enable, said Sascha Segan, lead analyst for mobile devices at PCMag.com. “It’s very early days for tablets,” he said. “The apps are still nascent, and while they are growing, it’s still clearly an embryonic technology. With Android tablets just entering the market, and the RIM PlayBook hitting shelves, the landscape is going to look totally different by the end of the year. Q4 2011 is going to be a great time for tablet users.” ▲



No Ties that Bind

Remote users have cut the wires that connect them to the network, literally.

Today, anyone with a mobile device that supports tethering and has an active wireless connection can use it to link a PC, laptop or other mobile device to the Internet.

Typically, tethering happens via Wi-Fi or Bluetooth over a 3G or 4G network, which means users can connect virtually anywhere at any time and — since many mobile devices can become mobile hotspots — using anyone's device. The impetus for tethering is its ease of use.

Phones often ship with a Wi-Fi hotspot mode built in, and even those that don't are simple to upgrade using free downloadable apps, taking IT out of the equation.

While this may be a relief for users who previously relied on an Ethernet connection and USB modem or an air card installed on a laptop to get online, it's a challenging development for IT administrators, said Albert Lee, an analyst with Enterprise Management Group. "From an IT perspective, when you set up a user to access the network with a laptop, you have all the control," he explains. "The laptop starts in IT, so you can make sure there's the right security in place to protect the data while in transit and on the client side and the network. Now, with tethering, the control is lost. It's up to IT to track down all the devices and make sure they have a secure connection."

If they don't, one of two things may happen. The first is fairly innocuous: Someone may "borrow" your bandwidth, using your wireless connection to access the Internet. The other is more nefarious. Someone can intercept your packets or, even worse, gain access to your laptop or network. To mitigate the problem, IT has to jump back in and ensure that the same technology that kept the laptop safe — strong encryption, a good password, and a firewall or VPN connection — is there on the mobile device, said Sascha Segan, lead analyst for mobile devices at PCMag.com. "The real breakthrough has been how easy it is to tether, so people are doing it without consulting IT," he said. "You've got to get those devices in so you can set them up safely."

Richard Schum, senior industry analyst at research firm INPUT said that, in some cases, agencies and organizations may just want to eliminate the threat completely. "The issue is that once you're tethered, essentially you've got wireless access to the Internet," he said. "That can be a big problem. Some administrators may just need to lock the devices down so tethering can't happen."

Putting a Cap on IT

While tethered security is the most pressing issue for IT administrators, there are other things to think about as well. For instance, while some employees might think twice about downloading videos on their mobile device, it can become very appealing to stream live content onto a laptop, said PCMag.com's Segan. Those agencies that have limited data plans can see mobile bills skyrocket when this happens. Even those organizations that have unlimited plans can run into trouble if their employees start using an inordinate amount of bandwidth, said Segan. "The providers that don't charge you for going over your data allocation may choke down your data speed for the rest of the month, which will impact productivity for those who rely on their devices for business applications and usage," he said.

Segan suggests setting up alerts that monitor all of your wireless accounts and ping you if any of those devices or monthly plans start getting close to their data allocation. You can also approach this problem from a process perspective, suggested Dr. Michael Salsburg, a spokesperson for the Computer Measurement Group, a nonprofit group focused on ensuring the efficiency and scalability of IT service delivery. "There's no way to block [tethered data access] for specific uses, but you can set up a policy and let users know that they can tether for business but not for video, and make the employees who go over their data limits personally responsible for those extra charges," he said. ▲



Rogue Mobile Devices Tax the System

Only two years ago, users got their hardware and devices at the office. Today, however, a growing number of employees are coming to IT with their own tablets and mobile devices demanding network access, and the ability to use those devices in their day-to-day work environments. And, increasingly, their requests are being fulfilled, even in the government sector, since cost savings and user satisfaction are top of mind. According to a November 2010 study from research firm Ovum and the European Association for e-Identity and Security (EEMA), 48 percent of employees are allowed to use their own mobile devices to connect to corporate infrastructures.

While it may be good for users, some IT managers are struggling with this decision, according to the same report. In fact, eight out of 10 CIOs surveyed said the practice of using smartphones in an enterprise increases its security vulnerabilities.

“From a user’s perspective, it’s more freedom because they are picking their own devices, but now, as an employer, you need to figure out how to secure the device. There may also be a legal liability question when you use a device for both personal and work,” explains Sascha Segan, lead analyst for mobile devices at PCMag.com. The worst part, he said, is that many users don’t even ask, going around IT and using their devices to perform job-related tasks, send and receive work e-mails, and access an organization’s data.

And, unlike in the old days when a company owned all the data on a mobile device and could wipe the data clean or remotely disable it, there’s no one silver bullet when it comes to managing these rogue devices, a fact that’s changing the way IT is handling almost everything under its care, including servers, remote access, and data storage.

Reining in Control

It’s fairly clear that allowing user devices to connect to an organization’s infrastructure works only if IT starts two steps ahead of users, taking not just technology but people

and processes into account, said Dr. Michael Salsburg, a spokesperson for the Computer Measurement Group, a nonprofit group focused on ensuring the efficiency and scalability of IT service delivery.

“You need to adapt all of the processes and best practices you use in the data center so that — from an end-user perspective — there’s no difference between how I use my laptop and how I use my tablet or smartphone to connect to the network,” he said.

For those organizations that are willing to allow access, standardization can definitely help, said Richard Schum, senior industry analyst at research firm INPUT, since it reduces problems for the IT department. For instance, the National Institute of Standards and Technology (NIST) is, in some cases, working on certifying mobile applications and platforms such as cloud computing as well as device- and operating-system specific security. For instance, BlackBerry devices can be configured using the Federal Information Processing Standards 140-2 (FIPS) protocol. “It makes it easy to set policies, and if something does go wrong, it takes some of the onus off of IT,” said Schum.

Network connections should also be secured. Anyone accessing the infrastructure via his or her carrier connection or Wi-Fi should do so over an encrypted VPN. “On the IT side of things, the main focus has to be on a secure connection,” agrees Albert Lee, an analyst with Enterprise Management Group. “Everything has to be under the auspices of the IT department, and based on the government labs and agencies I’ve been working with, there’s a different level of security needed due to data sensitivity, so additional planning is necessary.”

Even with a VPN, controls must be in place to make sure each user can access only what’s necessary for him or her to do the job. Unfettered access is a risk, which is why IT should follow the “less-is-more” mandate.

continued on page s7



Traveling with a Mobile Road Map

How do you keep track of something that by its very name is mobile? That's the question facing IT administrators as mobile phones and tablets enter the infrastructure. A second question: How do you limit your liability should a device go missing?

From a device management standpoint, before a mobile device is handed to an employee, it should be tagged with a unique identifier that is externally visible. In addition, devices should be inventoried and logged in and out manually every time they are assigned. Loaner devices or tablets that are used on premises are especially vulnerable since, unlike laptops, they can't be fitted with cable locks to make sure they stay put. Another best practice: Every device — whether tablet, mobile phone or smartphone — should be issued with a case.

“Assume any device you give out is going to be dropped several times, left in a restaurant, and given to a child to amuse him or her,” said Sascha Segan, lead analyst for mobile devices at PCMag.com. “People are butterfingers. People get drunk and leave their prototype iPhones in beer gardens, and everyone uses Angry Birds to entertain their toddlers.”

When it comes to safeguarding a device against loss, IT departments may want to take a page from the State of Iowa's playbook. The organization maintains strict written policies that help minimize risk should a device be lost. Devices — all of which must be password-protected — must have the ability to be remotely erased and disabled after 10 unsuccessful password attempts, and when they are reported lost or stolen. They are also instantly locked after a maximum of 15 minutes of inactivity, and, among other policies, are erased entirely

when an employee leaves government employment or no longer needs a mobile device for state business — even if that device is owned by the end user. The State of Illinois has similar policies in place, but it also requires all devices to be virus scanned before connecting to any state IT systems.

These are policies that should be emulated, said Richard Schum, senior industry analyst at INPUT, and augmented by centralized administration, which can help agencies cut down on loss, he said. “One of the major aspects of security that is sometimes overlooked is what happens if you have a phone out there that's been lost? This is one of the reasons that we think central management and administration of mobile devices is so important for agencies and subagencies,” he said. “When you have oversight, you can quickly mitigate risks.” As an added benefit, centralized management can also help keep carrier charges in check, he said. “When you're dealing with third-party carriers, you don't want to have a million different plans. You want one or two that give you what you need at the right price.”

With 72 percent of all organizations reporting that they have adopted mobile communications, and only 3 percent saying that mobile isn't in their plans, according to a recent INPUT study, not to mention the fact that an average of 13 percent of respondents' budgets is being used for wireless communications, such policies are critical.

“When done right, enabling mobile devices becomes very powerful for users and administrators,” explains PCMag.com's Segan. ▲



continued from page s5, Rogue Mobile Devices...

“Certainly, with the advancements in identity access management (IAM), you can use role-based security for any device that you’re using to connect to the Internet,” said Brad Eskind, principal federal technology leader at Deloitte. “This identifies you as an individual and the role you have [within an organization] to give you access to the applications you should have access to as well as to the right subsets of data, cutting down on malicious penetrations.”

Finally, organizations may want to look into mobile device management (MDM) solutions, which help IT distribute software to and configure mobile devices and increase security across the board. In some cases, MDM solutions can remotely lock a device, wiping out any data and proprietary information associated with it. “Allowing use of smartphones affects employee recruitment and retention,” said Schum. “This may not be a popular response, but it’s worth the effort to make it work.” ▲



Your Challenge:

More People Working in More Places

Mobile workers require more than just a notebook or tablet—they need network access, software, security, and support.

» Our Solution: A Team of Experts

We can help with deployments from 10 to 10,000 units. Our in-house specialists hold more than 500 active technical certifications and can design and deploy custom IT solutions—from inventory planning to asset disposition, and everything in between.

 We have the product selection, technical expertise, and purchasing contracts you need. Call an Account Manager today to get started.



Smart Buy HP ProBook 6450b
#11792314



Smart Buy HP 620
#11792277



Smart Buy HP ProBook 4520s
#12115446



1-800-800-0019

www.govconnection.com

gov is all you need™

GovConnection
A PC CONNECTION COMPANY