



<http://www.nojitter.com/post/232200692/a-pragmatic-take-on-byod-and-cloud-security>

A Pragmatic Take on BYOD and Cloud Security

IT is put back in charge of the enterprise environment and as long as they also supply the apps and applets that digital natives expect, then BYOD issues can be mitigated.

"Fear of the unknown is a powerful emotion. But when you're an IT exec, fear of the unknown--particularly when you're talking about moving into the cloud--really comes down to fear of making a costly mistake." Those words come from [Logicalis](#). And all too often, fear is compounded by all the negative coverage that appears on the Net.

There has been a lot of speculation about what computing experts think of the cloud, but the most important people in this space are the CIOs and CTOs. They are putting their jobs on the line and maybe the future of their employer, so one would expect them to be cautious.

To find out, Logicalis decided to explore whether the cloud was living up to their expectations. The company conducted an interesting research program: Instead of doing phone interviews, they analyzed more than 35,000 online forum and social media posts from the target market over 60 days, and found the comments to be overwhelmingly in favor of cloud computing. "Positive" and "very positive" comments outweighed "negative" and "very negative" comments by a dramatic 23:1.

The majority of the inputs came from tech-centered message boards and forums, followed by Twitter and industry blogs. Positive posts cited cloud computing as "cost effective," a means of increasing capacity beyond a current IT environment and an effective way to free up internal staff, resources and budget. Negative posts included concerns about the difficulty of transitioning and managing applications in the cloud as well as the perceived legal, regulatory and business risks associated with the cloud. And of course security is almost always perceived as being the biggest risk.

BYOD (Bring your Own Device)

Right now there's a lot of noise being generated about BYOD--Bring Your Own Device. IT doesn't like smartphones, but can't stop them coming into the company and being used on the corporate network. These days employees have the upper hand; it's ICT democracy in action.

But I'm old enough to recall the time when PCs entered our lives and IT didn't like them one little bit. When dumb terminals accessed IBM mainframe computers IT was in control. They had absolute power. Where would we be today if that kind of ICT dictatorship had prevailed?

"The seemingly obvious solution to making BYOD work for the enterprise would be to allow the smartphone to maintain dual personalities--you log in as your non-work persona, and you get all your personal settings; or you log in as your work persona and get an entirely separate interface that's walled off from the personal side. That work persona is completely managed and controlled by your corporate IT department." Those words come from "[Split Personalities for BYOD Smartphones](#)".

Split personalities are enabled by a software security mechanism: a "sandbox". That's the popular term and it's visualized in figure 1 below. In real life sandboxes are wide open, so it's a somewhat unfortunate term and it only works if the users follow corporate guidance. There is a wall between the business data and the user's personal data, but stepping over to the latter side is easy and it can be done without thinking, for example, by visiting Apple's tempting App Store while at work and downloading an app that might be infected. Therefore security can be breached unwittingly, but this "issue" is the same for notebook PCs.

As in so many other ICT areas, expert opinions are divided: some back the concept; others see it as an intermediate solution. Either way, it's effective if employees are made aware of the reasons why there's a wall and they respect corporate guidelines.



Figure 1. One security strategy is to adopt a "sandbox approach." This involves storing enterprise data and applications that are encrypted and password protected in one part of the

device. The remaining files, e.g. music, videos, and photos are retained and made available to users that are not logged onto the corporate network.

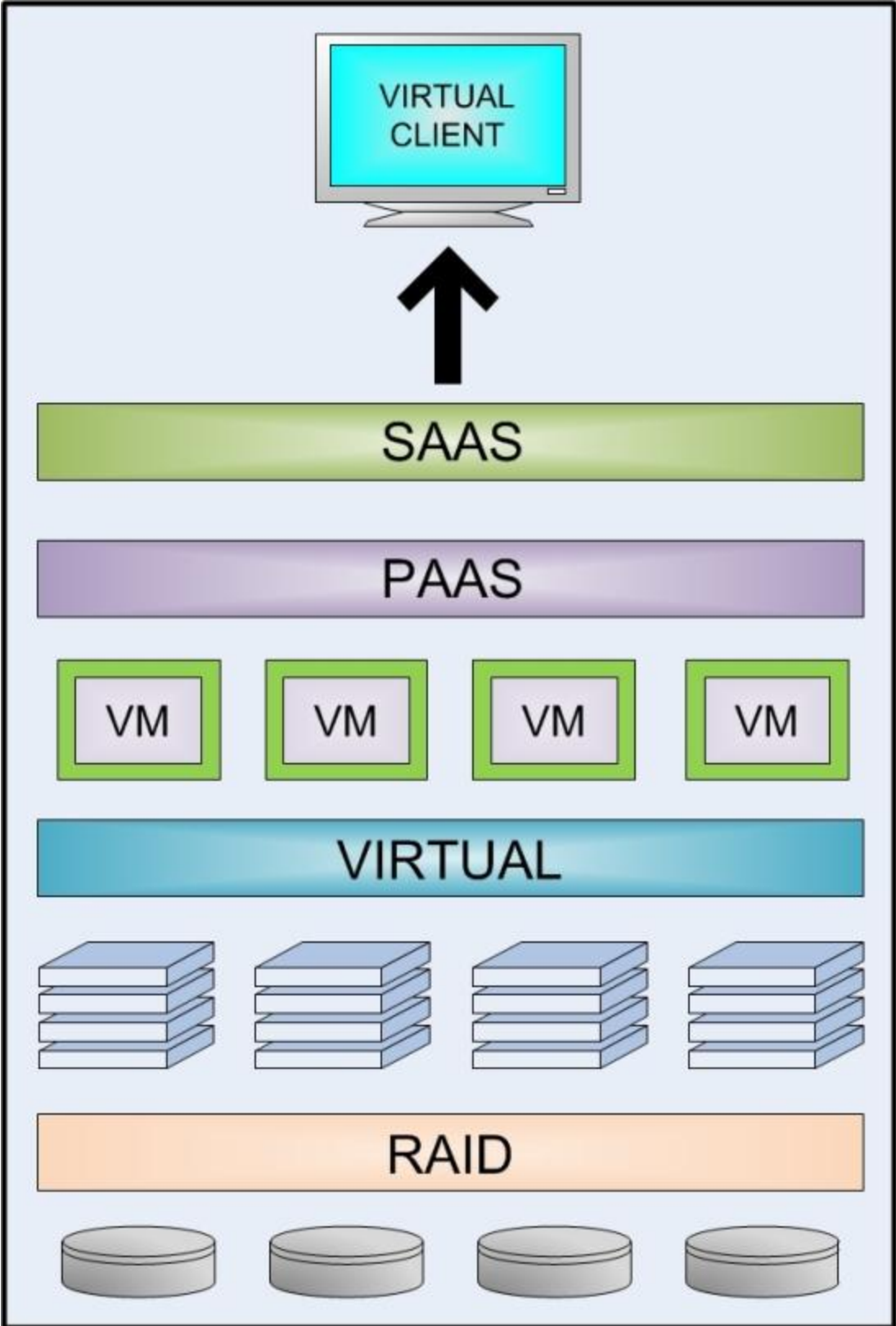
Be Pragmatic There is an obvious need to minimize breaches of security, but this task goes beyond simply securing the technologies. Solutions have to be pragmatic and relevant to the processes they are going to protect, so there may be trade-offs. Users have to work with the solution and if usage is too complex or cumbersome it won't be effective. For example, if corporate policies are too restrictive, users may look for ways of circumventing them. Moreover, lack of user adoption could result in the benefits of a mobile solution not being realized.

This means that C-level management should take a more active role as security shifts from being technology-centric to business risk-centric. Security decisions should involve business-level discussions, and management is in the best position when it comes to determining the risks involved. And as has been mentioned many times, the biggest security risk may turn out to be a disgruntled employee.

In addition, staff should be involved before solutions are implemented. They need to understand the reason for changes in work procedures and if necessary, training should be provided.

Manage and Secure the Apps

The new devices, smartphones and tablets, have to be managed. That's clear. IT needs to be aware of everything that is being used. Have any been unlocked? And in the event of a device being misplaced, lost or stolen, IT must be able to remotely wipe enterprise data, leaving personal data intact. The same function is enabled when employees leave the company, taking their personal device with them. However, it's really the apps that do the damage: malware compromises security and that's not new. Moreover, the cloud environment *can* be secure--in fact, it can be even more secure than a datacenter. But not all clouds are created equal, nor for that matter are all datacenters.



Security software from VMware, shown here in green, is "wrapped" around the virtual

servers. If a server is compromised the application continues to run on another virtual server. No malware reaches the client devices.

Enhanced security comes from virtualization. As illustrated in figure 2 above, there are four basic levels. RAID (Redundant Array of Independent Disks) combines multiple disk drive components into a logical unit. This is virtualized storage. At the next level we have lots and lots of servers. Google, for example, currently runs about 900,000 servers in different locations to power its empire.

These physical devices are virtualized. There are virtual machines (VM), a software implementation of the servers and they execute applications and programs like physical servers. Different servers run different apps, but each app will run on lots of different servers, so if one server falls over there will be no impact on performance at the user level.

If we go on keeping things simple but not too simple, then wrapping the individual VMs with security software can enhance security. So if one server is compromised, then it is shut down and once again there is no impact at the user level. No malware reaches the client devices.

If we skip through the rest of the stack, we see how the VMs enable the delivery of a computing platform as a service (PaaS), the key benefit being that the apps can be deployed without the cost and complexity of buying and managing the underlying hardware and software. And in turn software can be delivered as a service (SaaS) to the end-user devices.

Virtual Clients

End-user devices become virtual clients when this concept is employed. A virtual client doesn't need to run any software: no apps and no operating system. It becomes a de facto terminal. Recall these earlier words: when dumb terminals accessed IBM mainframe computers, IT was in control.

In reality the device is still a smartphone or tablet. It can be software-switched into terminal mode when employed in the enterprise and switched back to fuller functionality for personal use. And if it is compromised, there is no impact when it's in terminal mode. Right now VMware's concept is a work in progress and it is generating a lot of interest, but currently there is no information on how the terminal mode can be enforced.

Conclusions

BYOD is a hot issue, but it's not a not a new concern: IT didn't welcome the arrival of PCs. Almost inevitably the security issue has been overhyped by some sections of the media. The other side of the coin is the fact that C-level management in some companies is in denial and so far there haven't been any reports of major breaches of security caused by smartphones or tablets.

However, that is not a reason for rolling the dice and seeing what happens. A security solution should be implemented and right now the sandbox concept fits the bill, the only caveat being the need to inform employees and have them respect corporate guidelines.

Looking further down the road we have the more ambitious solution of VMware and others coming over the horizon. Virtualization can also securely isolate apps with different trust levels, quarantine compromised apps, and protect sensitive business data. IT is put back in charge of the enterprise environment and as long as they also supply the apps and applets that digital natives expect, then BYOD issues can be mitigated.