Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Security vs. Convenience – The Cloud – Mobile Devices – and Synchronization

The sea change has come. The mobility requirement, driven by the expectation that data and talk are available anywhere and any time make decision-makers and information workers more productive, has led to the need to synchronize data between smart phones, desktops, laptops, pad computers, and other similar devices. Combine this with the collaboration culture and you get cloud services – the only realistic way to achieve these simultaneous goals. Now consider the alternatives for these services.

- **Google** with the Android platform on mobile devices, reasonably integrated into everything desktop, laptop, pad, and phone, with Linux, OSX, and Windows supported.
- **Apple** with iPhone, iPad, Mac Desktops, and MacBooks, integrated through MobileMe then cloud services and barely tolerant of other operating environments.
- **Microsoft** with its limited cellular systems, no realistic pad computer, strong but not as dominant desktop and laptop positions, and Exchange servers for synchronization.
- **An emerging company:** A smaller, possibly emerging company, services your needs.
- **Roll-your-own:** It's harder but more certain to meet your specific needs for a time.

Each has its security and convenience factors, and each has its limitations.

Realistic options today and the security implications

Microsoft: For enterprises willing to go the Microsoft route, email and calendar synchronization is good to go through Exchange servers. The private cloud solution is widely used, but support for document sharing and collaboration is limited. Of course remote desktop support works, but it's too slow for realistic operation over the myriad of networks in use today, and trying to use a remote desktop to look at a document from a smart phone is ridiculous – even though it works – sort of. Try to support multiple users working together and you have to go to a sharing mechanism like WebEx, which works nicely from pad computers, but is all about meetings in person and not about collaboration on documents. For that you use change marking on documents and a person who owns the document mediates the changes. Social media? Forget it. If you want to be up to the latest on mechanisms, you will need a non-Microsoft smart phone. And that means all of the potential compatibility challenges.

Apple: Apple is a consumer electronics company that is being embraced by enterprises. As such, it is largely oriented toward individuals and small groups working together. But as cloud services of all sorts grow and social media becomes increasingly central to human interaction online, Apple which started ahead of the game by brilliant innovation, is slipping. MobileMe, which used to be .Mac, has lost its luster and is unable to keep up with the rest of the World. It doesn't support the platforms most users are now using, and the statistics show that, unless things change, Android platforms will outsell Apple by the end of 2013. From a security standpoint, Apple is all about Apple, and you have to go through and trust them.

Google: Google is emerging as a force in this market and in other related markets, and is clearly a major player now and into the future. Their purchase of hardware platforms, support of Android and its loose ties to the open source world, their incredibly effective infrastructure and acquisition and development strategy, all bode well for their future. But like all emerging giants, they are becoming more and more proprietary in their thinking and this drives into the security realm. The company store is not mandatory at Google like it is with Apple, but it's standard. And their easy integration of email, calendar, and contacts, along with their top of the line technology for integration of all things, drives better data quality, brings more information more readily to bear, and makes the cloud aspects of their operations more or less seamless. The only problem – you have to trust Google with your data. The day will come when it's not longer worthy of the trust, and your exit strategy will be tested – severely.

Some emerging company: There are many emerging services (e.g., dropbox and sugarsynch), but no other competitors fuse together the cloud, synchronization, and endpoint operating environments like these three. While Moodle may be used for coordinating meetings for a time, having the gmail calendars of all of the participants available will make the process far easier, and you can bet that google will take it over. Apple will have some variation as well, and Microsoft already has it's outlook scheduling capabilities. Niche after niche may emerge, but none will fulfill the enterprise need like the large players. For smaller players, for a time, some such companies may be worthwhile, and for specific verticals, like education, legal, etc. there will be successful niche players as there are already today. But whether the niches will win out over the major players is mostly a matter of whether or when the major players decide to buy the niches out.

Roll-your-own: The problem here is keeping up with all of the differing needs and platforms. If you have a relatively small number of requirements that can be met with relatively small effort, your own server may work, but remember, you will need application-level support for all of the different platforms you integrate with, and that can be pretty painful.

My current approach when I care

I recently purchased an ACER A500 to replace my iPad – partly over concerns about being too tightly tied to Apple services and infrastructure – and partly because it brings some unique potentials to the table. I like the mobility and convenience, but I am worried about security for key critical content that I want to bring with me. Here's my current best approach to using it in a more secure mode with the minimum of inconvenience. Note that this works only on a pad computer with the features identified...

> **To go from insecure to secure operations:** I go into airplane mode and disable all external communications channels. Then I reboot. From the clean reboot, I insert the USB drive with the content I want better protected. I use it at will, making certain that the programs I use to access the content don't make copies of content on the internal A500 file system. This I do by testing in advance and only using ones I have tested in this way.
>
> **Returning to insecure mode:** When I am done, I remove the USB drive, reboot to wipe out memory and processes that could store the data internally, and after the device is back up, I enable networking and go about my insecure business.

Slightly less secure with communications: If I need to communicate with the secured content, I go from secure to less secure by enabling wireless connections but turning off automatic updates and other related synchronization. I limit wireless to use the mobile hotspot of my cell phone, which is SSL protected to limit interference from other systems in the area, and behind the cell phone's network address translation (NAT) gateway to limit external attacks directly reaching the A500. I then run a secure shell session (SSH) back to infrastructure and move files one way or the other, or in limited cases, issue commands to remote systems. I then disable the WiFi access when not using it.

The reboot process takes less than a minute, so this whole color change process adds two minutes or less to my time, in exchange for which I get far better protection for the information I care about. Of course I can only use the information in limited ways, but then that's the whole point of doing things securely.

I could do a bit better with this device. For example, I could fill the local disk with empty content so no file system writes could be made by the programs I am using to access the USB drive. But that takes quite a bit of time because the internal storage is substantial. I could write custom software to access the USB drive and keep it in some special format or encrypt it, but then I would have to write all the software to access and display each file type, etc. I could also do a reboot from the write-locked local microSD card I can insert into the device forcing a restore from the device before startup. That's not bad, it only adds a few seconds to the reboot process... but I'll save that for another day soon when a commercial Linux vendor will introduce this capability in a more secure operating environment. I could also use cryptographic checksums to verify integrity of applications run in secure mode, but then I would have to write custom applications for that purpose, and that reduces simplicity from my perspective.

Conclusions:

Today, the iPad is still better ergonomically than the Android pad computers, but the competition is heating up and soon Android pad computers will beat iPad in the market and in the hearts and minds of the users. Microsoft will remain a non-entity in this space for the foreseeable future, but Exchange servers can be an effective way to control some of the content on these remote devices – at least keeping them from sending enterprise data to the amorphous cloud providers you may or may not trust.

The combination of cell phones for remote access and NAT gateway WiFi over SSL to pad computers is an increasingly compelling as a solution. The multi-mode operation of color changes is workable and more secure than many alternatives in the market today, but still not up the the surety level I like for important operations.

In the coming months, I expect to see at least one vendor come up with a bootable microSD card with a write-locked Linux distribution that will run on pad computers, and with special embedded security features designed to provide the sorts of features I want in a remote secure platform. The USB drives will be encrypted with FIPS certified hardware and software, and perhaps a biometric capability will be added. And with SSH tunneled through SSL, NAT gateway protection through the cell phone, and related features, I see a bright future for this technology, balancing convenience with security, while lightening my load.