

GroupLogic

5 Things You Need to Know About iPad in the Enterprise

Introduction

Without a doubt, iPads are one of the fastest adopted computing platforms in history. And, not just for consumers desiring to play Angry Birds. These tablets, with an entirely new browsing and usability paradigm, are rapidly making inroads into the enterprise, being tested, according to Apple, by more than 80 percent of the Fortune 100.ⁱ Aside from direct acquisition of the devices by the enterprises themselves, end-users are bringing them to work and using them in a variety of ways, intent on increasing productivity and making their work lives—and their personal lives—more efficient through easily accessible information away from a computer.

While iPad presents the potential to bring a wealth of measurable and profitable benefits to the enterprise as well as happier, and, hence, more productive employees, it also brings a number of challenges and risks that threaten to lead to security breaches and compliance violations, regardless of industry.

In this white paper, we'll discuss the top 5 Things you NEED to know about iPad and integrating them into an enterprise environment so you can protect and maximize existing IT and corporate assets, mitigate security and compliance risks, and keep IT in control, all while ensuring employees are happy and at their most productive.

1. iPads are Already in the Enterprise (like it or not)

With or without IT's blessing, iPad users are using their devices for work purposes (95% of employees say they use personally purchased devices for work use).ⁱⁱⁱ That means without a native file system on the device and enterprise security and management capability, users are employing the "work around," putting the enterprise and its assets at risk and compromising compliance efforts.

Even if your company institutes a "no tablet" policy, it's virtually impossible to keep employees from bringing their own devices to work—and coming up with their own ways to access files. End-users are forced to either email themselves a file or utilize unsecure environments from consumer-based cloud providers like DropBox to store and access files on iPad. That means uploading corporate data to an unsecure environment, then downloading it onto an iPad, viewing and/or saving it in third-party apps that are unsanctioned, inaccessible and unmanaged by IT, equating to a massive security risk.

Enterprises that directly acquire iPads for task workers, intent on deploying enterprise productivity applications on the device from sales force automation to field service, face the same issue as those contending with employees bringing their own devices into the workplace.

Whether you're an enterprise embracing the consumerization of IT and hearing from C-level executives on down that you need to support the iPad for business use, or you are looking at the iPad to deploy specific workforce applications to select employees, you're probably acutely aware of the need to ensure secure access to critical enterprise information—and to lock down the device if it poses a threat to your organization's critical information. The key is to address it upfront with the right solutions.

"Mobile devices are quickly becoming our primary computers...And tablets...are widely seen as potentially replacing the personal computer."ⁱⁱ

– Fred Vogelstein, Wired, May 2011

Forget whether you believe tablets and smartphones will replace the PC. Whether tablets like iPad settle in as an accessory or a replacement for the PC, tablets are not going away and are becoming a crucial part of productivity for enterprise workers as well as consumers.

iPad Enterprise Adoption Facts

- 15M iPads sold by the end of 2010 (Apple)
- 7.33 million iPads sold in Q4 2010 (Apple)
- More than 80% of Fortune 100 deploying or testing iPads (Apple)
- More than 500 of the 11,000-plus applications built specifically for the iPad are in the business category (WSJ)

Fact: 95% of consumer-purchased devices are used for work (Unisys)

2. Lack of Native File System and Centralized Storage

iPad introduces a completely new user mode and browsing experience. A revolutionary UI and paradigm shift in computing usability results in a new way of handling and interacting with files. On iPad, files must either be created on device or transferred to it via individual applications. This poses a game-changing paradigm shift in the way users are accustomed to accessing, editing and transferring files between devices and corporate file servers.

iPad does not come with a user accessible file system. When iPad is connected to a computer, it can sync music, videos, and apps through iTunes, but a user can't personally copy files over to the device the way they would to a PC's flash drive or other mobile device. iPad provides a way to search the user's music, video, apps, contacts, etc. but does not allow the user to browse or search the actual files stored on the device.

iPads also don't have a way to centrally store files anywhere on the device—most applications are universes unto themselves, and maintain their own file storage systems that can only be accessed via that individual app. There are a few consumer-based applications, like readers and editing-based applications that allow application-related files to be opened in another application. When this is done, the file is copied to that app's private storage area and then exists in two places on the iPad – multiplying versions. That means the unsecure “work-arounds” are required, putting confidential and critical files, enterprises have spent years, time and money creating, at risk.

3. No built-in access to corporate file servers

Out of the box, iPad is designed to receive files from iTunes syncing and through consumer cloud-based services like Apple's MobileMe. Unlike a Mac or PC, the iPad has no built-in ability to connect directly to a corporate file server, the hub of information for productivity and knowledge-sharing essential to people doing their jobs, regardless of what line of business or job function.

Again, the most popular “work-arounds,” present a security risk to the enterprise as there is no way to ensure consumer and cloud-based file storage services are transferring—and storing—files under the heightened encryption and password-protection required by most enterprises to ensure asset protection, mitigated risk and compliance.



4. Mobile device management provides no capabilities for managing individual applications

While some mobile device management (MDM) solutions allow for the provisioning, tracking and remote management of the device as a whole and for specific sanctioned mobile applications to the device, all enterprise applications are accessed through an on-device sandbox provided by the MDM vendor. Typically, within that sandbox are enterprise-focused, often custom-developed applications like field service, asset management, time tracking, sales force automation, email and PIM, etc.

If corporate documents are part of the predetermined enterprise application workflow such as an installation manual required by a field service rep, or access to equipment history for a technician, those documents are secure and can be locked down within the sandbox. However, once the user exits the MDM sandbox, the device user still cannot access enterprise files that exist on the standard corporate file servers, which may be required for other tasks outside of the predetermined workflow of the task-focused application.

In an effort to solve that problem, again, end-users turn to unsecure third-party cloud providers to gain access to corporate files on iPad. Once a user has installed a file-sharing app and moved corporate data into it, that data is almost certainly being stored unencrypted—whether on-device or in the cloud—and is outside of corporate control. The only way to remove that data is to wipe the entire device.



What is required to maintain IT control of corporate files is to take advantage of Mobile File Management (MFM) solutions that can address the security requirements of today's enterprise, which include:

- *On-device search, access, browse and view features which simply place a file browsing and storage system on iPad that is natively lacking for enterprise use;*
- *Rapidly deployable server-based software, installable on leading file servers;*
- *Centralized server and client management tools designed specifically for IT that allow rapid deployment and configuration of client and server deployments;*
- *On-device file encryption;*
- *Secure transfer of files through direct, encrypted connections between file servers and the device;*
- *Remote wipe capability that is application-specific to MFM;*
- *Direct integration with Active Directory for extending security protocols and permissions direct to iPad.*

5. Best practices for providing secure file access for the iPad

Secure file access for iPad is possible with the help of innovative software developers with experience in streamlining the interactions between divergent operating platforms within the enterprise such as Macintosh computers and Window-based servers. When considering the products available to help securely integrate iPads into the enterprise while allowing users to access their work files with ease, IT departments should ensure the following:

- File access on-device is password-protected
- *Corporate IT has management tools to ensure rapid configuration and deployment of client and server-based installations*
- Security standards are met for data transfer between server and device through over-the-wire encryption
- *Enterprise files on the iPad are kept encrypted between use*
- Access is controlled using corporate user accounts (aka Active Directory accounts)
- *The ability to email, print, and move files to other applications can be limited based on individual enterprise security requirements*
- The device can be remotely wiped of sensitive corporate data in the event the device is lost or stolen

Conclusion

iPad is making inroads into the enterprise – and its rapid adoption and popularity make it a key productivity enhancer for every worker as mobile employees become the norm, including executives, task workers and knowledge workers. However, its usability and browsing paradigm as well as its lack of native file and storage systems present security challenges for those enterprises desiring integrate them into workflow and IT infrastructure.

Until iPad is equipped with the Mobile File Management—its rapidly increasing presence in the enterprise presents a bigger and bigger burden for IT departments, whether the tablets are issued by the company or walk in via the employee. Mobile file management needs to be simple to use, secure to access and transfer critical files, integrate with existing security solutions like Active Directory and easily managed by central IT departments. Only then will the enterprise be able to truly unlock the power of iPad as business continues to grow more mobile.

About GroupLogic

GroupLogic® helps enterprise and education IT organizations simply and securely integrate diverse computing platforms into enterprise environments, connecting employees and students to enterprise files, content and assets to facilitate a more productive and efficient work environment. With more than two decades of experience, GroupLogic leads the marketplace in helping IT organizations effectively and easily manage the integration of Apple products into the enterprise ecosystem. Whether IT organizations are looking to integrate existing Apple assets, purchase additional Apple hardware like Macs and iPads, or want to take advantage of the hardware costs savings that accompany the adoption of IT consumerization, GroupLogic enables IT organizations to easily and securely manage the rapid integration of diverse platforms while ensuring resources are optimized. GroupLogic enables the enterprise to focus on what is really important – competitive differentiation, improved employee productivity, mitigated risk and reduced costs. GroupLogic's proven products—mobilEcho, ExtremeZ-IP, ArchiveConnect, and MassTransit—are in use by some of the world's most innovative companies, including Christie's, International Greetings and Omnicom Group.

ⁱAccording to Apple COO Tim Cook on the company's Jan. 18, 2011 earnings call; "iPad Adoption Up 80% in Fortune 100," Rue Liu, BusinessInsider.com, Jan. 18, 2011: <http://www.businessinsider.com/ipad-now-deployed-or-tested-in-80-of-the-fortune-100-2011-1>

ⁱⁱ"The Android Explosion," Fred Vogelstein, WIRED, May 2011: http://www.wired.com/magazine/2011/04/mf_android/

ⁱⁱⁱ"Consumerization of IT Benchmark Study", Unisys Corporation 2010: http://blog.unisys.com/files/2010/08/10-0190-CIT-SUMMARY_web.pdf