iOS Security and Mobile Device Management Whitepaper

February 2013

Jigsaw24 Professional Services - Jigsaw24 is a trading name of Jigsaw Systems Ltd, The Old Mill, High Church Street, Nottingham, NG7 7JA. Sales Tel 03332 400 100, www.Jigsaw24.com. Registered in England and Wales 2682904. VAT Registration No, 610706674.

Contents

Introduction

What is Mobile Device Management?

Primarily, enterprise MDM software solutions are a policy and configuration management tool for mobile handheld devices, such as tablets and smartphones.

In addition, MDM solutions enable swift deployments of these devices at large scale and ease the transition to a more complex mobile computing and communications environment.

Although delivered primarily as an on-premise appliance or virtual machine, some MDM providers offer a cloud based model.

Supporting both corporate-owned and personal devices, these solutions are also enablers for Bring Your Own Technology (BYOT) schemes.

Gartner indicates the main tenets of MDM as:

- Software Management; provision, manage and support mobile apps, content and OSs.
- Network Service Management; report on usage, and cellular and WLAN network information.
- Hardware Management; beyond basic asset management, allowing for inventory, provisioning, imaging, and reporting on performance, battery life, and memory.
- Security Management; enabling enforcement of security policies through remote wipe, passcode settings, encryption, authentication, access to secure network services.

Until recently, the industry standard for securely delivering mail, contacts, calendars and documents to a mobile estate in a corporate environment has been the BlackBerry; deployed, managed and secured through the BlackBerry Enterprise Server (BES). It is against these standards that other smart devices, and the architecture that supports them, are being evaluated for adoption in the enterprise. With industry experts expecting 80% of all businesses to support a tablet estate by 2013[1] , and with the vast array of platforms and operating systems on the market, one of the major concerns for organisations is which manufacturer, or manufacturers, will provide the most benefit, without compromising the security and the integrity of the enterprise. Similarly, organisations are looking to Mobile Device Management (MDM) solutions to ease the deployment and management of these platforms, as well as to provide a security standard across a range of devices from different manufacturers. Understandably, the granular lock down that the BES enables is not something that enterprises are willing to part with should they adopt a tablet platform.

Although comparisons to BlackBerry and the BES architecture are prevalent to the discussion of the adoption of new technologies, it is just as important to acknowledge cultural changes, caused by the consumerisation of IT, that now blur the lines between personal and business devices and data. To that end, prior to the discussion of what technologies to adopt, enterprises should evaluate any existing mobile device policy that is currently enforced and revise it accordingly. The assumption of this document is that an enterprise mobile device policy has been agreed and that it has taken into consideration: firstly, the philosophy and culture of the company; secondly, a thorough risk assessment of corporate data; and finally, the security policies and regulations that need to be enforced. Only then is a company in a position to fully evaluate the technologies and deployment schemes that will best support it.

This document provides an overview of the security technology and features that exist within the iOS platform and then outlines the Mobile Device Management tools inherent in Apple's native architecture. As an extension of this, an overview and comparison of industry standard enterprise infrastructures that provide basic MDM features and third party MDM solution providers will be discussed. The intention of this whitepaper is to enable organisations to objectively evaluate iOS as a viable and secure platform to deploy within an existing enterprise infrastructure, and the additional tools available to manage these devices and build bespoke enterprise-grade security solutions.

[1] "Gartner's Top Predictions for IT Organizations and Users, 2011 and Beyond: Its Growing Transparency," Gartner 2010.

iOS Security

Apple are committed to ensuring that every component of the iOS security platform provides organisations with the resources and flexibility to create enterprise-grade security solutions, bespoke to the needs of each business, without making the device and architecture difficult or cumbersome to use. The primary concern of this chapter is to address the main security technologies of iOS that make it enterprise-ready. Secondary to this, key built-in iOS features that enable MDM solutions to provide additional levels of security and management over a large scale deployment of iOS devices will be introduced, but discussed further in following chapters.

System Architecture

A secure system architecture tightly integrates hardware and software to provide the foundation of the iOS platform, and validates activities across all layers of the device to ensure only trusted code and apps can run on a device.

A secure boot chain contains components that are cryptographically signed by Apple to ensure integrity, and prevents the lowest levels of software from being tampered with whilst ensuring that iOS can only be run on validated Apple devices. If, for some reason, any level of the boot process is unable to load or verify against the next, boot-up is stopped and the user is required to restore the device to factory default settings.

Regular software updates combat any emerging security concerns and, as of iOS 5, can now be delivered wirelessly to enable rapid adoption and prevent legacy operating systems existing simultaneously. This process is authenticated against the Apple installation authorisation server, which sends the device cryptographic measurements for each part of the install. Devices are also prevented from downgrading to older versions of the software, to prevent any malicious attacks that have been created by reverse engineering any software updates and patches. Comparatively, the Android platform, described as "insecure, with a multiple-personality disorder," by Garner's Infrastructure Security Analyst Eric Maiwald, opens itself to the risk of viruses and data-gathering Trojans due to the multiple versions of the OSs on the market.

All iOS apps available on the App Store are verified by Apple and require, by mandate, all executable code to be signed using an Apple-issued certificate, which ensures that all apps come from a known and approved source. This acts as a deterrent to the creation of malicious apps, as well as extending the concept of chain of trust from the OS to apps. Unlike other mobile platforms, users are unable to install unsigned apps from websites that may potentially contain malicious code, unless they have jailbroken their iOS device. Jailbreaking a device gives the user root access to the operating system and enables the installation of software from outside of the Apple App Store environment, which increases the risk of exposure to malicious attack. However, many third party MDM solutions will detect a jailbroken iOS device and automatically revoke access to corporate resources and wipe sensitive data from the device. As an additional security measure, all third-party iOS apps are "sandboxed", to prevent compromising the OS, other apps, or data within other apps; application programming interfaces (APIs) provide secure communication between apps, should they need to transfer data.

Encryption and Data Protection

Encryption and data protection provide a second layer of security, to protect a user's data, should other parts of the security infrastructure become compromised. With a dedicated AES 256 crypto engine, built into the DMA path between the flash storage and main system memory, the hardware of every iOS device ensures speed and power efficiency whilst performing complex cryptographic operations. Furthermore, a device's unique ID (UID) and device group ID (GID) allows data to be uniquely tied to a particular device so that if the memory chips are removed and placed into a different device the files are inaccessible.

Above and beyond hardware encryption, Data Protection technology is leveraged to secure data stored in the iOS device's flash memory; designed specifically for mobile devices to account for events such as incoming calls while the device is locked, without decrypting sensitive data and downloading new information. When a new file is created on the device it is encrypted with a unique 256-bit key, which is used to secure, open and decrypt existing files as they are read from the flash memory. Furthermore, a new file is assigned a class by the app that created it, which determines when the data is accessible based on the different policies of each class. For instance, one of the classes allows for files to be securely written to memory while the device is locked, such as downloading mail attachments or songs from iTunes.

When iOS is installed on a device, a random key is generated and used to encrypt the metadata of all files in the file system. The "Erase all content and settings" option, which a user can initiate or can be exploited by MDM solutions to issue a remote wipe, is designed to erase this random key and therefore render all files associated with it cryptographically inaccessible. All these keys and Data Protection classes are managed by four keybags: System, Backup, iCloud Backup and Escrow. The latter of these keybags, Escrow, allows iTunes to sync and back up without the need for the user to enter a passcode, and can also be leveraged by an MDM server to remotely clear a user's passcode.

Network Security

Organisations can safeguard data in transit by leveraging industry standard network security measures, as iOS supports: Secure Socket Layer (SSL v3) and Transport Layer Security (TLS v1.1, TLS v1.2); Virtual Private Networks (VPNs); Wi-Fi protocols and authentication methods; and Bluetooth encryption modes. Settings for these network services can be installed manually by the user or installed as part of a Configuration Profile, which can be pushed to the device via an MDM solution. Unlike other platforms that require firewall software to protect against open communication ports against intrusion, by limiting listening ports and removing unnecessary network utilities iOS also removes the need for firewall software.

The following passcode policies are made available for enforcement by all MDM solutions, through Exchange ActiveSync (EAS), or by installing Configuration Profiles on the device:

- Allow simple value
- Require alphanumeric value
- Minimum passcode length
- Minimum number of complex characters
- Maximum passcode age
- Passcode history
- Auto-lock timeout
- Grace period for device lock
- Maximum number of failed attempts

Device Access

Flexible security policies and device configurations can be set by the user, or enforced by the enterprise through MDM, to ensure the device remains compliant with corporate security policies. These following iOS features will warrant further discussion in following chapters, however it is important to indicate that the following lock down settings can also be performed on an individual basis, by the user.

A user may secure an iOS device with a passcode that can range from the default four-digit PIN to longer, alphanumeric passcodes, and automatically induce a wipe of the device after 10 failed passcode attempts; the threshold for automatic wipe due to incorrect password entry can be lowered using MDM solutions or through Exchange ActiveSync (EAS). Device passcodes also secure more than just unlocking the device, as they provide entropy for encryption keys, which means that data in certain protection classes is also secured. Further to this, the passcode is integrated with the device UID, which means that brute-force attempts must be performed to attack the device. To discourage brute-force attacks each passcode entry takes approximately 80 milliseconds to authenticate, which would translate to 2½ years to manually crack a numeric only nine-digit passcode. If the user has enforced the automatic wipe after 'x' number of failed attempts anyway, then this becomes a moot point.

Device restrictions can be implemented to allow the user to: prevent use of services such as the camera, Safari or the App Store; stipulate access to content, such as films and apps, based on age restrictions; and control privacy settings on services like Bluetooth sharing, contacts and location services. Many more device restrictions are available to the user but there are additional restrictions available to IT administrators through MDM solutions or by installing Configuration Profiles on the devices. These additional features will be discussed in more depth later in this document.

Apple's Mobile Device Management Infrastructure

All MDM solutions for iOS devices are built on core Apple technologies such as the Apple Push Notification service, Over-the-Air Enrolment and Configuration Profiles. With these foundations an enterprise has the ability to securely enrol devices, wirelessly configure and update settings, monitor and report on compliance and remotely lock or wipe devices. Through this chapter these technologies will be detailed and the various tools that Apple provide within the native infrastructure to leverage these technologies will be introduced.

The foundations of Apple's MDM

The Apple Push Notification service (APNs) acts as an intermediary between an iOS device and an MDM server, and it communicates with this server to identify any pending tasks that require appropriate actions. Removing settings and data, providing requests for device or network information, or updating policies are all tasks that can be set on the MDM server and actioned through the APNs. For instance, if an IT department updates its Wi-Fi settings, the MDM server can configure an enrolled iOS device with new account information over the air, via the APNs. This prevents the end user from having to manually modify settings or calling into the help desk, as the appropriate configuration is already in place. Some network configuration may be required if the organisation decides to place the MDM server and iOS devices behind a firewall, as certain ports are required for communication.

The main function of the push notification service is to wake the iOS device and force it to check in with the MDM server to directly receive new configuration information and settings, all of which are provided over an encrypted SSL/TLS connection. In order for the APNs to provide these actions and to enrol devices in MDM an SSL certificate must be requested, downloaded from the Apple Push Certificates Portal and uploaded to the MDM server. For information on how to request an Apple Push Notification certificate, visit **www.apple.com/uk/iphone/business/integration/mdm**.

Devices can be enrolled Over-The-Air once the MDM server and network are configured, which allows them to be managed without further user interaction. This enrolment process is a scalable way to securely associate devices with users and the MDM server, within an enterprise environment, and is made up of three key phases; user authentication, certificate enrolment and device configuration. Many MDM solutions integrate with Active Directory, or similar directory services, to ease user authentication, during which the user's device information is captured. After authentication the iOS device receives an identity certificate from the enterprise Certificate Authority (CA), which then enables the device to receive encrypted device configuration information over the air. At the end of the enrolment process the user is informed of the access rights that the MDM server is requesting, agrees to these policies and then the device is dynamically configured with settings. Educating users in the reasons for managing their devices, such as complying with corporate policy, will alleviate resistance to enrolment in MDM.

Configuration Profiles contain account settings, policies and restrictions and are delivered to the device as XML files and installed on the iOS device. These files can be signed and encrypted so that the settings cannot be altered or shared with others. Furthermore, effective creation of these configuration profiles can act as both the carrot and the stick for users, such that, should the user decide to remove the profile they will instantly lose access to the services, such as VPN and mail, that are included as part of the profile. Settings like Exchange ActiveSync accounts, VPN, Wi-Fi, passcode length and complexity, MDM enrolment, device restrictions, certificates and web clips can all be included in a Configuration Profile.

Query devices, manage settings and apps, install and remove Configuration Profiles and remote wipe iOS devices after the end point is enrolled in MDM. Apple allows third party MDM providers to leverage a finite number of application programming interfaces (APIs) that they can integrate into their solution to remotely manage iOS devices. Although this essentially means that all iOS MDM vendors have the ability to provide exactly the same features and services, some achieve these better than others, and some offer additional features and support for additional platforms that enterprises looking to deploy a device agnostic BYOT scheme would benefit from. These differences are discussed in following chapters.

Configurable Settings

Supported configurable settings:

Accounts:
- Exchange ActiveSync
- IMAP/POP Email
- Wi-Fi
- VPN
- LDAP
- CardDAV
- CalDAV
- Subscribed calendars

Passcode policies:
- Require passcode on device
- Allow simple value
- Require alphanumeric value
- Minimum passcode length
- Minimum number of complex characters
- Maximum passcode age
- Time before auto-lock
- Passcode history
- Grace period for device lock
- Maximum number of failed attempts

Security and privacy:
- Allow diagnostic data to be sent to Apple
- Allow user to accept untrusted certificates
- Force encrypted backups

Device functionality:
- Allow installing apps
- Allow Siri
- Allow Siri while locked
- Allow use of camera
- Allow FaceTime
- Allow screen capture
- Allow automatic syncing while roaming
- Allow voice dialling
- Allow In-App Purchase
- Require store password for all purchases
- Allow multiplayer gaming
- Allow adding Game Center friends

Applications:
- Allow use of iTunes Store
- Allow use of Safari
- Set Safari security preferences

iCloud:
- Allow backup
- Allow document sync and key-value sync
- Allow Photo Stream

Content ratings:
- Allow explicit music and podcasts
- Set ratings region
- Set allowed content ratings

Supported queries:

Device Information:
- Unique Device Identifier (UDID)
- Device name
- iOS and build version
- Model name and number
- Serial number
- Capacity and space available
- IMEI
- Modem firmware
- Battery level

Network Information:
- ICCID
- Bluetooth and Wi-Fi MAC addresses
- Current carrier network
- Subscriber carrier network
- Carrier settings version
- Phone number
- Data roaming setting (on/off)

Compliance and security Information:
- Configuration Profiles installed
- Certificates installed with expiry dates
- List all restructions enforced
- Hardware encryption capability
- Passcode present

Applications:
- Applications installed (app ID, name, version, size and app data size)
- Provisioning Profiles installed with expiry dates.

Supported management commands:

Managed settings:
- Install Configuration Profile
- Remove Configuration Profile
- Data roaming
- Voice roaming (not available on all carriers)

Managed apps:
- Install managed app
- Remove managed app
- List all managed apps
- Install Provisioning Profile
- Remove Provisioning Profile

Security commands:
- Remote wipe
- Remote lock
- Clear passcode

Native Apple MDM Solutions

Apple have three key software solutions for managing iOS devices in certain enterprise deployment scenarios, but these can also be leveraged to support third party MDM solutions for more complex deployments; the iPhone Configuration Utility, Apple Configurator and Profile Manager. All three solutions are free to download and are a great way to get to grips with the basics of creating Configuration Profiles and managing iOS devices even if they do not become the MDM tools of choice for an organisation.

The iPhone Configuration Utility enables the creation, encryption and installation of Configuration Profiles, as well as the ability to capture the device information of the iOS device. The iPhone Configuration Utility supports iOS 3.0 to 6.0 and can be installed on: Windows XP Service Pack 3 with .NET Framework 3.5 Service Pack 1; Windows Vista Service Pack 1 with .NET Framework 3.5 Service Pack 1; Windows 7 with .NET Framework 3.5 Service Pack 1; or Mac OS X 10.6 and above. As previously discussed, these Configuration Profiles can be made up of various network and device settings, and can be distributed to the device via USB connection, Outlook email, a URL, or wirelessly through a third party MDM solution. One of the best features about the iPhone Configuration Utility is that, when an iOS device is connected via USB and a Configuration Profile is installed, it is possible to view the console log to determine any failings in the creation of the profile. This useful tool is perfect for understanding how to create a Configuration Profile. The iPhone Configuration can also be used by an IT administrator to track and install provisioning profiles and authorised apps directly onto iOS devices over a USB connection.

Apple Configurator can be used to mass configure and deploy up to 30 iOS devices simultaneously via USB connection and, although it shares certain features with the iPhone Configuration Utility, it takes things one step further. Requiring only a Mac computer, running OS X Lion v10.7.2 and iTunes 10.6, the Apple Configurator can facilitate: iOS updates; set lock screen and wallpaper; dictate a device name; install apps; install documents; create and install Configuration Profiles; and create a backup of one device's settings to restore at a later date, or deploy to other devices. To support different deployment models, Apple Configurator has three simple options: Prepare devices, by installing Configuration Profiles and enrolling in MDM, to provision iOS for their day to day use; Supervise devices, whereby the iOS device is used as a shared resource, returned to IT after use, and reset back to its original settings; or Assign devices, check out the device to a specific user, restore that user's backup (including all their data) and when the device is checked back in back up the data for later use – even on a different device. Generally speaking, when used in isolation from other solutions for management purposes, Apple Configurator is best used for smaller deployments that need regular attention from the IT department. However, used to create Configuration Profiles, create a base image and combine with third party MDM solutions, this is a powerful tool. Furthermore, with the Volume Purchasing Program (VPP), unlike some third party MDM solutions, IT have the ability to deploy paid apps to Supervised devices through Apple Configurator and not require the device to have an AppleID. Therefore the VPP codes can be revoked and reused on different devices.

Profile Manager offers MDM and configuration to OS X and iOS devices providing the Mac that is installed on, and which is acting as the MDM server, has a static Internet network address and is not on a closed network. Offered free as part of OS X Lion Server, Profile Manager is made up of three components: a web-based admin tool for creating configuration settings for devices and manage enrolled devices; a self-service portal for users to enrol their devices and download configuration profiles; and the MDM server. The fact that the administration tool is web-based also means that it is accessible on iOS devices. If an organisation decides not to use Profile Manager for its MDM features, this software can still be leveraged to create Configuration Profiles and distribute them to users for them to install manually.

It is also possible to integrate Profile Manager with directory services, such as Active Directory (AD), to configure multiple directory accounts. This allows IT administrators to create Configuration Profiles that contain common policies and settings that need to be provided across specific user groups that already exist within AD, without having to create these groups again within Profile Manager. As expected of an MDM solution, Profile Manager allows IT admin to interrogate iOS for device information, update device settings OTA and remote wipe, lock, or clear a password.

To manage with EAS, or not to manage?

Exchange ActiveSync (EAS) provides basic policy configuration tools, and for many organisations starting down the path of mobile device adoption, these tools offer the foundation for securely providing push email to devices.

In order for users to install email on iOS, IT administrators may enforce the need to protect the device with a passcode of minimum length and complexity. Further to this, it is possible to ensure that the device is wiped if a maximum number of failed passcode attempts have been made. As S/MIME is fully supported by iOS devices, since the release of iOS 5, Apple secures the integrity of email through complex encryption anyway.

However, securing and managing devices in the enterprise is now much more than just securing the integrity of email. Although ActiveSync is a useful email synchronisation protocol, it is recommended that enterprises look to full MDM solutions to manage and secure mobile devices above and beyond just email; managing apps, documents and network settings to name but a few.

Third Party MDM Solutions

As stipulated in previous chapters, all MDM solutions for iOS are built around key Apple technologies; Apple Push Notification service, Over-the-Air Enrolment and Configuration Profiles. Third party MDM solutions extend these core technologies and can integrate with the tools that Apple provide, such as the Apple Configurator, to allow management of much larger scale deployments of iOS devices in an enterprise environment. The greatest benefits of these third party solutions are the over the air enrolment and on-going management of devices, automated granular remote wiping and revocation of corporate network settings at extremely large scales, should a device break corporate policy. As Apple only opens a finite number of application programming interfaces (APIs) to developers, in many respects, the iOS management feature sets of these third party MDM solutions can be fairly similar. Therefore, in this chapter the discussion will address the key questions that inform an organisation's choice of third party MDM solutions, above and beyond those regarding support for the Apple environment. Further to this, certain features from specific MDM solution providers will be highlighted to indicate benefits in certain deployments of mobile devices within the enterprise.

"What is the key driver for mobility in your organisation?" should be the core question that informs any enterprise mobile device and MDM strategy. Surprisingly, for many organisations, this is often one of the last considerations made as the proliferation of smart devices in enterprise has been swift, and proactively identifying departments that would gain the most benefit from wide spread deployment and support for these devices has come secondary to a reactive response to provide support for these platforms as quickly as possible. Identifying this key driver will inform a whole host of decisions, such as: the employee demographic to be supported with mobile devices; the choice of mobile platform; mobile apps; management solution; security policies; content delivery; size of deployment; and required speed of deployment. If the key driver for mobility in a sales led organisation is to give their outbound teams the competitive edge with interactive and engaging presentations, access to CRM systems and the most up to date collateral whilst on the road, perhaps the enterprise would only need to manage a deployment of corporate owned iPad, with an iOS only MDM solution. However, if an enterprise is looking to empower all employees and provide secure access to corporate email, contacts and calendars then a completely cross platform MDM solution that supports corporate and personally owned devices might be more appropriate.

"What platforms do you support now?" and **"what platforms do you want to support in the future?"** are questions that naturally arise from identifying the key driver for mobility. When asked exactly how many devices and what platforms are already accessing corporate data, few organisations are actually able to quote statistics with any certainty. Some organisations are only able to manually track corporate devices that have company data plans. Others have run Exchange logs and discovered hundreds, sometimes thousands of devices that they were unaware were accessing corporate data. The choice of platform to support will be based on the employees, or departments, identified as the key drivers of mobility within the organisation and dictated by the necessary levels of security that

need to be enforced, without hampering the productivity of this demographic. Furthermore, as the market leaders in mobile devices change roughly every 18 months, it is recommended that an organisation consider an MDM provider that has the flexibility to support these changes in the market.

"Do you want to manage mobile devices separately to your desktop estate?" should be a consideration of IT departments that are being asked to manage more and more platforms, but without any additional budgets. By replacing existing enterprise solutions with those that offer cross platform management for mobile devices and desktops, an organisation may future proof itself, saving money and time on the management and support for this solution it in the long run.

"Do you want to deploy MDM on premise, as an appliance or virtual machine, or in the cloud as a SaaS solution?" is often something that is predetermined by the preference and philosophy of the organisation. Some prefer the security of an on premise solution, whereby the organisation has the peace of mind of being in complete control of the management solution and the infrastructure behind it. Others are drawn to SaaS solutions for the opposite reason, and wish to outsource the required infrastructure to the MDM provider or trusted partner. This decision is also based on whether the organisation is looking for a Capex or Opex payment method, perpetual licenses and annual maintenance or subscription licenses respectively. Although some vendors claim to support all three deployment methods, some of the SaaS offerings offer fewer management features and support for fewer platforms.

The answers to these questions will often immediately reduce the number of third party MDM solutions applicable to the deployment and management methods desired by the organisation. What follows is a breakdown of a few enterprise ready third party MDM solutions, all of which support a variety of mobile device deployments.

MobileIron

Identified as a leader in Mobile Device Management solutions by Gartner, MobileIron is a cross platform solution that gives IT and users real-time intelligence and control over content, activity and apps in order to secure data, reduce wireless cost, and improve user experience. Founded in 2007, MobileIron was built from the ground up as a solution provider of MDM, and supports management for Android, BlackBerry, iOS, Symbian, webOS, Windows Mobile and WIndows Phone. As of July 2012, MobileIron announced support for Mac OS X, which will allow IT administrators to provision and enforce: passcode restrictions; Wi-Fi, VPN and email configurations; certificates to authenticate users, apps and devices; and remote lock and complete wipe for lost or stolen OS X devices. MobileIron prides itself on adding additional layers of security and management to such a wide range of devices without impacting on the user's experience.

The MobileIron solution is comprised of an agent on the mobile device and back-end server, the Virtual Smartphone Platform (VSP), which is available as virtual software or an appliance for onsite deployments. Having an agent, or app, installed on a user's device enables jailbreak detection and the ability to integrate the device and analyse its current state. A single MobileIron server has the ability to support 100,000 devices, or 1,000 concurrent connections per second, which makes it one of the leading solutions on the market for supporting extremely large deployments of mobile devices. The solution is also available as a SaaS offering known as the MobileIron Connected Cloud, although it is currently only able to provide support for iOS and Android devices.

MobileIron has some key distinguishing features that make it a perfect enterprise mobile management solution that extends beyond device management. These features make it a particularly useful tool for organisations looking to deploy a platform agnostic mobile device policy that is required to support profiles for corporate owned and personally owned devices.

Quick and easy enrolment of new devices and those already in the field is achieved through integration with various directory services, such as Active Directory (AD), and MobileIron's MyPhone@Work. IT administrators are able to import users from AD and create group policies for the required security settings and network services configurations that are appropriate for the user. Furthermore, IT admin may be inclined to create a policy for a corporate device and one for a personal device. For instance, the former may be more invasive, with tight security lock down, but allow greater access to corporate data, and the latter providing just secure push email, contacts and calendars without invading the privacy of the individual. Further still, policies might be set based on the security of the user's chosen platform, in order to gain a level of consistency across the various mobile platforms on the market.

Once these policies are created, a user can quickly and easily enrol their own device in the MobileIron MDM solution over the air through MyPhone@Work, which can be accessed through a web browser or natively on the employee's smart device via the MobileIron app. During the enrolment process the user can indicate whether the device is corporately or personally owned, accept the organisation's mobile device policy, and receive the correct Configuration Profiles for that specific platform. In addition, through MyPhone@Work, an employee can perform basic administrative tasks, such as remote wipe, on the devices they have enrolled. Naturally, should the organisation not wish to entrust the user with enrolling devices it is possible for IT administrators to mass provision devices over the air.

Automate remote wipe and revocation of network service privileges using the MobileIron Sentry, which provides access control for email. Essentially this means that, should the device break any of the organisation's policies and be considered 'out of posture', the Sentry will automatically remove all corporate services delivered by Microsoft ActiveSync-enabled systems, such as Exchange, Lotus Notes, Gmail, and Microsoft Office 365. IT administrators are also able to view the Sentry from an iPad app, which allows IT to quickly see every networked device trying to connect to ActiveSync, block offending devices, allow devices access, enrol devices and remotely wipe lost or compromised devices.

Manage applications through MobileIron as IT administrators have the ability to blacklist applications that are deemed a security risk or inappropriate. If the user were to install a blacklisted app this would throw the device out of posture and MobileIron would automatically remove corporate data and revoke access to network services. On iOS and Android, MyPhone@Work provides an enterprise app storefront for the discovery and distribution of enterprise apps and the recommendation of external third-party apps. These are either approved by IT and available in commercial app stores or created by IT for internal business use. Since the release of iOS 5, iOS devices support granular removal of any 'managed apps', which applies to any app downloaded through MobileIron's enterprise app store. Therefore it is possible to remote delete business apps on a personally owned device, without incurring the risk of deleting an employee's personal data or apps.

MobileIron's mobile content management solution Docs@Work is also now available for iOS devices, and planned for Android, and is made available to the user through the native MobileIron app. IT administrators are able to make files available to be viewed and stored offline, within the secure confinements of the MobileIron app, and selectively wipe documents when the device falls out of posture. As an additional layer of security, IT can control whether third-party apps can access this stored content and protect the data-at-rest with the built in Data Protection of iOS. Furthermore, Docs@Work can dictate that all email attachments may only be viewed and stored on the device within the secure confines of the MobileIron app and, with SharePoint integration, the user also has secure access to SharePoint file shares.

Support for Global HTTP Proxy settings in iOS 6 means that MobileIron can ensure that IT administrators can now scan and filter web content, even if the device is joined to a WI-Fi or cellular network that they have no control of. When the Global HTTP Proxy setting is configured on an iOS 6 device, HTTP traffic is routed to a proxy server that the IT admin specifies to add an additional level of security. This feature is available when combining iOS devices supervised with Apple Configurator and enrolled in MobileIron.

In only five years, MobileIron has grown to be one of the most comprehensive enterprise MDM solutions on the market, and continues to future proof itself by expanding into mobile application and content management. The recent announcement that MobileIron will support Mac OS X further illustrates that the future of device management will require a solution that supports desktops and laptops as well as smart phones and tablets. For organisations looking for a cross platform, on premise MDM solution, that thoroughly supports corporate and personally owned devices, with options for either Capex or Opex procurement, then MobileIron is one of the best in the market place today.

Absolute Manage MDM

'Absolute Manage MDM' is Absolute Software's offering for the deployment, management and security of iOS and Android devices within the enterprise. Approaching the market very differently from MobileIron, Absolute Software was founded in 1993 and originally provided a solution known as 'Computrace', which was pre-built into desktops and laptops by leading OEM manufacturers like IBM, and allowed organisations to track and secure these endpoints within a single cloud-based console. From this background in supporting and managing a range of laptops and desktops, Absolute Software released 'Absolute Manage', which allows organisations to remotely manage and secure all their endpoints from a single console, including PC, Mac, iOS, Android and Windows Phone devices. Absolute Manage MDM is responsible for managing the iOS, Android and Windows Phone devices and can be bought and installed independently of the rest of the suite, as an onsite software solution. Although the Absolute Manage MDM solution shares features provided by MobileIron, there are some interesting defining aspects that set it apart.

AbsoluteApps, AbsoluteFind and AbsoluteSafe provide mobile application management, location services, and content management, respectively, to iOS devices via three native apps. AbsoluteApps is similar to MobileIron's enterprise app storefront, as it provides users with a list of recommended apps for easy selection that, if downloaded through the app, are considered as 'managed apps'. Furthermore, in-house apps can be remotely distributed through AbsoluteApps and optional Configuration Profiles can be listed for on-demand installation. AbsoluteFind allows IT to track devices on an iPad, and administer security functions remotely, and AbsoluteSafe is the content management app. A useful feature of AbsoluteSafe is that it is possible to define timed access to documents, whereby a document is automatically removed from the device after a specific time period.

Reduce calls to the IT help desk with notifications sent to a user's device identifying it as out of posture and why it is no longer compliant. IT administrators can define the content of these notifications so that, should a user install an application that pushes the device out of compliance with company policy, the user is told what app needs to be removed in order to regain access to corporate data and network services.

Having entered the MDM market from a background in managing and securing desktops and laptops, Absolute Software's Absolute Manage MDM is a useful tool for organisations that are looking to manage PCs, Macs, iOS, Android and Windows Phone, all from a single management console.

Casper Suite

JAMF's Casper Suite is considered to be a Best of Breed client management toolset for the Apple platform by many engineers versed in Apple's infrastructure. The Casper Suite supports management tools primarily for Mac OS X, but also provides an MDM solution that can be installed independently if required. Through the MDM tool, IT administrators can run inventory of installed apps and device information, create and distribute Configuration Profiles over the air, send remote security commands, and distribute apps and eBooks through the Casper Self Service iOS app. The Casper Suite is the perfect tool for enterprises looking only to deploy, manage and secure Mac OS X and iOS devices, or are looking to manage these separately to their other desktop and smart device environments.

Once the key driver of mobility for an organisation is defined it becomes much easier to recommend both a mobile platform and an MDM solution for additional support, should the deployment scenario require it. These three solutions are perfect examples of the range of solutions that are in the MDM market place, and each have their use cases for deploying iOS in the enterprise.

Summary

Apple makes every effort to ensure that all apects of the iOS device and supporting infrastructure are secure, innovative, and ready for use within the enterprise. From hardware-based storage encryption that provides instant remote wipe capabilities, to mandating code signing, sandboxing and entitlements in apps that protect against viruses, malware, and other exploits, Apple illustrates commitment to creating modern mobile-centric privacy and security technologies to ensure that iOS devices are secure in the enterprise, and for personal use.

The Apple Push Notification service, Over-The-Air Enrolment and Configuration Profiles form the foundations of all Mobile Device Management solutions, and Apple provide three tools that support smaller deployments of iOS devices, or can be integrated with third party MDM solutions for larger deployments; iPhone Configuration Utility, to create configuration profiles; Apple Configurator, to create a 'base' image of an iPad and Prepare, Supervise or Assign devices; and Profile Manager as Apple's own MDM solution.

In choosing a third party MDM solution for an organisation, it is necessary to identify the key driver for mobility within the organisation. This will not only aid in establishing the employee demographic that will gain the most from the deployment of mobile devices, but also the platform type, necessary security policies, and mobile device management solution. Of the hundreds of MDM providers on the market, some were originally founded as MDM solution providers and others have added MDM functionality to desktop and laptop management solutions. In order for IT departments to support more devices with little, or no additional budget it is important for organisations to choose an MDM provider that is either positioned, or moving towards, a platform that allows for the management of all enterprise end points from a single console.

How Jigsaw24 can help

With over 20 years' experience of integrating Apple devices into large corporates, and smaller business environments, Jigsaw24 are equipped to consult on mobile device security, and whether iOS addresses the security requirements and regulations of your organisation, as well as advise on Mobile Device Management solutions that ease the deployment, management and security of a mobile estate. Having delivered large scale iPad deployments within enterprises like News International, and MDM solutions for 1,700 iOS devices, Jigsaw24 are able to support organisations in their adoption an iOS estate; from consultancy, architecture design, proof of concept, supply, installation through to on-going telephone support or support contracts. Please contact us for advice, or more information on deploying iOS within your organisation.

"Jigsaw24 are a key support partner for News International's technology team – we are working together on a range of IT initiatives as we look to expand our Mac and iPad estate to develop a best of breed, scalable and high-quality Apple infrastructure. We are committed to partnering with Jigsaw24 as we move towards achieving this goal"

Please visit our website to read the full News International case study:
http://ow.ly/fFFdA

Jigsaw24 are the most magical IT company, providing Insanely Great creative technology solutions and services for more than 25,000 enlightened customers, including large businesses, creative professionals, media companies, education institutions and prosumers. With over 20 years' experience, our incredible team have gained Apple's highest customer satisfaction levels and more accreditations than you could shake an iPad at (including Apple Authorised Reseller, Apple Solution Expert for Creative and Education, and Apple Authorised Service Provider). With offices in Manchester and Nottingham, Jigsaw24 now report annual sales of £60m and a strong balance sheet with £7m net assets.

Get in touch with us at **B2B@Jigsaw24.com** or call us on **03332 400 100**

Jigsaw24 Professional Services - Jigsaw24 is a trading name of Jigsaw Systems Ltd, The Old Mill, High Church Street, Nottingham, NG7 7JA. Sales Tel 03332 400 100, www.Jigsaw24.com. Registered in England and Wales 2682904. VAT Registration No, 610706674.