cloud security alliance℠

Mobile Device Management: Key Components, V1.0

September 2012

Ping Identity®

Document Sponsor

Contents

Acknowledgments

CSA Mobile Working Group Co-Chairs

David Lingenfelter, Fiberlink
Freddy Kasprzykowski, Microsoft
Cesare Garlati, Trend Micro

Initiative Lead

Guido Sanchidrian, Symantec

Contributors

Jane Cosnowsky, Dell
Sam Wilke
Allen Lum, Control Solutions
Jay Musterman, Cox Communications
Somanath NG, Infosys
Eiji Sasahara, IDC
Alice Decker, Trend Micro
Pamela Fusco, Virtuosi Group
Nader Henein, Research In Motion
Paul Madsen, Ping Identity
Tyler Shields, Veracode
Subbu Iyer, Zscaler

CSA Global Staff

Aaron Alva, Graduate Research Intern
Luciano JR Santos, Research Director
Evan Scoboria, Webmaster
Kendall Scoboria, Graphic Designer
John Yeoh, Research Analyst

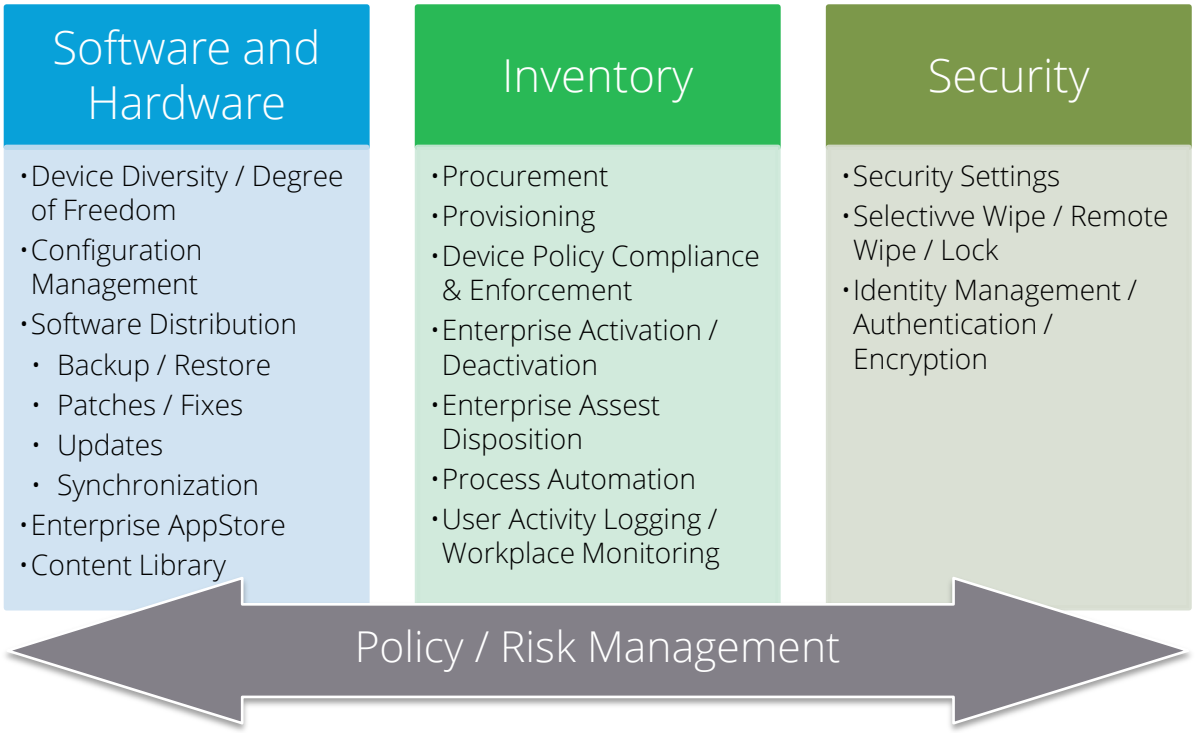
SECTION 1: Introduction and Context

With the growth in the number of applications, content, and data being accessed through a variety of devices, **Mobile Device Management (MDM)** is vital to managing the mobile enterprise. MDM is about much more than device management alone—it includes system-centric functionality to secure and manage data and applications, as well as information-centric functionality such as the delivery of the enterprise application store or content library.

MDM is a critical component of the device lifecycle, covering the device hardware, software, and attached services.

Full lifecycle management is required, and IT is fully responsible for the company-owned devices, including setting hardware/OS standards, application support and enterprise liability. However, organizations might choose a "degree of freedom" for their users, such as increased hardware and OS choices by **Bring-Your-Own-Device (BYOD)** support, or might provide limited capabilities such as corporate email or web services only. Both will create shared responsibilities and a mix of enterprise and user liabilities that should be properly defined, communicated, and managed.

SECTION 2: MDM Key Components to Consider in Both Scenarios – BYOD or Company-Owned Devices



2.1 Policy

Rating[1]: Must Have

The definition and distribution of a **policy** is a critical prerequisite of mobile computing strategies. Organizations should assess the needs of the workforce and build or revise the mobile policy accordingly. Risk assessment and management should be performed to recognize the significance of IT and information risk, which both defines a basis for developing awareness and enables analysis of the business risk impact. A well-defined policy provides management direction and support for IT and information security and is the foundation for a solid MDM framework implementation.

[1] The initial rating is based on common importance and risk level of each component. Depending on organizations individual risk assessment results, the rating might change dynamically case-by-case.

2.2 Risk Management

Rating: Must Have

Risk management means the entire process of analysis, planning, implementation, control, and monitoring of defined measurements and the enforced policy. Organizations should consider the impact of the introduction of mobile devices as end-point devices within their corporate network. If risks are identified, the appropriate mobile device policies can be applied. In an extreme case, if the risk is deemed too high, additional controls should be implemented to bring the risk to an acceptable level, allowing seamless access to IT resources from mobile devices. On the other hand, if the risk is low or non-existent, the organization can require minimal controls for the mobile devices, thereby reducing overall costs.

As part of risk management, organizations should perform risk assessment periodically (i.e. once a year) or on-demand (i.e. introducing new devices, services, or significant infrastructure changes) to provide a temporary view of assessed risks and to review the risk management process, either in parts or entirely, and make necessary changes accordingly.[2]

2.3 Device Diversity / Degree of Freedom

Rating: Optional

Both scenarios—BYOD and company-owned devices—require segmentation and acceptable usage planning built on a multi-dimensional matrix, which includes the user's role, responsibility (including ownership and support), data, networks and applications, and which states the user's degree of freedom for each area. This planning also defines the capabilities provided, such as corporate email, web services, support, multimedia, specialized applications and services, corporate databases such as CRM, and analytics.

2.4 Configuration Management

Rating: Must Have

Configuration management involves automated configuration of device settings, such as password strength and policy, email, VPN and Wi-Fi. Configuration management aids in the elimination of user errors and minimizes vulnerabilities caused by misconfiguration, including configuration lockdown according to a degree-of-freedom definition, as well as hardware lockdown such as camera, Bluetooth, and Wi-Fi. Configuration management is also used in an effort to enforce corporate IT mobility policies.

2.5 Software Distribution

Rating: Must Have

Software distribution includes applications and software accessed over-the-air or by PC synchronization. It includes updates for applications or OSs, patches, fixes, backup and restore functionality, background synchronization, and basic file distribution capabilities. Backup and restore functionality accessed over-the-air or via PC-sync in particular becomes important in situations of device crash and replacements, intentional wipeout (i.e. in case of lost or stolen device) or unintentional wipeout (i.e. kids play with device and try password too often), so the device can be recovered quickly without significant productivity loss. Aligned to the corporate mobile policies it ensures the distribution of only security assessed mobile applications to the device. Along with

[2] Visit European Network and Security Agency (ENISA) website at http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms for an introduction on Risk Management and Risk Assessment.

Configuration Management, software distribution helps to enforce the corporate approach of black-listing and/or white-listing applications and other software on the device. Mobile Device Management systems generally do not have a capability to analyze mobile applications for security risk. The analysis of these applications should be conducted separately in order to populate the white-list and black-list approaches with actionable application security assessments.

2.6 Enterprise AppStore

Rating: Optional

An **Enterprise AppStore** ensures that only secure and trusted applications along with associated content will be deployed on mobile devices while providing several paths of accessibility: through deployment of mobile applications over-the-air, recommended apps from the public AppStore, or via a company-specific app repository. AppStores include appropriate code-signing of specialized or in-house applications to ensure the integrity of the application. Enterprise AppStores provide an excellent environment in the corporate mobile ecosystem to implement security testing and application whitelisting.

2.7 Content Library

Rating: Optional

A **content library** distributes corporate content, such as documents and multi-media videos, to provide a secure enterprise container with near-real-time updates and specific views. The library may include the secure usage of Cloud storage providers, or sandbox/virtualized environments to separate corporate content from private content. In the case of different containers it may be necessary to control applications and information differently with different policies depending on whether they or corporate or personal apps and information.

2.8 Procurement

Rating: Must Have

With devices evolving into application development and integration platforms, IT is likely taking ownership of the end-to-end solution by contracting wireless carriers and programs and managing service usage. However, the finance department maintains responsibility for monitoring and controlling mobility costs, such as contract and expense management. It is important to collaborate and align with Legal and HR departments to define certain terms and conditions in the policy and employee agreements. In particular, BYOD creates a mix of corporate and personal liability and responsibility. Liability for all parties should be clearly defined in these agreements and should include subjects such as private usage of corporate services, expense compensations, employee privacy policy, shared responsibilities for device and content security, misuse, secure wipe of the device including personal data in the event the device is lost or stolen, or the rights to control the device through a device management client.

2.9 Provisioning

Rating: Optional

Provisioning devices with a three year refresh is acceptable for company-owned devices, but IT cannot possibly manage employee-liable devices that are refreshed annually (or in even shorter cycles for smartphones and tablets). Expectations about end-user support should be clear and frequently refreshed, as self-help is often not accepted by some users, in particular those with brand new devices.

2.10 Device Policy Compliance & Enforcement

Rating: Must Have

Device policy compliance and enforcement is involved in device supply, control, and tracking. Asset inventory assessments are critical prerequisites for policy enforcement to comply with corporate and regulatory requirements around policies, encryption, jail-broken or rooted-device detection, and privacy-related separation of personal content vs. corporate content. Compliance and enforcement also includes approval and review processes of apps in the organization's AppStore, as well as approval of mobile configurations to ensure that they meet the organization's security policies before roll out. The organization will allow or deny access to devices based on their approval status. This is an ongoing monitoring and enforcement process, often described as Plan-Do-Check-Act approach of policies in various Information Security Management System standards and frameworks such as ISO 27001 or COBIT. It also requires alerts and notifications capabilities to provide asset reporting about devices, users, and apps. As part of the organizational infrastructure change control or similar processes, it is highly recommended to document that the policy and standard has been applied to the device and has been acknowledged by the user before the device is distributed.

2.11 Enterprise Activation / Deactivation

Rating: Must Have

Enterprise activation or deactivation is usually a self-service functionality that activates or connects mobile devices to the enterprise network, or that allows or denies access to users based on directory groups. A proper implementation of it (in particular an implementation as a self-service) will reduce the administrative burden of provisioning and re-provisioning at the IT department. User acceptance is an important factor of it and should be clarified and well communicated in the beginning. In particular in environments where users bring in their own devices, choosing enterprise activation will likely share certain details like operating system, device identifier, IMEI number, etc. as part of the provision process. The process can be either automated through a provisioning portal to enter the required details and follow the workflow to activate the device, or it can be a manual process where the administrator will do the complete activation by taking the required details from the user. In addition, after enterprise activation some characteristics of the device may be changed like enabled encryption, changed password settings, certain application restrictions, etc.

2.12 Enterprise Asset Disposition

Rating: Must Have

Enterprise asset disposition involves removal of physical devices by decommission or by releasing the device to the BYOD owner in case of device exchange, upgrade, or permanent decommissioning. Appropriate technical and procedural controls should be in place on inventory management, user receipts or acknowledgements, and related physical actions required for proper handling during decommissioning. It is important to securely wipe the corporate data from a personal device before it is decommissioned. If the device itself is not owned by enterprise, it should be handed over to the device owner ideally without touching the personal data, music, and apps.

2.13 Process Automation

Rating: Optional

Process automation creates and implements automated processes that link together people, processes, and technology. It automates regular tasks like device registration and lost devices (i.e. if a device is lost or stolen,

an automated workflow should be initiated that remotely wipes the device and revokes particular access rights. Then, a new device should be provisioned, with appropriate pre-load and configuration prior delivery to the user). Process automation also includes technical tasks such as backup restore, as well as procedural tasks where human attestation is required (i.e. management sign-off for the order).

2.14 User Activity Logging / Workplace Monitoring

Rating: Must Have

More and more organizations are turning to workplace monitoring[3] and data loss prevention (DLP) technology. Workplace monitoring is usually governed by a variety of privacy laws, rules, and regulations. In some countries, the laws on telecommunications regulate the monitoring of email and other electronic communications. In other countries, an employer's rights to monitor employee communications may be governed by collective bargaining agreements, employment contracts, or general privacy and data protection legislation. It is important to understand that privacy is treated as a fundamental human right and, as such, cannot be bargained away. This becomes more complex with environments with both corporate supplied and BYOD devices where laws and regulations are significantly different. Organizations are highly recommended to seek legal counsel to understand the privacy and data protection laws of the individual countries in which they operate.

2.15 Security Settings

Rating: Must Have

According to company policy, **security settings** provide advanced security on devices irrespective of ownership. They set, deploy, and update settings like passwords, wipe, and application/resource restrictions, usually without any user intervention. Security can be broken into two basic components; user security and data security. While user and data security are tightly coupled there are some distinct differences which must be accounted for and sometimes handled quite differently. In both cases companies must take steps to protect the user and the data from potential threats.

2.16 Selective Wipe / Remote Wipe / Lock

Rating: Must Have

Selective wipe securely wipes the corporate data from a personal device, without touching the personal data, music, and apps. It will also delete documents from the user's Content Library. If a device is lost or stolen, a **remote wipe** must be performed by either the administrator or the end user. The remote wipe will, in effect, wipe all information from the device returning it to factory default configuration. Similarly a **Lock** can be performed on a device by the administrator or end user to ensure that protection is in place should the device become temporarily misplaced. If the wrong password is entered multiple times, an automatic wipe will be triggered.

2.17 Identity Management / Authentication / Encryption

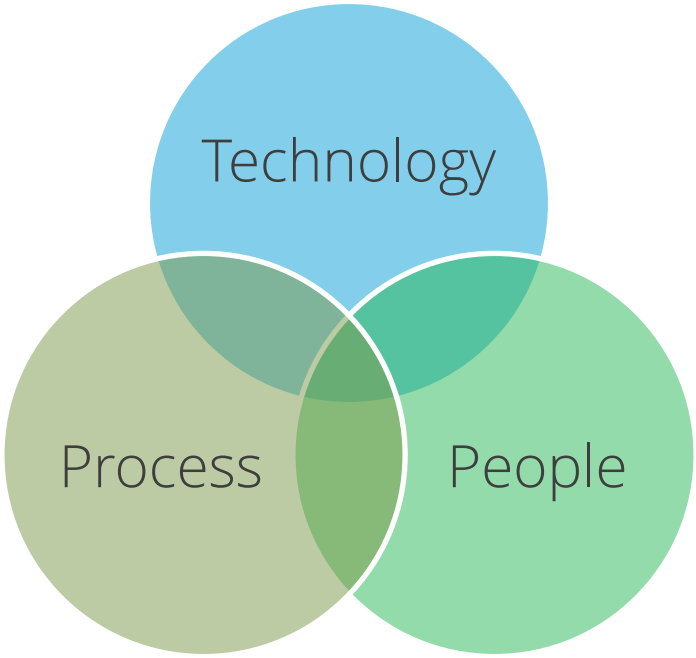
Rating: Must Have

Identity management, authentication, and encryption involved management of strong encryption of local data (device memory, external memory cards) and data in motion (such as email S/MIME encryption and

[3] The term "monitoring" is used broadly to refer to any reading, collection, or storage of electronic communications. Monitoring is, therefore, more than the interception of communications in transit. Copying of employee emails for backups or scanning messages to detect viruses are both considered to be monitoring.

authentication). It requires certificate distribution capabilities and certificate-based authentication (including device ID, OS version, phone number) to identify the device and user properly. Strong certificate-based authentication enables secure access to corporate email, web-based applications, VPN and Wi-Fi. It comes along with overlaying identity management processes and mechanisms by which enterprise employees are issued accounts and credentials required to provide access to the device, the business applications and services based on a context-aware policy that includes who they are, their role, their device, their network and their information and application. It could also enables employees access to cloud applications and services on mobile devices via single sign-on credentials and identity brokering to authenticate to third-party SaaS.

SECTION 3: CONCLUSION



Mobile devices have quickly become a mainstay in enterprise environments, and while mobile devices continue to be consumer driven in both form and function they have found their way into our day-to-day business lives. Mobile device management, like management of any technology or resource in the corporate space, has to start with the basic understanding of the key components of that eternal "people, process, technology" triangle. While most companies already have security policies in place, those policies need to be reviewed and possibly updated to account for the many components of mobile technology that have been spelled out in this document. Every company will have a different tolerance for risk and will adopt mobile technology in different ways, but there are still several fundamental components of mobile device management that have to be considered and incorporated into policy and practice to ensure that introducing this technology will not compromise security.

As the mobile technology continues to advance, and new uses for it are discovered some of these key components outlined in this document may become more critical to a successful security strategy than others. There may also be new components to mobile device management that come into play as the technology continues to advance. Mobile devices are a great personal enabler and the consistent availability of mobile devices makes the integration of personal and business objectives almost inevitable. As such the Cloud Security Alliance Mobile Working group will continue to work on educating and developing guidance's around mobile devices and how best to manage and integrate them into our work environments.