5 Myths of BYOD Management

...and How to Secure Your BYOD Strategy
Contents

1.0 Summary ........................................................................................................................................... 3
1.1 Myth 1: Mobile Device Management (MDM) is a Complete BYOD Solution ......................... 4
1.2 Myth 2: Sensitive Corporate/Agency Data Can Be Safely Stored Locally on the BYOD . 6
1.3 Myth 3: Sensitive Data Can Be Securely Originated and/or Created on the BYOD....... 7
1.4 Myth 4: BYOD-based Apps Should Have Access to Sensitive Corporate Data ............... 8
1.5 Myth 5: Mobile Device Management (MDM) Equals Data Leak Prevention (DLP) .......... 9
1.6 The Solution: The Answers to a Comprehensive BYOD Security Strategy ................. 10
1.7 Conclusion .......................................................................................................................................... 13
1.0 Summary

The implementation of Bring Your Own Device (BYOD) initiatives across all sectors has continued to grow, and with this have come new data security challenges with regard to effective management of these programs:

- How best to secure these personal devices?
- How to effectively & efficiently implement and maintain software solutions across disparate endpoint technologies, operating systems and form factors?
- How to effectively keep track of these devices - and accommodate more frequent device turnover?
- How to best monitor employee usage of company resources and data?
- How to ensure employee privacy as well as vital private company information are protected?
- How to ensure that employees are not using these devices to send/store proprietary data into the “public” cloud?
- How to ensure that de-provisioned employees keep their own personal information, but do not leave with sensitive company information?
- How to ensure that BYOD programs evolve to reflect individual employee privacy rights, a company’s right to protect and manage their own proprietary information, and compliance with existing regulatory structures?

From these challenges have arisen a variety of “BYOD strategies” to attempt to tackle them, but with competing vendor-influenced information in the marketplace, the most effective strategies to adopt are not always objective or clear. In fact, in the case of BYOD management, a number of myths and misconceptions have been circulated with regard to what makes up a secure and successful BYOD program.

This white paper covers the five (5) most pervasive myths concerning the current perceptions of BYOD management:

1. Mobile Device Management (MDM) is a Complete BYOD Solution
2. Sensitive Corporate/Agency Data Can Be Safely Stored Locally on the BYOD
3. Sensitive Data Can Be Securely Originated and/or Created on the BYOD
4. BYOD-based Apps Should Have Access to Sensitive Corporate Data
5. Mobile Device Management (MDM) Equals Data Leak Prevention (DLP)

Of course, knowing what the myths are is only half the battle. Therefore, this document also offers a recommended multi-vendor approach with solutions that are actually available today for attaining the most well-rounded and effective BYOD strategy for your organization.
1.1 Myth 1: Mobile Device Management (MDM) is a Complete BYOD Solution

Mobile Device Management (MDM) systems allow for remote, centralized control over a fleet of mobile devices, whether they happen to be company assets or the employees’ own (as the “your own” part of a BYOD program). This management typically includes such features as over-the-air policy updates, distribution of apps/data and configuration settings to ensure all devices contain the necessary resources.

Why is this commonly-held idea a myth?

The features listed above are essential to any BYOD program, but they are not a panacea to securing today’s BYOD devices, any valuable company data on them, or for ensuring regulatory compliance.

MDMs primarily install their device agent software at the application (“app”) layer of the PDA, smartphone, tablet, etc. devices which then allows for remote administrative control from a central authority using the MDM’s proprietary console. This reality means MDMs are generally barred by the BYOD operating system manufacturer’s APIs (if provided at all) to reside at lower device operating system and communication layers to properly secure or even monitor potential data egress points.

Some MDMs have “poison pill” features that wipe the device if the MDM software is removed against authorization, but until such time that all BYOD devices are physically partitioned (ex. Partitions like: Manufacturer-only, personal, business, crypto, etc.) and are designed to allow for deeper third-party integration through APIs that the manufacturers might provide, this will continue to be a security challenge that none of the MDM vendors openly discuss, but are attempting to work around.

To further explain the prevailing mythology, let’s begin by listing the core security features that most MDM systems provide - i.e. what MDMs typically excel at:

- password strength and protection beyond the manufacturer’s features
- remote wipe/kill of the device if it is reported lost or stolen
- storage/media card encryption, or more recently, “containerization” of apps-data

While these are definite strengths, current MDM systems are adequate ONLY if a device surfaces on the network again (which would allow them to be wiped/killed by the MDM), is lost and never found (which would result in loss of the device, but would not expose its data), is physically destroyed beyond forensic recovery (similar to above), or is stolen by unsophisticated thieves (which is an exercise in wishful thinking). In other words, several of these conditions rely on luck rather than security, or simply are not desired outcomes from a data security perspective.
Furthermore, there are commercially available forensic recovery solutions (and, almost assuredly, state-sponsored forensics and “Dark Web” solutions as well) that are able to crack iOS and BlackBerry device passwords as well as their encryption under various scenarios - especially in the case of their ‘protected’ data backups. The assumption should be that all BYOD devices are vulnerable, rather than the reverse.

Finally, there is also the scenario of the ‘insider threat’, which MDM systems do not address at all. Accidental, and unfortunately some intentional data leakage by disgruntled or exiting employees, will assuredly occur without other contextual and content-aware controls in place beyond MDM.

In the face of these more sophisticated threats, MDM systems simply add a small hindrance to those determined (and with the proper tools) to get at valuable company data on or from a BYOD.
1.2 **Myth 2: Sensitive Corporate/Agency Data Can Be Safely Stored Locally on the BYOD**

Securing company data is not only essential with regard to privacy and proprietary knowledge concerns, it is also mandated under various regulatory statutes. Thus, how this data is created, stored and handled is of utmost importance.

On the surface, this concern appears to be met with MDM systems, even if employees are storing corporate data on their own devices, but this approach provides a false sense of security.

**Why is this commonly-held idea a myth?**

The practice of storing data locally on a BYOD device is inviting a company data breach whether you employ a MDM system or not.

As mentioned previously, the MDM approach of data encryption along with wipe/kill functions simply provide the lowest, and most Draconian, bar of protection, but this is not enough from a data security perspective. In the hands of a determined and knowledgeable party, sensitive data can still be accessed or sent off from that device. All methods of possibly moving sensitive corporate data to a BYOD, including local data synchronization as connected to corporate desktops (ex. iTunes, ActiveSync, MTP, etc.) need to be secured intelligently or potentially blocked/shadowed.

*Consider this scenario:*

An organization allows employees to dock their personal mobile devices to company laptops, desktops and servers. Once docked, these devices can easily transfer private personal information or confidential company information in staggering quantities and at blistering speeds. Because these data transfers occur inside the company firewall, they are completely unhindered, unmonitored and unrestricted.

An employee can then takes his/her device outside the office where it is essentially “in the wild”. If that device happens to be lost or stolen, the data found within, whether it is encrypted or not, could be mined for the information which had originally been added to it at corporate headquarters.
1.3 **Myth 3: Sensitive Data Can Be Securely Originated and/or Created on the BYOD**

Of course, personal devices are now utilized for much more than communication. To be as productive as possible, employees also expect to create content on these devices. While the increase in productivity is a definite boon to organizations, it does provide an added security and data integrity concern.

**Why is this commonly-held idea a myth?**

The same issues found in our second myth apply here as well, but there also exists another concern - backups of important company data. If data is created on an employee’s personal device, the organization is effectively leaving it up to the employee to backup his/her device or hoping that the device will make it safely to the office so that it can be appropriately backed up there. Again, this strategy relies more on good fortune than effective planning.

Should the device be lost, stolen, remotely wiped/killed by a MDM or destroyed prior to a backup occurring, this potentially critical company data is likely gone.
1.4 Myth 4: BYOD-based Apps Should Have Access to Sensitive Corporate Data

You’ve heard it many times: “There’s an app for that.” Regardless of the personal device utilized, there are multitudes of applications – especially on mobile platforms – which can handle tasks employees may want to perform.

Even if a particular BYOD device app does a necessary job very efficiently, having an employee use it to access and handle company data may not be the best strategy, however.

Why is this commonly-held idea a myth?

Unless YOUR company or agency wrote the BYOD app, your control over how the app handles data is usually minimal. In fact, when users download and install third party apps on their devices (or use an embedded app for the first time), they will often have to allow that app access to data present on the device. This access is usually given quite freely (somewhat akin to a consumer skimming or skipping over a Terms of Service document).

For mobile devices that run mobile operating systems like Google’s Android or Apple’s iOS, there are some other issues that broaden their threat profile:

- average users of Android/iOS-based mobile devices tend to install more 3rd party applications than those of Windows-based computers. The more 3rd party apps used on a mobile device, the more chances that one of them is malicious or has security vulnerabilities due to its poor design, this can result in easy hacking and data loss.
- data leaks can be initiated by users with malicious intent who copy sensitive information from their PCs to flash memory, cameras, and all other types of portable storage.

While some MDM systems provide app control such that only approved apps can be downloaded/installed, not all do. Most leading MDMs are moving toward a virtual app partition model as well, but this is pure mitigation until the devices and APIs evolve as discussed earlier.
1.5 **Myth 5: Mobile Device Management (MDM) Equals Data Leak Prevention (DLP)**

Some mobile device management (MDM) systems claim their solutions offer data leak prevention (DLP) due to their inherent encryption/wipe/kill features. But is this truly all that a company, and its compliance rules, would require to secure their sensitive and valuable data?

**Why is this commonly-held idea a myth?**

Looking at MDM systems as an overarching security strategy that includes “DLP” is patently incorrect according to definitions established by industry analysts who focus on data security.

By their widely accepted definition, a true DLP solution features the ability to analyze any of data-in-motion, data-in-use, and/or data-at-rest by its actual content. These types of analyses, which are crucial to monitoring and ensuring data integrity, are absent in today’s MDM systems.

Furthermore, regardless of the MDM system deployed, none currently provide sufficient protection against the user/insider that is an accidental - or worse, intentional - data leaker.

Finally, while MDM systems are trusted with access to the device and data, none currently filters any outgoing communications or removable media for its content. Nor do MDM systems value the context of the user, data, or BYOD egress points.
1.6 The Solution: The Answers to a Comprehensive BYOD Security Strategy

With regard to BYOD security, a Mobile Device Management (MDM) system is only effective as a component of a larger data security strategy. While the MDM system can usually handle general “management”, encryption and the “last line of defense”...
In this way, we achieve three vital security outcomes:

- **Secure Data Handling** - employees do not use (and are contextually blocked from using) the local data-handling apps on the BYOD device itself during this secure session - thus ensuring that company data is not exposed to a ‘wider-than-wanted’ audience or otherwise insecure device.

- **Secure Data Storage** - secured company data can only be accessed via the virtual portal, and if modified, can only be saved back to the main server or printed to internal printers - and not ever saved locally to the BYOD device fixed storage, its removable storage media, or to an outside printer. Because company data exists only on corporate servers rather than on BYOD devices, it can be properly secured and backed up.

- **Secure Data Monitoring** - Finally, during each employee session, the vDLP solution securing the hosted Windows session filters any content going out through any network egress points (such as email, the web, or IM), hosted apps, printing, mapped shares, or removable media allowed by the virtual hosting software. If contextual controls (such as access to specific peripherals and network services based upon group memberships or other ACLs) are lacking for the hosting solution, a host-based endpoint DLP solution fills this gap as well.

### Applications & Data Integrity

Again, mobile corporate users need any virtual sessions to be as productive and creative as possible to achieve quick adoption of this model and to ensure that fewer “exception requests” (for not participating) are generated.

This means that hosted applications generally need to include the following types of applications to replace what they would normally use locally to work on data or to communicate while in session:

- an Internet browser
- an Outlook (or other chosen email) client
- an approved Instant Messenger (IM)
- Microsoft Office or similar Suites
- other vertical applications which an organization or the mobile workforce may find essential for their productivity and efficiency

Concerns about data integrity can be mitigated because company data in this proposed scenario are only saved back to corporate servers which are not only secure, but are also regularly backed up. A much higher percentage of all created content can be retained, regardless of the status of the device that originated it.

With a vDLP solution, all apps which touch company data are found within the hosted virtual session - and therefore exist only on the home server. With this approach, an employee can use the apps they require and the organization can be assured that they retain control over their data that is only saved back to the server and not to BYODs.
MDM Systems ≠ Data Leak Prevention

Again, while MDM systems offer an integral role in BYOD security, it needs to be clearly stated that MDM does NOT equal DLP.

Dedicated DLP solutions can help organizations dealing with the rapid integration of personal mobile devices into the enterprise by employing the basic fundamentals of determining what data and content is business critical, defining how it can be accessed, stored and sent outside the company (or even to groups within the company) all while using comprehensive security technology to protect the company’s confidential data.

As more personal mobile devices enter the network, data leaks can emanate from a variety of sources that include USB flash memory, smartphones, tablets, digital cameras, and even MP3 players. Network-based applications, “Cloud” storage and social media access may also introduce hard-to-control data leaks without a DLP solution in place.

Effective DLP requires both contextual and content-based controls that provide multi-layered inspection for fine-grained control over a full range of data leakage pathways.

These pathways often lead to a USB connection, so applying contextual controls and content filtering where possible at select endpoint data exchanges where personal mobile devices are used is critical for secure data protection. IT staffs can help identify and match end user (or preferably user-group) access rights to their job requirements to minimize security risks while maximizing productive use of personal mobile devices on the job.

The Outcome

In the end, users may still argue that they don’t always have sufficient access, bandwidth, or connectivity when out of the office (airplane-mode, third-world travels, etc.) and need to have the data local, but for most organizations the vDLP model will be a better tradeoff than the very real risk of losing sensitive data that could result in bad PR, lost goodwill, lost business, as well as major fines and other penalties resulting from compliance breaches.
1.7 Conclusion

Companies across all industries are fighting to secure their proprietary and confidential data behind firewalls and complex passwords, unfortunately, the reality is that this data is most likely still slipping through the cracks. The introduction of employee-owned “BYOD” devices and the consumerization & mobility of the modern workplace presents new security and data leakage threats that organizations must now address and combat.

As mobile devices are mostly used outside of protected office networks, conventional perimeter-based security components cannot be used to monitor and control their independent communications. Also, by virtue of their physical mobility, smartphones, tablets and laptops can be lost or stolen more easily. As a result, the data stored on lost or stolen mobile devices can be immediately accessible to whoever physically has the device.

Effective BYOD security requires not only a method to manage, track and, if necessary, wipe a mobile device, but also a data leak prevention (DLP) strategy. This DLP approach should require both contextual and content-based controls.

Data Leak Prevention can help organizations dealing with the rapid integration of personal mobile devices into the enterprise by employing the basic fundamentals of determining what data and content is business critical, defining how it can be accessed, stored and egressed, and using comprehensive security technology to protect the company’s confidential data.

A Best Practice Equation for Your BYOD Security Strategy

The following simplified equation illustrates a comprehensive BYOD security strategy:

BYOD Security = “MDM” + “App” + “VPN” + “VM” + “DLP”

- “MDM” is the Mobile Device Management software for controlling local device apps, SD card, remote wipe/kill, password policy, encryption, etc.
- “App” is the virtualization hosting application (Citrix Receiver, etc.) for connecting over the Internet to the company’s “virtual portal”
- “VPN” is the Virtual Private Network SSL connection (through DMZ/Firewalls) used by the hosting application that also helps authenticate users along with directory services
- “VM” is the “Virtualized Machine” Windows OS environment (ex. Citrix, WTS, MS RDx, etc) controlled session where “internal” applications are published and data is accessible/editable
- “DLP” is the Data Leak Prevention at the VM Windows OS session for all data egress points (email, web, IM, print, mapped USB) to prevent data leakage both to the BYOD device and Internet.
About DeviceLock, Inc.

Established in 1996, DeviceLock is a leading provider of endpoint device/port control and data leak prevention software for business, education and government institutions around the world.

DeviceLock, Inc. is a worldwide leader in endpoint device control and endpoint data leak prevention security. Our DeviceLock product is currently installed on more than 5 million computers in more than 70,000 organizations around the world.

The company’s customers include medium to large financial, health care, energy, and manufacturing commercial entities, as well as various state and federal government agencies, departments, and military branches.

DeviceLock, Inc. is an international organization with offices in San Ramon (California), Vancouver (Canada), London (UK), Ratingen (Germany), Moscow (Russia) and Milan (Italy).

Contact Information
DeviceLock USA:

3130 Crow Canyon Place, Suite 215, San Ramon, CA 94583, USA
TEL (toll-free): +1-866-668-5625
FAX: +1-925-886-2629
us.sales@devicelock.com
support@devicelock.com
www.devicelock.com