

SOTI®



White Paper

# BYOD 2.0



ENTERPRISE MOBILITY MANAGEMENT

Copyright 2015© SOTI Inc. All rights reserved.

**SOTI.net**



## BYOD 2.0 Demanding a New MDM Approach

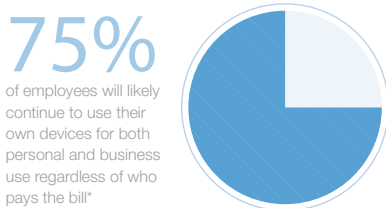
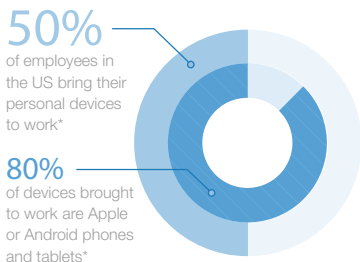
With all the attention being paid to the BYOD (Bring Your Own Device) phenomenon in recent years, it comes as no surprise to see the industry already coining the term BYOD 2.0. With this rapid evolution, comes some interesting opportunities and challenges.

The democratization of devices in the workplace is placing an increased onus on IT departments to find effective and efficient ways to manage disparate types of devices and applications. To do that, they are investing in increasingly comprehensive MDM (mobile device management) tools that can do far more than remote diagnostics, tracking and lockdowns. Yet not all devices – or solutions – are created equal.

According to Forbes writer Bob Egan, BYOD 2.0 is defined as the move away from either business- or employee-centricity, and toward the intersection of the two. It's clear that this is where the business world is heading today. Whereas BYOD in its earliest iteration was a corporately mandated, hardware-centric proposition focused on managing and enabling devices remotely; it has evolved into enabling and developing mobile apps and content over multiple operating systems and consumer devices (i.e. operating system and security centric).

The business case behind BYOD has become a compelling one. An April 2013 Gartner report by David A. Willis in fact notes that BYOD strategies “are the most radical change to the economics and the culture of client computing in business these days.” The benefits cited include new opportunities for the mobile workforce, increased employee satisfaction, and reduction or elimination of costs.

Cisco estimates that the net cost saving from employee-owned devices will likely exceed 20%. With this comes new business models in which employees bear some of the costs associated with the device, while CIOs for their part maintain control only on the “space” on the device that directly relates to enterprise data and applications.





## Moving Beyond The Blackberry

In the early BYOD days, enterprises restricted the use of devices that enabled access to corporate data. In many cases, employees would have two devices to cover personal and business use. BlackBerry virtually monopolized the enterprise space because of the inherent control over management and security, so there was little need to support other mobile platforms in the workplace.

In the past few years, there was been a groundswell of workers interested in using their own device for both business and personal use; and who want to personally select and purchase their devices for enterprise applications and data access. This rapid consumer acceptance of both Apple and Android has put increasing pressure on organizations to accept these devices in the workplace. This has disrupted both the technical and financial aspects of device deployment and management.

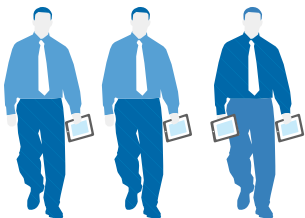
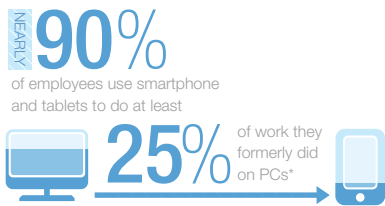
According to a 2012 McKinsey & Company report “BYOD: From company-issued to employee-owned devices”, of 3,000 workers surveyed who use mobile devices for their jobs:

- 80% of smartphones were employee owned
- 67% of tablets were employee owned
- Employees took on 63% of device costs and 62% of mobile data service costs

Gartner for its part reports the following:

- BYOD is the #2 technology initiative for CIOs in 2013 (behind business analytics and business intelligence)
- The number of workers having mobile access to applications will soon double
- Over half of the eligible workforce, and two-thirds of households already have a smartphone that can run apps and has a capable browser
- Over 60% of workers report using a personal device at least once a day in their work
- 44% use a personal smartphone in their job

The functionality of devices has also taken on added dimensions. Gartner notes that mobile computing in the workplace quickly expanded beyond simple field communications (the first stage) to asynchronous communications, limited file sharing, simple collaboration and basic workflow (the second stage). The third – and current – stage is mobile workforce enablement through mobile applications for the entire population of workers.



More than two-thirds of employees would prefer a single mobile device for both work and personal use\*

## ⚠ The Risks For The Rewards

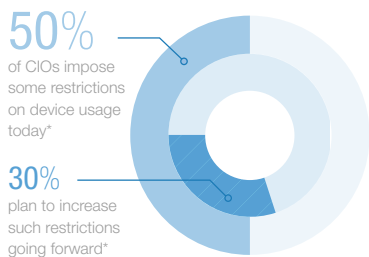
Despite the productivity gains, which are significant, organizations are facing a number of challenges – not the least of which is effective and secure mobile device management. Given the fact there are three major platforms (iOS, Android and Windows), coupled with a growing concern over data security, fragmentation is a significant and very real concern.

The fragmentation began in 2007 with the advent of iPhones, which made it all too easy for employees to use their devices to connect to the enterprise server. Android fragmented the market even more. From a device management perspective, organizations found themselves grappling with how to manage different platforms without spending inordinate funds on purchasing and deploying corporate phones, while managing data security and privacy. This is not an issue that is specific to any one industry. Today almost every vertical, from healthcare and education to finance and government, is facing a similar dilemma.

MDM has had to transform to keep pace. Originally focused on managing ruggedized devices in the field, original MDM offerings were never intended to address consumer mobile devices in a productivity setting. The increased complexity that comes with BYOD 2.0 has made MDM a more exacting science that requires functionality that extends well beyond managing email and enabling VPN access.

To that end, there has been a wide range of MDM offerings developed over the years. Many are either platform (e.g. iOS), function (e.g. security) or device specific (e.g. smartphones). However, as convergence in the enterprise continues, the ideal approach is creating a “single pane of glass” for remote management of all devices – from PCs and laptops to smartphones and tablets.

In fact, there is now an emergence of a more appropriate label: EDM (enterprise device management), which encompasses solutions that take on an increasing portion of the management burden – from managing passcodes and encryption to application management, remote troubleshooting/diagnostics and policy compliance – as seamlessly as possible.



## The Multi-Platform Approach

Businesses are just now discovering the true potential of mobility in the wake of massive consumer adoption, and are learning to redefine how they operate. Yet securing and managing mobility in a BYOD 2.0 world cannot be solved with a cookie cutter solution. Although organizations have many common pain points as they seek to enable and manage BYOD, many are leveraging mobility beyond that and need advanced, flexible mobile device management tools to optimize their mobility and get the most out of their investments

**50%**

of employers will require employees to supply their own device for work purposes by 2017\*\*



MDM solutions have to evolve and redefine themselves in parallel. Having been in the industry for more than a decade, SOTI knows first-hand that moving beyond enterprise and device specific offerings to encompass consumer devices is an extremely challenging path. An integral part of this discipline is addressing the specific requirements and features of different operating systems, and incorporating the various jurisdictional controls for privacy and identity.

In the years when BlackBerry dominated the enterprise space, many initial MDM offerings were Windows-based niche solutions for ruggedized devices in the field (e.g. scanning/signature capture for couriers). It was Apple that changed the rules once again with iOS 4. With that launch, it became the only company to introduce its own MDM functionality, providing an easy, simple interface with MDM tools.

Android is another matter altogether. Google for its part restricts its own APIs (application programming interface), which demands a different, more painstaking MDM approach. Since device manufacturers must create their own APIs, all Android devices cannot be managed the same way. In other words, what may work for a Samsung won't for an LG or HTC. Solving this dilemma means forging individual relationships with each device manufacturer to allow permission to manage its devices, and then applying a portable management layer stack. To date SOTI has signed agreements with 32 of the top Android manufacturers worldwide.

Today, SOTI is the only MDM provider with remote capabilities that can span all three major platforms, as well as multiple devices. This latter capability is especially compelling as the Internet of Things adds an entirely new layer of complexities to remote device management.

**-30%**

By 2016, the average amount a qualified employee currently receives for the business use of a personal smartphone will be reduced by 30%\*\*

## The New Features That Count

As BYOD adoption increases and the Internet of Things takes hold, the need for remote control of more diverse functions will grow exponentially. It will include software installation, synchronization, and troubleshooting. It will also need to address more recent innovations such as containerization to isolate management of functions from personal use; and geofencing to restrict access or usage based on geographical boundaries.

Containerization in particular has become a major area of concentration for developers and businesses. By way of explanation, enterprise applications enable access to certain data, analytics, sales figures, contacts, etc. While there are obvious security concerns that go with that, the same level of management is not required for an individual's personal emails and apps. To address this need, SOTI has embedded an SDK to enable management within a specific application. In other words, users can create a "container" with embedded management functions for a more secure user experience.

Today, a comprehensive solution is one that enables organizations to centrally manage, support, secure and track mobile devices regardless of the type and platform. Essential functions for managing in a BYOD world include:

- Multi-platform, web-based administration
- Access to corporate "sandbox" on personal devices to block access to unwanted features, applications and games
- Live tracking and reporting of device information (status, security, condition)
- Remote control and help desk to lower support costs and increase device availability
- Location services and geofencing to keep application usage within a specific area or trigger an action when a device is entering a restricted area
- Web filtering to enforce responsible use in the workplace
- Grant or block access to corporate resources; lock down/wipe lost or stolen devices

The evolution of BYOD has been rapid and profound. While security initially focused on the device (i.e. the endpoint), today device management must also address a diverse range of applications, data controls and capabilities. As a result, comprehensive MDM tools that can deliver seamless management are becoming essential to BYOD success.

As the world mobilizes, the stakes have changed. Mobility will impact everything from how an enterprise conducts customer relations to how they manage building access. For many operations it has become a business imperative from the perspective of productivity, employee satisfaction and cost savings. Optimizing the potential of that mobility lies in the management infrastructure behind the devices, whatever and wherever they are.

### NO DIRECT SUBSIDY

for personal devices

### BY 2016

By 2016, most employees using a personal device in business will receive no direct subsidy for its use\*\*



By 2016, the typical organization will spend over \$300 per year per employee on mobile applications, security, management and support\*\*

### Notes:

\* Source: BYOD: From company-issued to employee-owned Devices, June 2012





\*\* Source: Gartner, Bring Your Own Device: The Facts and the Future, April 2013

## About SOTI

SOTI is a proven product innovator and EMM Industry leader. Over 15,000 customer across 170 countries rely on SOTI for their EMM needs. We empower the enterprise to take mobility to endless possibilities.

## For more information

For more information about **SOTI MobiControl** visit us at [www.soti.net](http://www.soti.net) or email SOTI Inc. at [sales@soti.net](mailto:sales@soti.net).

-  [facebook.com/soti.net](https://facebook.com/soti.net)
-  [@SOTI\\_Inc](https://twitter.com/SOTI_Inc)
-  [linkedin.com/company/soti-inc](https://linkedin.com/company/soti-inc)
-  [youtube.com/sotiinc](https://youtube.com/sotiinc)