Evolving Requirements for Bring Your Own Device (BYOD) Management

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for ManageEngine
August 2016
# Table of Contents

- Executive Summary ................................................................. 1
- The Reality of BYOD Requirements .......................................... 1
- Addressing the Challenges of BYOD ......................................... 2
- Successful BYOD Management ............................................... 3
- EMA Perspective ................................................................... 4
- About ManageEngine .............................................................. 5
Executive Summary

“Bring your own device” (BYOD) management practices evolved from a business need to support a mobile workforce that also uses their devices to perform non-business tasks. Principle challenges to BYOD enablement revolve around the need to rapidly and reliably deliver business applications and data to mobile users without violating enterprise requirements for security and compliance. BYOD management practices and solutions empower end users while protecting business interests by isolating enterprise resources, actively preventing data loss, and ensuring security requirements are continuously met.

The Reality of BYOD Requirements

The consumerization of IT forever changed how business professionals regard and use their computing devices. When mobile device manufacturers began directly marketing their products to home consumers (rather than businesses), employees discovered the power of choice in the devices and applications they regularly use to perform job tasks. No longer content to rely solely on whatever resources their employers provide for them, workers began purchasing their own devices and using them to perform job tasks. Most organizations were caught unprepared to support the large influx of new devices and severely lacked the processes and infrastructure for supporting non-business-owned devices. Today, three quarters of enterprise mobile devices are personally owned by their users.

Since traditional endpoint management processes (which were developed principally to support enterprise PCs) rely on end-to-end device control, user-owned devices could not be managed with existing solutions in most cases. To enable remote access to business applications and data from all user devices, many IT managers simply threw up their hands in defeat and disabled or circumvented security protocols essential to keeping business safe.

As if the need to support non-business-owned devices was not challenging enough, users with enterprise-owned mobile devices broadly expect to use them to perform both business and non-business purposes. Understanding that employees do not wish to carry multiple devices, 86% of organizations now allow their employees to use business-owned devices to perform non-business tasks. From an IT management and security perspective, the actual owner of the device is mostly irrelevant in comparison to how the devices are actually used. Any device used for both business and non-business purposes must be secured and supported without limiting its performance and use. BYOD management solutions were developed specifically to help organizations meet business security requirements while supporting and securing devices used for these dual purposes. Despite broad acceptance and understanding of BYOD management processes, relatively few businesses have wholly embraced the solutions, and only 16% of organizations consider themselves to be fully prepared to support BYOD requirements.

\[1\] Effective BYOD Management: Empowering a Mobile Workforce, May 2016
Evolving Requirements for Bring Your Own Device (BYOD) Management

Addressing the Challenges of BYOD

In traditional business PC environments, organizations were able to largely standardize which devices (principally Windows-based devices) employees used to perform job tasks. With the adoption of BYOD policies, however, end users are able to choose which devices they wish to employ. This freedom of choice resulted in a broad diversity in mobile device types and operating platform—including, iOS, Android, and Windows—all of which need to be provisioned, secured, and supported by the business. Additionally, applications installed on BYOD endpoints cannot be restricted to just business-approved software, and any enterprise support and risk mitigation tasks performed on the endpoints must not impact any non-business use of the devices. Ensuring proper security while enabling broad access to business services without performance degradation seems to be a direct contradiction in directives, and is often the cause of much frustration among IT managers.

When it comes to enterprise mobility management, 75% of surveyed organizations report that meeting security requirements is the number one business concern. In fact, two-thirds of businesses surveyed by EMA indicated they were aware of a mobile device-related security breach that occurred during the previous 12 months—and those were just the ones that had detected a breach. Lack of control over the use of business resources is at the heart of mobile security challenges. For example, since users often employ non-business software to perform personal tasks, it is not unusual for them to use these unapproved applications to also access business resources. This is a particular problem when non-business software is used to distribute business data. In fact, 80% of surveyed organizations reported they were aware that employees regularly used unapproved and unsecure methods of data distribution, such as public email packages, cloud-hosted data storage platforms (e.g., the standard edition of Dropbox), Facebook, and text messaging (Figure 1). In this way, sensitive data is taken outside the control of IT operations and may place the business at risk.
Evolving Requirements for Bring Your Own Device (BYOD) Management

In addition, mobile devices utilized in BYOD environments are themselves beyond the control of the business. Considering that one out of every 12 devices is lost or stolen each year, businesses are substantially placed at risk if compromised devices contain sensitive business data or have direct access granted to business systems and services. Similarly, when employees leave an organization, they may walk away with company data, applications, and access privileges installed on their personal devices. It should also be noted that when mobile devices are used to perform non-business tasks, they have an increased risk of being infected by malware—including viruses, spyware, adware, worms, and Trojan Horses—which could then be passed on to other business devices and systems. EMA primary research indicates a full third of all organizations are challenged by mobile device-related malware incidents each year, 70% of which occur on employee-owned devices. Furthermore, even organizations that introduce security practices and solutions may still be at risk of security breaches by users who circumvent security policies. One out of every seven surveyed business users admitted they had rooted or jailbroken their mobile device, violating restrictions imposed by their organization.

Successful BYOD Management

Establishing effective control over mobile devices in a BYOD environment without reducing user productivity or their performance of non-business tasks on their devices requires a multifaceted approach to endpoint management. Key practices and solutions for enabling optimal BYOD management can be logically organized into four principal categories:

- **Resource Isolation** – Business applications, data, and services must be logically segmented from a user’s personal, non-business resources. The most popular method for achieving this is containerization, which effectively sandboxes the business environment, preventing access from unapproved applications. Compromised devices can then have access easily denied or completely removed to just business resources without impacting any non-business software. Additionally, users must be able to reasonably expect that any business security and management services will not intrude upon their personal space. Users are more likely to employ business-provided resources when they know their personal files and applications will not be exposed or affected.
• **Data Loss Prevention** – All enterprise data must be secured with encryption when stored on the hosting environment, while in transport over networks, and when in use on remote devices. Secure methods should be provided for data distribution and document sharing, including the employment of a business-dedicated email package that does not allow data distribution to unapproved recipients. The copying of business data should be prevented at the device level by blocking connection services such as over Bluetooth or USB ports.

• **Security Assurance** – Only devices that are secured should be able to access business applications, data, and services. Active scans for viruses and other malware should be required on all supported devices and rooted or jailbroken devices should be identified. Any devices determined to be out of compliance or otherwise compromised (such as if the device is lost, stolen, or in the possession of a terminated employee) should be blocked from accessing business resources and any business data stored on the remote device should be locked or wiped.

Naturally, it is impossible to effectively perform all of these security monitoring and enforcement tasks through purely manual processes. Automated monitoring and management solutions are essential to ensuring enterprise requirements for security are achieved without diminishing user productivity. As an example, the ManageEngine Mobile Device Manager Plus solution suite was purpose-built to centrally manage and secure all iOS, Android, and Windows mobile devices in use by enterprise employees, regardless of whether the device is business-owned or user-owned. The ManageEngine platform can containerize individual applications or entire user workspace (i.e., all business applications and files) so that they are isolated from a user's personal apps and data. Applications are centrally managed and securely distributed with strict authentication and access rites that enable granular whitelisting and blacklisting of individual software elements. All data is encrypted when at-rest and in-motion, and transport layer security (TLS) is enabled over SSL connections. Any mobile devices that are used to access business resources are automatically identified and recorded in a centralized asset database. Rooted or jailbroken devices are automatically detected, and any compromised devices may be remotely locked, wiped, or prevented from accessing business systems.

**EMA Perspective**

Nearly every modern business is reliant on a mobile workforce, and user expectations for access to business resources from their personal devices are only increasing. Organizations that embrace BYOD management practices and solutions are better positioned to ensure their employees are able meet evolving business requirements and to compete in today’s more dynamic marketplaces. In fact, 76% of surveyed organizations that have adopted a BYOD management platform indicated to EMA that they were satisfied or very satisfied with their ability to support their mobile users. This is not surprising considering how successfully BYOD management solutions increase the effectiveness of IT operations. For instance, organizations that have adopted automated solutions for configuring and supporting email report 20% fewer email-related user problems than those that do not. Similarly, organizations that provide application management support are 19% less likely to have software-related problems. More efficient management processes can also have a

---

**Organizations that embrace BYOD management practices and solutions are better positioned to ensure their employees are able meet evolving business requirements and to compete in today’s more dynamic marketplaces.**
Evolving Requirements for Bring Your Own Device (BYOD) Management

profound effect on reducing the cost of operations. A whopping 93% of surveyed organizations that had adopted BYOD management solutions reported to EMA that they had achieved quantifiable cost savings from the platforms.

Comprehensive BYOD management solutions, such as those offered by ManageEngine, are the cornerstone of any modern endpoint management strategy. Not only do they resolve many of the urgent problems of today in the secure delivery of applications, data, and services to mobile users, they also lay the groundwork for the emerging challenges of tomorrow. As business professionals continue to increase the number and diversity of devices they regularly use to perform job tasks, their expectations will increase for consistent and reliable access to business resources. Organizations that fail to achieve control over broadly distributed and widely accessed apps and data place their business at risk and will see diminishing performance from their workforces. BYOD management practices and solutions empower users with greater performance, productivity, and job satisfaction while ensuring businesses meet security and compliance objectives.

About ManageEngine

ManageEngine is focused on delivering the real-time IT management tools that empower IT teams to meet organizational needs for real-time services and support. Worldwide, established, and emerging enterprises—including more than 60% of the Fortune 500—rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops, and more. ManageEngine is a division of Zoho Corporation with offices worldwide, including the United States, India, Singapore, Japan, and China. For more information, please visit http://buzz.manageengine.com/; follow the company blog at http://blogs.manageengine.com/ on Facebook at http://www.facebook.com/ManageEngine and on Twitter @ManageEngine.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA’s clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries. ©2016 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
3431.081816