MATRIX42

Is Your Company Mobile Ready?

Experience the productivity and flexibility of mobility while keeping your data and devices secure and in compliance.

Table of Contents

The Dynamic Mobile Enterprise

The work environment of today is much different than it was several years ago. The only way to stay competitive as a large enterprise is to make sure the right people have access to the right resources, tools, data and information – securely. This complex demand is compounded by a very dynamic workforce where people can be in multiple places throughout the course of a day working on multiple devices—both personal devices and company owned. And today's workforce has an expectation of connectivity and flexibility that has not existed before.

- Shipments of tablet computers to enterprises around the world are expected to rise from 13.6 million units in 2011 to 96.3 million units in 2016.[1]
- The average number of devices carried by a mobile worker has grown to 3.5, up from 2.7 in 2011. 92 percent of mobile workers believe their smartphones should be enabled for both work and personal use.[2]
- 86 percent of organizations either permit the use of personally owned devices connected to the network or are moving that way.[3]
- A survey by Harris Interactive and CareerBuilder in June 2012 found that 69 percent of employees from ages 25 to 34 work after leaving the office.[4]
- According to the September 2012 Q3 iPass Mobile Workforce Report, mobile employees work as many as 20 additional hours a week when away from the office.

With this proliferation of mobile devices that connect to the corporate network, CIOs need to balance their responsibility to maintain the security and integrity of corporate data with a new generation of employees who expect IT to allow them to use any device – personal or company issued – to access corporate networks.

For organizations that are used to maintaining strict security and access policies, they are faced with new situations that are not quickly and easily resolved if the right policies are not in place along with the means to enforce those policies:

- An employee purchases an iPhone and asks the IT department to configure it to receive corporate email and access the company intranet. *Do you have a corporate IT policy for this?*
- A business manager in the company purchases iPads for the entire team to improve productivity without clearing it first. Now team members are downloading dozens of applications and using these apps to get their job done at work and remotely. *Do you have a corporate IT license compliance policy for this?*
- The CFO lost his brand new Android device while traveling on a business trip. It contained company financial information and a list of the company's top 500 customers with detailed contact information. *Do you have a corporate IT security policy for this?*

[1]"Worldwide Enterprise Tablet Market Forecast Report," Infinite Research, January 2012
[2]"iPass Global Mobile Workforce Report – Q1 2012"
[3]"2012 State of Mobile Security," Information Week, May 2012
[4]"How Millennials Work Differently From Everyone Else," Forbes, Sept. 13, 2012

As Table 1 demonstrates, the business, the end user and IT each have different questions or concerns about using smartphones and tablets in the enterprise. According to a recent CIO magazine survey, 87 percent of respondents identified productivity benefits – more than any other factor – as a top driver for their company's mobile technology investments. The survey offered further proof that increased productivity and the other benefits of mobile solutions are highly valued within an organization.

The role of IT is to balance the demands from increasingly sophisticated users and the mission-critical growth and business development demands of executives with the need to maintain security and control of corporate data and assets. This is complicated by the combination of ever-growing volumes of data and assets.

Table 1: Organization-wide Questions about Mobile Devices in the Enterprise

Business	End user	IT
How can smart devices help our employees be more productive?	Can I access the information and resources I need to do my job effectively from anywhere at any time?	How do I keep sensitive corporate data from being accessed on a lost device or by a former employee?
Does the flexibility offered by smart devices improve employee morale and job satisfaction.	Can I use my own personal device to access the corporate network and my email? Or can I use personal applications on my company device?	Are we in compliance for all the applications employees are running on their devices?
Can we cut costs by allowing employees to use their personal devices for work?	Is there a quicker way to provision or add apps to my device without waiting for IT to respond to a help desk ticket?	How do I keep end users from circumventing IT processes and putting the company in jeopardy?

This paper will go through the main challenges that companies need to address as part of their mobility strategy, how they can implement an effective bring-your-own-device (BYOD) policy and five critical steps that need to be part of the company's solution for managing its mobile devices.

Top Mobility Challenges

As smart devices proliferate in the enterprise, virtual workplaces become more prevalent and workers access company resources with multiple devices from multiple locations, work is no longer a place, it's an activity. This creates many opportunities for companies, but it also presents many new challenges:

Mobility is one of the greatest threats to enterprise data security

Companies are struggling to secure and manage their mobile devices, which can lead to potentially higher capital and operational costs and greatly increases the security risk level of the organization. Whether mobile devices are company or employee owned, a solution must be implemented to standardize security across all devices, protect sensitive corporate data and meet compliance standards.

Siloed management of mobile devices is inefficient and expensive
Using tools provided by the carrier or device manufacturer that individually manage each device or creating proprietary infrastructure and tools to support a mobile device management initiative is time consuming and expensive. Also, integrating with third-party infrastructures is complex and challenging.

Device proliferation and diversity within the enterprise is creating complexity for the IT department
Numerous mobile platforms now need to be managed within the enterprise. With desktops and laptops, it was easier for companies to standardize on a single OS, a few different hardware options and create standard configurations for easier management. With mobile devices, employees are using their preferred device, whether it runs iOS, Android, Windows or others. And in the case of Android and Windows, there are many unique devices. Not only does IT need a way to identify all mobile devices within the enterprise, it needs to know how to manage each unique device and OS.

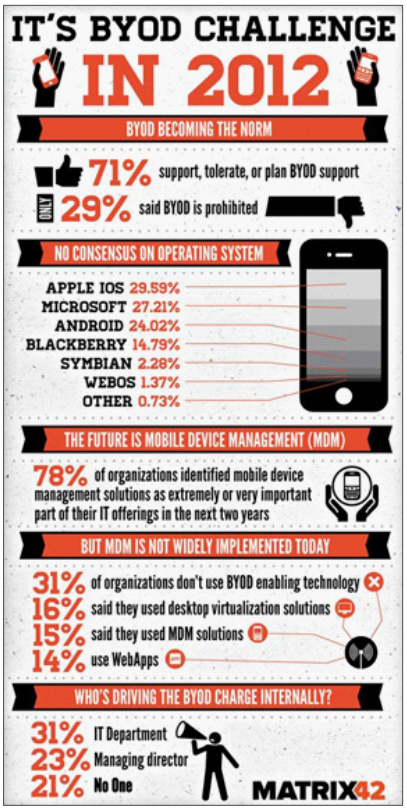
Provisioning, configuring and securing mobile devices can be time consuming and expensive
The mobile device management complexity is also creating a lack of standardization and security. Configuring access to HVD (Hosted Virtual Desktops) or cloud services via SaaS (Software as a service) and VDI (Virtual Desktop Infrastructure) to mobile devices is also complex and challenging if a management solution can't support these environments.

Is Your Company Mobile Ready?

The same *Information Week* study that found 86 percent of organizations either permit the use of personally owned devices connected to the network or are moving that way also found only 40 percent of organizations limit the range of devices supported and require that users connect them to a mobile device management (MDM) system. Many seem to rely on users agreeing to policies and then trusting the user to do the right thing. For as much effort as companies have made over the years to secure their data, this seems like a very unnecessary risk to take. It's much like locking all the windows and doors on your house and then leaving the garage door wide open.

Neglecting or delaying the implementation of a holistic mobile device management strategy and solution across all of your corporate devices and tablets can easily lead to user downtime, increased security risks and increased IT costs for your company. IT Administrators must be able to maintain complete control over device access, and other compliance-related management activities, along with any configuration changes relative to business service access (e.g. security applications, firewalls, network access control, patches, policies, etc.). This also includes the ability to distinguish personal user data from corporate data, to further support BYOD initiatives, while still protecting user privacy.

BYOD on Your Terms



Most companies have now adopted, or are planning to adopt, a BYOD policy. This helps companies save money by transferring some of the hardware costs to employees, improve employee satisfaction and productivity, and create a partnership with employees to maintain security rather than have them circumvent IT processes.

A survey of nearly 600 enterprise IT professionals at CeBIT 2012 found that BYOD is becoming the norm, with 71 percent supporting, tolerating or planning BYOD support. (See infographic)

Nearly two-thirds of survey respondents said there is at least some level of acceptance of BYOD by their IT department, and 78 percent said mobile device management will be a key part of their IT offerings in the next two years.

The reality is that for companies to remain competitive today, it is imperative that end users be provided a way to access company resources and data through any handheld devices and tablets from anywhere and at any time. BYOD is quickly moving from an option for companies to a mandate. With tech-savvy users that are able to configure their own devices if they don't get the access they want as quickly as they want, companies really have no choice but to figure out how to make it work.

The good news is that MDM solutions can help IT give their users the flexibility they want while maintaining the level of control they require. The key to a successful BYOD policy is to utilize the proper tools that provide employees with the flexibility for a greater choice of devices while maintaining security by offering it within enforceable company policies.

Five Key Steps for Managing Mobility and Reducing Risks

Advanced mobile devices and applications are critical to an enterprise's success. Managing the current mobile technology used by employees and ensuring the success of future deployments can be challenging. Enterprises need a comprehensive mobile device management solution that encompasses deployment, security, monitoring, management and support. A solution must provide the technology to simplify these processes across multiple device types and mobile operating systems. The following are five key steps that are covered by a holistic MDM solution along with key features that should be evaluated:

Step 1: Automated Deployment of Devices

- Automate all the tasks that make a device ready for business use such as email setup, application access, password policies, etc.
- Activate devices using SMS, email, URL and other flexible options
- Enroll corporate and employee-liable devices individually or in scale
- Authenticate users and devices through basic and directory services-based authentication
- Instantly configure policies, settings, certificates and access to enterprise accounts over the air
- Wirelessly provision internal and recommended apps through the enterprise app catalog

Step 2: Secure the Devices and Reduce Risks

- Ensure authorized and compliant devices have secure access to business resources and accounts
- Protect personal and corporate data and the entire device through encryption and passcode policies
- Prevent unauthorized device use by locking down device features and enforcing restrictions
- Audit devices for compliance with corporate policies, settings, applications, third parties and more
- Automate business policies for non-compliant or jailbroken devices
- Protect lost or stolen devices with lock and wipe features

Step 3: Monitor Devices

- Monitor devices and network health status and statistics for exceptions
- Track user activity such as app downloads, voice, SMS and data usage against pre-defined thresholds and whitelists or blacklists
- Monitor system access and console user activity through detailed event logs
- Set up alerts and automated business rules for specific device or network actions, user actions or system performance
- Generate actionable reports with automated distribution across the IT team
- Establish automated process to proactively respond to issues

Step 4: Manage Applications

- Manage and control applications efficiently across the device fleet
- Provide self-service access to approved applications through company's service catalog
- Streamline and automate mobile asset and inventory management
- Update and provision new policies, settings, certificates, apps, software and access to enterprise accounts – Exchange Active Sync, Wi-Fi, VPN, CA, LDAP and more – over the air
- Push down configuration profiles, apps, software or remote lock/wipe commands on-demand, at a scheduled time or the next time a device or group of devices checks in

Step 5: Support Users and Devices

- Keep mobile workers productive by quickly and efficiently diagnosing and resolving device issues in real time
- Perform device diagnostics remotely to identify issues

- Provide remote assistance to mobile users and communicate from the console via SMS messaging
- Take remote control of a device for more efficient troubleshooting
- Provide users with remote management capabilities through a self-service portal
- Manage troubleshooting cases and system incidents using an integrated case management system

The Matrix42 Advantage

Mobile Workplace Management from Matrix42 makes it easy to launch a BYOD program that meets the needs of both employees and IT through either a cloud-based or premise-based offering. Employees can use their favorite mobile devices to access the network, request support and receive services, while IT can maintain control over all of the organization's mobile devices, provide a higher level of service and reduce costs.

Matrix42 is the first company to fully integrate mobile device management with Self-Service allowing end users to request and provision services and devices at any time, through their ServiceNow service catalog or one provided by Matrix42, as part of a BYOD policy. These automated processes remove common, repetitive IT tasks from the helpdesk and lets end users solve their IT challenges on demand to reduce service costs by up to 70 percent.

In addition to tracking software licenses, assets and contracts, the inclusion of license, contract and asset management provides analysis of end users' work profiles to evaluate the devices, apps and services they prefer. IT administrators can ensure all mobile devices connected to the network are inventoried, secured and managed within company policies, whether they support BYOD for employees or the devices are owned by the company.

Conclusion

Developing a mobile strategy is critical to the success of an organization's mobility initiatives. More importantly, CIOs and IT directors should take the time to think through their strategies, solutions and products – because decisions that seem clear and easy often aren't. IT departments also need to think about restructuring their organizations to reflect the everyday and prevalent need for mobile device management. Having mobile device experts within your IT department focus primarily on infrastructure is not the only use for their skills. Moving them, for example, to the application developer's team is one option that helps bring mobile device management into the mainstream IT function, according to Forrester.

Last and most important, IT organizations should consider a comprehensive and holistic mobile device management solution that encompasses the five steps previously discussed: deployment, security, monitoring, management and support. A solution that is able to simplify these processes across multiple device types and mobile operating systems and provide automation and self-service options to handle common tasks will increase the flexibility and productivity of employees, maintain the security of corporate data and reduce management costs.

Matrix42 software manages more than 2.5 million clients and has been providing workplace management solutions for 20 years. Visit us at www.matrix42.com or contact us at info@matrix42.com or 888-694-2872 to find out how 2,500 customers worldwide are taking control of their workplace to improve employee productivity, IT efficiencies, cost savings and user satisfaction.

MATRIX42

U.S. Office
3400 N. Ashton Blvd Ste. 110
Lehi, Utah 84043

Tel. +1 (801) 653-3700
Email info@matrix42.com

German Office
Dornhofstraße 44-46
63263 Neu-Isenburg, Germany

Tel. +49 (0) 6102/816-0
Email info@matrix42.de