WHITE PAPER

Addressing the Complexities and Growing Requirements of the Future Mobile Enterprise

IDC OPINION

Mobile enterprise adoption is growing tremendously as organizations leverage the rising number of mobile devices used by their employees. Organizations are beginning to realize that a new breed of valuable mobile applications are available for use but that IT and lines of business (LOBs) need to build a strategy for grappling with the inherent complexities in managing these assets. IDC believes that organizations need to consider the following in order to successfully deploy a mobile enterprise solution:

☑ BYOD and consumerization of IT represent the largest drivers of mobile enterprise deployments and the most significant challenges for organizations because the majority of smartphones used for business today are owned by employees rather than organizations.

☑ Many organizations are shifting away from device-based security and management toward application-, content-, and information-oriented security and management. By doing so, organizations are dealing with the critical requirement of safeguarding corporate data on devices they do not own.

☑ Organizations must balance IT challenges and mobile users' growing needs. Increasingly challenging security, management, and deployment risks are expected in the new mobile enterprise model, and at the same time, mobile users will demand the highest levels of mobile design, user experience, ease of use, and discoverability.

IN THIS WHITE PAPER

This white paper discusses the key market trends and challenges facing organizations as they seek to deploy mobile enterprise solutions and examines the growing requirements of these firms. It also delivers an overview of how enterprises can address the challenges in terms of repackaging and optimizing applications to better operate in a converged, dynamic mobile world.

SITUATION OVERVIEW

Enterprise Mobility: Key Trends and Challenges Facing Businesses

Mobile Enterprise Trends

Major shifts are altering the way organizations begin to deploy, manage, and secure mobile devices, content, applications, and information. The following key mobile enterprise market trends are significantly changing the direction of organizations:

☒ **End-user usage and company support of employee-liable devices will have the largest impact on the mobile enterprise.** A tremendous groundswell of smartphone device growth is being fueled by employees bringing devices to the enterprise. IDC estimates that in 2012, 55% of all smartphones used for business will be owned by employees rather than the business itself; this trend is expected to continue through 2016. In addition, while BYOD is a reality today for end users, what is perhaps more impactful is the adoption and support of BYOD policies by organizations. Savvy organizations will embrace BYOD to expand mobile use within the company, recognize increased cost savings, and provide a broader sense of choice to employees and partners.

☒ **Applications become king, and the focus of end-user design, management, and security goes beyond the device and begins to center around the application.** The idea of consumerization of IT is often mistaken as just a device phenomenon; however, consumerization of the application is also beginning to take shape. In a world where powerful and glimmering smartphones provide end customers with beautifully designed user interfaces and applications with impressive user interfaces, the stodgy business application is no longer an acceptable design for a mobile solution. Increasingly, mobile application vendors are providing enterprises and end users with business apps that can compete on design with some of the best consumer-oriented applications. In addition, because the majority of the applications now reside on devices not owned by an organization, an increased emphasis on securing and managing the application beyond the device is emerging.

☒ **Technologies such as cloud-based mobile computing and HTML5-based mobile apps drive faster and broader adoption of mobile enterprise solutions.** In the past, mobile solution deployments were often expensive and siloed operations that took six to eight months or more to complete, and the solutions were not terribly scalable. Today, cloud-based mobile technologies allow organizations to make a significantly lower and more manageable initial investment in mobile enterprise solutions and complete deployments in a matter of weeks rather than months. Similarly, companies and developers are beginning to warm up to HTML5 technologies to deploy mobile B2C, and increasingly B2B and B2C Web applications, often augmenting native applications. As HTML5 continues to expand its capabilities, the opportunity to leverage known Web technologies to build apps and reach a broader audience with a browser-based delivery is gaining favor with ISVs and enterprise organizations.

Seeking a Strategy: Key Mobile Enterprise Decision Components

Deploying a mobile solution is a complex undertaking involving many moving parts. While many organizations often have policies in place around mobile devices, few have thought out strategies for a complete rollout. Contributing to the complexity are individuals who bring devices to the enterprise that may or may not be authorized or organizations that mandate use of specific devices without much thought — often putting extreme pressures on IT and LOB organizations to make it all work.

It is critical for businesses to consider the complexities of mobile enterprise deployments and understand that device choice in itself is not necessarily the most important factor in planning. Often, an organization is very tactical in its decision to roll out a mobile offering; for example, "We need to mobilize our salesforce." While that decision may be a good start, it is critical to think in broader terms of what the decision means and how it will impact activities across the company. For instance, there may be an opportunity to expand the scope of such a deployment from the outset, such that it supports a broader user base, not just the salesforce. The following cornerstones represent the key components of a mobile enterprise solution and what should be considered.

Software

Mobile enterprise software represents a significant piece of such deployments and is a key to any strategic deployment to help realize a company's mobile goals. Software includes mobile enterprise management, mobile enterprise security, and mobile enterprise application platforms. All three core mobile software markets are growing at strong rates globally (see Figure 1).

FIGURE 1

Key Worldwide Mobile Enterprise Software Markets, 2011 and 2015
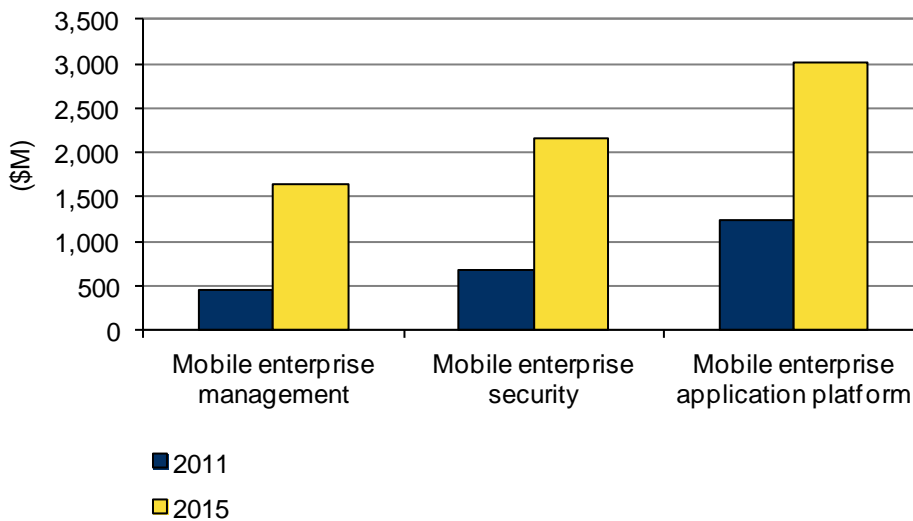
Source: IDC, 2012

Mobile Enterprise Management

Mobile enterprise management consists of mobile device and mobile application management software that addresses core device needs such as device provisioning, configuration settings management, inventory/asset management, software distribution, remote device wipe/lock of device, and policy management. Mobile application management delivers a more granular level of management, security, and corporate policy control of applications and content, enabling organizations to enforce or restrict user access, provide application deployment and provisioning, and offer application-level security such as data wipe and newer protections around risk management. In many cases, organizations are beginning to consider management first as a way to get a handle on the existing corporate-liable device set and the sprawl of employee-liable devices entering the enterprise before considering actual application enablement.

Mobile Enterprise Security

Mobile enterprise security software addresses multiple segments of potential security threats across the enterprise space, including core content and threat management, mobile security and vulnerability management, and identity and access management.

- **Mobile secure content and threat management (MSCTM)** products defend against viruses, spyware, spam, hackers, intrusions, and the unauthorized use or disclosure of confidential information on mobile devices. MSCTM is broken into three areas: mobile threat management (MTM), mobile information protection and control (MIPC), and mobile VPN:

    - **Mobile threat management.** Antimalware (which includes antivirus and antispyware), antispam, intrusion prevention, and firewalls for mobile devices

    - **Mobile information protection and control.** File, full disk, or application encryption for mobile devices; also includes data loss prevention technologies (Virtual data partitioning, either by hypervisor or by container, is also included in this category.)

    - **Mobile VPN.** VPN clients and infrastructure for mobile devices

- **Mobile security and vulnerability management (MSVM)** solutions provide device wipe, device lockdown, configuration settings, vulnerability status (e.g., Is the machine jailbroken?), and patching for mobile devices. MSVM also includes mobile security, policy, and compliance management. Application vulnerability assessment scanning falls within this category as well.

- **Mobile identity and access management (MIAM)** solutions provide authentication and authorization technologies (such as PKI and SSL certificates) for transactions conducted from mobile devices that support network access for mobile devices.

- **Mobile other security (MOS)** covers emerging security functions, such as antitheft/antifraud.

Mobile Enterprise Application Platform (MEAP)

MEAP represents the core platform that enables integration with back-end systems and creates mobile enterprise applications on the front end. MEAP typically includes the platform, development tools, and front-end applications and may be delivered as an on-premise solution or a cloud-based offering. Increasingly, organizations are opting for cloud-based solutions to lower initial costs and to increase speed to market. MEAP solutions enable B2C-, B2B-, and B2E-type mobile applications.

Services

Services consist of professional services that help with consultation and implementation as well as mobile operator services that provide key network connectivity to enable a mobile enterprise solution.

Professional Services

Professional services and systems integrator firms provide two core functions in the delivery of mobile solutions for enterprise customers. First, professional services provide a consultative set of services to help companies define a strategic direction for their mobile offerings. Such consultative offerings may start with an understanding of the business challenges and business process workflow and begin to plot out a way to address those issues in a methodical strategy that will address current and future needs. Second, once a strategy is in place, professional services providers assist in the key implementation process and may assist in supplier selection, application development, and back-end integration. Such providers may deliver a specific set of services (e.g., building an application or integrating a back-end application or business process), while others may expand on this and act as a single turnkey partner, coordinating the entire solution delivery including software, telecom, and hardware needs.

Mobile Operator Services

Mobile operator services consist of core telecom services (data and voice) required for connectivity but also can add value with an integrated network solution, international voice and data management offerings, telecom expense management functions, and other services. Many mobile operators may provide more advanced services including testing, hosting, kitting/staging, and life-cycle management. More recently, mobile operators have also begun to provide mobile strategy and architectural planning services and partner with best-of-breed ISVs and others to become a single-source provider for enterprise customers.

Devices

Mobile devices (largely smartphones and tablets) are being developed and enhanced at a frantic pace to keep up with tremendous popular demand. These devices provide more advanced functionality, storage, performance, and application capability. Hand in hand with the device selection is the operating system (OS) that resides on the smartphone and tablet, the functionality of which may be more consumer or business focused. All of the major smartphone OEMs have increased their focus on enterprise implementation, building separate business units to complement their solutions with key management, security, and application enablement functionality. Form factor, battery life, application development environments, geographic considerations, and

user segmentation are just a few factors organizations must consider in deploying a mobile solution; however, best-of-breed providers of services and software typically work with all of the core operating systems and devices in the marketplace today.

Mobile Enterprise Deployments: Challenges for IT

IT organizations face many challenges in the deployment of mobile enterprise solutions, including:

- ☑ **BYOD explosion.** IDC estimates that 55% of all devices being used for business purposes are owned by employees rather than the corporation. CIOs and IT managers no longer have the control to manage the influx of devices into the enterprise. Regardless of policy or steadfast denial, the reality is that this trend is here to stay. The savviest organizations will recognize and embrace this trend and begin to set policies and strategies to leverage the influx of devices to enhance mobility across the organization. The ability to manage applications and devices and enable security at the point of engagement with employees is critical.

- ☑ **"Buy first" frenzy.** Given the growing number of iconic devices entering the market, management can often make device deployment decisions without regard to management, security, application enablement, or user segmentation. The potential for thousands of devices to be purchased and thrust upon an organization puts a tremendous strain on the IT department and corresponding stakeholders (such as LOB) to support, manage, and deploy on devices that may not be best suited for the enterprise or a particular organization. Recognizing and avoiding the potential "buy first" frenzy may enable organizations to seek out the best suppliers and effectively manage mobile application deployment challenges.

- ☑ **Device and OS decisions.** IT organizations and developers alike have finite resources and must make decisions about the number of devices and operating systems they will support. Recent IDC data suggests that 91% of developers will write to three or fewer operating systems and two-thirds of developers will write to only two operating systems. Given the dizzying number of devices and the rapid speed of innovation in the smartphone market, decisions on which and how many operating systems to support are critical. As discussed, many factors impact this decision, including user segmentation, application deployment, security, management, development resources, and, of course, end-user requirements.

- ☑ **Application enablement technology choices.** IT organizations must make hard decisions regarding key technology approaches for both the back end and the front end of mobile enterprise solutions. It is critical to understand and incorporate end-user needs in this decision because increasingly mobile applications go beyond a company's employee base (B2E) and into its partners (B2B) and customers (B2C). The decision to deploy in the cloud and on-premise, or a mix of both, is also important. Many companies still prefer on-premise for security or personalization concerns, but a growing number of customers are seeking cloud-based deployments because of their lower up-front cost and faster implementation. Further, the decision to build device-native apps (designed for a specific OS), HTML5-based mobile Web apps (which can run on multiple operating systems), or a hybrid is vital; however, it is not an either-or scenario.

Often an HTML5 Web app may be developed to augment an existing device native app to expand the availability of the app to more users. In addition, the use of a hybrid application may prepare an organization for transitioning to a full HTML5 app as this technology matures.

☑ **Security threats.** The pervasive use of a wide variety of mobile devices that often contain or transmit sensitive corporate information combined with the use of a new breed of applications that may include geolocation or voice-activated search features makes mobile devices a significant potential security threat. Successfully securing devices from all types of threats is also a major challenge for IT.

Mobile Enterprise Deployments: Challenges for End Users

The push and pull between end-user needs and wants and IT requirements is reaching a high point. With a large number of device and application choices entering the market and the adoption of BYOD policies, the end user is more important than ever to determining mobile technology paths within an enterprise. Key end-user challenges are as follows:

☑ **Usability.** Given the tremendous number of applications and devices entering the mobile enterprise market, the usability of consumer apps has seen an incredible jump. Today, end users are faced with sometimes less than stellar, stodgy business apps for mobile that don't offer the great experiences provided by their personal applications. For applications to meet user expectations, and hence be effectively adopted, it is important for companies to work with end users to ensure a more productive environment and an experience equal to that provided by consumer-oriented apps. In the same light, security and management begins to come to the forefront, potentially slowing or even severely hampering performance with complex passwords and access procedures. IT must balance security and management requirements with end-user needs to achieve a productive flow and strong design.

☑ **Discoverability and deployment.** In the past five years, an application explosion has created fantastic new experiences for end users. However, the volume of applications is beginning to choke users with an overwhelming array of choices. The mobile enterprise may compound this issue by offering a mix of productivity and corporate applications available in vast app stores on an already cluttered phone. However, if managed well, mobile enterprise app stores vastly improve this experience by allowing a single point for end users to find what they need as a particular employee of a company, knowing updates and additions to their work apps are all in a single location. Such a private app store is one of the few IT/end-user win-wins where IT gets more control, management, and security and end users receive an improved experience.

☑ **Device choice.** With the majority of smartphones now being owned by the employee rather than the organization, the onus moves to the employee to wade through the large volumes of smartphones and balance attributes such as fashion versus functionality. In addition, with the end user being the primary acquirer of the device, retail mobile operator stores become the typical channel

for purchase. End users may not be equipped to understand which devices are best used for their organization or their particular job function or business process, and retail outlets too must step up their ability to address this new customer base with the power of the consumer and the work requirements of an organization. Organizations, OEMs, and mobile operators must keep this in mind when providing solutions for this newly empowered end user.

IBM Mobile Enterprise Strategy

IBM has organized itself across three customer needs categories to deliver comprehensive mobile enterprise software and services:

☑ **Build & Connect** enables the development of mobile applications and multichannel sites, allowing customers to connect to and run back-end systems in support of mobile. Build & Connect allows organizations to develop, integrate, and manage mobile applications across multiple platforms, technology types, and end-user segmentations in the cloud. IBM Worklight and IBM WebSphere Cast Iron are the core offerings for Build & Connect. IBM's recent acquisition of Tealeaf provides analytic technology that allows developers to test applications during the development stage to ensure an efficient application development process, quality applications, and high end-user satisfaction.

☑ **Manage & Secure** controls and protects mobile devices and applications and addresses broader mobile governance. Manage & Secure includes comprehensive management and security components that span mobile devices but also work with a wider set of client devices (desktops and laptops) as well as servers and nontraditional endpoints (e.g., autos, vending machines). IBM Endpoint Manager for Mobile Devices for mobile visibility, security, and management and IBM Security Access Manager to authenticate and authorize mobile users and devices represent the key offerings for this segment. On the services side, IBM seeks to utilize managed services for complete mobile landscape management.

☑ **Extend & Transform** extends existing business capabilities to mobile devices and transforms the business by creating new opportunities. It allows organizations to build upon the core mobile enablement and add key mobile social collaboration technologies and enable mobile browser themes to any multichannel site, significantly enhancing the on-device experience. Core software components include IBM's mobile solutions for social business, such as IBM Exceptional Web Experience solutions and IBM Mobile Connect for VPN security. IBM Worklight within Extend & Transform also provides mobile enterprise management and security functions as part of its platform offering. IBM services offerings provide organizations with mobile deployment services driven by each customer's unique needs and goals.

FUTURE OUTLOOK

Today's BYOD and consumerization trends continue as the norm as we look forward to the future. IDC's most recent research on the business use of smartphones suggests that 55% of all devices are owned by employees rather than the business. As organizations continue to investigate and deploy mobile solutions, they will recognize the need to make mobile not a separate entity or an additional planning item but an embedded use case that requires proper integration across back-end technologies, policies, and end-user work trends.

In addition, smartphones and tablets are just the beginning. Increasingly, a larger number of mobile technologies and apps will be embedded into consumer-oriented and business-specific nontraditional IT devices that will work their way into organizations and begin to interoperate across mission-critical business functions. The need to deploy, manage, control, and secure mobile applications and devices and create a layer of services required to support them will come to fruition. The mobile platforms, applications, management, security, and services delivered around these technologies are the important building blocks of today that will provide an important, scalable foundation for future technology deployments.

CHALLENGES/OPPORTUNITIES

Mobile enterprise deployments are complex, constantly moving environments that require multiple pieces to come together to be successful. Organizations face the challenges of working across multiple facets of their business to address key issues such as the BYOD wave, the technology conundrum of ever-developing new technologies on top of existing offerings, and growing management and security requirements. Multiple pressures are impacting IT organizations as they simultaneously try to satisfy end users' never-ending quest for more and often multiple devices and have enhanced consumer-like end-user experiences. IT organizations are also tested by management to roll out particular devices that raise the bar of manageability and control and keep pace with competitors that may be gaining competitive advantage by rolling out new advanced mobile applications.

CONCLUSION

Given the complexities of the mobile enterprise, it is critical for organizations to think comprehensively in their mobile view. Although typical deployments may begin with a very tactical plan (such as "We need to mobilize 200 salespeople"), it is vital for organizations to think bigger and address long-term needs from technological, cultural, and policy/compliance perspectives. A consultative strategy as a starting point is important to set longer-term goals and to incorporate all enabling technologies, including both the back end and the end-user side, that will ultimately be scalable, secure, and offer the required level of control. Recognizing key trends that put pressure on IT organizations and challenge mobile application developers to enhance the end-user experience is crucial.

Although many best-of-breed solutions exist across multiple parts of these offerings, it is important to consider leveraging a single provider that can address many of these

components in-house and partner for best-of-breed technologies. Consultation, implementation, technology development, and support are the key stages along the way. A single provider or a tightly coupled set of partners can go a long way in delivering integrated, scalable solutions that can grow as your technology and end-user needs increase.

Copyright Notice