IDC TECHNOLOGY SPOTLIGHT

Securing Productivity in the Borderless Enterprise

January 2016

Adapted from *Worldwide Enterprise Mobility Management Software Forecast, 2015–2019* by Stacy Crook, IDC #257408

Sponsored by Microsoft

As companies increasingly look to transform their businesses with mobility, they need to consider the core management and security infrastructure that will enable these services. This Technology Spotlight examines the important role played by enterprise mobility management (EMM) technology in managing the security challenge posed by the combination of mobile devices and cloud-based software-as-a-service (SaaS) apps. It also explores the role of Microsoft's Enterprise Mobility Suite (EMS) in the strategically important EMM market.

Introduction

For the past several years, organizations around the world have evaluated how key technology trends such as mobile, cloud, social, and big data positively impact business operations and revenue. Throughout enterprise computing history, IT professionals have held primary responsibility for choosing whether to proactively engage with technology trends. However, the pervasive consumerization of IT has moved more of this decision-making power into the hands of the end user. This shift has forever altered the dynamics between users and IT, but savvy organizations will see it as an opportunity to capitalize on the benefits these transformational technologies offer.

It is no secret that mobile device use in business settings is rising. According to IDC's latest business use smartphone study, 30% of total worldwide smartphones shipped in 2015 were used for business. Astoundingly, 74% were personally owned. Bring your own (BYO) devices represent a mix of operating system (OS) types; in addition, new form factors such as wearables are entering the enterprise environment, creating an increasingly heterogeneous endpoint environment for IT to manage. However, managing the device is just the tip of the iceberg because BYO devices typically contain both corporate-provided applications and personally owned applications. Given the dual nature of these devices, employees often leverage personal apps such as cloud storage for mobile access to work documents. This trend, often referred to as "shadow IT," poses a major security risk because IT has little visibility into what corporate data may end up in these third-party public cloud environments. To stay competitive, companies need to empower their end users with mobile technology while avoiding the potential compliance risks these devices and usage paradigms introduce.

EMM technology is an increasingly critical tool in managing the security risk associated with the combination of mobile devices and the cloud.

Definitions

Enterprise mobility management is a software technology designed to manage and secure mobile devices, applications, and content. As a marketplace, EMM includes the submarkets of mobile device management (MDM), mobile application management (MAM), and mobile content management (MCM). Each of these submarkets is a combination of management and security technologies optimized for mobility.

Mobile device management solutions include many of the standard features found in PC management solutions as well as additional functionality that addresses the unique needs of mobile devices. Some key features of a MDM solution are:

- Device provisioning and management configuration settings
- Inventory/asset management
- Remote wipe/lock
- Remote control for systems diagnostics
- Policy/compliance management (encryption management, device posture, etc.)
- Authentication and certificate management
- Real-time device monitoring, location information, GPS tracking
- Reporting and analytics on devices

Mobile application management refers to a solution by which specific mobile applications can be managed, secured, and distributed by IT organizations. These solutions typically allow for enhanced policies to be applied to individual applications or a grouping of apps. MAM solutions either supplement MDM functionality or function as standalone offerings. Common functionality within MAM includes enterprise app storefronts, single sign-on, containers, and app wrapping.

Mobile content management solutions for the enterprise allow IT to provide mobile devices with secure access to files/content/data sitting in various data stores. Such solutions may also provide mechanisms to securely collaborate on this content. These products allow IT to manage who gets access to what information and may tie in with other back-end or mobile-specific policy systems, including identity and rights management systems. Preventing data loss is a key goal of these products, and they do so by providing IT with a mechanism to control data flow in and out of the secured app, as well as secure communication between apps. These solutions assist with compliance and governance by offering reporting on user activity with mobile content. MCM solutions are either cloud based or on-premises based and may also provide access to content that is in the cloud or behind the firewall.

Mobile identity and access management (MIAM) technology is often present in EMM suites in various forms. MIAM solutions provide authentication and authorization technologies (such as PKI certificates, SSL certificates, and password management) for transactions conducted from mobile devices and that support network access for mobile devices. Single sign-on and provisioning of mobile devices are included.

Benefits

The adoption of EMM technology has broad-reaching benefits for IT, the business, and end users.

The combination of cloud and mobile devices creates new security and management challenges for enterprise IT operations and security teams. In the past, IT issued and owned the majority of enterprise client computing devices; how the company managed and secured those assets was of no concern to employees.

Today, employees have their own devices with their own applications, and they want to use them for work. Each enterprise must make decisions about whether it allows a bring your own device (BYOD) policy, and if it does, which devices are acceptable. However, the majority of organizations have mobile devices connecting to their infrastructure, and these devices are connecting to the cloud. The real challenge for IT organizations is how to enable secure collaboration and protect information whether they control the device or the applications. It's a tricky issue — and one that EMM can help address.

EMM is most often offered in a suite, where companies can turn on the functionality as needed. Depending on corporate culture or security attitude, a company may fully manage all devices or fully manage the devices of certain people or use cases (such as a kiosk) and manage only the applications and data of another set of users. EMM's modular nature allows it to serve a variety of use cases. Across usage paradigms, EMM provides a number of key benefits for IT:

- Cross-platform provisioning, configuration of devices and/or users
- Integration with identity systems to help ensure that only authorized users get access to data
- Conditional access policies to ensure that only compliant devices access the corporate network
- Enterprise app stores that allow mobile applications to deploy in a more secure, streamlined manner
- Granular policies around applications to provide security for data at rest, within workflows, or over wireless networks
- Enhanced browsers to provide secure Web interactions
- Integration points with other security products for deeper threat prevention

Today, businesses operate in a fiercely competitive environment. To help businesses maintain competitive positioning, teams need to be able to collaborate in real time from any place. They also need assurance that they have the most current information and content in client-facing interactions. Given the sensitive nature of the content shared among teams inside and outside the enterprise, security must underlie each of these exchanges. Examples of how EMM enhances business operations include:

- Content is the lifeblood of sales and marketing, but it may also be some of a company's most sensitive information. By creating policies around content, EMM allows organizations to share content internally without the worry that it will end up somewhere it shouldn't.
- Enterprise application stores allow companies to manage mobile applications over their life cycle and ensure that only authorized employees have access to an application. Lines of business can also leverage these app stores for version control and ensure that employees are always accessing the latest versions of the app with the most up-to-date customer information and content.

EMM also benefits the end user. In fact, end users are arguably the most important constituent because their acceptance of the solution will contribute to its success or its failure. Mobile solutions have to enhance the user experience, not hinder it. This can be a tall order because security

solutions typically require additional steps to access information. However, EMM enhances the end-user experience in several ways:

- Enterprise app stores offer a single place to find all provisioned corporate apps
- Simplified mobile workflow via single sign-on and inter-app communications
- Corporate apps and data may be managed by companies on a user's device, reducing the risk that personal data may be seen or interfered with

Trends

Most enterprises have mobile devices connecting to their network — whether they realize it or not — and could benefit from EMM. However, given the trend toward OS convergence, using a form factor alone to identify a mobile device is quickly becoming insufficient. IDC believes OS vendors will seek to simplify experiences for the development community, the enterprise, and end users by running a single OS across all form factors.

The changing usage paradigms are also important to discuss. In addition to mobile employees, companies are supplementing their workforce via contract workers. Companies need to enable these worker types with access to the data they need for their jobs but be cautious of privacy concerns. IT also needs an easy way to revoke access when such employees are no longer under contract.

One of the most interesting outcomes of consumerization is in the area of user experience. Before this phenomenon hit, corporate applications were utilitarian, and mobile applications were no exception to this rule. As people have become used to the slick experiences offered by consumer apps, they now hold enterprise apps to the same standard. Interacting with a mobile business app might never be as fun as interacting with a mobile gaming app, but companies can improve the user experience of their applications. While most people primarily associate identity with security, this functionality can play a key role in enhancing these experiences. By tying policies to identity instead of a device, IT can offer users a continuous experience as they switch devices throughout the day. Because most users interact with a variety of application types on a daily basis, IT should also seek solutions that allow for single sign-on. Leveraging identity to streamline workflows for the end user can boost productivity and overall satisfaction.

IDC's annual enterprise mobility survey finds mobile applications related to productivity score highest in user adoption year after year. However, the collaboration experience on mobile devices has historically left something to be desired. This can largely be attributed to email applications that didn't live up to the native experience and the disjointed inter-app workflows necessary to share, save, and edit files. Despite these issues, IDC sees a sharpened focus on usability characteristics for secure productivity applications and believes these are worth investigating. Data protection must also be a core consideration for mobile productivity applications given the sensitivity of the data exchanged through these apps. If an organization doesn't invest the time to find a user-friendly suite of mobile productivity apps, it is all too easy for mobile employees to find insecure workarounds.

Considering Microsoft

Microsoft's key offering in the EMM software market is the Enterprise Mobility Suite (EMS). The suite includes four key components that provide an integrated set of access management, data protection, and management capabilities for mobile devices, apps, and content. Today, EMS includes the following four main components, which are constantly being refined according to customer need:

- **Microsoft Intune,** a cloud-based cross-platform device and application management solution
- **Azure Active Directory (AD) Premium,** Microsoft's flagship identity-as-a-service offering that provides identity services and secure access for applications running on-premises as well as over 2,500 cloud applications

- **Azure Rights Management,** which offers encryption, identity, and authorization policies designed to secure corporate files and email across phones, tablets, and PCs
- **Microsoft Advanced Threat Analytics,** which leverages analytics technology to identify suspect behavior with the goal of detecting and preventing data breaches

Microsoft's EMS is a relatively new offering that builds upon the company's strengths in the foundational markets of endpoint management (ConfigMgr), productivity (Office Suite), and security (Active Directory). Despite these strengths in traditional desktop computing, Microsoft recognized the need to enhance its portfolio with offerings to meet the needs of next-generation cloud and mobile computing environments. The first step in this journey was to introduce Microsoft Intune, a cloud-based solution that enables IT administrators to manage cross-platform mobile devices and applications individually or in combination. An important aspect of Intune application management is the integration with Office mobile apps. This integration allows for a deeper, more granular level of policy management for these applications than that offered by a third-party EMM solution. In addition, the company has recently added the ability for customers to manage Office apps without enrolling the devices in Intune MDM. This is a useful feature for companies with large BYOD or extended enterprise populations that may not want or legally be able to manage the full device. Related to this ability to provide secured workflows within Office apps is Azure Rights Management, which encrypts files and email and tracks documents according to IT policy.

Because an information protection solution such as Azure Rights Management grants access to information based on specific user attributes, it is important for the software to be closely integrated with the identity system. Azure Active Directory Premium provides identity and access management across on-premises applications and a broad swath of cloud-based applications. In addition to providing identity for internal employees, Azure AD provides federated identity for external parties, such as business partners, and time-bound access to data. This is an important feature because employees need to collaborate and share sensitive data with third parties but may not want them to access this data forever. Azure Rights Management protection also travels with the data, whether it is saved in a mobile app or a back-end server (on-premises or in the cloud). Microsoft recently added threat analytics to the suite in the form of the Advanced Threat Analytics solution. These capabilities provide IT with security and visibility into the path of corporate data; they also provide end users with streamlined workflows across the applications they access daily on their mobile device.

While EMS serves as an effective standalone EMM solution, Microsoft's other mobility-related technologies can play a complementary role in enabling enterprise mobility rollouts. One of the most powerful is the integration between ConfigMgr and Intune to enable unified endpoint management — the ability to manage all endpoint devices through a single console. Another example of such synergies is the ability to manage and deploy Windows 10 devices in a simplified manner. With ConfigMgr and Intune, customers can manage devices with either a traditional PC agent or an MDM agent (cloud, hybrid, or on-premises) and also have multiple options to deploy Windows 10 (upgrade, wipe and load, provisioning, Azure AD join). Microsoft also offers various deployment options based on whether the device is company owned or employee owned. The majority of business use applications are Windows based and may never be rewritten in a mobile optimized format. Azure RemoteApp fills this gap by providing remote access to Windows-based applications on mobile devices.

Challenges

One challenge that Microsoft has had to overcome in the EMM market is the perception that its brand is tightly associated with Windows. While it is true that Microsoft might have some inherent advantages in managing its own OS, the company is clear about its commitment to fully support other OS types, and it has reinforced this commitment by providing zero-day support for all major operating systems for the past two years. Aside from supporting other operating systems in its mobile

management console, Microsoft has also developed the full suite of Office mobile apps for these other platforms, which are manageable without enrollment in Intune MDM.

From an organizational perspective, Microsoft and other large vendors with a footprint in the traditional desktop software market have to adapt their engineering practices to keep up with the fast pace of change in the mobility market. Microsoft in particular has experience doing so on the OS/device side of the company, and it is also now producing weekly updates for the EMS suite to support this need. In parallel, the company has to ensure the various engineering teams involved with the EMS suite are in lockstep with each other to create the seamless integration points that drive the customer experience.

Conclusion

A major shift is happening in the IT landscape, and companies that choose to embrace the change have the opportunity to become industry leaders. The combination of cloud and mobility can serve as an especially effective lever in achieving this goal, allowing for greater employee productivity and responsiveness to customer requirements. While adapting to such trends is necessary for competitive advantage and growth, it also introduces new risks into the enterprise computing environment.

When evaluating solutions to help manage these risks, organizations should consider how well an offering meets the needs of IT, the business, and end users. Security is of the utmost importance, but if this functionality negatively impacts user experience, employees will find other, less secure ways to get work done on their mobile devices. Thus, it is crucial for potential buyers to understand how an EMM solution supports the tenuous balance between risk mitigation and end-user productivity.

Aside from the pure functionality of an EMM solution, companies need to consider how the offering fits into the broader IT infrastructure strategy. While a few companies have the luxury of adding employees to support enterprise mobility rollouts, this task often falls to the current IT staff. Therefore, organizations should consider not only how well a potential EMM system integrates into the existing infrastructure from a technical point of view but also how well it complements the IT administrator's existing workflows and workload. Solutions that can be consumed through the cloud but allow the IT administrator to leverage current consoles and maintain established processes can be helpful in this regard.
