SOLUTION BRIEF:
5 MUST-HAVES FOR AN ENTERPRISE
MOBILITY MANAGEMENT (EMM) SOLUTION

5 Must-Haves for an Enterprise Mobility Management (EMM) Solution

Who should read this paper

VPs or Directors of IT Operations, Directors or Managers of Mobile Strategy, Mobile Architects, and Mobile Program Managers

Symantec

Content

The Challenge: Enabling Mobility While Protecting the Enterprise

With the rise of mobile devices in the workplace, businesses face a conundrum. Eager to reap the benefits of mobility, yet justifiably uneasy about the significant risks involved, organizations are struggling to find the right approach. Proven benefits of mobility include happier employees, increased productivity, and greater business agility. Risks include everything from critical data losses to devastating reputation damage. Ready or not, organizations must tackle the issue head-on. The question isn't, should employees be able to use mobile devices for work. Mobile devices are already an inescapable part of the workplace landscape. It's up to IT to both incorporate these devices and manage them within the security of the network. In addition to smartphones, IT must also secure tablets, laptops, portable printers—anything that can connect to your network. The horse is out of the gate so to speak. Now, businesses must get ahead of the curve to take advantage of what mobility offers while ensuring security, privacy, and control for the enterprise.

IT Has Their Work Cut Out For Them

With the mobility trend in full swing, most organizations today are already vulnerable to potential security risks. The security basics of yesterday—policy, encryption, and authentication—no longer cover fundamental security needs. Businesses must act quickly to get the most from mobility while effectively protecting information and systems. IT organizations across the board are working to:

Mobilize business processes and the workforce. Today's employees want flexibility. They want to be able to choose how to do their jobs better on their terms. This includes using the most convenient device to get work done. People rely on multiple devices today—including tablets, smartphones, and laptops—to do work and manage tasks outside of traditional office hours. When employers do not give their employees a way to do this, employees find their own ways. The idea is to leverage the mobility trend for your benefit by making sure employees can be as productive as possible with their devices and apps. A workforce with relevant and secure mobile apps, either custom-developed or commercially off-the-shelf, can streamline business processes, enhance productivity, and improve customer service.

Protect corporate data and apps on mobile devices. When smartphones and tablets began emerging a few years ago, organizations scrambled to manage the devices themselves. As more and more employees opted to use their *own* devices to get work done, companies began to realize that it wasn't the devices they needed to secure as much as the *information* on those devices. To protect corporate data from mobility-related risks, IT must effectively stop or control the following:

- Employees adopting unapproved mobile/cloud apps for work;
- Corporate data leaks into unmanaged mobile/cloud apps;
- Attackers targeting mobile devices with malware; and
- Unauthorized access to corporate data.

Enable BYOD and/or CYOD Programs. BYOD is all about allowing employees to leverage the devices they already own and know how to use to do their work. When mobile devices first appeared in the workplace, some companies made the mistake of encroaching on user privacy by enforcing control at the device level (versus the app or data level). Due to liability concerns such as this as well as added overhead, IT should not be in the business of managing personal devices and/or apps. Instead, the focus must be on securing the corporate data on those devices, in addition to mobile platforms. CYOD, or Choose Your Own Device, is an option whereby organizations can give their employees a choice of devices to use at work. This strategy often goes hand in hand with a "corporate-owned personally enabled" (COPE) policy model, where the employee is allowed to use the device for personal activities even though the device remains the property of the business. Essentially, organizations are coming to the realization that the device is not the ONLY issue. It is just one piece of the puzzle.

Alphabet Soup

When first looking into managing mobility, it can be overwhelming. The acronyms alone are daunting. There's MDM (mobile device management), MAM (mobile application management), and MCM (mobile content management). For a time, there was debate over whether MDM or MAM was the best way to manage enterprise mobility, but it's clear now that that was the wrong question. Device management alone (MDM) isn't enough because while controlling devices is important, you also have to manage employees' use of apps and data. Application management (MAM) focuses on controlling apps and the data those apps access or store. Policies are applied to the apps versus the device. MCM focuses on providing mobile access to enterprise content repositories such as Sharepoint, Documentum, or Network File Shares in a secure and managed way. In truth, the best strategies encompass all of these approaches.

The Solution: Enterprise Mobility Management (EMM)

There's no one right way to manage mobility. In general, companies are moving away from point solutions to platforms that address the need for management and security across devices, applications, and data. An Enterprise mobility management (EMM) solution should give customers the flexibility to implement controls at the device or app/content level based on the corporate strategy for mobility. For example, a company may choose to use MDM on company-issued devices, and MAM on personal devices. Leading-edge EMM solutions offer comprehensive policy and configuration management tools, giving organizations the ability to implement consistent controls across diverse mobile platforms by using a combination of device and app policies.

When searching for an EMM solution, keep the following five must-haves in mind:

1. Device management (MDM)— Perhaps the most valuable feature of MDM is that it allows IT to remotely shut down a device when it's lost or stolen. The best EMM suites will offer MDM. They will also offer remote device reset; over-the-air hardware, software, and network inventory capabilities; and mobile software management, including app delivery. They should offer support for a variety of mobile operating systems, ensuring access by a greater variety of devices. Companies should select an EMM solution that has broad platform coverage. This gives them the ability to provide device choice and allows them to manage multiple mobile initiatives from a single solution, for example, operational devices for retail or warehouses, as well as BYOD.

2. App management (or App Policies and App Store)— App distribution—getting the app on the device—can be done via MDM or MAM. Once distributed, the apps don't have to be managed by any type of policy. App management is about applying policies to individual apps so that you don't have to control the device, as in the case of personal devices for partners or contractors. Approaches include Software Development Kit (SDK) allowing developers to pre-integrate features such as user authentication, compromised device detection, data loss prevention policies, certificates, branding, over-the-air app configurations, and app tunneling. Policies might include authentication requirements, copy/paste restrictions, content sharing restrictions (blocking AirDrop on a per-app basis or only allowing files to be opened by specific apps), or not allowing local data storage.

App wrapping is another way to give existing internal applications an extra level of security and management capabilities without further development or code change. Administrators can quickly and easily wrap applications from the admin console, in full confidence that their applications are secure.

Finally, an enterprise app store can improve mobile worker productivity by giving employees easy access to the apps they need, as a part of MDM. The app store should be easy to use, enabling self-service distribution of apps to employees and other authorized users with roles-based corporate security and data protection. In addition, it should secure corporate data on mobile devices, regardless of ownership, and be part of a unified platform that enables user productivity while protecting enterprise data.

3. Threat protection—Enterprise-grade mobile app security should protect valuable intellectual property. Antivirus/anti-malware protects the mobile operating system and files system from traditional virus or malware threats, in addition to new threats such as risky apps, for example apps that "steal" data from other apps by collecting contacts, or apps that require high data and battery usage.

An EMM solution should allow IT to centrally manage mobile threat protection and leverage app risk data by implementing policies, for example, the ability to blacklist apps based on certain risk characteristics, for example, an app that has high data usage. Central management includes things like distributing a mobile security app to devices, running remote scans of the device, viewing threats, and setting compliance policies based on the device's security posture (for example, the ability to block email access if malware is found; block email if virus definitions are not current; or block access to corporate apps if no mobile security app can be found on the device).

Mobile threat protection defends both users and the enterprise against malware, greyware, privacy risks, performance risks, fraudulent websites, and other digital threats. The best solutions apply real-world information on actual behaviors to protect privacy, detect malware, and mitigate performance risks such as battery drain. Mobile threat protection can be centrally managed through an EMM console where administrators can set threat compliance requirements and remediation.

4. *Access and authentication controls* — Access and authentication controls manage access by requiring successful recognition of a policy-defined password, pattern swipe, biometric scan, voice, or facial recognition. The best EMM suites allow IT to group users—by department, for example—and grant access only to the resources a specific group needs. The capability allows you to define what users can do on the network with specific devices and under what circumstances. And, it manages mobile access to corporate systems. A strong EMM solution should offer authentication with time-saving features such as single sign-on, whereby employees can use the same credentials to log into a laptop and other corporate systems. Single sign-on also makes it easy for a user to move from app to app without re-authenticating every time an app is opened. The idea is that once users have authenticated themselves to an app, that app is able to "pass" credentials to another app.

5. Content management—MCM allows users to access content from mobile devices in a secure and managed way. This includes email attachments, content pushed by an admin, and content accessed from back-end content repositories, such as Sharepoint, Documentum, or Network File Shares. You must be able to provide access to secure corporate content from anywhere. An EMM solution should give employees a secure way to access files, view mobile documents, and collaborate on corporate content. Content management also includes data loss prevention. The best solutions will offer encrypted on-device data storage, authentication options, policy-defined cut-and-paste controls (to prevent data leakage), and/or change to open-in controls to prevent content from being opened/accessed by non-approved apps. For content push, an EMM solution should be able to control document versions, alert users of new files, and remove content once it's expired.

Conclusion

The mobility trend can be daunting because the stakes are high. It's imperative you protect sensitive corporate and customer data, yet also take advantage of the significant agility that is possible. The fact is, you can securely enable a mobile workforce. You can protect corporate information in addition to devices. And you can have one solution that effectively manages devices, apps, and data. Look for a holistic solution that allows you to implement consistent controls across diverse platforms. Choose a vendor you can grow with, one that is likely heading toward a platform approach that offers partners and customers APIs on the back end to hook into existing back-end architecture and on the front end to build management and security into apps[1]. Fortunately, with a comprehensive strategy and the right solutions, it is possible to increase productivity without sacrificing security, resulting in a more secure mobile enterprise.

[1]- IDC EMM Forecast 2013

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data-intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of $6.9 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com