White Paper

BYOD 2.0: Moving Beyond MDM

BYOD has quickly transformed IT, offering a revolutionary way to support the mobile workforce. The first wave of BYOD featured MDM solutions that controlled the entire device. In the next wave, BYOD 2.0, control applies only to those apps necessary for business, enforcing corporate policy while maintaining personal privacy. The F5 Mobile App Manager is a complete mobile application management platform built for BYOD 2.0.

by Peter Silva
Technical Marketing Manager

Contents

Introduction

You might refer to it by many names: bring your own danger, bring your own disaster, bring your own detonator, or what most people call it, bring your own device (BYOD). What used to be inconceivable—using one's own personal mobile device or smartphone for work—is now one of the hottest trends. The idea of using a personal smartphone at work sprouted when many executives got their first iPhones back in 2007 and wanted access to corporate resources. Since then, BYOD has transitioned from a fad to a major transformation of enterprise IT. As a result, the contract between IT organizations and employees has shifted from one of corporate provisioned and managed laptops and Blackberries to one where workers are free to bring the device of their choice (i.e, laptops, smartphones, and tablets). These personally owned devices are typically used for a mix of both business and personal applications.

As more smartphones, tablets, and other types of mobile devices make their way into employees' hands, requests for corporate access from those devices are increasing, which represents a huge challenge for IT departments. Not only has IT lost the ability to fully control and manage these devices, but employees are now demanding that they be able to conduct company business from multiple personal devices. Initially resistant to the idea due to security concerns, IT teams are slowly adopting the concept, but hesitantly, still concerned about the inherent risks of allowing personal devices to access and store sensitive corporate information.

Mobile devices are a double-edged sword for enterprises. CRN reported on a Poneman Institute/Websense survey[1] finding that 77 percent of responding business professionals said that the use of mobile devices in the workplace is important to achieving business objectives, but almost the same percentage—76 percent—believe that these tools introduce a serious set of risks. While organizations understand the risks, the survey showed that only 39 percent have security controls in place to mitigate those risks. As a result, 59 percent of respondents said they've seen a jump in malware infections over the past 12 months due specifically to unsecured mobile devices, including laptops, smartphones, and tablets. It's clear that there is a significant business risk with BYOD, and it's not going away.

1 CRN.com, March 8, 2012

BYOD Drivers

In 2013, the mobile workforce is expected to increase to 1.2 billion[2]—a figure that will represent about 35 percent of the worldwide workforce—and many of those workers will be using their own devices.

People have become very attached to their mobile devices. They customize them, surf the web, play games, watch movies, shop, and often simply manage life with these always-connected devices. Those organizations that have implemented BYOD programs are reporting increased productivity and employee satisfaction at work. The 2012 Mobile Workforce Report from enterprise WiFi access firm iPass[3] found that many employees are working up to 20 additional hours per week, unpaid, as a result of their company's BYOD policies. Nonetheless, 92 percent of mobile workers said they "enjoy their job flexibility" and are "content" with working longer hours. In addition, 42 percent would like "even greater flexibility for their working practices." Organizations have been able to reduce some of their overall mobile expenses simply by not having a capital expenditure for mobile devices and avoiding the monthly service that come with each device. In addition, in some cases, BYOD implementations can brand the IT organization as innovators.

The flipside of the convenience and flexibility of BYOD are the many concerns about the risks introduced to the corporate infrastructure when allowing unmanaged and potentially unsecured personal devices access to sensitive, proprietary information. Applying security across different devices from a multiple number of vendors and running different platforms is becoming increasingly difficult. Organizations need dynamic policy enforcement to govern the way they now lock down data and applications. As with laptops, if an employee logs in to the corporate data center from a compromised mobile device harbouring rootkits, keyloggers, or other forms of malware, then that employee becomes as much of a risk as a hacker with direct access to the corporate data center.

Mobile IT is a major transformation for IT departments that is deeply affecting every major industry vertical, and the effects will continue for years to come.

Enter BYOD 1.0.

2 International Data Corporation (IDC), Worldwide Mobile Enterprise Management Software 2012-2016 Forecast and Analysis and 2011 Vendor Shares, Sept. 2012

3 ComputerworldUK, "BYOD Makes Employees Work Extra 20 Hours Unpaid," August 22, 2012

BYOD 1.0 (2009-2012)

BYOD 1.0 is the industry's first attempt at solving problems related to personally owned devices in the workplace. BYOD 1.0 consists of two primary components—mobile device management (MDM) and device-level, layer 3 VPNs. The primary aim of MDM is to manage and secure the endpoint device itself, including varying amounts of protection for data at rest on the device (which is typically limited to enabling native device encryption via configuration). The primary aim of the layer 3 VPN is to connect the device back into the corporate network, providing data-in-transit security for corporate traffic.

Both of these BYOD 1.0 components have a drawback—they are umbrellas that protect and manage the entire device, rather than zeroing in on just the enterprise data and applications on that device. Since these are usually dual-purpose (work/personal) devices, this device-wide approach causes issues for both workers and for IT.

Employees don't like that BYOD 1.0 imposes enterprise controls over their personal devices, applications, and information. One of the most commonly cited examples is that of the employee who leaves a company and has his device wiped by the organization, losing photos of his family along with the enterprise data and applications. People are also concerned with the privacy of their personal data under a BYOD 1.0 scheme.

From an IT perspective, organizations agree—they don't want to have to concern themselves with personal data or applications. As soon as they manage the entire device or simply connect that device to the corporate network via VPN, that personal traffic also becomes an IT problem.

While BYOD 1.0 helps to enable the use of personally owned devices in the enterprise, the device-level approach certainly has its drawbacks. BYOD 2.0 seeks to solve these shortcomings.

The shift from BYOD 1.0 to BYOD 2.0 builds on many of the concepts developed during BYOD 1.0, adding a new set of frameworks that enable IT organizations to wrap enterprise applications in a security layer.

BYOD 2.0 (2013-)

Throughout BYOD 1.0, F5 has provided connectivity for mobile devices into enterprise networks with VPN functionality, most commonly through iOS and Android versions of the F5® BIG-IP® Edge Client®. This layer provides management capabilities as well as functionality such as authentication and authorization, data-at-rest security, and data-in-transit security, among others.

BYOD 2.0 builds on the BYOD 1.0 foundation but makes a substantial shift from a device-level focus to an application-level focus. BYOD 2.0 seeks to ensure that the enterprise footprint on a personally owned device is limited to the enterprise data and applications and nothing more. This means that mobile device management is supplanted by mobile application management (MAM), and device-level VPNs are replaced by application-specific VPNs. These application-specific VPNs include technology such as BIG-IP APM AppTunnels, a single secure, encrypted connection to a specific service such as Microsoft Exchange.

The BIG-IP Edge Client application from F5 Networks secures and accelerates mobile device access to enterprise networks and applications using SSL VPN and optimization technologies. Access is provided as part of an enterprise deployment of BIG-IP® Access Policy Manager® (APM) and Edge Gateway SSL-VPN solutions.

With this approach, workers are happier than with BYOD 1.0 because the enterprise manages and sees only the enterprise subset of the overall data and applications on the device, leaving the management of the device itself, and of personal data and applications, to the device's owner. IT staff prefer the BYOD 2.0 approach for the same reasons—it allows them to concern themselves only with the enterprise data and applications they need to secure, manage, and control.

BYOD 2.0 and the aforementioned application wrapping frameworks are changing the dynamic in the mobile space. By combining mobile management functionality and access functionality into a single offering, these wrappers give enterprises a mobile IT solution that extends from data and applications on the endpoint into the cloud and data center.

Different types of environments will require different types of access control mechanisms. The traditional enterprise data center will still accommodate the traditional, VPN gateway appliance approach to controlling access. By contrast, a deployment of applications into an Infrastructure as a Service (IaaS) public cloud, such as the Amazon Elastic Compute Cloud (Amazon EC2), might require a virtual edition of a VPN gateway that sits alongside virtual machines hosting the organization's applications. A Software as a Service (SaaS) application might not require a VPN at all, but it will still require the identity and authorization data that a VPN provides today.

Across an organization with a hybrid deployment of all of these types of back-end environments, the next-generation access offering must provide end-to-end security, from the application instance on the endpoint device all the way to the data center cloud, with a single authentication and seamless personal experience. It must also provide a single pane of glass view for management of the distributed application environment.

Introducing F5 Mobile App Manager

F5® Mobile App Manager (MAM) is a mobile application management and access solution that securely extends the enterprise to personal mobile devices. It manages applications and secures data while satisfying the needs of employees and enterprise IT departments. For IT, it limits the burden associated with securing and controlling personal data and mobile use. For employees, it safely separates personal data and use from corporate oversight. F5 MAM is a complete mobile application management platform offering security, management, and compliance for BYOD deployments. It is a true enterprise device, data, and information management solution that fits the needs of the mobile enterprise better than MDM solutions.

As the proliferation of mobile devices in the enterprise has created new challenges for IT administrators, they must be able to control devices coming into their network, track inventory, monitor for threats and vulnerabilities, and protect corporate information. At the same time, they must simplify the process of provisioning devices for WiFi, VPN, etc., and support configuring access to email, contacts, calendars, and other essential communication tools.

Figure 1: F5 Mobile App Manager

These administrators also need tools in an extremely heterogeneous device environment with platforms as different as Android, iOS, Windows Phone, and others. Unlike existing offerings, F5 MAM includes a suite of business productivity applications and capabilities to separate and secure enterprise mobile applications while providing end-to-end security.

For organizations that still require some device-level control for managed devices, the F5 MAM provides advanced mobile device management, including asset management, location tracking, control over device settings, network configuration, secure policy management, user management (LDAP/AD), remote access (i.e., lock, wipe, and reset), push notifications, and complete device lifecycle management.

Administrators can manage devices globally, by groups or individual devices. Corporate IT can push policy and configuration requirements to company divisions quickly and easily while enforcing compliance. This allows administrators to maintain consistent policies across all the devices in the enterprise.

F5 MAM Workspace

Organizations and employees both want the ability to segregate professional and personal information. F5® MAM Workspace is an innovative solution allowing enterprises to truly create a virtual enterprise workspace on a wide variety of mobile devices. With MAM Workspace, individuals can have separate sectors and associated policies for their personal and enterprise uses of a device. This enables IT to control how employees access key corporate information while ensuring that employees maintain the freedom to take full advantage of their mobile devices.

MAM Workspace delivers an enhanced security framework by providing secured containers in which all enterprise data and information for an employee are stored. The benefit is the ability to support a secure, separate, and customized enterprise workspace that, from a user's perspective, cleanly segments personal and business uses of a device. Secured applications require no special handling by the user and can be installed in the normal way for a given platform. All secure application data is encrypted on disk, including data saved to removable media, if such an action is allowed. The secure MAM Workspace can be protected by a password or PIN that is independent of the device password. IT can also reset a user's MAM Workspace password, lock down a user's MAM Workspace, or wipe the device in the event of a policy violation.

F5 MAM App Wrapper

Organizations can also add their own applications to the secure workspace. MAM makes creating a secure application a simple and quick experience. Organizations have the ability to add any application to the secure, IT-controlled environment. In addition, there is zero need to recompile to create a secure application. F5® MAM App Wrapper scans the existing code in third-party apps, identifies any security vulnerabilities, and injects new proprietary code. This wraps and secures the app for manageability and deployment.

MAM App Wrapper is unique and highly efficient as it eliminates the need for developers to recompile their original code in order to make apps secure for deployment and management via the administrator portal. This process is automatically handled by the MAM App Wrapper when an application is uploaded, with no API or software development kit (SDK) necessary.

F5 MAM Connect

Email is one of the most critical communication tools for organizations and employees alike. No email, no work. Often, organizations will allow corporate email configuration on a personal device, delivering messages directly to the person's default email app on the mobile device. Many organizations will use Exchange ActiveSync (EAS), the push messaging component of Exchange Server that relays messages to mobile devices. EAS is an XML-based protocol that communicates over HTTP or HTTPS and is designed to synchronize email, contacts, calendar, tasks, and notes from a messaging server to a mobile device.

EAS offers some built-in security, like the ability to communicate over SSL and the ability to use certificates or two-factor authentication. It also has some device-specific security features such as remote wipe, password policies, and encryption policies. These deployments, while secure, still reside in the user's personal apps, comingling corporate data with personal data. That means IT becomes responsible for the user's personal email app and the employee has uncontrolled access to corporate information.

F5® MAM Connect is a secure, wrapped personal information manager (PIM) client that integrates with Microsoft Exchange and delivers enterprise email, calendar, contacts, tasks, and notes to the employee. MAM Connect offers EAS synchronization, global address list integration, secure storage, and networking and is fully managed via the MAM management console.

F5 MAM Browser

Many web browsers, including mobile browsers, are configured to provide unfettered functionality to the detriment of security. Browser vulnerabilities are one of the easiest ways to get malicious code running on a smartphone, and many mobile apps are reliant on the mobile device's browser for functionality. Plug-ins and add-ons to support Java, JavaScript, Ajax, and other interactive web enhancements can expand the risk. In addition, tools like tracking cookies can impair a user's privacy, and all these browsers are susceptible to cross-site scripts and other website vulnerabilities. Plus, as with email, corporate web navigation is being handled by the person's personal, default web browser. This is not to mention the IT nightmare of needing to support all of the various mobile browsers residing on employees' smartphones.

Figure 2: MAM Browser

The F5® MAM Browser is a secure and managed browser delivered within MAM. It provides employees with a full-featured browser, separate from their personal browsers, with the control IT needs for secure browser access. It facilitates integrated blocked and safe lists without reliance on proxies, provides controls for enterprise proxy configuration, and allows administrators to push configuration via the web-based MAM portal.

F5 MAM App Store

Most smartphone owners are very familiar with their respective app stores, which enable them to get music, games, apps, and other additional functionality on their smartphones. Tap an icon, find an app, install, enjoy. It should be no different for

enterprise mobile app deployments, but with management and security as top priorities.

The F5® MAM App Store is the enterprise content and application store where IT wraps and secures apps for manageability and deployment. When secure applications are distributed via the MAM App Store client, the system has the ability to filter secure apps from the MAM App Store view depending on the availability of the MAM Workspace on the device.

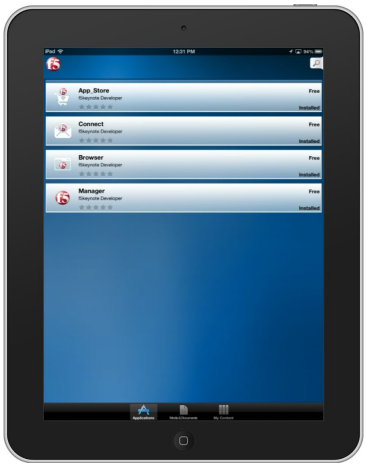

Figure 3: MAM App Store

Small and large enterprises can now ensure that each department, specific team, or role has access to the most up-to-date business applications, documents, and business media available in the MAM App Store. MAM App Store is platform and device agnostic. It can be used to distribute content for x86 (PC, Mac, Linux) and multiple mobile devices across a variety of operating systems (Android, iOS, Windows Phone, etc.). It provides web-based portals for store management and developers, plus client interfaces for user browsing and download, including items for purchase.

MAM App Store offers a full-featured catalog including screen shots, descriptions, recent change history, featured apps, ratings, and reviews. Administrators have the ability to both push and pull apps. MAM App Store is ideal for enterprises and service providers that need to deploy custom applications, impose specific licensing terms on applications, and have complete control over the deployment, update, and revocation of applications on employees' devices.

Conclusion

Whether organizations are prepared or not, BYOD is here, and it is transforming enterprise IT. It can potentially provide organizations a significant cost savings and productivity boost, but it is not without risk. F5 provides strategic control points for mobile applications from the endpoint to the data center and to the cloud, enabling unparalleled security, performance, and agility.

F5 Mobile App Manager helps organizations make the leap to BYOD or transition from controlling the entire device to simply managing corporate applications and data on the device, solving the work/personal dilemma. With F5® MAM, BYOD 2.0 is now a reality.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com