mobile spaces

Comparing Mobile App Security Approaches

The expanding app economy

The new app economy is estimated to consist of 150,000 app developers and companies (Mobilewalla December 2011) that are helping fill commercial app stores with over 1.5 million mobile apps today.

By contrast, the Good Dynamics Developer Network (GDN) provides developers with direct access to the Good Dynamics platform: SDK, servers, resources, and support needed to build, deploy and manage policies for secure mobile. Initially introduced in October 2011, GDN now is hosting the testing and production of over 300 unique, registered apps.

CIOs increasingly leverage mobile apps and BYOD as strategic tools to make each employee a mobile worker, with constant access to business applications and real-time information. However, the use of enterprise apps on employee-owned mobile devices creates new data vulnerabilities for IT security.

In an effort to secure corporate information, enterprise IT are given a confusing array of mobile security approaches, which are promoted by various vendors and are further complicated in the absence of industry standards. Existing IT mobile security and management tools used to secure corporate-owned devices are not inherently designed for the nuances of governing a personal device that contains both proprietary and private data. Legacy data protection approaches like containerization and virtual desktop infrastructure (VDI) force organizations to make tradeoffs that limit user productivity.

To help IT and CIOs sort through the myriad of options available, **this resource organizes solutions into three general categories – container, app wrapping and virtualization – and provides a comparison among them.**

App workflows and BYOD

"We're excited to see technologies that extend policy controls to an entire workflow of apps, so that any app invoked by the corporate app is treated with the same policy, as opposed to wrapping and containing a standalone app. This capability will help preserve user experience and further enable mobilization of enterprise resources. Ultimately, technology innovations in this area may render BYOD a nonissue."
Forrester Research Analyst Chenxi Wang in Computerworld April 2013

Container

Proprietary container solutions manage apps that are provided by the container vendor — typically email, contacts, calendar and browser. They provide strong isolation of enterprise data, but containers are difficult to extend to third party apps. In addition, they require the user to use the container vendor's user interface, instead of the native user experience.

Software containers extend to third party apps with app recompilation, requiring the use of the vendor's SDK. Often, this means that the app vendor must maintain multiple versions of code as well as modify the original code to accommodate the security SDK. This approach limits the number of apps available to the enterprise and precludes the use of the latest software from the app vendor; the app vendor must add another phase to their release process to ready the app for containerization.

App Wrapper

To broaden the set of available apps compatible with containerization, vendors are turning to a new technique called app wrapping. This approach does not require the use of an SDK to reprogram original app code, but instead the vendor patches the app's executable code with security libraries that control how data is stored, shared and transported. This approach introduces license and copyright challenges for the enterprise; public app stores do not typically give the enterprise the right to modify third party executables (e.g. APKs). Because built-in apps cannot be patched either, it is likely that code obfuscation techniques used to troubleshoot the patching process creates more complications than success.

Virtualization

Virtual Desktop Infrastructure (VDI) is another legacy approach to the use of apps for BYOD. Initially designed for laptop use, these systems are the most secure from a data isolation perspective; VDI runs apps in the cloud, storing no data on the device, and only uses the device to render the screen. Usability is problematic, since apps cannot run natively or offline.

Device virtualization offers an alternative to hypervisor technology. Type 1 Hypervisors, or "bare metal" hypervisors, are tightly coupled with the hardware and, in effect, host the OS. While they provide the strongest isolation for natively running apps, they are difficult for mobile device manufacturers to integrate with their entire product line and limit the number of secured devices to a

The Android wildcard

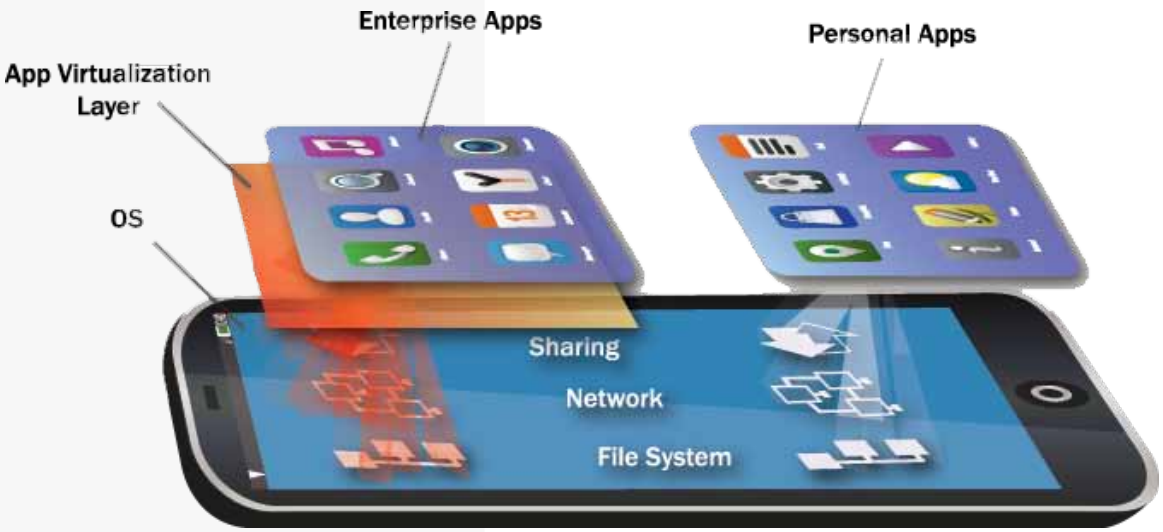
BYOD policies can't be prescriptive on what personal devices employees use for work. Chances are that device will be an Android device but the actual type of Android device will vary greatly. In Q1 of 2013, Kantar Worldpanel ComTech reported that Android finished the three-month period with 51.7 % of smartphone sales. A quick survey of the Verizon Wireless and AT&T Wireless online stores showed that they were each selling over 20 different Android smartphones.

very small set.

Type 2 Hypervisors load inside the OS just like an app and, as a result, negatively impact device performance and battery usage. Devices with this functionality are limited because productization requires kernel integration by the device manufacturer. As a result, hypervisors are poor solutions for BYOD since they cannot provide enterprises with a widespread standard for security and they negatively affect the user experience.

MobileSpaces

MobileSpaces uses app virtualization technology to create a trusted enterprise workspace on employee-owned devices that runs built-in, public app store and custom apps -- all secured and isolated from personal apps. The MobileSpaces workspace downloads as an iOS or Android app and installs a virtual runtime environment that is policy controlled and cloud managed via a browser-based console.



The workspace protects corporate information against leakage and loss by encrypting all data at rest, controlling data sharing between enterprise apps and connecting directly to the enterprise VPN. IT administrators can select any mobile app for workspace use and assign it via policy and without modification, tailoring workspaces per employee role and providing a true native user experience that preserves the way apps are licensed, distributed and updated.

Summary

Enterprise IT solutions that protect proprietary data on an otherwise unmanaged device need to be compared from several perspectives: security, performance, usability, device choice and app choice. The following table contrasts how different approaches to enterprise mobility stack up against one another.

MobileSpaces secures any mobile app for enterprise use, protecting corporate data while also addressing the nuances of BYOD. Unlike container solutions that alter the user experience and require the use of SDKs or app wrapping for security, MobileSpaces uses app virtualization technology to enable the use of any mobile app (built-in, public app store, custom enterprise) for enterprise purposes without software modification. This gives line-of-business managers the widest selection of applications to create new business workflows for their employees.

Technology	Vendors	Security	Performance	Usability	Choice	
					Device	App
App Virtualization	MobileSpaces	●	●	●	●	●
Container	Good Enterproid OpenPeak	●	●	●	●	●
Device Virtualization	VMware Samsung BlackBerry	●	●	●	●	●
VDI	Citrix	●	●	●	●	●
App Wrapping	Mocana Symantec	●	●	●	●	●

Device-specific solutions, such as Samsung KNOX, BlackBerry Balance or VMware Horizon, require functionality to be embedded in device firmware for full IT control. This precludes a fleet-wide standard for mobile security and necessitates IT prescribe which personal mobile devices can be used for work. MobileSpaces leverages application-level security to provide an easily deployed and scalable BYOD solution that overcomes device fragmentation by normalizing all devices to a single IT standard for application security and manageability. With it, your company can choose the apps that it needs to run, on the devices that users want.

VDI is a legacy approach best suited for laptop use. VDI runs apps in the cloud, storing no data on the device and only using the device to render the screen. Usability is problematic, since apps cannot run natively or offline. This approach also significantly limits the apps – built-in or those specifically designed for mobile devices – that could otherwise be used as part of your company's workspace,

App-wrapping technologies limit enterprise app choice too. This technique is largely reserved for the development of custom apps because of potential licensing issues encountered with commercial apps and the preclusion of a device's native apps. There is no standard for wrapping apps, so pre-wrapped apps that are available in the public app store can only be used with the mobility management solution of the vendor that wrapped the app.

MobileSpaces can help your company unlock the full potential of BYOD and the mobile app economy.

Contact us at info@mobilespace.com for more information.

June 2013

About MobileSpaces — www.mobilespaces.com

MobileSpaces helps enterprises secure any mobile app for BYOD, enabling new workflows for business while protecting enterprise data and respecting employee privacy. The company is headquartered in Silver Spring, Maryland, USA with offices in Tel Aviv, Israel.

mobile spaces