Implementing Your BYOD Mobility Strategy

An IT Checklist and Guide
# Content

1. Overview ........................................................................................................................................... 1

2. The BYOD Checklist .......................................................................................................................... 1
   2.1 Application Choice .......................................................................................................................... 1
   2.2 Installation and Configuration ....................................................................................................... 2
   2.3 Device Performance ....................................................................................................................... 2
   2.4 Device & Carrier Agnostic ............................................................................................................ 2
   2.5 Security ............................................................................................................................................ 2
   2.6 Employee Privacy .......................................................................................................................... 3
   2.7 Management Infrastructure .......................................................................................................... 3

3. BYOD Approaches .............................................................................................................................. 3
   3.1 Mobile Device Management (MDM) ............................................................................................. 3
   3.2 Encapsulation .................................................................................................................................. 4
   3.3 Virtualization .................................................................................................................................. 4

4. Divide by Enterpoid ............................................................................................................................. 4
   4.1 The Divide Approach ..................................................................................................................... 5
   4.2 Divide vs. Virtualization ............................................................................................................... 5
   4.3 Divide and Device Management .................................................................................................... 6

5. Conclusion ........................................................................................................................................... 7
1. Overview

Forrester Research reported in July of 2011 that nearly 60 percent of companies allow employees to use personal devices for work. “Bring Your Own Device (BYOD)” policies allow employees maximum choice and flexibility but raise new challenges in maintaining the personal privacy of the user, managing and securing valuable corporate information assets and providing IT with an unpredictable and inconsistent mobile environment. There are also mobile technology considerations. While mobile devices are surpassing PCs and laptops as a user’s primary computing platform, they do have limited access to power, network, and hardware resources. Devising a BYOD solution that will support both personal and business roles requires attention to all of these challenges.

This whitepaper provides a checklist of key BYOD considerations and evaluates how different technologies rate. While all product approaches have value in meeting specific types of business challenges, understanding their strengths and weaknesses with respect to business goals is the best way to ensure success.

2. The BYOD Checklist

When BlackBerry devices first made their appearance in the corporate world they were almost exclusively a corporate liable device model where the company owned not only the mobile device, they owned the cell number, the data, and they were fully managed by IT who dictated what could and could not be done by employees. Back then there was little or no personal apps or usage of the device, and they were only to be used for company business.

Today business IT faces a complex myriad of technology issues and choices as they endeavor to mobilize their entire workforce. BYOD adds yet another dimension as companies work to securely overlay business functions on a wide range of devices, both corporate and employee owned, to ultimately give employees the flexibility to get the resources needed to do their job, anytime and on any device, without compromising user experience or privacy.

This checklist was designed to help IT strategists and architects identify and track key considerations for BYOD mobility, especially when evaluating the many technology approaches to its implementation.

2.1 Application Choice

An important aspect of modern mobile operating systems is its access to a rich selection of applications. Choice in personal applications to support personal life and choice in secure business applications to quickly meet the demands of an ever-changing business environment. Having access to the broadest set of personal and business applications increases the value of the device both personally and in business.

Unlike the earlier BlackBerry model that was based primarily on secure email, the common practice of working in concert with multiple applications is what makes creative and productive decisions
possible. Key to realizing this benefit is a BYOD solution’s ability to install business applications quickly, execute multiple secured applications simultaneously, and quickly and efficiently jump between them. Increasing the difficulty of business application installation and/or restricting the user’s ability to quickly switch focus can significantly restrict employee productivity.

2.2 Installation and Configuration
Implementing a BYOD solution should be easy and require minimal effort by the company and end user to become functional. Given the nature of most fixed IT budgets, any required cost and overhead for deploying BYOD is usually reflected in restrictions of other valued IT services. By ensuring that your BYOD solution of choice can use a single configuration for your mobile devices – without worrying about individual device idiosyncrasies and capabilities – further reduces the demand for IT support services.

2.3 Device Performance
BYOD should enable productive mobile device use and not require an inordinate percentage of the device’s capabilities to operate. Different BYOD approaches impact a device’s functional capacity in different ways and it is important to recognize the amount and type of overhead and its impact on user productivity. High overhead BYOD approaches will, by their nature, limit device choice to higher performance platforms.

2.4 Device & Carrier Agnostic
For corporate BYOD initiatives to be successful, IT cannot prescribe what personal devices employees can use at work or dictate a specific telecom carrier for their service. The best approach involves a single software download that can be loaded on any device in an operating system (OS) family. BYOD solutions that require device and/or kernel-specific engineering by the carrier or manufacturer will not succeed since this requires IT to maintain a list of devices that can be used to access IT services. These modifications limit BYOD to specific operating system releases and/or device models, which result in rising costs and adding latency to device availability.

2.5 Security
The base premise of BYOD is the use of a single device for both business and personal roles and the protection of business information assets from breach. It is also defined by how well company policies can be implemented and enforced on the device even if that device is no longer under the control of the employee.

There is a wide range of approaches that attempt to address these requirements but it is important to focus on the needs of your business and how a specific security model can match those needs. Products vary in the ease in which security is implemented and policies are defined and enforced. Designs range from vendors providing massive malware/virus security lists and large collections of highly specialized management policies to architecturally based security mechanisms and dynamic rule-based approaches for defining and enforcing policies.
2.6 Employee Privacy
On par with corporate security is employee privacy. This issue typically only surfaces after employees connect their device to work and fully understand what IT controls are capable of. Mobile device management solutions were designed to provide control over the total device. As a result, when an employee puts their personal device under employer management they give IT access to the list of personal apps installed on their device and their location based on GPS.

The success of your BYOD initiative hinges on employee adoption and retention. An important step in establishing trust between employees and IT is choosing a BYOD solution that prevents IT from seeing personal data on employee-owned devices.

2.7 Management Infrastructure
Structuring a device to support BYOD is only half a BYOD solution. The backend management and reporting infrastructure available to both the user and to IT is equally important. Management should cover the use of personal applications, business applications, and access to information assets. Important areas to focus on include:

- Application Distribution Management — Management of business and personal applications including deployment, installation, updating, deleting and/or blocking
- Policy Management — Development, management, and enforcement of company business and security policies
- Business Application Environment Management — Full inventory and management of the application environment(s) and the ability to act appropriately when the device is no longer under user control

How the management infrastructure is hosted is also important and options range from in-house servers to infrastructure-less, cloud-based services.

3. BYOD Approaches
There are several approaches that are positioned to help IT solve the challenges of BYOD. Most solutions have been repurposed to address the new challenges of using personal devices at work. However, only Divide™ by Enterprid™ has been purpose built to address the unique issues of both the employee and IT.

3.1 Mobile Device Management (MDM)
MDM-based approaches extend the BlackBerry philosophy to support BYOD by managing the entire device and protecting valuable company information assets. Typically MDM systems have an easy to download client and a reporting backend that can either be hosted in-house or available through a vendor-sponsored cloud service. In MDM environments application choice is unrestricted meaning users can easily jump between multiple applications and solutions and they typically scale across entire product families. However, because all applications operate in the same execution environment, personal applications can be considered a potential security threat to both business
information assets and the applications that support them. Personal apps can therefore get “blacklisted” meaning the MDM system will block their use altogether. A dual persona solution complements MDM by offering an environment where personal applications can be downloaded, accessed and used without IT oversight or corporate liability as it relates to the nature of the content.

3.2 Encapsulation
Encapsulation paradigms require individual business application binaries to be modified to operate inside a hardened, secure shell where all input/output (I/O) is encrypted and immediately routed off the device to an Internet accessible secure server. This approach typically ensures that business applications and their I/O are secure from personal application attacks. SDKs, tools, and peer experts are typically provided to assist a company’s in-house software development team as they build, test, and deploy the wrapped mobile applications needed for business. Once encapsulated, the overhead to installing business applications on the device is very low and management and reporting are typically done on either an in-house server or a vendor-supported, cloud-based service.

Encapsulation-based approaches enable all applications, both business and personal, to operate in the same mobile environment without the overhead of a monitoring system, this is done by isolating each business application with a protective shell and I/O encryption. As a result, the ability to work in concert with a number of business applications may be restricted, thereby reducing application agility.

3.3 Virtualization
One approach to implementing dual persona is through machine-based virtualization. While this approach is highly successful on servers and desktops, virtualization requires the integration of a hypervisor into the mobile OS by either the wireless carrier or device manufacturer. To support dual persona, the hypervisor must emulate two independent physical devices in software as virtual machines (VMs) each supporting their own operating system and application stack. This allows for two completely independent virtual devices, one for business and one for personal, to coexist in a single physical device.

Hypervisors are not native to any mobile operating system and must be integrated to – and supported on – specific OS releases and devices by either the device manufacturer or wireless carrier. This added step fragments BYOD scalability by limiting availability to vendors that make the engineering and support investment for a specific virtualization product. Once the integration has taken place, then one must consider the added computational overhead and unconstrained power consumption of simulating two complete devices – including two separate hardware emulations with their respective operating system and application stack.

4. Divide by Enterprid
The Divide platform offers enterprise IT a different means to BYOD by using a dual-persona approach that is managed via the cloud by both IT and employee.
4.1 The Divide Approach
As a mobile-centric company, Enterproid understands that a successful BYOD solution for device mobility presents unique challenges like device fragmentation, the privacy and governance over the content stored on a mobile device, and security and management concerns. With the Divide platform, those challenges are addressed to maximize the benefit to all ecosystem stakeholders – employees, employers, wireless carriers, and device manufacturers. Divide empowers users with unrestricted device choice that fits the full range of their personal needs while enabling them to have secure access to their enterprise data, all while also protecting their privacy.

By providing two personas, the Divide platform secures business applications from potentially breaching personal ones by architecturally eliminating the need to wrap each business application in a shell to protect it. Standard applications execute in native binary form providing unrestricted application choice. Custom applications can take advantage of additional Divide environment services such as security key management and on disk encryption.

4.2 Divide vs. Virtualization
While virtualization is a great solution for many use cases, its limited scalability and increased performance and power requirements reduce its value as a BYOD solution. Virtualization does provide a dual persona alternative to the Divide platform but its impact on device choice is significant. Divide installs as a simple download, runs on non-rooted devices using stock mobile operating system distributions. The Divide platform does not require manufacturer or carrier-specific modifications to platform kernels. As a lightweight dual persona solution that shares much of the device resource, Divide significantly reduces the device overhead required by virtualization by eliminating duplicate cycles supporting dual hardware emulations, operating system, and application support stacks. This enables Divide to support a very broad choice of devices and not be limited to just the higher performing ones that can be integrated with a hypervisor.
4.3 Divide and Device Management

The Enterproid philosophy towards management is to move as close as possible to the business related issues of managing and accessing information assets. For the end user, the Divide platform provides access to a full set of device management capabilities. For example if a device is lost, the end user can easily wipe (full or partial) the device of its data remotely while operating independent of IT. Device location, device usage, and personal Android Market applications are all easily viewed and managed, again all without any involvement from an organization’s IT department.

For IT administrators, Enterproid has a robust fleet-management console for supporting policy development, application deployment, and security enforcement for the work persona. Administrators can see all connected personal devices, set policies by group as well as perform remote commands such as wiping corporate data, locking the corporate persona, or performing password resets. Expense management tools also help identify roaming devices and display network operator usage data. The Divide platform preserves employee privacy by limiting IT control to the work persona. However when granted permission by the user, the IT console can also perform additional remote commands such as device location or a full device wipe. With no business-proprietary data stored on the device, the platform is easy to set up and deploy without introducing additional risk to the business.

The Divide platform provides the enterprise with a flexible and powerful tool to implement a full-featured cloud based mobility management solution. The platform also works with leading MDM vendors for companies with an existing MDM solution that is now implementing a BYOD or dual persona initiative.

### A Summary Comparison of BYOD Approaches

<table>
<thead>
<tr>
<th></th>
<th>Divide™</th>
<th>MDM</th>
<th>Encapsulation</th>
<th>Virtualization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Choice</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Performance</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Agnostic</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Privacy</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Ease of Installation</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Management Infrastructure</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
</tbody>
</table>
5. Conclusion

As mobile devices quickly become the primary computing platform for the world, BYOD solutions attempt to embrace that trend by enabling employees to use their single personal mobile device for all aspects of life – personal as well as business.

As a mobile-centric company, Enterprid and it’s Divide platform is the only lightweight, dual persona BYOD solution that excels in addressing all key issues required for mobile business platform success. By focusing on stakeholder needs and not the underlying technology, Divide delivers the following important benefits to employees and organizations:

• Maximum business and application choice
• A carrier- and device-agnostic client that is downloadable for each product family
• Maximum device choice for employees
• High application agility in dual persona profiles
• Executes on non-rooted, stock operating systems and scales across an entire device family
• Government grade secure container that isolates business applications from threat
• Management and client safeguards to protect employee privacy
• Comprehensive infrastructure-less management and security console for both user and IT

The Divide platform fully meets the challenges of mobile productivity for both work and personal life and is a leader in defining next generation enterprise mobility. To learn more about how a dual persona mobility solution can enhance your organization’s mobile productivity, please visit our website at http://www.divide.com.

The Divide Platform available from Dell Inc.
Contact your Dell sales representative or call 866-550-8412 x5131269
www.Dell.com/divide