Applications – the centerpiece of a BYOD environment.

November 2012

Summary

Most businesses, today, realize that it has become a necessity to offer solutions to help employees better manage agendas and activities on the device of their choice. Bring Your Own Device (BYOD) is bringing an end to juggling multiple mobile devices.

Enterprise mobile applications and applications management form an important part of BYOD. This paper discusses various aspects of application development and management and the importance of data security for a successful BYOD implementation.

Table of Contents

Introduction

What is BYOD?
Employees or end users bringing personally-owned devices to work, and using them to access corporate resources.

What is consumerization of IT or CoIT?
The migration of consumer technology into commercial or enterprise technology.

The rise of bring your own device (BYOD) programs is the single most radical shift in the economics of client computing for business since PCs invaded the workplace.

"Bring Your Own Device: New Opportunities, New Challenges", Gartner, Inc., 16 August 2012

It is estimated that by 2016, 350 million workers will use smartphones — 200 million of whom will take their own devices to the workplace.

"Mobile Is The New Face Of Engagement", Forrester Research, Inc., February, 2012

The living room is a riot of toys and colors as Adam sits on the sofa and works on his tablet, while minding his toddler. Amy sits on her favorite bench in a quiet, verdant nook of the park, seemingly talking to herself. But in fact, she's connected to an important business call. Jack is getting ready to board his flight when a customer calls, seeking important information. Jack does not have the time to take out his laptop. Instead, he takes his smartphone out, taps on a few screens and is instantly connected to his enterprise network. He is able to send the information to the customer.

Adam, Amy and Jack have several things in common. They're working from any location, on any device — laptops, tablets, and smartphones — and they can connect to their enterprise network to get their work done. Smartphones and tablets are better suited for a number of work situations as they are more portable, have longer battery life and can connect easily over different networks.

Today, for several functions and roles, work is no longer a place you 'go to', sit at a desk and work on a device provided, managed and controlled by the employer. For a growing majority of companies and employees, work can be done from anywhere, anytime and on any device. And because such a model can deliver business agility, higher productivity, employee-satisfaction and higher talent-acquisition and retention, employers are looking at ways to enable this model of working.

Enter "bring your own device", or BYOD.

To implement a successful BYOD program, CIOs need to first determine the end objective of implementing the program and then build it up, so it fits into their larger business and IT strategy. Then they need to:

- **Define clear HR and business policies.** This includes setting policies around ownership models (company-owned, employee-owned or company-owned personally enabled (COPE) or hybrid), accessibility of corporate data, payment models, level of device acceptability, terms of use, and regulatory and compliance issues around personal and corporate data.
- **Secure and protect the data.** CIOs need to go beyond securing the device and network, and envision a converged information security approach that includes integrated security for devices and platform, data protection through encryption, virtualization, disaster recovery, VPN, next gen firewall and application control and proactive detection of risks through regular audits.
- **Empower workforce with access to data and applications anytime, anywhere.** With key pillars in place, the next steps would be to truly drive productivity by enabling access to the right set of data and applications anytime, anywhere.

Applications are the way forward.

1

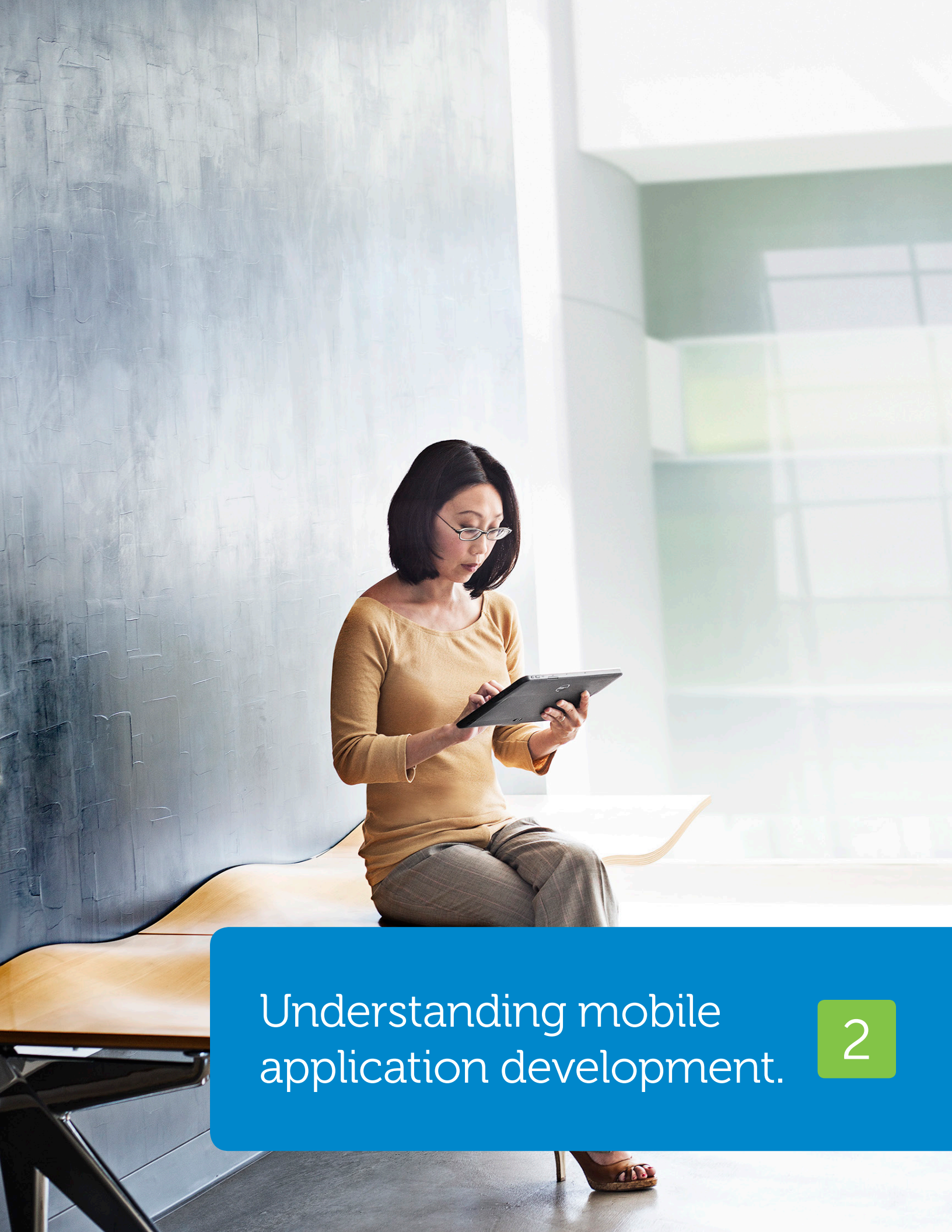
Applications are the way forward.

BYOD is not new. For years, employees have been connecting to the enterprise on their personal devices by checking their emails on their smartphones or home computers or using simple applications to do things like setting up meeting reminders or integrating their calendars.

But these simple applications are a thing of the past. Today, organizations have to invest in applications to exploit the full benefits of BYOD and stay ahead of the curve.

Applications are the forces that empower a BYOD environment and play a vital part in ensuring its success. And the right ones can make all the difference in increasing employee productivity and customer engagement:

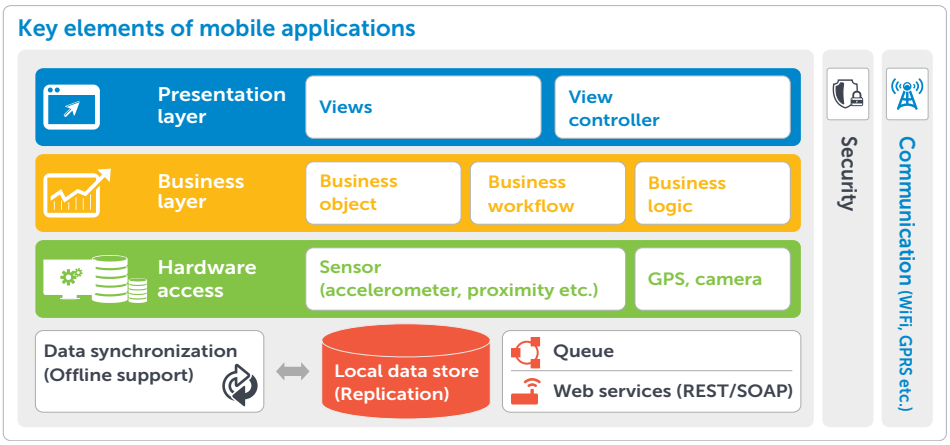
- Insurance agents might need an application that enables them to customize a policy while talking to customers across the table.
- Doctors might need and application that enables them to enter vital statistics on their tablets at the patient's bedside.
- Field agents might need an application that enables them to add a service request that updates the backend database.



Understanding mobile application development.

2

Understanding mobile application development.



The key to understanding mobile applications is determining what types you need; understanding the various platforms on which they can be developed; and then deploying, managing and securing these applications.

Developing mobile applications.
Mobile applications comprise three key elements — the hardware, which hosts the data, the middleware that connects the hardware to the application, and the display of the application. Before you create a mobile application, you need to understand the following:

- What types of users do you need to support?
- What kind of connectivity does the user generally have?
- What platforms do you need to support?
- Can the data be stored locally?
- How can you deploy, manage and secure applications from each platform?
- Do users need to sync to the cloud?
- How critical is it for the user to access the latest data?

Investing in user experience.
In the past, enterprise applications were more functional in nature, which left much to be desired with regard to the user experience. Having used high-quality consumer applications in their personal lives, users now want, and even demand, similar experiences at the workplace. Today, employees seek smart, useful and user-friendly applications to enable them to work efficiently. Companies realize that it pays to invest in user experience — they are able to attract and retain talent and increase productivity by giving their employees their preferred tools for the job.

Understanding applications and platforms.
There are three types of applications: native, web and hybrid. It's important to understand the differences and know which fits your business and requirements. Native applications are high performance, but can work only on the platforms for which they've been created. Web applications can work on multiple browsers, but cannot make use of or talk to a device's multiple features. A hybrid combines both; it is a web view that operates in a native application container.

Applications can be developed on several mobile platforms, depending on the need, use and nature of the application. They can be developed on native platforms using software development kits (SDKs) or mobile enterprise applications platforms (MEAPs). They can be developed using HTML 5 for mobile web applications or as part of an application container using a hybrid method. A hybrid application uses the web view components but runs in a native container.

Types of applications

	Native	Hybrid	Web
Device access	Full	Full	Hybrid
Development cost	Expensive	Reasonable	Reasonable
Speed	V. good	Good	Depends on connectivity
Graphics capability	V. good	Good	Reasonable
Deployment	App store	App store	No app store
Offline usage	Yes	Yes	Limited

The three types of applications have their own advantages and disadvantages. While MEAP is considered one of the better ways for enterprise application development, it requires certain investments. HTML 5 is considered to be an important tool to develop cross-platform enterprise applications, but it has limitations due to different browser implementations, OS versions and screen sizes (especially in Android). Native applications on the other hand do well on several performance parameters like usability, overall performance and offline performance. They provide easy access to the latest API's and hardware interfaces. However, native applications are labor intensive to develop as special skills are required for each mobile platform.

While the native versus HTML 5 debate continues, an enterprise needs to carefully select the best application for the need. For example, a travel portal application may be a good candidate for mobile web and hybrid platforms, while a retail application that uses camera, GPS and augmented reality may be best developed on native platforms.

Understanding deployment.
Enterprises can deploy applications in different ways. The two most popular ways are using web application container and native application container.

Web containers are a way to have multiple enterprise mobile applications deployed within a single application. Applications can be developed using web technologies like HTML 5, JavaScript and CSS and have access to only web functionality exposed by the web container. The web container cannot be used to deploy native applications.

- iPhone
- BlackBerry
- Android
- Windows Phone
- Symbian OS

Mobile platform SDKs

- PhoneGap
- Titanium

Cross platform tools

- Kony solution
- Sybase unwired platform
- Antenna mobile platform

Mobile enterprise application platform

An important thread that binds all enterprise applications is security. Mobile applications can be secured using industry best practices. One such practice is using native containers.

The web container can, in some cases, provide the hardware features to the web applications inside the container by using JavaScript extensions. The web container can also provide access to corporate infrastructure behind firewalls, using application level VPN.

Applications in web containers are managed by a central administrator, making it easier to secure authorization, monitor and push applications as well as dispatch updates and patches.

In the case of a native container, the applications are native applications. The native container may hold other native applications within itself if the OS supports this functionality at the framework level. The native container provides the API's to securely store enterprise data on the device.

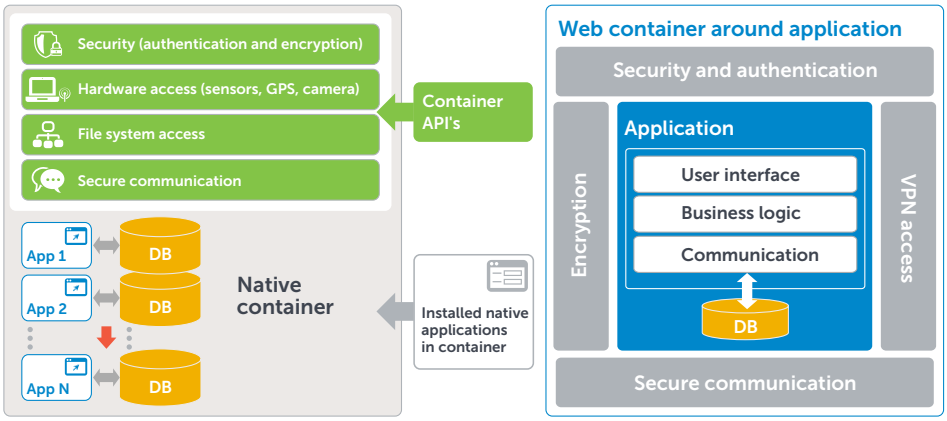
In some cases, the native container can be merged with mobile device management (MDM) agent; this helps in device and application management.

The native container also provides functionalities like remote wiping of the enterprise application data.

Native containers are gaining popularity because they do not interfere with other experiences on the device, and they keep corporate data secure.

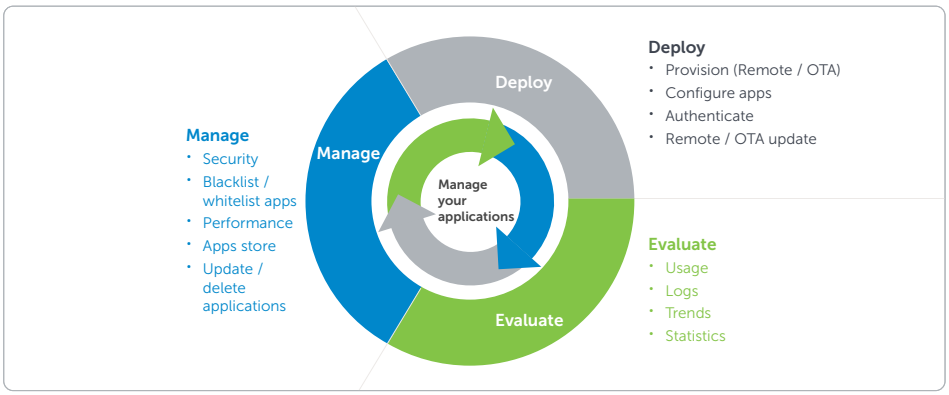
Application virtualization.
Virtualization is another way by which enterprises can deploy applications onto mobile devices. The applications in this scenario are actually virtualized images delivered via a container application; such an environment makes it easier to manage applications while providing more security. Enterprises using this model should be aware of the challenges that come along with it, like the potential for compromised user experience, the need for device connection to the network, in order for the applications to work and certain integration issues.

CIOs need to weigh pros and cons of both methods along with their business need to adopt either method.



Managing applications. 3

Managing applications.



Application management starts with sound policies governing the BYOD environment and encompasses deployment, socialization and evaluation of the applications.

Create a mobile app store.
A mobile app store provides enormous benefits, because it's the enterprise's direct link to the users of the applications.

Through the app store, IT can deploy new applications, retire old ones or update and modify applications. Applications within the app store can be developed to work on any kind of device or OS, ensuring that they'll work on both corporate and personal devices.

Like consumer app stores, an enterprise app store can enable users to rate, review and give feedback on applications. With access to this data, IT can keep a pulse on what's efficient, what's not working and what's no longer useful. The app store also helps streamline and manage applications efficiently by supporting remote provisioning, managing software and licenses and scanning for malware. This can reduce the rate of application failures and has a direct impact on employee productivity and BYOD success.

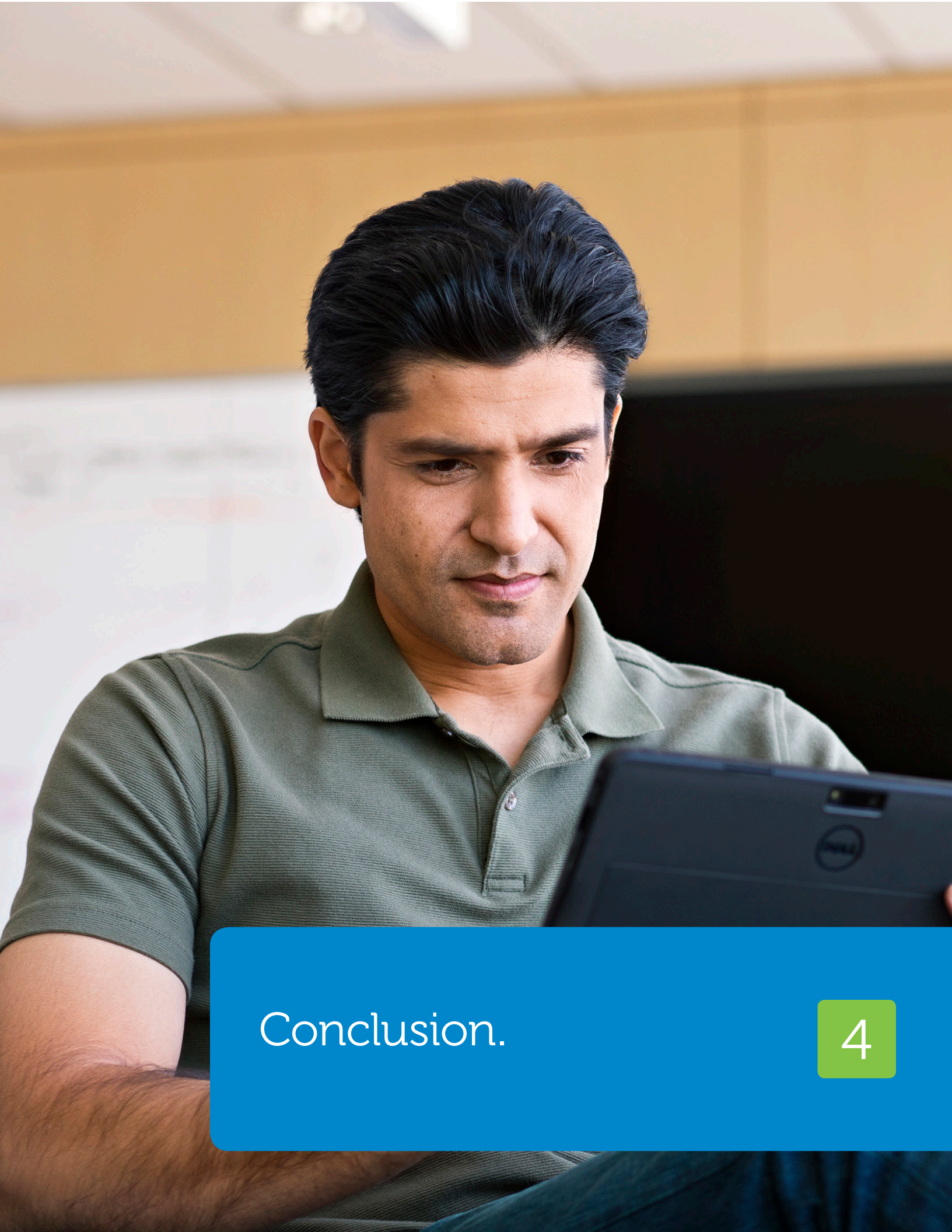
Develop a sound policy for BYOD.
The right policies can make all the difference in a BYOD environment. For instance, you may have restrictions on who can use their personal devices to access corporate data; who can access which applications and whether or not you will reimburse employees for going over their data plans or minutes. Create policies that employees will trust and follow, and make sure you review and update them regularly so they stay current and relevant. Juggling multiple devices, OSs and applications can be quite challenging, so you need to clearly map the devices, OS types and application types to the correct user profiles.

Enterprises with a BYOD environment should adopt procedures that separate personal and corporate data and applications on the device. This strengthens employee-employer trust, because users know that personal data cannot be monitored or compromised. When an employee leaves the organization, you need to clearly define a policy for wiping, remote-wiping and disabling access to all company-owned applications.

When introducing an app store, enterprises should roll out an instructional plan, promote applications through a tailored and structured marketing program, and continuously monitor applications in the app store.

Ensure security.
Managing and securing a BYOD program can be quite challenging, especially with the proliferation of devices, platforms, applications and operating systems. CIOs are constantly challenged on many fronts while trying to secure endpoints, networks, infrastructure, OSs and, most importantly, data and cloud-syncs. Security threats are lurking behind every instance of data stored locally, a stolen device or inadvertent spam clicks. Because of the complexity of securing this entire infrastructure, CIOs often fall in the trap of looking at security in silos. Instead, CIOs should aim for a comprehensive view, taking in devices, applications, network, infrastructure and data cohesively. Then, they should set in motion a security plan that is constantly monitored. Additionally, it's important to focus on securing the data, rather than the endpoints. On the network side, most routers, switches, firewalls and VPNs have built-in security features. CIOs could also consider opening up VPN tunnels for applications or users, which makes managing network security easier.

Mobile device management and mobile application management are great ways to ensure security, as they take care of several security protocols, including how users interact with their devices; managing devices, data and applications; and helping manage costs by enabling the setting of policies.



Conclusion.

4

Conclusion.

Adam takes a break from work and helps his son make an airplane with his Lego pieces. On finishing her call, Amy slips her smart phone into her jacket and steps onto the jogging track. And as he prepares to take off, Jack is smiling to himself; he knows he has made a customer happy.

Adam, Amy and Jack all have several things in common.

Their organizations enable a work policy, by which they can connect to the enterprise from any location, work on a device of their choice and connect to corporate data on applications that are efficient and user-friendly. They have the flexibility to divide their personal and professional lives the way they need, as well as a mutually trusting relationship with their employer.

Enabling a BYOD environment provides enterprises with happier and more productive employees as well as improved customer engagement. But in order to realize these benefits, CIOs have to constantly balance the needs and demands of this new generation of employees. They must have a plan for maintaining control of their IT environment and how their IT department will successfully support today's workers.

BYOD is constantly changing the game for businesses, employees and IT, and to be successful in this new paradigm, CIOs have to find a way to maximize end user productivity without sacrificing IT control or security.

For more information about solutions for your organization, contact your Dell account representative or visit dell.com/services.

Scan or click this code to learn how Dell Services can help your organization.

November 2012 | BYOD Whitepaper.indd | Rev. 1.0