Making Everything Easier!™

VMware Special Edition

BYOD

FOR DUMMIES®

A Wiley Brand

Learn to:

- Get your head around BYOD
- Make sense of MDM, MAM, MCM and VDI for BYOD
- Securely support your end users

Brought to you by:

vmware®

Charles Barratt
Courtney Burry
Justin Venezia

About VMware Inc.

VMware (NYSE:VMW), a global leader in virtualization and cloud infrastructure, delivers customer-proven solutions that accelerate IT by reducing complexity and enabling more flexible, agile service delivery. VMware enables enterprises to adopt a cloud model that addresses their unique business challenges. VMware's approach accelerates the transition to cloud computing while preserving existing investments and improving security and control. With more than 500,000 customers and 55,000 partners, VMware solutions help organizations of all sizes lower costs, increase business agility and ensure freedom of choice.

For more information, visit www.vmware.com

BYOD

FOR

DUMMIES®

A Wiley Brand

VMware Special Edition

BYOD

FOR DUMMIES®

A Wiley Brand

VMware Special Edition

By Charles Barratt, Courtney Burry and Justin Venezia

FOR DUMMIES®

A Wiley Brand

BYOD For Dummies®, VMware Special Edition

Published by
John Wiley & Sons, Ltd
The Atrium
Southern Gate
Chichester
West Sussex
PO19 8SQ
England

For details on how to create a custom For Dummies book for your business or organisation, contact CorporateDevelopment@wiley.com. For information about licensing the For Dummies brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Visit our Home Page on www.customdummies.com

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

ISBN: 978-1-118-83227-1 (ebook)

Introduction

Welcome to *BYOD For Dummies*, your short and sweet guide to embracing the bring your own device (BYOD) trend while retaining your sanity in the process.

Remember the days when each employee had their own PC (which you gave them) that sat in a fixed location (the office) with a set of applications (which you deployed to every device)? Well – a lot has changed since then.

Today, whether you like it or not, employees and contractors alike are bringing a whole slew of new devices into the workplace to access corporate applications and data. And for the most part these aren't devices that you are doling out, but their own.

Now, on the plus side, this means that you can wash your hands of buying and procuring hardware. But on the down-side this also means that you no longer control the devices, what's on them and what's hitting your corporate network. And nobody likes to be out of control.

BYOD is here to stay but we're here to help. The tips and advice in this book aren't only about helping you to get off on the right foot when it comes to supporting BYOD; they'll also help you improve end user satisfaction and productivity. And, more importantly, they enable you to simplify the day-to-day management of end users, enhance security and contain costs in the process.

About This Book

This book aims to provide you with information to tackle and support BYOD initiatives. It's full of useful information and tips to help you plan and implement a BYOD strategy based on your requirements. This guide can help you consider your technology options and ensure that you cover all of your bases before you get started.

Foolish Assumptions

In writing this book, we made some assumptions about you:

- You work in IT or within an IT organization.
- You want to understand how to tackle BYOD.
- You're looking for information, tips and tricks about how to get started.

How This Book is Organized

BYOD For Dummies is divided into seven small but perfectly formed chapters:

- **Chapter 1: What's the Big Deal with BYOD?** Head here for a quick overview of BYOD, things to think about when building your plan, and the pros and cons of common technologies used to tackle BYOD.
- **Chapter 2: Making the Case for BYOD.** Head here to discover the costs and benefits of BYOD.
- **Chapter 3: Approaches to BYOD.** Get to grips with a squillion acronyms in this chapter and understand how they all relate to BYOD.
- **Chapter 4: Delving Deeper into Deploying Enterprise Mobility Management for BYOD.** Get your hands dirty in this chapter as you discover all the tips and best practices you can leverage around MAM and MCM for BYOD.
- **Chapter 5: Getting a Helping Hand with Desktop Virtualization.** Keep the end user in mind as you read this chapter and discover how VDI can help with your BYOD plans.
- **Chapter 6: Rollin' Out EMM and VDI with BYOD.** This chapter looks at the key policies and procedures you need to keep in mind when rolling out BYOD.
- **Chapter 7: Ten (Okay, Seven) Useful Resources for BYOD.** In the famous *For Dummies* Part of Tens we give you some extra reading to further your understanding of all things BYOD.

Icons Used in This Book

We highlight crucial text for you with the following icons:

The Dummies man indicates real-life examples to illustrate a point and inspire you.

The knotted string highlights important information to bear in mind.

Home in on the target for tips to enable you to support BYOD.

Watch out for these pitfalls.

Where to Go from Here

As with all *For Dummies* books, you can either read this guide from cover to cover or flick straight to the section that interests you. Whether you read it in small doses using the section headings or all in one session, you'll find plenty of information to get you on your way to supporting BYOD.

Chapter 1

What's the Big Deal with BYOD?

In This Chapter

- Defining BYOD
- Discovering the origins of BYOD
- Recognizing the benefits
- Knowing the challenges

Bring your own device has become so popular, there's no shortage of terms used to describe it. BYOD (bring your own device), BYOT (bring your own technology) and BYOS (bring your own stuff) are just a few. But for many of us actually bringing these devices into the workplace, SYOM (spend your own money) may be the most appropriate term of all.

In a nutshell, BYOD is the idea of allowing employees to bring in the devices of their choice (laptops, PCs, tablets and smartphones) to access corporate resources and get their work done.

BYOD puts the choice and the purchase of the device squarely on the employee. Employees simply show up to work with their own bag of preferred devices in tow. They're happy because they feel empowered and IT is happy because they don't have to spend money.

But what does BYOD really mean for companies? Is it really as simple as it sounds? What are the pros and cons of embracing this trend? Why should IT folks care about what their end users are bringing into the workplace – after all, if you ignore it, surely it will eventually go away like a bad tattoo or a shotgun wedding, right?

In this chapter we answer these questions.

Going back in time . . . how BYOD began

The term "BYOD" was coined back in 2004 by some scholars from Germany, England and Switzerland for their research.

BYOD as we know it today really came into its own in 2009 at Intel, when IT began to notice a large influx of employee-owned devices coming into their offices. Rather than run for the hills and outright reject this trend like many of their other Fortune 1000 peers, Intel chose to embrace this as a means of saving money and increasing worker productivity.

The term really started to catch on in 2011, which was roughly a year after Apple introduced the first iPad into the market. Employees were enamored by what these new gadgets could do and IT pros found more and more employee-owned tablets and smartphones cropping up within the ranks.

Today, according to recent findings from Juniper Research (August 2012), the number of employee-owned devices being deployed in enterprises will more than double to over 350 million by 2014.

However, while many companies have made the move to embrace BYOD, a full 46 per cent of employees say that their employer either doesn't know that BYOD is actually taking place or, worse still, knows but chooses to ignore it, according to IT solutions provider Logicalis (The BYOD Divide, November 2012).

Enjoying the Benefits of BYOD

The truth is, BYOD can actually be a good thing for employees and IT organizations if done right. So rather than ignoring the writing on the wall and hoping that one day you'll wake up to find all those Android, Apple and non-standard, non-corporate issued devices are gone, it's better to see how you can weave BYOD into your larger workplace mobility strategy.

Ultimately, companies that do make the move to BYOD enjoy many benefits; the two most widely touted being:

- **Cost savings.** BYOD can provide you with the opportunity to get out of the device procurement business and save money. With fewer PCs to buy, you can use the money elsewhere. Some organizations do subsidize BYOD policies with a stipend, but this still usually results in a lower cost overall.

According to Cisco (Cisco IBSG Horizons Study, 2012) you can see cost savings of as much as $3,150 per employee per year if you implement a comprehensive BYOD program that gives your employees access to all the information they need to do their jobs from their personal devices.

We say cost savings – however, if not done correctly BYOD has been known to cost companies more money than sticking with corporate-owned, corporate-issued devices. Costs that can add up include securing and managing BYO devices, stipends, risk management and internal app development.

- **Increased worker productivity.** The theory goes that employees who are free to choose and use these devices from home and at work to access corporate resources work harder and are happier doing it.

  In a recent study, Cisco (Cisco IBSG Horizons Study, 2012) found that this can amount to $300 to $1,300 per employee, depending on the job role.

So with BYOD you can get your employees to work harder, enjoy it *and* pay out of their own pockets for devices and technologies that make their work experience even better.

It's a bit like having kids buy and wrap their own Christmas presents from Santa Claus. They get what they want and Santa gets a little break.

Watch Out Below: Identifying the Challenges

Like anything that seems to be too good to be true, BYOD isn't all happy, shiny people and devices. You need to look into and plan for a number of issues before you get started:

- **It's my data, right?** Given that employees are accessing and saving corporate data to personal devices, you need to understand how that data will be retrieved and wiped when that employee decides to move on. Without good planning, corporate data can walk right out the door – do not pass go or collect $100.
- **You uploaded *what* onto my corporate network?** In the past year the number of viruses downloaded by tablet

and smartphone users has exploded, with Android the most targeted mobile platform bar none according to a report by IT security experts Kaspersky. Imagine having all those viruses and Trojans gallop their way onto your network when employees connect in.

To make matters worse, a whopping 80 per cent of end users don't run any kind of anti-virus software on their personal devices so it may not be until that application has infected your entire network that the owner of the BYO device realizes that they have anything to worry about. And in this case, you're the one who has to clean up the mess.

- **So now I'm responsible for data compliance on employee-owned devices?** If your company needs to follow specific compliance mandates like HIPAA or PCI you have certain rules around security and safeguarding data that your employees need to meet – even if they're using their own devices.

  However, it may be difficult to set and enforce policy around BYOD. After all, the devices don't belong to you and the company, do they?

  But if Joe in accounting forgets to adhere to regulations on his new iPad that he's using for work and you happen to fail an audit; well, you're likely looking at a fine that's significantly more than we'd ever make in our lifetimes.

- **I have to manage *how* many devices?** These days most employees carry two or three devices for work. And in the event that your company chooses to manage these, that means two to three times the number of hours to manage, patch and update images and applications for end users.

- **What do you mean, no one here knows how to do this?** Finding the right skill-set in-house to tackle new initiatives like BYOD, ensure the right security policies are in play and manage the ins and outs of workplace mobility isn't always a slam dunk. Often you'll need to look at retraining staff or searching for new hires and contractors to help you make all this work. And finding new hires with the right skill-set may take more time and money than you have set aside in your budget.

The moral of the story is to make sure you do your homework before you get started. BYOD has many advantages but you need to plan for some challenges before you dive in.

Chapter 2

Making the Case for BYOD

In This Chapter

- Getting buy-in for BYOD
- Knowing the costs and benefits

Planning for BYOD isn't something you want to do in isolation. In fact you may have to bring more people into the planning process than you'd like, but in the end this will set you up for success. In this chapter we think about how to get your stakeholders on board with BYOD.

Setting Expectations for BYOD

As you build relationships and identify key stakeholders you need to include your counterparts from information security, networking, application development, end user computing and IT architecture, marketing, HR, finance, procurement and sourcing to just name a few.

Getting these stakeholders bought in to a company-wide BYOD vision ensures that they're invested so that they can help you move forward and bring in the right tools where needed. But you need to do more than just get them bought into the vision and help with the tools – you also need to make sure that the stakeholders are in agreement on the investment required as well as the expected return.

This amounts to ensuring everyone has a clear understanding of how BYOD fits into the company's goals, what technical and business processes need to be put in place or modified and, more importantly, the expected returns to the company.

If everyone's under the impression that they'll see return on investment (ROI) on your BYOD project in six months' time, but you know it'll take 18 months, you'll definitely run into problems.

Be sure to get consensus on the timeline as well as the costs and the benefits as you scope out your program and build your business case. For many, a failure to do so has meant cost overruns, poor employee adoption and lots of finger pointing – mostly in your general direction.

Building the Business Case for BYOD

When building the business case for BYOD, you need to weigh the costs and returns to get a good sense of the ROI of your project.

Some key costs to consider include the following:

- **The costs of BYO devices and stipends.** You need to decide if you're going to provide your employees with a stipend to cover the costs of their devices and their wireless plans.

  

  Interestingly, according to Gartner (Gartner Press Release, "Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes", 01 May 2013, `www.gartner.com/newsroom/id/2466615`), roughly half of BYOD programs provide a partial reimbursement, but full reimbursements for all costs are becoming rare. Mass market adoption of BYOD coupled with the steady declines in contract fees, are swaying employers to remove subsidies all together. You may find that even if you do open your wallet and allow employees to expense their monthly carrier bills, many of them won't bother to do so but they'll feel a lot better about you and the company for the offer.

- **The costs of managing and securing BYOD.** Not only do you need to look at your infrastructure and networks to make sure that they can handle an increase in traffic from BYOD, you'll also likely need to bring in some type of enterprise mobile management (EMM) platform to help you manage and secure access to corporate assets (you can find more on EMM in Chapter 3).

- **The costs of servicing and supporting your end users with BYOD on a day-to-day basis**. You need to decide if you have the staff and resources in house to support this cost, if you'll outsource it or if you'll bring in additional contractors to help support your employees on an ongoing basis.

You need to weigh these costs against the hard and soft returns to the organization:

- **Revenue per employee.** At the end of the day, if your employees are more productive, revenue per head should go up.
- **Employee satisfaction.** While not tied directly to a company's top line, the ability of a firm to attract the best and the brightest in the industry is often directly related to company reputation and employee morale.
- **Contribution margins (the marginal profit per unit of sale).** With BYOD, if you can contain your variable costs (for example, the cost of device procurement) and increase your total sales (due to the fact that your workers are now more productive) you can increase your total contribution margins and company profits.

While your CEO cares about revenue and contribution margins, your CIO probably only wants to know if you can help deliver better service level agreements (SLAs) at lower costs. So you need to know if the cost savings from not buying devices is greater than the costs (outlined above) of having to support this new program.

The benefits of BYOD are still a mystery to many CIOs, with only 22 per cent believing that they have a strong business case in place to support it, according to Gartner (Gartner Press Release, "Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes", 01 May 2013, `www.gartner.com/newsroom/id/2466615`). Make sure your CIO isn't one of the 78 per cent that are in the dark, by weighing the costs and benefits and putting forth a solid plan that has cross-functional buy-in early on.

Chapter 3

Approaches to BYOD

In This Chapter

- Getting to grips with MDM, MAM and MCM
- Combining it all together with Enterprise Mobile Management
- Taking a tour of virtual desktops
- Looking at BYOD in practice

Now that you've weighed the pros and cons of BYOD (Chapter 2) and decided to move forward, you need a solid management plan.

As part of this, you'll want to understand your employees' needs and the ways that they'll be accessing company applications and data. Ask yourself if they'll be mobile or remote, what assets they'll need and if you'll subsidize employees' devices and monthly plans.

And don't stop there! You also need to decide how you're going to enable and control access to corporate assets, entitle policy, ensure compliance and support your end users on an ongoing basis.

Luckily, a number of technologies have emerged over the years to help you better manage and control BYO devices, data and applications and this landscape of technologies continues to evolve. This chapter walks you through that evolution. You've gotta love the IT industry's obsession with TLAs (Three Letter Abbreviations); the mobile world really has built up its own suite of them. Prepare for acronym overload!

In the Beginning was MDM

Back in the day when BlackBerries were everywhere, IT managed what you could do on them. But these were corporate issued and corporate owned, not BYO devices. If you decided to part ways with your company, you also broke up with your phone.

With the advent of Android and Apple phones and tablets, employees started to bring their own devices into work. Luckily, Apple and Google developed a set of Mobile Device Management (MDM) application programming interfaces (APIs) that companies could write against to allow IT to manage these devices. MDM gave IT the ability to take control of an entire device and in the process set policies, encrypt access and even remotely wipe everything.

But given that employees were using their own devices, many of them weren't exactly thrilled about having IT run the show. After all, why would you want IT to restrict access to the features you want to use, force you to use ridiculously long passwords and routinely wipe all of your personal files in one fell swoop?

Plus, while MDM enabled companies to wipe everything remotely, this still didn't prevent a bigger problem around leaky data. With MDM, employees still had the ability to cut and paste corporate files into personal email accounts and cloud-based apps such as Evernote.

IT departments needed something beyond MDM that would allow them to control and secure BYOD devices and content. And this is how Mobile Application Management (MAM) came front and center.

Just Call Me MAM

Unlike MDM which looks at device management, MAM is really geared around provisioning, managing, monitoring and removing enterprise applications and data. With MAM, applications are isolated within their own containers and policies can be set around these isolated applications.

One of the most popular approaches today to MAM is through *application wrapping*. Typically application wrapping enables IT to insert policies without changing the way that the application works.

You can decide to enforce a PIN for access to specific applications, dictate which applications can be used to open attachments and limit an employee's ability to cut and paste between applications. You can even intercept a communication and force it through your network or prevent it from going through to a given application.

All this means that you can plug a lot of the holes contributing to leaky data. What's more, employees no longer feel like you're the mothership aggressively taking over their device.

Or at least that's the theory. The problem with a lot of wrapped apps made available in app stores is that they're dependent on MDM in order to work. Also, wrapped apps may be going by the wayside if Apple and Samsung have anything to do with it. Recently, both companies announced that they're introducing new features into the KNOX and IOS platforms that help remove the need for app wrapping all together.

Plugging into MCM

Time for another three letter word: MCM or Mobile Content Management. Also referred to as MIM (Mobile Information Management), MCM enables mobile users to securely access, edit and share files with other users across devices and locations.

Many public share file sites are available for people frustrated with FTP and Sharepoint. Dropbox, Box and Google have all managed to attract end users in droves. But while these sites provide a great way to collaborate, they tend to leave IT out of the equation as IT can't control any of the files on them. It's really a 'don't ask, don't tell' kind of thing – end users tend to use these sites without asking IT for permission to do so. If file sharing is in the cloud, you need to worry about the legal ins and outs of the data too, because the laws of that country, wherever the date center is, apply. Nightmare!

The other pitfall with public file share sites is that once files are shared, they tend to take on a life of their own. Many of these files are never deleted. If someone leaves a company, they may find that they still have access to all of their former files. The folks on the shared folder from their previous employer may be happily oblivious to this fact for months on end.

And this is really where enterprise MCM solutions come in. MCM is designed to enable employees to access and share files across devices (including BYO devices) but they enable IT to get back in the driver's seat when it comes to controlling and monitoring access.

EMM: Don't Forget About Me

When you combine MDM with MAM and MCM you get comprehensive Enterprise Mobility Management or EMM, which brings together the best of device management, application management and file management under one roof. Some EMM solutions also look at financial management and carrier contract negotiations so that your organization can contain the costs of voice and data plans now that your employees are negotiating their own contracts.

Going Remote with VDI

When it comes to BYOD, you have many ways to support end users. But you'll find that some of your employees are truly mobile (like your sales force) and others are what you might call remote. They aren't constantly on the go, but they aren't necessarily working from the office either.

These remote employees may use mobile devices like tablets and smartphones to *consume* content, but more than likely, they'll use a laptop or PC to *create* it.

When it comes to remote employees, virtual desktops provide a secure, streamlined way to support access. With desktop virtualization (or virtual desktop infrastructure; VDI), the operating system, data and applications are decoupled from the end device and moved into the data center where you can

manage them. The device essentially becomes an empty shell that employees can use to view the assets that they need.

Similar to the concept of application wrapping, which allows applications to be separated into their own containers, VDI with BYOD enables you to isolate the corporate image and applications that you provision out to an end user from their underlying personal image.

As a result your employees and contractors can keep their personal applications and data. In fact, if they want to upload sketchy apps they can go right ahead. Because what hits the corporate network is only the VDI image that you (as IT) have entitled and are managing.

The downside with VDI with BYOD is that it doesn't prevent leaky data. VDI makes it harder for data to walk when a device goes missing, but it doesn't prevent files from being shared in ways they shouldn't be.

As a result, it's often smart practice to pair up VDI with MCM or EMM solutions to ensure that you have all of your bases covered. And fortunately, several companies are looking at providing you with a suite of products that do just this.

BYOD Technology in Practice

Before you get started with BYOD, do an assessment of your employees to understand what devices they'll be using and where they'll be working. Will they be truly mobile or remote? Will they be creating content or consuming it? Answering these questions can help you successfully plan a combination of technologies to best meet their needs and your requirements.

So how is BYOD being rolled out and supported right now? EMM and VDI are both being widely deployed by organizations across the board but VDI has undoubtedly been around the longest.

One firm that turned to VDI to tackle BYOD is law giant Foley and Lardner. Take a look at how this has panned out for them so far in the nearby sidebar "BYOD: Doing more with less."

BYOD: Doing more with less

When its IT staff was reduced, Foley & Lardner LLP, a technology leader in the legal industry, had to rethink its approach to end-user computing. Foley has approximately 900 attorneys and 1,170 support personnel, many of them highly mobile.

When the US economy stumbled in the late 2000s, the firm's IT organization adapted by "doing more with less," including rethinking its entire approach to delivering end-user computing. Foley decided to replace its traditional desktops with a "desktop as a service" model. Under this model, the firm's IT department centrally manages a fleet of virtualized desktops for use by Foley employees.

Employees can access their systems either on-site or remotely. For on-site access, the IT team procures and manages a fleet of both thin and zero clients. Zero clients are typically installed in situations where attorneys need or prefer a smaller form factor client to conserve desk space. For remote access (Foley supports 18 US offices with its virtualized desktops) the attorneys use either firm-issued laptops or mobility devices they own or purchased as part of the firm's BYOD program. Foley was ready to embrace this model partly because the firm was already familiar with virtualization; its servers are 75 per cent virtualized.

Foley's adoption of BYOD relieves its IT team of handling mobile device procurement, repair and disposal. Attorneys are reimbursed for equipment purchases up to a maximum of $3,800 every three years.

"VMware won us over with their depth of knowledge about end-user computing," notes Kevin Moll, Senior Desktop Engineer at Foley. "They were able to articulate a clear vision for enterprise space desktop virtualization."

By enabling a BYOD model, Foley's three-year mobile computer costs have decreased by 22 per cent. Managing its on-site desktops requires fewer tech touches. Before, provisioning new desktops required at least four hours of a technician's time. Configuring a new zero client can be completed in about 10 minutes. Streamlined provisioning makes it easier for Foley to manage its IT resources. This is particularly helpful when it's time to refresh the firm's desktop systems.

"It's not uncommon to deploy 400 to 500 machines in a short period of time," notes Moll. "But today, local technicians just unbox and plug in the new units. Other resources can handle image deployment and software installation. Someone at the helpdesk, for example, might build desktops as a secondary role during light shifts."

Repair times are shorter, too. Before, if a desktop failed, users had to

wait several hours for repairs to be completed. Today, software issues can be resolved in seconds by just pointing to a new virtual desktop.

While these efficiencies benefit Foley's IT organization, the most important outcome is the reduction in unplanned downtime, as the firm's legal professionals rely on their desktops to deliver billable services.

Attorneys working remotely are also more productive. They can access their desktops and critical applications from their mobile device of choice, including iPads and laptops. Their desktops are consistent regardless of device, so attorneys don't have to hunt for icons when they want to launch applications. They're in the same place regardless of whether they're working on- or off-site.

Virtualized infrastructure also helps Foley better protect client data, another critical business priority. "Users connect to their desktops that reside in the data center behind our security infrastructure," notes Rick Varju, Director of Engineering and Operations, Foley. And if a mobile device is lost or stolen, Foley takes the additional precaution of remotely wiping it clean.

Chapter 4

Delving Deeper into Deploying Enterprise Mobility Management for BYOD

In This Chapter

- Asking the right questions about MAM and MCM solutions
- Checking EMM capabilities

We hope we're making it abundantly clear that no single tool works for all scenarios when it comes to BYOD. Some users need a highly locked down environment where management of the device is key (MDM). Many of your users need to collaborate on documents and sync and share information (MCM). And other employees need access to corporate applications across devices, and you want to make sure that these are trusted apps (MAM) downloaded via per application virtual private networks (VPNs) to ensure all your precious data is encrypted along the way. So you can see that a bunch of tools make up EMM that you'll want to take a look at. Skip back to Chapter 3 if you need a recap on this acronym overload!

Clearly all these options make your job a little more complicated. But the good news is that many traditional software vendors who have played for years in the desktop world (virtual or physical) such as VMware, have recently introduced tools that pull all these solutions together so you can securely serve up apps, desktops and content through

one platform to your end users. This chapter delves deeper into deploying EMM and BYOD.

Getting Started with MAM

When rolling out MAM or MDM, you need to make sure that your users know what administrators can and will be doing around BYOD. Given that employees feel that big brother is all too often watching them, it's important to communicate if you'll be tracking and interrogating their devices (MDM) or just setting policies around their applications (MAM).

You'll likely want to distribute and monitor corporate applications based on device ownership models but you also want to provide your end users with a simple way of enrolling their BYOD devices themselves. Enabling end users to enroll on a self-service basis is a great way for you to provide acceptable policies around usage while ensuring that your end users are aware and okay with them.

A few key questions to ask your provider before you get started with any MAM solution include:

- What's your strategy for third party applications and can you secure them without source code access?
- If the device gets lost, can you wipe the application and content?
- Can you enforce two-factor authentication (2FA) or single sign-on (SSO) on all corporate applications accessed on each device?
- Can you ensure that data doesn't leak from one application to another?

Be sure you get yeses to all of the above before you move ahead.

What to Look for in a MAM Solution

Here are some of the key things you need (at a minimum) in a MAM solution in order to be successful:

- **Application delivery from home-grown applications and trusted applications from public sources.** You'll no doubt develop your own applications and need to deliver those to your end users along with apps for job functions from public app stores such as Google Marketplace or the Apple store. Your MAM platform needs to be capable of delivering from both sources.
- **Application updates.** After you have your applications on the device you need to ensure that they're updated in a simple way. iOS 7 will simplify this with its capabilities. Your MAM platform should also simplify by managing applications through the entire lifecycle from procurement and development through to the securing, distribution, tracking and update of your applications.
- **User authentication.** You don't want to provide passwords for the sake of it, but at the same time you need to ensure a healthy level of governance on the data accessed by your end users. Your MAM solution needs to establish the type of authentication needed per application. Some could be simple passwords, some directory based, some 2FA and others via security certificates. However you skin it, your MAM platform needs to offer flexibility.
- **User and group access control.** For administration purposes you really want to assign permissions to groups of users, perhaps defined as part of your user segmentation process. At other times you'll want to assign a specific application to an individual. The access control should be pretty granular too, allowing different users different access to features of the application. Just because a device is mobile doesn't mean that your security should be different; it just needs to be relevant.
- **Application based VPN.** This is a big one that you really need to make sure is nailed down. MDM solutions offer device-based VPN connections so everything's tied to the company network, which isn't great. Application based VPNs mean that you set the specific applications that must connect to the office to get access to data.
- **Over the air (OTA) capabilities.** As the name suggests, OTA makes BYOD possible when you don't need to physically take each device and add/configure to the network. Any platform should enable users to self-enroll and leverage OTA as a way to simplify this.

- **Reporting and tracking.** You need to be able to track usage and report back on the effectiveness of the BYOD implementation. The IT department needs to be able to configure logging and filter logs on the severity of security breaches such as jailbroken devices, number of failed logons and inappropriate device usage when reporting on usage.
- **Licence control, administration and Apple Volume Purchase Programme (VPP) integration.** BYOD is great in practice, but you want to make sure that you're not paying over the odds for applications or, on the flipside, don't have enough applications to support your end users. Well, MAM reporting answers the questions about which users are doing what and when, which is very handy if you have external audits.

While your choice of technology is important, the first thing on your mind needs to be defining your strategy, device ownership models and which devices you plan on supporting (corporate-owned, corporate-shared and/or employee-owned) first.

You also need to think about operational readiness and the business processes you'll need in place to support MAM, especially given that many of your applications are likely designed to work and be accessed behind the firewall on a full-size monitor. What needs to change, what can stay – these are key questions you need to tackle.

Controlling Corporate Data with MCM

MCM solutions are designed to put you back in the driver's seat when it comes to controlling how data is managed and accessed.

As with any tool that provides users with access to corporate data, one or two users will always bend the rules and provide access to users that shouldn't be on the receiving end. On the bright side – if you consider this a bright side – most of those users tend to be leaving the business and would have taken data off the network with or without MCM!

From an infrastructure point of view, make sure that you're able to plug into your existing data sources with your MCM solution, otherwise you're going to end up with duplicated versions of data along with a humungous storage bill. If your storage platform supports de-dupe technology (which eliminates redundant data), that can save you some cost on the implementation. Also, if you're following a cloud route (and many businesses are), make sure that your MCM solution works on both public and private cloud platforms to really enable you to drive down your costs.

Controlling content

So you've made content available to your users via BYOD – well done. You now need to make sure that you can control the access of that data by users and applications. This is where Mobile Content Management comes to the table.

You'll likely already have invested heavily in a directory that supports numerous other business functions, namely Active Directory if you use Microsoft. At a minimum your MCM solutions need to be governed by your directory; that is, new starters, leavers and movers. If it doesn't, you have some work to do with your MCM and MAM vendor. MCM requires a good level of directory integration and if you're going down the Software as a Service (SaaS) route you're going to need some form of enterprise server to link the SaaS service to your directory structure, securely of course.

BYOD architectures also typically involve an element of Data Loss Prevention, you got it – DLP. If you implement this, you need to make sure that users adhere to the policies both online and offline.

What to look for

As soon as you start to consider BYOD projects you really need to think about EMM. MCM is great but it definitely isn't the only element in a good BYOD implementation. You need to have a broader plan. Think about how you want to procure your service. Do you want an SaaS model or an upfront purchase? How will you manage remote users versus mobile users?

When it comes to getting started, we suggest you include MCM as part of a larger Enterprise Mobility Management (EMM) platform. You can make your life a whole lot easier with a solution that looks at all the technologies we spell out in this guide – namely MDM, MAM, MCM and VDI (gotta love those acronyms!). Choose a software vendor that has a good vision and is financially stable, and check that they can provide the following functions:

- Document collaboration
- Document versioning
- Managed and controlled access to services using your corporate directory (usually Active Directory)
- Data storage in the cloud or on premises
- Audit and reporting capabilities of who did what, where and when
- Remote wiping capabilities if your devices are lost or stolen
- A simple to use interface
- An application that integrates with others on the device (policy permitting)
- Encrypted communication
- A *client* (hardware that accesses the server) for all devices
- The ability to simply share content to all desired users
- Integration into collaboration tools such as Outlook
- Access to files when not connected to a network through Sync capability
- Connection to your network drives and other content management systems
- Two-factor authentication support
- Support and adherence to data loss prevention (DLP) and risk management policies.

Now, this isn't an exhaustive list, but ensure that you have all the items on here as a minimum to make sure you get off on the right foot with a BYOD solution.

Chapter 5

Getting a Helping Hand with Desktop Virtualization

In This Chapter

- Seeing how VDI can help with BYOD
- Building your BYOD initiative with the end user in mind
- Getting sound BYOD advice and best practices

When you think about BYOD, a common question that pops up is: how can I securely deliver IT services to any type of device on any type of network?

Ask this question to a room full of technical folks and this discussion quickly turns into a session that generates a lot more questions than answers. For example:

- The IT security person asks how the data is encrypted and how untrusted devices can be isolated so they don't infect the network.
- The networking person asks what types of connections BYOD devices will connect to and how much Internet, network and/or wireless capacity he'll need to consider adding.
- The desktop support person asks if she'll have to fix personal devices as well as corporate-owned devices.
- The software deployment person asks what software people will use to connect and how it'll be deployed to their endpoint.
- The application team wants to know if they'll need to develop applications that are now mobile friendly, how soon they're needed and who'll be funding them.

- The CIO asks how soon he'll be able to use his iPad at work and his PC at home; lugging around a corporate-owned laptop is too cumbersome.

And this list of questions can go on and on and on. Although these questions are valid and you need to consider them for a comprehensive BYOD solution, don't lose sight of what's most important – the vision and reality of delivering IT services to your business units and customers using any type of device over any type of network. This chapter explores how VDI can help you get there.

BYOD and VDI – The Perfect Fit

VDI (virtual desktop infrastructure; we touched on it in Chapter 3) gives you a method for delivering the corporate desktop to any device, over any type of network – with benefits. The concept is quite simple – take what already works (the desktop and all of its applications) and deliver it securely to mobile, tablet, PC – in fact, any type of device.

That vision has resonated with several companies who have developed turnkey VDI solutions – easily addressing most of the questions asked by IT security, desktop and application teams and, most importantly, the CIO. Those questions that can't be addressed by a product can be addressed with the right planning, testing and "out of the box" thinking.

Take a look at how VDI can help by circling back to the list of questions:

- **IT security.** VDI in its simplest form sends the screen scrapes, mouse movements and keyboard strokes between the client and virtual desktop in the data center. Most VDI vendors send this over proprietary protocol, which has encryption capabilities.

  You can separate network traffic (the second question) with some simple networking and security principles. BYOD devices can be isolated to their own wireless or cabled networks. In addition, network access control

can be used to validate and isolate non-trusted devices on the wire. Firewalls can provide the filtering needed to only allow VDI traffic (the screen, keyboard and mouse stuff) between the endpoint and the virtual desktop.

- **Networking.** Most VDI vendor protocols are optimized for the network, including low-bandwidth and high-latency connections. Using VDI also allows chatty or network-demanding applications to remain in the data center, since they'd go from the application servers to the virtual desktop.

  As for adding network capacity, understanding the current network traffic patterns and proposed traffic needs for VDI is vital. If your network is 90 per cent utilized and you choose to add VDI, chances are you won't have a good experience. It's impossible to drive a Buick through the eye of a needle!

- **Desktop.** A simple BYOD policy and communication on how much help users can expect to receive with BYOD easily sets expectations.

- **Software deployment.** The user owns the device, so in most cases the traditional ways of sending software to a device are useless. You can cast this worry aside – make it user self-service by giving staff downloadable access to the VDI software with simple installation and configuration directions.

- **Applications.** The application runs in the desktop, so no changes here, and no additional development costs.

- **The CIO.** Be smart and build your VDI solution based on defined, realistic business and technical requirements so you can give a realistic completion date. The CIO isn't only the project sponsor; he's also a VDI consumer and most likely your boss.

VDI and BYOD are a match made in heaven (particularly for your remote users), at least to the naked eye. In order to ensure this marriage lasts, you need to be prepared to work hard – plan, test and validate the solution and, most importantly, work through the common technical and operational challenges of BYOD.

BYOD and VDI: Build It and They Will Come . . .

Where do you start with building a BYOD service using VDI? What features and functionality can you deliver? How fast can you get this up and running? Well, it depends . . .

We see quite a few people whose VDI implementation goes like this: buy servers, install the VDI brokering software, build the desktop image, poke a couple of holes in the firewall, install some VDI clients and away they go. This works until a BYOD infects their entire network because they didn't have some level of separation between managed and unmanaged devices, or a BYOD device streaming YouTube brings the wireless network to its knees and knocks off all the VDI users sharing that same WiFi network.

The first step to ensuring that your BYOD roll-out is well received, secure and scalable is simple – plan the work; work the plan. Taking a methodical and thorough approach can ensure that your BYOD implementation using VDI is successful. Good news about VDI travels fast; good news about VDI with BYOD travels even faster. Which means you'll have people beating down the door to get on board.

BYOD and VDI planning and implementation takes time – if you rush it, you may overlook something! Mileage varies, but large enterprises typically take several months to plan, design and validate a BYOD/VDI solution.

Starting with simple VDI lifecycle principles is the foundation for building VDI with BYOD. Then, consider the following issues to help align the design to ultimately provide unified experience for end users:

- **End-user computing (EUC) strategy and vision.** Laying out the roadmap of what EUC services will be delivered and when is key. Make sure your EUC plan aligns with the business objectives and goals, including BYOD.
- **Business/technical objectives and requirements.** Build what your business needs and wants, not what IT wants! What may be the cat's meow for IT may not suit the

needs of the BYOD consumer. Deliver a service that meets the needs of your BYOD consumers.

- **Proof of concept.** A proof of concept helps to validate whether what you're trying to achieve is possible. It also provides valuable information on what to expect from a BYOD/VDI solution.
- **Desktop assessment.** As part of a unified BYOD experience, staff typically use a virtual desktop all the time from any type of device. Having an understanding of the applications and the performance characteristics of the desktop prior to delivering a desktop can help IT properly size the solution and deliver an "equal to or better than a physical desktop" experience to the end user.
- **Plan and design.** Here's where you take the requirements and data from the assessment, and build the design blueprint. Align the design with requirements, build what's achievable and realistic, and leave no stone unturned. Build the design in a strategic way that can scale up and out very easily. And don't forget to ensure the BYOD requirement is considered in each design phase. Some of those phases include networking, security and compliance, image lifecycle management endpoint, access and authentication, and availability and resiliency, just to name a few.
- **Build and validation.** The only way to ensure your design will work is to build a prototype and conduct design validation and performance testing. This is where the rubber meets the road – test and validate key aspects (both for functionality and scalability), including the use of BYOD. Functional test plans need to include testing and validating BYOD devices accessing VDI resources.
- **Pilot.** Welcome to the test drive phase. During the pilot, identify BYOD users and let them do some "real world" production testing. The feedback from your BYOD users can let you know if you've met the mark with the BYOD solution. Solicit feedback – don't assume no news is good news; take the feedback and act upon it to fix issues or align the needs of the business with the BYOD solution. (Read more on piloting in Chapter 6.)
- **Production.** Don't simply open the BYOD floodgates; gradually and systematically get your BYOD and internal users on board. Take the time to ensure that the VDI

> system and dependent infrastructure can handle a gradual increase in user demand and correct as needed. Focus on the end user experience – if that suffers, so will your BYOD program and adoption of VDI!

If you've done VDI designs (with or without BYOD) before, most of this should be old hat. Most of the tuning, optimization and design for VDI apply for VDI with BYOD. That includes image optimization, application delivery, host sizing and performance, and so on. Just make sure every design decision aligns with the business and technical requirements – including BYOD.

While this chapter covers how to approach BYOD with VDI, many of the steps listed above apply equally to any EMM solution you plan on rolling out to help tackle BYOD.

Chapter 6

Rollin' Out EMM and VDI with BYOD

In This Chapter

- Getting some rules and regs in place
- Security and policy considerations for BYOD
- Testing the water with a pilot
- Rolling out your BYOD initiative

With any type of program, whether you're leveraging MAM, MCM or VDI, you need to have rules and standards, checks and balances, and policies and procedures to keep things in line. The last thing you want is an out-of-control BYOD program – it's like letting zoo animals out of their cages and running wild with only a simple chain-link fence keeping your data inside your network.

In this chapter, we explore how to keep BYOD under control and secure. We also cover how to conduct a BYOD test-drive and later roll out the initiative in full.

Following the Rules of the Road for BYOD

Some simple guidelines can help lay down the law with BYOD, keeping things safe, secure and well-managed. Here are some things to think about from a policy/procedure perspective:

- **Acceptable use policy.** You need to remind users that, even with BYOD, they're still responsible for complying with the company's acceptable use policy. Although the device may not belong to the company, other assets and services used by the BYOD user still are.

  

  Ensure users connecting to or using any asset of the corporation understand and accept the terms and conditions of acceptable use by presenting them with a disclaimer or legal notice when connecting to company IT services.

- **Authentication and auditing.** A key element with BYOD is ensuring users are who they say they are, monitoring and tracking what network(s) their BYOD devices connect to, and how they access and use applications. Auditing mechanisms need to include methods to capture client information (device ID, IP address and so on) and typically move from the traditional corporate-owned endpoint into the VDI session or MAM/MDM session.

- **Supported devices and features/functionality.** Most companies who have BYOD typically provide a set of minimum requirements and/or an authorized list of BYOD devices that can be used in a BYOD program. This helps with end user supportability and operational issues, as well as keeping any feature/functionality communications crisp and clear – the take-home point is that the end user, as well as the company, knows exactly what services can and can't be delivered.

- **End user support.** Companies choosing a BYOD model can formulate a strategy and support statement around what level of support they're planning to provide for customer-owned devices. This is a paradigm shift from supporting corporate devices – since the user owns the device, the ability to service the asset becomes a privilege and is no longer a right.

  In the case of hardware failures, the ease of moving the user to another device is a huge benefit, but the burden of repair is now on the end user.

  At times, this can be an unexpected expense – you may want to consider taking out a support contract for users.

To Secure or Not to Secure, That is the Question . . .

IT Security – the group responsible for keeping data and services secure – are sometimes considered a nuisance when they shoot down a project or initiative that you feel could be a significant benefit to your company. Some people feel these folks burden us with all the "extra" stuff we have to bake into our base desktop images and endpoint. Sometimes we think they just don't understand or care about the business.

But that's dead wrong. With a little education and including them *early* (yes, that means from the beginning), you can easily mitigate this common challenge. And, let's face it – IT Security has the ultimate responsibility to ensure things are secure, data stays where it needs to stay, and employ sensible risk management to keep the bad guys away.

In this section, we focus on some key things to consider when securing your BYOD implementation.

Network access

Customers who have a BYOD not only need to consider securing data, but also the path to get to their desktop and the data. Work with your security team to develop an access strategy that keeps only the necessary traffic from unmanaged BYOD endpoints entering your data center. This may include additional layers of security such as two-factor authentication that can ensure the user who's connecting from their iPad is really who they say they are.

Using a BYOD dedicated network with authentication enables users who are part of a BYOD program to authenticate to an authorized network.

Since the security of a BYOD endpoint can't be effectively assessed or guaranteed (because the user owns the device), putting BYOD on the trusted network opens the doors to a myriad of security concerns and exposes critical resources to a potentially unsecured endpoint.

Clipboard and printing capabilities

Another item to consider is the movement of data into and out of the virtual desktop session. One way to move data between the endpoint and the virtual desktop is the clipboard. Discuss cut/copy/paste features with your IT security group. In most cases this is disabled. Most solutions have built-in controls to manage clipboard access through GPOs (group policy objects) if granular control of the clipboard is needed.

Another mechanism for data movement is printing, so you need to consider whether to allow users to print sensitive documents to a printer directly attached to the endpoint. This is one of the more challenging aspects of a BYOD from a planning and security perspective. Business units may need to print to locally attached printers, but IT security may not allow users to print data outside of network printers. Again, consult your business units and IT security team to determine the best approach based on your requirements.

USB mass device support

Similar to printing, USB device support also provides a mechanism to move data between BYOD devices and virtual desktops, virtual workspaces or other assets within a corporate data center. Having a mechanism and corporate policy on USB mass storage devices is important.

If you need data transfer, look into alternate auditing and compliance mechanisms, such as data loss prevention tools, to ensure that sensitive data stays within the boundary. However, these tools do provide a noticeable amount of additional compute resources. Carefully plan your implementations, taking into account the impact of DLP (data loss prevention) and data movement between endpoints.

Defense in depth

In addition to controlling traffic coming into the network, controlling access to resources is equally important. Typical implementations provide "unrestricted network access" to other resources on the corporate network.

A fault in one layer of security (such as an improperly configured perimeter firewall or endpoint/device analysis) could expose the corporate network to a system vulnerability. As an additional layer of protection, secure the BYOD session to provide an additional layer of protection for these types of vulnerabilities.

Device compliance

With some BYOD technologies, you may need to enforce specific endpoint standards – such as RAM, CPU and/or anti-virus protection. In some cases, this would require a deeper level of inspection typically provided by endpoint analysis technologies.

With BYOD, this topic becomes more sensitive – since the company no longer controls the asset, but you still need to mitigate any risks that may be introduced from an unmanaged, potentially insecure and contaminated endpoint. If you choose not to do endpoint inspection, strictly control and monitor network traffic and peripheral access instead.

Testing, Testing: Trialing with the Pilot

Before your BYOD solution goes prime time, you need to conduct a controlled pilot. Select a small group of users that can use their BYOD devices and test-drive your EMM/VDI solutions with BYOD. Make sure your selection of users can test all the access methods. Ensure the user group represents a diverse selection of BYOD devices, so you can test as many BYOD scenarios as possible.

The feedback from the users about end user experience and usability is critical. You can use this information to fine tune or adjust the solution as needed. Additionally, monitoring the performance of the virtual desktops and dependent infrastructure gives you a holistic picture of how things are performing.

Use the pilot to shake out the issues, get user feedback and refine your BYOD. You'll learn the most from this phase of the deployment, so don't ignore the data – use it to refine a rock-solid BYOD solution!

Crunch Time: Planning and Rolling Out

Once your pilot is underway and you have some real world data, you can develop and fine-tune your plan on how to roll out your BYOD solution through VDI and EMM.

The plan needs to be simple, sensible and realistic. A gradual, controlled rollout of BYOD services minimizes the impact on other departments – such as your help desk or support teams. If a gradual increase in infrastructure resource usage and demand goes unchecked or is not appropriately accounted for, it can add gradual stress on your BYOD deployment. If this is the case, you can stop, try a different solution, and then continue the rollout. If you have to bring a significant amount of users in at once, make sure the help desk is well staffed to handle a large number of support calls.

This is BYOD – which means the support teams will be dealing with lots of devices they've never touched before. Most of the users probably won't have read any communications or directions about BYOD, and need that extra hand-holding to get their devices online and connected.

Keep an eye on the network, storage, virtual desktop, compute hosts and dependent infrastructure – proactively finding an issue and fixing it prevents large-scale outages and keeps the BYOD user happy. What more could you wish for?

Chapter 7

Ten (Okay, Seven) Useful Resources for BYOD

In This Chapter

- Bedtime reading with whitepapers
- Keeping ahead of the game with the latest reports

Looking to scope out your BYOD project some more? Well here are our picks of the great resources you can leverage to help ensure that you start out in the right direction.

- **Peer Research Report – Insights on the Current State of BYOD:** `www.intel.com/content/www/us/en/mobile-computing/consumerization-enterprise-byod-peer-research-paper.html`
- **Forrester Research, Inc., Report (July 2013): Prepare Your Infrastructure and Operations for 2020 with Tools and Technologies:** `www.forrester.com/Prepare+Your+Infrastructure+And+Operations+For+2020+With+Tools+And+Technologies/fulltext/-/E-RES98541`
- **Forrester Research, Inc., Report (November 2012): Building The Business Case For A Bring-Your-Own-Device (BYOD) Program:** `www.forrester.com/Building+The+Business+Case+For+A+BringYourOwnDevice+BYOD+Program/fulltext/-/E-RES61616`
- **Implementing a BYOD Strategy: Ten Mistakes to Avoid:** `www.eweek.com/mobile/slideshows/implementing-a-byod-strategy-10-mistakes-to-avoid/`

- **The BYOD Opportunity – Whitepaper:** www.vmware.com/files/pdf/view/VMware-BYOD-Opportunity-Whitepaper.pdf
- **Mobile Secure Workplace Design Considerations Guide:** www.vmware.com/files/pdf/view/Mobile-Secure-Desktop-Design-Guide.pdf
- **Mobile Secure Workplace Online Bootcamp Series:** http://communities.vmware.com/community/vmtn/view/msdbootcamp


EXPANDING THE POWER OF VIRTUALIZATION
From the data center to the cloud to mobile devices.
VMware, the industry-leading virtualization software company, empowers you to innovate by virtualizing infrastructure and streamlining IT operations. With VMware technology, you can efficiently and reliably deliver services that are accessible on demand from any device, anytime, anywhere—making your organization more agile, more responsive, and more profitable.
Visit vmware.com to learn more.
vmware®
Copyright © 2013 VMware, Inc.

Embrace BYOD and retain your sanity in the process

Corporate owned IT is a thing of the past. BYOD is a reality and employee owned devices are making their way into your organization. You can fight this trend or you can embrace it. If you embrace it, you have some serious challenges ahead not least of which are how you're going to manage BYOD devices, secure data and keep your costs under control.

This book spells out everything you need to think about in order to successfully support BYOD and enables you to retain control and your sanity in the process!

- ***Set your BYOD plan in motion* — *discover what to think about when building your BYOD plan***
- ***Discover what the options are* — *understand the pros and cons of common technologies used to tackle BYOD***
- ***Get your hands dirty* — *find out common tips and best practices that you can leverage around VDI and EMM (including MAM and MCM) for BYOD***

Open the book and find:

- **A look at BYOD — where it all began and why you should care**
- **How to build the plan and make the business case**
- **An overview of different approaches to tackling BYOD**
- **Best practices around how to get started**

Charles Barratt is Business Solutions Architect for VMware within the Accelerate Advisory practice. Charles has 18 years within IT from Consultant, Architect, to Board Director and then VMware. **Courtney Burry** is a Director of Product Marketing at VMware in the End User Computing Group. She has been at VMware for the past four years in product marketing and has worked extensively around VMware's Horizon Suite of products including Horizon View, Horizon Mirage and Horizon Workspace. **Justin Venezia** is currently a Consulting Architect with VMware's End User Computing Global Professional Services Engineering team, developing advanced and customized solutions for VMware's End User Computing customers.

FOR DUMMIES®
A Wiley Brand

ISBN: 978-1-118-83227-1
Not for resale