The New BYOD:

Best Practices for a Productive BYOD Program

WHITE PAPER

vmware®

Overview

Introduction

Over the past few years, the term "BYOD" has become a popular term in the workplace as mobile devices in the enterprise have become common for many organizations. However, aside from being trending term, its meaning is more than just an acronym. BYOD is one part of a much larger, deeper-rooted trend: The consumerization of IT, which can be traced back to the early 2000s. Around that time, most everyone had a personal computer, which enabled them to work from home after hours – and to realize the benefits of using the devices that they had carefully chosen and were comfortable using, rather than the corporate devices their IT departments had issued them.

BYOD and the consumerization of IT continued to grow as devices became cheaper and more connected. Where IT leaders were once solely concerned with reining in all the unapproved devices accessing the corporate network, a recent Intel and readwrite report shows 49 percent of U.S. IT managers "strongly agree that BYOD improves worker productivity." The next era of BYOD has arrived, and IT departments are thinking about it as a strategic value-add rather than a threat that needs to be controlled.

"Businesses are getting smarter about how they're doing BYOD," says Nick McQuire, CEO of the Global Enterprise Mobility Alliance (GEMA). "Pushing device and connectivity costs to employees was the original attraction. While that is true in some cases, many companies have found there are a lot of nuances to the business case," McQuire says. One of those is the sheer number of devices entering enterprises today. Pew Research Center data shows mobile device ownership has skyrocketed over the last few years. The average user already owns multiple mobile devices.

Whether a company supplies devices or not, employees will have other personal devices that they want to connect to the corporate network. Because most users today own multiple devices, business leaders and IT departments must create a strategy for managing and securing the BYOD devices that will inevitably enter the workplace. BYOD programs provide users with a secure, IT-approved method for accessing corporate resources from their personal devices.

Beyond providing essential security, business and IT leaders who have embraced BYOD have realized its potential to add value to a number of business areas. These companies, McQuire says, are "better at understanding the benefits and understanding why you do BYOD. They're good at linking BYOD to overall business initiatives. IT departments that recognize the need to enable security and understand the driving forces for it, have a strong awareness of the technology an employee uses on a daily basis. While mobile devices are one type of device an employee uses, IT departments have widened this scope to also consider desktops, laptops and rugged devices as not only manageable endpoints, but endpoints worth securing. While it is difficult to quantify exact increases in productivity resulting from BYOD, there are several immediate benefits. Implementing BYOD programs for workers that are not provided corporate devices will in most cases substantially increase an enterprise's mobile-accessible workforce. According to Gartner, BYOD could expand the total number of mobile users in an organization by 50 percent or more. If all of a worker's devices are corporate-connected, accessibility increases even further.

Today's savviest enterprises are leveraging BYOD as a tool to drive mobile accessibility, increase IT oversight and enable employees to complete a business task at a moment's notice, on whichever device is nearby. This whitepaper will outline the basic measures business leaders and IT professionals are taking to turn their BYOD programs into major productivity gains.

Think of BYOD as an Enabler

IT departments need their BYOD users to enroll in Enterprise Mobility Management (EMM) to minimize unauthorized access to corporate networks and keep the organization safe from security breaches. To get employee buy-in, business leaders and IT personnel must educate employees about how enrolling in the program will benefit them.

First, position BYOD as a perk. BYOD offers employees the choice to work how they want, on the devices they choose (or the ones they already have). To both the employee and employer's benefit, employee devices are likely to be customized with apps and productivity tools that users have already identified as helpful. Highlighting the flexibility and choice BYOD offers will help ensure the program is perceived as one that enables employees to do their jobs more productively and more efficiently.

Beyond providing employees with choice, BYOD programs can help employees and businesses as a whole achieve overall business goals. Think about how BYOD can further existing organizational goals. Could your sales force use their mobile devices in the field to engage prospects and customers? Does your organization's global reach make it vital for employees to receive emails around the clock? Are your employees interested in teleworking or alternative work schedules? A BYOD program can help streamline business processes, drive sales and improve customer engagement.

GA Communications Group, a firm based in Chicago, has successfully implemented a BYOD program that gives users distinct advantages. Technology Director Jason Dittmer says the main draw is the ability to access daily timesheets for logging billable hours, which must be completed daily, through a virtual private network (VPN) connection. The VPN profile is pushed to user devices through a web app. In the app, employees can fill out and submit their timesheets. "In the agency world, timesheets are king," Dittmer says. "They're a big part of everybody's day, so if you run out the door and you're on the train and forgot, you can pull out your phone, connect to the VPN and enter in that time."

In the future, Dittmer plans to use iBeacons and a scheduling app to simplify conference room scheduling. If an employee needs a conference room, he or she will be able to connect to the iBeacons in the office, and the schedule will display on his or her phone.

Identifying how BYOD will enable employees can help drive adoption and create a positive image of the program. But before business leaders and IT professionals can take this stance, they must make sure that what is most important to them – IT oversight and top-tier security – is firmly in place.

Get the Right Tools in Place

The introduction of the iPhone® disrupted the enterprise mobility market and created a ripple effect that is still apparent today. Employees began bringing their personal iPhones to work, favoring them over their old corporate devices. Some of them found ways to access their email and other resources, and IT personnel scrambled to rein in unauthorized access and stop the threat of data loss. IT personnel couldn't stop the influx of iPhones and other smart devices, so instead they had to find ways to provide secure access to corporate resources to an ever-expanding array of device types.

Before rolling out a BYOD initiative, IT personnel should prepare for the influx – in terms of both network architecture and management. IT personnel must ensure their network architecture can handle increases in Wi-Fi traffic. They must also ensure their existing device management platform can scale to accommodate management of employee devices. If IT has already invested in an EMM system, they should ideally be able to leverage existing policies that have been developed for corporate devices, extending the necessary policies, apps and content from the same console.

In a BYOD scenario, the devices that enter your enterprise will vary greatly. An EMM solution that only supports a limited number of device types and operating systems will at best only enhance the productivity of some employees. At worst, it will lead to employees with unsupported devices finding workarounds and exposing enterprises to security breaches. An Mobile Device Management (MDM) solution such as AirWatch, which supports all major device types and platforms, will encourage universal enrollment and will be the best prevention against data loss.

It is also important to find a solution that can keep up with the pace of innovation in the market. Mobile operating system updates are released as often as every two weeks, and new devices are introduced frequently. Each new device type or OS update is a chance for a potential security vulnerability to arise. AirWatch is OEM-agnostic and can provide same-day support for all major device types and operating systems. AirWatch also provides IT administrators with a single console that provides oversight of all devices, whether they are corporate-owned, BYOD or shared devices. The multitenant architecture of the AirWatch platfrom enables administrators to set limits on management of employee devices, while fully managing corporate-dedicated devices.

However, some organizations will not want to provide access to all device types and operating systems, instead choosing to give employees a list of approved device types that the organization has deemed secure. AirWatch offers the ability to restrict access to content based on device type, operating system or operating system version. AirWatch can also limit the number of devices a particular user can enroll. This enables organizations to set boundaries and protect their networks from excess devices until the architecture is in place to handle added traffic.

BYOD planning is just one piece of a much larger enterprise mobility puzzle and should be considered in context. Technology is cyclical in nature, and when it comes to addressing needs in the market, a point solution or vendor will often quickly pop up and fill the void. Rather than implementing a stopgap solution to plug potential data leaks

and stop unsupervised devices from entering the corporate network, today's most mobile organizations have found comprehensive solutions that can scale as their mobility initiatives expand.

For instance, your first priority may be to provide email access on employee-owned devices. But inevitably, employees will grow to rely more and more heavily on their mobile devices, so IT personnel need to consider how they will be expected to enable BYOD beyond email. Think ahead and purchase a solution that can support apps, content access, secure connections to enterprise repositories and seamless intranet browsing on employee-owned devices.

The hard part comes after the technology is in place. After IT personnel have selected the appropriate tools, they must consult with business leaders and other relevant groups to develop policies that address the legal and privacy implications of the BYOD program.

Communication is Key: Establish Clear BYOD Policies and Terms of Use

An April 2014 study showed many employees still don't take BYOD seriously. BYOD policies can help ensure employees opt in by outlining both the risks unauthorized access poses and the benefits BYOD programs provide. The BYOD policy should clearly define the rules of the program, in accordance with government regulations and company security policies. It should also clearly outline what IT will be able to see and manage on personal devices, so there is no fear of personal data being compromised or exposed. Before releasing the program organization-wide, IT departments should get executive-level buy-in and input from a variety of departments to ensure all concerns are heard and all needs are met.

Privacy is a major concern for many employees and may be a hindrance to enrolling in BYOD programs. AirWatch enables companies to separate corporate and personal data on devices through customizable privacy policies that can be based on device ownership type. Administrators can configure policies to prevent data collection from personal email, content or applications on an employee-owned device. GPS location, personal user information and telecom data can also remain private, and employee-owned devices can be protected from a full device wipe or remote control. AirWatch also allows businesses to mitigate risks that are presented when employee-owned devices are accessing corporate resources. With custom Terms of Use (TOU) agreements based on user role, organization group and device platform, users can be informed about data that will be captured and what they are allowed to do with the device.

Mohegan Sun, a casino and resort in Connecticut, recently implemented a successful BYOD program. Director of Information Technology Danny Lynn says it was not in the budget to upgrade company-owned employee devices from iPhone 4 and 4S devices this year, so he created a BYOD program that would give employees the option to take over the contract, upgrade their devices and transition to BYOD.

As Lynn began outlining the specifics of the program, he realized he would need a BYOD policy that communicated the rules and upgrade options and also enabled enrollment of other personally-owned devices. Lynn says several employees with company-owned smartphones had requested access to company email on their personally-owned iPads. Employees who were not provided corporate devices also requested the option to enroll their personal devices.

Lynn and Mohegan Sun's vice president of IT wrote a BYOD policy and terms of use agreement from scratch that was customized to the employees' needs and use cases. The team sought review from their legal team, and once it was approved, they launched the program. The contract is brief and to the point, Lynn says: It clearly outlines what administrators will be able to see on employee-owned devices and gives the Mohegan Sun IT department permission to wipe compromised devices. Though Lynn did not experience pushback from employees who were worried about their privacy, "some employees have been worried about losing everything, so we encourage them to do backups as needed," Lynn says.

To connect BYOD devices to the network, employees can now review the contract, install the AirWatch® Agent, and accept the Terms of Use, which Lynn customized through the AirWatch console.

GEMA CEO Nick McQuire recommends starting with a basic BYOD policy framework and customizing it to meet industry, geographical or organizational needs. "There are a number of different BYOD policy tool sets available from mobility specialists and GEMA members across the world such as Vox Mobile," says McQuire, who also recommends Gartner as a good source of guidance. "Companies can start with a baseline template and then craft their own addendums and inputs from there."

Jason Dittmer, Director of Technology for GA Communication Group, researched online and found a suitable BYOD policy. He then sent it to his legal team for revisions. Then, he and his IT colleagues came up with a customized method to help ensure employee-buy in.

The small, Chicago-based firm makes BYOD a part of company culture from the outset by introducing the company's BYOD program and policy during the onboarding process. "Anybody who wants to be part of the network is given instructions for enrolling into MDM or is sent to IT for set up," Dittmer says. Currently, GA Communications Group is enabling access to secure Wi-Fi, email, VPN and a company app catalog.

Part of the set-up process is showing employees how to access the self-service portal, where they can see all managed aspects of the device. For employees worried about IT collecting personal data, the self-service portal has helped convince them to enroll, Dittmer says. Through the self-service portal, employees are able to see what IT is managing on their devices.

Here are a few links to online resources for BYOD policy templates, which can serve as a good starting point for a customized policy that suits your organization's needs:

- TechRepublic BYOD Policy
- White House Bring Your Own Device Toolkit
- IT Manager Daily BYOD Policy Template
- Gartner BYOD Mobile Device Policy Template
- Vox Mobile BYOD resources page

Transitioning From Corporate-owned to BYOD:Provide Employees with Options

If you are gradually transitioning away from corporate-owned devices to a primarily BYOD model, providing employees with several options may help ease the transition. Mohegan Sun casino and resort has implemented a plan to gradually transition its users to a BYOD model.

"When the iPhone 5 came out, employees wanted to upgrade to the latest device," says IT Director Danny Lynn. Lynn provided employees the option to buy out their mobile contracts from Mohegan Sun, upgrade their devices, and enroll in the organization's BYOD program. Though the upgraded hardware becomes the employee's property and responsibility, Mohegan Sun still covers the monthly bill. "Employees wanted a choice, and that is what drove us to implementing our BYOD policy."

"From that point forward, any hardware upgrades, repairs, problems or anything related to the phone itself becomes the employee's responsibility," says Lynn. "This is a good thing for companies because you are reducing your future capital outlays for phone upgrades." Employees that do not want to cover the cost of an upgrade simply keep their existing devices.

While partial or full bill reimbursement may help ease the transition from corporate-owned to BYOD, covering employee cell phone bills has the potential to negatively affect an enterprise's bottom line.

A telecom expense management program can ensure data plans stay within budget. AirWatch has built-in telecom expense management features, such as the ability to restrict downloading documents to Wi-Fi only or restrict access to native features such as video calling, which can consume large amounts of data. AirWatch also partners with telecom expense management providers such as Wandera, which offers data compression and management.

Before the BYOD rollout is complete, IT personnel should consider if and how they will support employee-owned devices.

Offer Assistance: IT's New Role as Consultant in a BYOD Environment

The influx of personal mobile devices into corporate networks – and the cloud-hosted data they access – has fundamentally changed the way people work, and by necessary extension, the way IT departments operate. Mobile offers an opportunity to work more efficiently. Efficiency increases when people are enabled to access email or perform work-related tasks across all the devices they own. It sounds simple, but providing access to multiple device types – and often to multiple devices per user – creates a myriad of new challenges for IT departments, says VDC researcher Eric Klein.

"When an organization has to manage those devices in a way that's going to be cost efficient and protect them from the risks associated with opening up their corporate data on these platforms, there's a whole range of issues that [they] have to deal with," Klein says. MDM controls can take care of the basic issues, such as offering a way to wipe corporate data or lock a device that's left behind in a cab or on a plane. "But there are so many other things an organization has to consider."

GA Communications Group technology director Jason Dittmer says transitioning to the cloud has been a major consideration in the company's BYOD deployment. "We've made a huge push to move a lot of our internal systems to the cloud. In the traditional settings, everybody was guarding what they had to manage in that server room." Today's IT departments are more focused on managing an array of services, such as cloud storage providers and MDM, Dittmer says.

IT departments managing BYOD programs are also routinely asked to troubleshoot on a much wider range of devices. According to Dittmer, the way IT interacts with employees has changed as a result. "BYOD is a huge shift for how employees work and are used to interacting. Because there are so many more variables in a BYOD setting, the IT department does become more of a consultant."

Some organizations have set up an IT genius bar where employees can come during certain hours for help connecting their devices or troubleshooting issues. Though Dittmer's organization is small enough to allow users to drop by the IT department anytime they have questions, he says using a simplified management platform for both BYOD and corporate devices has given his department the time to take on a consultative role when needed. He says the concept has also helped broaden his and his colleagues' IT knowledge.

"I think people in an IT department have to have a broader, more in-depth range of knowledge because now they're managing so many different systems," Dittmer says. "Now nobody [in our IT department] is doing one thing anymore. All four of us have to know all these systems." For organizations that do not have the resources to provide IT support for employee-owned devices, the AirWatch self-service portal is a useful tool where employees can ensure their devices are in compliance and troubleshoot any issues.

Now that you've empowered employees to manage and troubleshoot their own devices, what's next?

Prepare for the future of BYOD: BYO Everything

"The way we work is changing," says VDC researcher Eric Klein. "Not just the next generation of employees – all of us."

The mobile revolution has redefined business. It is hard now to imagine not being equipped with at least one or two mobile devices as essential working tools. But there is more change ahead. A new IP-connected device seems to enter the market every day. Soon, many of these devices will be considered essential and picked up – or put on – just before we head out the door to the office.

And while the Internet of Things offers tremendous potential for revolutionizing business processes, it also introduces new challenges and security threats. IT must consider these challenges and threats now. Implementing a solid enterprise mobility management platform to handle a BYOD program along with corporate-owned and line of business devices is the best way organizations can prepare for the hyper-connected future.

It is also a tremendous opportunity for IT leaders to demonstrate their value. IT is at a crossroads: With more technology entering the workplace than ever before, IT leaders have an unprecedented opportunity to be proactive and become central to business strategy. "For a long time, IT has been relegated to being behind the scenes," Klein says. "Mobile changes the equation entirely; it's a great opportunity for IT to actually reassert itself in the business. Now that the ability to integrate devices into your business is apparent, it has opened up a whole new world of opportunity."

Additional Resources

Sign Up for a Hands-on Lab

http://vmware.com/go/try-airwatch-hol

Visit Our Website

www.vmware.com/enterprise-mobility-management

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com