WHITE PAPER — **FEBRUARY 2017**

THREE-PART GUIDE TO DEVELOPING A BYOD STRATEGY

vmware® airwatch®

An IT Architect's Guide to Implementation Considerations and Best Practices When Developing a BYOD Strategy

As the consumerization of IT continues to grow, so has the popularity of Bring Your Own Device (BYOD) programs in the workplace. Organizations have recognized that enabling employees to use their personal devices to access company resources not only reduces costs, but also increases employee productivity, effectiveness and job satisfaction. BYOD enables organizations to drive mobile accessibility by enabling employees to integrate their personal and work lives to be productive on any device, any time and anywhere.

Although today's savviest enterprises are leveraging BYOD, common challenges such as user experience, employee privacy, and program functionality are inherent. If not properly addressed, these issues can lead to low adoption rates and even program failure. This document is intended for organizations that are contemplating implementing a BYOD program or for business leaders and IT personnel already in the planning stage. This guide assumes that your organization already leverages an OEM-agnostic enterprise mobility management (EMM) solution that can accommodate both employee- and corporate-owned devices. Specifically, it addresses three components of a comprehensive BYOD strategy that will not only help administrators adequately prepare, but also build, implement, and sustain a successful program.

PART 1:

Outline a Policy

Device-based Considerations

User-based Considerations

Application-based Considerations

PART 2:

Prepare the Infrastructure

Email Access

Corporate App Access

Compliance

PART 3:

Develop an Implementation Plan

Schedule Pilot Test – Phase Rollout

Provide End-user Support

PART 1: Outline a Policy

For the organization, a BYOD policy needs to manage risk and maintain IT compliance and security. For the end user, it should protect the privacy of personal information stored on the device, and be seamless enough to promote productivity. Before you get started, you'll need to outline basic policies and rules based on device-, user- and application-level considerations that will make your program as effective as possible. With custom Terms of Use (TOU) agreements based on user role, organization group and device platform, users can be informed about what data will be captured and what functions enterprises can access on the device.

Device-Based Considerations

A BYOD program entitles users to bring in any device of any operating system or platform to access corporate applications and data. This can include personal laptops, mobile phones, tablets and/or wearable technology. As administrators of the program, you will need to specify:

- What types of devices will be supported
- What operating systems and versions will be supported
- The maximum number of devices allowed per user

Minimum Device Security

Once a device is activated, administrators can set the minimum device security requirements for connecting to corporate resources, without removing access to personal applications such as camera, music or social media. Some of the common minimum device standards to consider include:

- Passcodes – the first level of security to prevent unauthorized access. You can specify length and complexity levels.
- Restrictions – restrict access to specific features or services, i.e. browser or Bluetooth.
- Certificates – used to validate the user and device. You can associate functions to the certificate so that those functions can be removed if the certificate is revoked.

Terms of Use

With the melding of personal and corporate data on one device, Terms of Use agreements need to be drafted, shared, and electronically signed so end users are informed of the business' rights.

User-Based Considerations

User Privacy

The biggest objection to BYOD adoption is the concern for user privacy. From the organization's perspective, enabling an employee to access company apps, data and information from a personal device requires strict security measures, such as the need for a passcode and certain restrictions. For users, the main concern is that their personal data and apps may

become visible and even manageable, resulting in a breach of privacy. IT administrators should carefully think though the rules and policies associated with user privacy, including what data and activities IT may have access to and which device functions can be managed by IT. To ensure that privacy settings are not perceived as violating a user's personal privacy, it's important to develop a clear end user communication plan.

Factors to consider include:

- What admin controls IT has over an activated device
- Exactly what data can be seen or monitored
- Who in the organization can assist with privacy inquiries

User Groups

Frequently, there can be a need to offer varying levels of accessibility or restriction based on level of employee responsibility or job title. IT admins can create user groups with tiered policies for security, privacy, and app distribution based on device ownership. User groups enable you to:

- Assign varying access levels to user groups for security reasons
- Group users based on role/function/division/location, etc.

Application-Based Considerations

Applications used in the enterprise often contain sensitive business data, and providing secure access to these applications from an employee's personal device is paramount. It's necessary to create policies to determine not only which apps will be accessible to employees, but more importantly, how those applications will be accessed to best protect company data.

Recommended Application Access Methods

There is often more than one way to access business data on a mobile device, and this can become a challenge for IT. For example, corporate email can be accessed via the native email application, a third-party email application, the device web browser, or via a virtualized application or desktop that is running in the data center. Many SaaS applications provide native mobile versions of their applications, as well as access via the web browser. Since security is critical, there is often a balancing act between securing application data and providing the optimal user experience. A common way to achieve this is to enable native versions of the applications for the OS and use security layers such as application management policies, device management policies and identity and access management (IAM).

The key decisions to make around application access methods include:

- Provide a framework of access methods for all apps enabled for BYOD users
- Provide a seamless experience for app access on the device platforms used
- Use device management, application management, and IAM policies to secure access to corporate applications

Application Risk Profile

When creating an application policy for BYOD, beware of treating all enterprise applications as equals. While all applications are used for a business purpose, they all have very different risk profiles. For example, an application for travel and expense reporting contains less sensitive data than an application that contains earnings forecasts or a client list. From a BYOD perspective, applications with lower-risk profiles should be made readily available to any user on any device. This will reduce the barriers to adoption, and enable users to see the value of accessing enterprise applications from the convenience of their own device. IT can provide seamless security measures for this, such as challenging the user for a secondary form of authentication.

For those applications that contain very sensitive business data, it is recommended to set stricter application and device-level security policies and establish a higher trust between the user, the device and the application before gaining full access.

The process of taking a device from an untrusted state to a secured access state should be transparent for a user. The enterprise application portal should provide a simple workflow for users to activate a higher trust profile on the user device to meet the level of trust required to access these secure applications.

Factors to consider related to application risk profiles include:

- Determine whether business-critical data is in the applications made available to BYOD users
- Consider which applications can be accessed without any trust between the user, device and organization
- Determine which applications need that additional level of trust between the user, device and organization
- Outline the appropriate authentication methods enabled for these applications, such as multi-factor or step-up authentication
- Provide a seamless way to take a device from an untrusted state to trusted, with an intuitive workflow for end users

Part 2: Prepare the Infrastructure

Now that you have considered the fundamental rules for device- and user-level restrictions, it's time to configure parameters at a deeper level to set rules for content access, as well as compliance and remediation. These technical considerations are crucial to ensure that corporate data is kept secure by restricting access to only those devices that meet corporate security requirements.

Email Access

Employee access to email is critical to the success of a BYOD program. This functionality must be secured so that corporate email remains within the managed app set on the device. For this function, admins need to consider:

- What method is approved for employees to access email, such as an account that can be removed if the employee leaves the company
- Ways to mitigate unmanaged device access or unauthorized mail clients
- Which applications can open, edit, save and share email attachments

Corporate App Access

Employees rely on apps on their devices to maintain productivity. Apps can come in many different forms such as web, SaaS and mobile apps, and can be distributed in two ways: a self-service application access (users may select apps through an enterprise app catalog and download onto their device) or by admin-provisioned app access made available to users automatically by IT, often due to a licensing or approval requirement.

The decisions that need to be made for application access include:

- Which apps will be managed by IT and which ones will not
- Identifying which apps are available to users through a self-service catalog
- Identifying which apps will be automatically pushed to activated devices
- How to manage the reimbursement for purchases from a public app store

Compliance

Compliance rules are a set of rules that ensure that all devices abide by the BYOD policy. Compliance violations can vary in severity, ranging from a missing passcode to a jailbroken device attempting to access sensitive corporate data. Common violations in a BYOD program include: not accepting terms of use, unauthorized passcodes, device last seen/ checking-in, compromised status and having an unsupported OS version.

For maintaining compliant devices in a BYOD program, admins should consider:

- What compliance rules will be necessary for your company
- A compliance escalation process for continual violation of set policies (i.e. notifications to IT or manager, blocking functions on device, revoking access to apps, or even a wipe of enterprise data from the device.)
- Measures to enable users to remedy their own basic compliance violations through warning, notifications and instructions for issues of lesser severity

Part 3: Develop an Implementation Plan

Once you've developed a comprehensive BYOD policy and thought about how to prepare the infrastructure based on that policy, the last thing to consider is how to roll out the program to the company and drive adoption. This section outlines recommendations for a successful company-wide implementation.

Conduct a Pilot and Phase the Rollout

A pilot phase will help validate features, functionality and use cases within a small group in your organization. To make the most of your pilot program, we recommend these general best practices:

- Select a pilot group and collect targeted feedback on each component of the solution. Where possible, the pilot group should include a representative cross-section of the workforce to ensure diverse feedback.
- Establish a structured timeline by defining what functions need to be tested and when.
- Test all instances and functions—such as the activation process, email, and access to internal docs and apps—across different OSs and device types.

A phased rollout helps avoid overwhelming users with too much at once and progressively shows the benefits of the program.

- Phase the availability of capabilities and ensure it is completed before full implementation of the program.
- For each phase, determine user groups given access, supported devices, policies applied, and timing.
- Rollout may be phased based on geography, department, job function, etc.

Provide End-User Support

Once you begin the rollout process for your BYOD program, it is imperative to support employees throughout the change by providing clear internal communication and marketing initiatives, as well as adequate user training.

Internal Communications and Marketing

Internal communications and marketing play a big role in the successful rollout of a BYOD program. The idea is to educate and excite users about the new tools they will be able to use, while simplifying their day-to-day work. The creation of clear company communications and internal adoption campaigns are an effective way to raise awareness of the new technology and educate users on the benefits to them.

Examples of topics that an internal campaign should address are:

- Software functionality and limitations
- Key milestones for rollout schedules and impact to user groups
- Instructions for device enrollment
- Benefits of program adoption for individuals
- Specify the terms of use, i.e. access requirements, privacy and compliance

Staff Training

Training is another key component of adoption and program success. Users need to understand how to access and implement the new tools and resources available to them. A few ideas of effective training tools are:

- Short training videos
- One -pager "cheat sheets"
- Scheduled IT workshops and drop-in clinics

End User Campaign Kit

VMware AirWatch® has created a complete end user adoption campaign kit to help enterprises create awareness and educate employees on the benefits of BYOD. The kit includes pre-designed and pre-written materials and assets such as emails, posters, FAQs, PPT and a video, all ready to be used out-of-the-box or customized to your company's brand standards.

Use Executive Sponsorship to Increase Adoption

Research shows that active and visible executive sponsorship is seen as the top contributor to change management success. For this reason, it is important to make executive sponsorship a priority when implementing a BYOD program.

.

Executives as BYOD Program Advocates

Users are more inclined to participate in a new program once they see that it matches the strategic vision of the organization. Recruiting the top line to promote the program lets employees know how important it is to the company.

Executives as Early Adopters

Even more compelling than an executive promoting a new program is an executive actually using it themselves. This can help accelerate the uptake of the solution across the organization. The voice of senior leaders brings a natural authority from their positions of leadership. Users are more likely to join a BYOD program if they can see first-hand success from those they trust. Increase the likelihood of your program's success by encouraging executives to:

- Be an early adopter of the program
- Advocate by matching their organization's strategic vision with the program
- Help employees understand the productivity, efficiency and usability benefits of the program

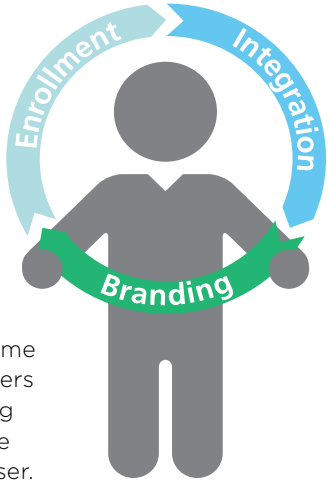
TO LEARN MORE

Learn more about how VMware AirWatch® Enterprise Mobility Management can help you successfully implement and manage your BYOD program by visiting www.airwatch.com

Simplify the User Experience

1. Simplified Activation Process

Streamlined activation in the BYOD program makes the onboarding experience for users simple, and will increase the likelihood that they recommend the program to other employees. Integrating the EMM solution into the company's Directory Services environment enables employees to use a common username and password.



2. Seamless App Integration

Successful BYOD rollouts give users access to their core apps without being challenged for authentication every time they use it. To achieve this, the solution should provide users seamless access from a trusted, activated device. Enabling single sign on (SSO) and identity management to federate application identities will streamline the process for the user.

3. Customized Branding

Customized branding of business applications, including corporate logo and color schemes, enables users to easily identify which apps on their personal device are for business purposes. One way to implement corporate branding is to configure an email signature for all users accessing email on their BYO devices. This signature can specify that they've been enabled by the BYOD program and can help accelerate adoption within the organization, i.e. "Sent from my smartphone enrolled in the <company> BYOD Program."

Mobility programs like BYOD have the potential to deliver real transformation and growth. Employee productivity, user choice, device flexibility and lower operational costs are among the many benefits achieved through successful BYOD program deployment. The key to ensuring value is thoughtful, methodical BYOD program creation and implementation. Using the strategies and tactics within this whitepaper, IT leaders and administrators alike can begin creating a BYOD strategy that delivers the promised value of business mobility.

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