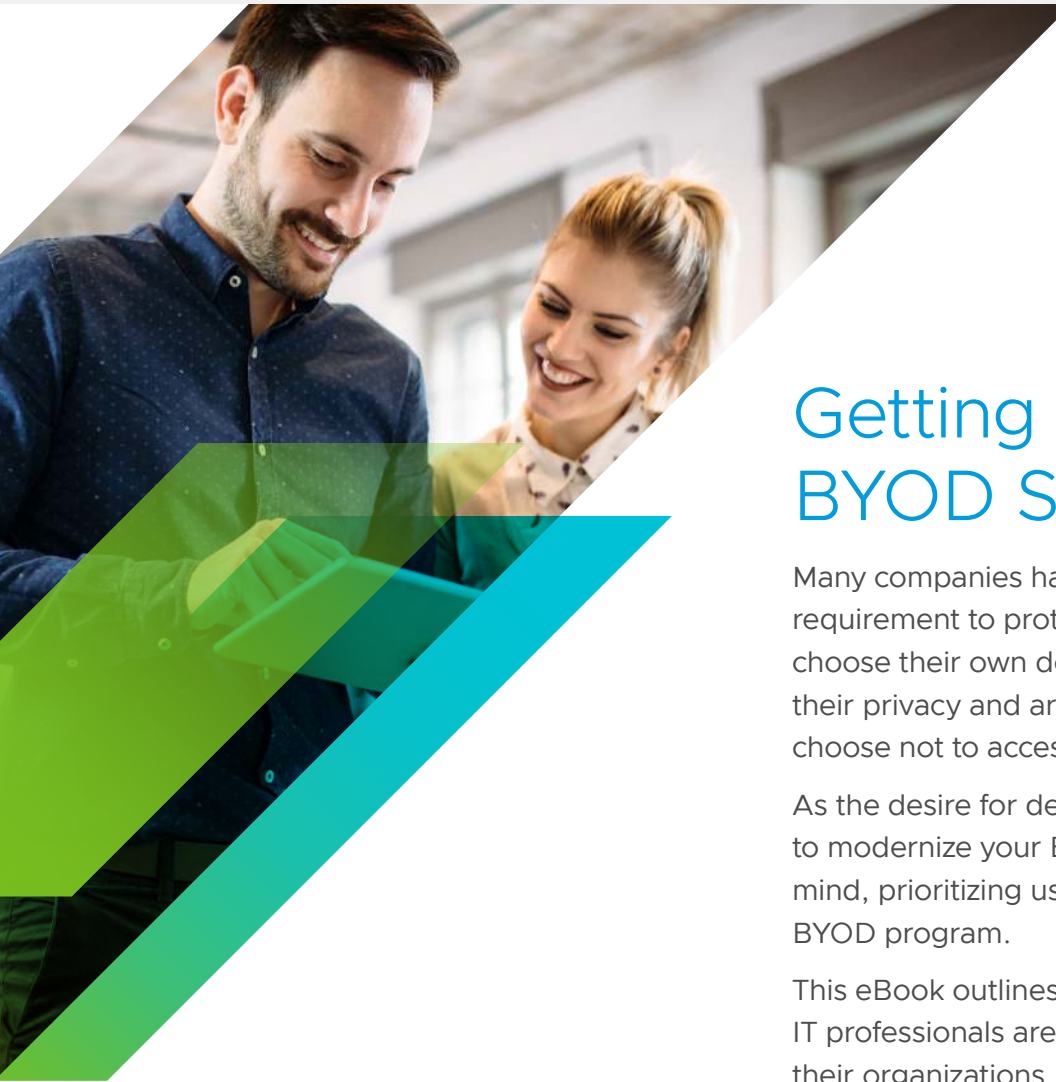




5 Steps to Modernize Your BYOD Strategy

Evolve Your BYOD Strategy
with Workspace ONE





Getting More from Your BYOD Strategy

Many companies have implemented a BYOD strategy with the minimum requirement to protect company information while allowing employees to choose their own device. However, many users are still concerned about their privacy and are either unsatisfied with their BYOD experience or choose not to access corporate resources on their device at all.

As the desire for device choice continues to grow, now is the time to modernize your BYOD strategy. While security still remains top of mind, prioritizing user privacy and experience will lead to a successful BYOD program.

This eBook outlines the five best practices business leaders and IT professionals are taking to ensure successful BYOD programs in their organizations.



1 Focus on User Privacy First

For a successful BYOD program, IT needs to consider employee privacy from the very start. Create a BYOD policy that ensures devices are trusted and that corporate data is safe, while also making sure that users are educated and comfortable using their own device to access corporate data:

- Ensure that user privacy is a priority throughout the planning, implementation, and life of the BYOD program.
- Be transparent with users and clearly explain the benefits of having corporate information on their personal device.
- Assure employees that they have control over their device, every step of the way.
- Implement a digital workspace solution that provides transparency into what IT can and cannot see, as well as what data is being collected.





2 Create Clear BYOD Policies and Terms of Use

Establish basic policies and rules based on device, user, and application-level considerations to make your program as effective as possible. Terms of Use agreements help inform the users what data may be captured from their device and what functions IT can access. When outlining your policies, be sure to follow these guidelines:

- Leverage existing policies that have been developed with legal and HR for corporate devices and extend the necessary policies, apps, and content to BYOD.
- Carefully think through 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.
- Clearly communicate privacy policies in a transparent, easy to understand way to establish trust.
- Consider the differences in users based on role, location, function, and other criteria and assign policies accordingly.





3 Give Users Control

Employees not only want options, they want to remain in control of their experience, especially when downloading work apps on their devices. Providing access to applications that have less sensitive data without a full management profile on the device helps employees feel more comfortable in adopting the new technology. Giving employees the power to decide when they are ready to access more business-sensitive apps and the ability choose the level of management allows them to remain in control of their device:

- Offer an intuitive experience for application access.
- Consider which apps can be accessed without any trust between the user, device, and organization and which apps need more security.
- Provide a seamless way to take a device from an untrusted state to a trusted state, with an intuitive workflow for employees.





4 Give Users a Personal, Consistent and Productive Experience

Employee experience is emerging as a strategic imperative as a growing number of studies find a direct correlation between a positive employee experience and business outcomes. When employee experiences are meaningful and fulfilling, employees are more engaged and productive. Make user experience a top priority for your BYOD program:

- Provide users with a personalized experience such as a role-based app catalog.
- Make it easy for users to collaborate with colleagues.
- Allow employees to spend more time on meaningful work by automating simple tasks such as approving expense reports.
- Keep users informed with real-time prioritized notifications.

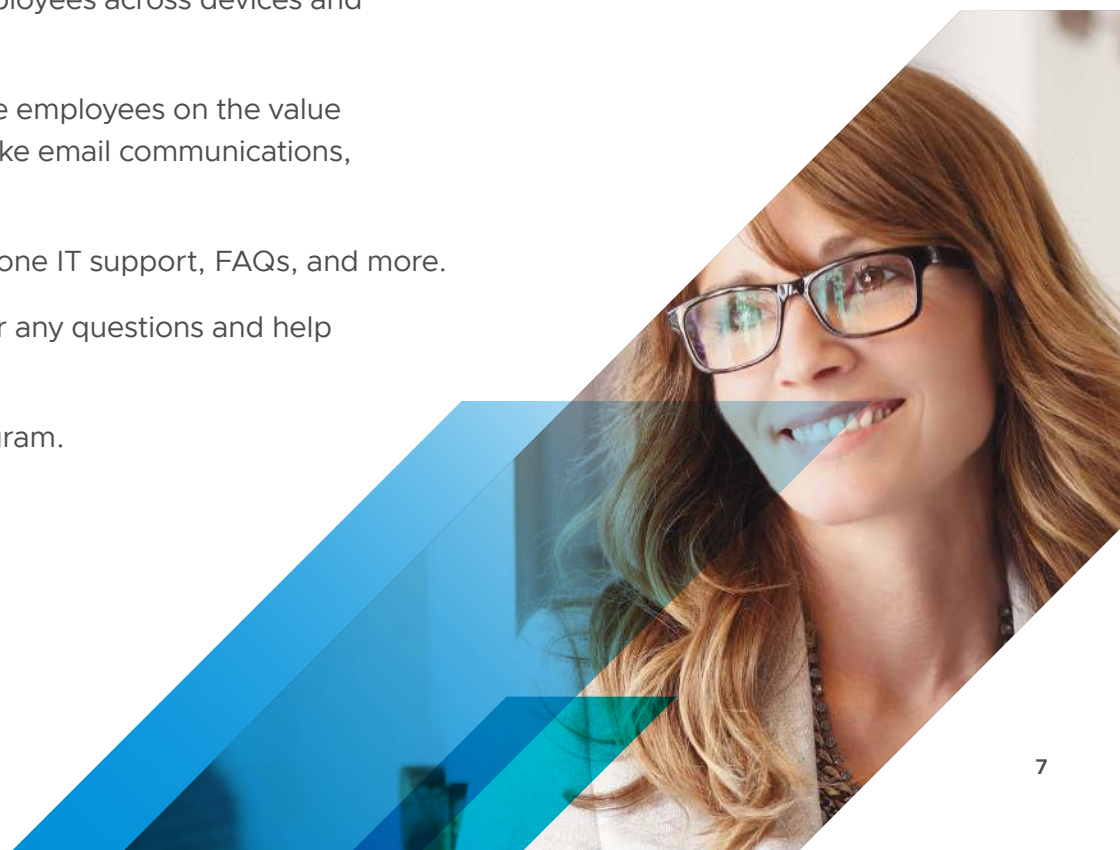




5 Drive Employee Adoption with an Adoption Campaign Plan

The right digital workspace platform should be intuitive, so you can focus your efforts on driving employee adoption. Preparing an adoption rollout plan for user education and support is imperative for success. This will help employees clearly understand the benefits prior to and throughout the process of accessing corporate resources on their personal device. Support employees with this transition by taking the following steps:

- Deliver a consistent, intuitive onboarding experience for employees across devices and operating systems.
- Create a tactical adoption campaign across teams to educate employees on the value of adopting a digital workspace. This should include things like email communications, posters, trainings, and more.
- Ensure support access is readily available including one-on-one IT support, FAQs, and more.
- Set up help desk events for subject matter experts to answer any questions and help alleviate any privacy concerns.
- Assign executive sponsors to advocate on behalf of the program.





Evolve Your BYOD Strategy with Workspace ONE

The best way to modernize your BYOD strategy is to start with the right platform. VMware Workspace ONE® is a digital workspace platform that allows IT to securely deliver and manage any application on any device by combining access control, application management, and multi-platform endpoint management in a single console, in the cloud or on premises.

Workspace ONE delivers the security that IT needs while also providing the experience and privacy employees want by providing BYO transparency and a personal, engaging, consistent and productive experience.

Workspace ONE includes user-centric features such as a personalized app catalog with single-sign-on capabilities, and mobile workflows with one-click actionable notifications that automate business processes—all without having to log into multiple applications.

To help users feel in control and confident in their privacy, *Workspace ONE Privacy Guard* notifies users of exactly what IT can and cannot access or see on their device along with device permissions and the company's privacy policy.

To facilitate employee adoption, VMware provides a complimentary Adoption Kit that includes best practices, campaign plans, tools, and out-of-the-box resources to help build a successful internal BYOD campaign.

For more information on BYOD and Workspace ONE, visit

www.vmware.com/workspace-one.com.

Join us online:



vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Copyright © 2019 VMware, Inc. All rights reserved.
This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.
VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: 5632-VMW-5STEPS-MODERNIZE-YOUR-BYOD-STRATEGY-EBOOK-20191017 10/19