jamf

WHITE PAPER

BYOD Made Manageable

How to balance good IT security practices with user privacy and personal data protectionto increase user adoption of BYOD programs

The rise of smartphones as an umatched personal productivity champion has resulted in an always-connected, modern, mobile workforce—and a big challenge for IT management.

CRITICAL ELEMENTS OF SUCCESSFUL BYOD

Alleviate IT security concerns + Ensure privacy for the user + Reduce program cost and complexity = Increased user adoption

Smartphone ownership is ubiquitous, and most employees are bringing them to work, regardless of company policy. In the past few years, IT managers have tried various iterations of personal device policies: everything from an outright ban of personal devices to a wide open policy of Bring Your Own Device (BYOD). The success (or failure) of a BYOD program hinges on user adoption, requiring the right balance of IT control and personal privacy. This paper outlines a strategy for striking that balance and making BYOD work.

PRIVACY MATTERS TO USERS

Our smartphones carry the most private kinds of data: our personal correspondence, photos, contacts, and documents. Even the choice of apps installed on the device can reveal very private information about our hobbies, habits, and lifestyle. It's no surprise that most employees are reluctant to give access to that information by enrolling their personal smartphone in a Mobile Device Management (MDM) system controlled by their organization's IT group.

When BYOD programs fail, one common reason is users' reluctance to volunteer access—or even the perception of access —of this personal data to an IT admin. Personal privacy matters, and users are increasingly sensitive to any attempt at breaching the privacy barrier in the name of IT control.

SECURITY MATTERS TO IT

For the IT manager, the idea of unfettered access to internal resources from personal devices with unknown configuration and security controls is the stuff of sleepless nights. Smartphones are a common target for malware and present a potential vector for intrusion when connected to an organization's network.

Without any visibility or control of the endpoints, good IT security is an impossible task. The need for security is what pushed many organizations to use MDM for their BYOD program, and require employees to enroll their personal device to gain access to the internal network, mail, calendars, and VPN.

STRIKING THE BALANCE

Both users and IT have perfectly valid concerns. The employee doesn't want to give up access and control of their private data, and the IT admin doesn't want to expose their internal network to threats from unsecured endpoints. For many organizations, this logjam meant failure for their BYOD program.

One solution to satisfying both concerns is to rethink the role of MDM as it applies to BYOD. Instead of a one-size-fits-all approach, IT managers can choose an MDM tool that's designed for BYOD, with privacy protections to satisfy the employee and strong security controls to satisfy the needs of good IT security.

SIMPLER IS BETTER

A simple approach to managing devices in a BYOD environment helps IT and the user be more successful. Unnecessary complexities such as dual personas or segmented data containers change the native user experience on the device—often for the worse—and inhibits user adoption. MDM tools that are sold as the solution to BYOD security may end up driving users away due to this overburdensome complexity. Once users opt-out of device management, IT security becomes an impossible task.

The alternative is a tool that is designed for BYOD management and eliminates the complexity of one-size-

fits-all MDM. This preferred method does not require multiple tools or apps to enforce corporate policies, and eliminates distractions and unnecessary steps both for IT admins and users. The goal for a successful BYOD program is safe, secure access to corporate resources—not additional hindrance and complexity.

MDM FOR BYOD

To satisfy this need, leading organizations choose a feature set built specifically for BYOD, without unnecessary complexities and added costs. This approach still gives IT all necessary security controls, and protects the user's personal device by allowing them to see exactly what the IT admin can and cannot do.

Example BYOD management controls

IT admin can:

- Lock the device and remove a passcode
- Apply institutional configurations, like Wi-Fi, VPN, mail, and passcode requirements

Install and remove institutional apps and the data used by those apps IT admin cannot:

- Erase private data like photos, personal mail, or contacts
- Remove any personal apps
- View any private data including the names of personal apps
- Restrict the usage of the device or limit the personal apps that can be installed

Conclusion

A successful BYOD program is a benefit to employees and IT admins alike. Users get easy access to critical resources like mail and calendars without sacrificing personal privacy, and IT admins can preserve good IT security with personally owned devices. With the right MDM solution, IT can concentrate on addressing critical enterprise needs without friction from the technology itself or from users. And users receive comfort and familiarity with their own device without intrusive IT involvement.

To learn more about how Jamf can make an impact on your Mac and iOS management, visit **jamf.com/products/Jamf-Pro**.