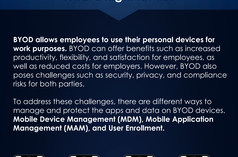
mobile mentor

BYOD 101

SECURE EVERY DEVICE

Workers are using personal devices for work more than ever. Millions of people use their own laptop and smartphone to access company email, Teams and OneDrive. But when companies fail to properly secure company data on personal devices it leaves a major security vulnerability.



What's Right for Us?

BYOD allows employees to use their personal devices for work purposes. BYOD can offer benefits such as increased productivity, flexibility, and satisfaction for employees, as well as reduced costs for employers. However, BYOD also poses challenges such as security, privacy, and compliance risks for both parties.

To address these challenges, there are different ways to manage and protect the apps and data on BYOD devices. **Mobile Device Management (MDM)**, **Mobile Application Management (MAM)**, and **User Enrollment.**

Mobile Device Management

MDM is a solution that allows IT administrators to **enroll**, **configure**, **and manage** BYOD devices remotely. MDM can enforce policies such as **password requirements**, **encryption**, device restrictions, and app installation. MDM can also **wipe or lock devices** in case of loss, theft, or breach.

+

- Provides comprehensive control and visibility over BYOD devices
- Enhances security and compliance of BYOD devices
- Supports a wide range of device types and platforms

—

- Requires users to enroll their devices and accept IT policies
- May affect user privacy and device performance
- Creates tension between IT and end users

Mobile Application Management

MAM is a solution that allows IT administrators to **manage and protect only the apps** that access organization data, without enrolling the devices. MAM can apply **app-level policies** such as **data encryption**, **copy-paste restrictions**, **app access control**, and **data wiping**. MAM can also configure app settings and deploy app updates.

+

- Protects organization data at the app level
- Preserves user privacy and device autonomy
- Supports devices that are not enrolled or managed by another MDM provider

—

- Provides no control or visibility over BYOD devices
- Depends on the availability and compatibility of MAM-enabled apps
- May not prevent data leakage from unmanaged apps or sources

User Enrollment

User Enrollment is a solution for iOS devices that allows IT admins to **manage and protect a separate work profile** on BYOD devices, without affecting the personal profile. User Enrollment can apply policies and settings to the work profile, such as **VPN**, **Wi-Fi**, **email**, and calendar. User Enrollment can also **remove the work profile and its data remotely**.

+

- Creates a clear separation between work and personal data
- Minimizes the impact on user privacy and device functionality
- Supports devices that are enrolled or managed by another MDM provider

—

- Requires users to switch between profiles
- May cause compatibility issues with some apps and features
- May not prevent data leakage from the personal profile

Unmanaged Devices

Unmanaged devices are devices that are **not enrolled or managed by any security controls** from the organization. This approach essentially treats the device as an external entity and does not provide any form of corporate control or management over the device or the data on it. **Unmanaged devices rely soley on user discretion and device security features** to protect organization data.

— Risks of unmanaged devices

Reduced Security:

An unmanaged strategy can **increase the risk of data breaches**, as your business has no control over the device or the apps and data on it. This can lead to data loss, theft, or unauthorized access.

No Compliance:

Your business will have no control over the device itself, which can limit some of your ability to enforce security policies. Without some form of enrollment **there is no method of policy enforcement**.

Limited Control:

An unmanaged strategy does not provide your business with **any control over the device or the data on it**, which can limit the ability to enforce security policies and protect sensitive information.

Are You Ready?

BYOD offers many advantages for both employees and employers, but it also comes with many challenges. To overcome these challenges, you need a solution that can manage and protect the apps and data on BYOD devices, without compromising user privacy and device performance. **MDM, MAM,** and **User Enrollment** have their own benefits and negatives, depending on your needs and preferences.

BYOD 365 by Mobile Mentor will give you the ability to **secure company data on personal devices** while simultaneously **providing the privacy** your employees deserve.

Download our **BYOD Whitepaper**

Check out our **BYOD articles**

Consult with one of **our expert team**

mobile mentor

mobile-mentor.com