Bring Your Own Device (BYOD)

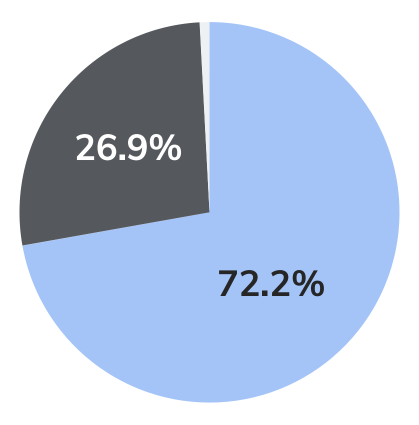
for

Android VS **iPhone**

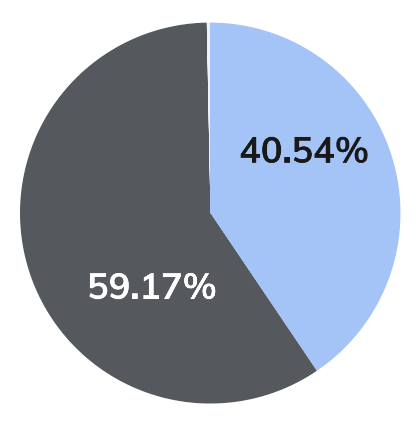
Did you know?

The global Bring Your Own Device (BYOD) market is projected to grow **$587.3 BN** by 2030, expanding at a **16.20%** CAGR throughout the review period (2022-2030).

The global market share of Android and iOS devices



The market share of Android and iOS devices in the US



" Although iOS is the popular smartphone choice in the US, it is Android that dominates the market globally. "

Why adopt Bring Your Own Device for Android and iOS?

34% — **increase in productivity** for businesses when using Bring Your Own Device (BYOD) smartphones to get work done.

58 minutes — of work time and personal **time saved** for every employee when adopting BYOD policies in the workplace.

$350 — in **savings for businesses**, per year, per employee, when implementing a basic BYOD policy in the workplace.

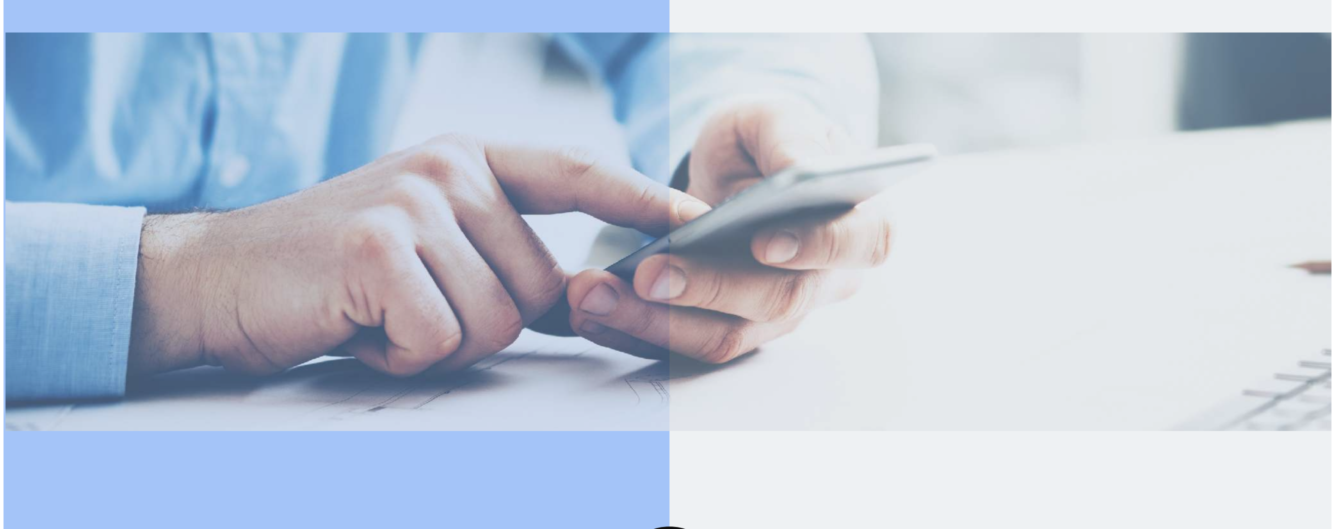
30% of organizations have no safeguard against malware for their BYOD policies

How IT admins can enforce BYOD security on

Android & **iPhone**

1 DEVICE ONBOARDING

Adopting a solid device onboarding strategy is the first step to securing your organization's Android and iOS BYO devices.



ANDROID ENTERPRISE PROFILE OWNER ENROLLMENT

- Personal devices can be enrolled as Profile Owner in Android Enterprise (AE).
- A separate encrypted work container is created on enrollment.
- Policies & configurations pushed by admins will only be applicable to the work container.

VS

iOS USER ENROLLMENT

- User Enrollment was introduced on iOS 13 and above.
- It relies on Managed Apple IDs to create a separate APFS storage volume.
- The organization has full control over this volume, while staying clear of personal user data.

2 APP & DATA SECURITY

A strong BYOD strategy relies on successfully separating work apps & data from a users' personal space, thereby ensuring privacy & security.

ANDROID WORK PROFILE

- Admins can establish encrypted containers on AE devices.
- It helps ensure that organizations can’t interact with personal data on the device.
- Admins can restrict the sharing of work data outside of the container.

VS

iOS BUSINESS CONTAINER

- Business Container forms a discrete partition between work and personal apps & data.
- It helps to control data flow between managed and unmanaged apps.
- Admins can set up restrictions to prevent managed data from being accessed by unmanaged sources.

MANAGED GOOGLE PLAY

- Admins can select, approve and deploy apps using Managed Google Play.
- They can customize configurations and permissions for these apps.
- Users can download the approved apps from the custom app store.
- Downloaded apps will only be accessible inside the work profile.

VS

APPLE APPS & BOOKS

- Managed Apple IDs can be used to link the iPhone with Apple’s Apps & Books.
- Admins can distribute, update, and remove VPP and enterprise apps/app licenses on iOS devices.
- Features like silent app installation, managing app configurations & permissions, will not work on personal iPhones.

3 NETWORK & ENDPOINT SECURITY

Protecting your BYO devices from threats and malware involves enforcing the right controls to secure your network and endpoints.

ANDROID WORK PROFILE PASSWORD

- Admins can mandate a Work Profile Password on the Android device container.
- They can set up rules on minimum length, complexity, failed attempts, and more.

VS

iOS DEVICE PASSCODE

- Admins can enforce passcode for the iOS device as a whole.
- Admins cannot enforce a separate passcode for the iOS container.
- Admins cannot enforce complex characters or alphanumeric rules.

ANDROID REMOTE ACTIONS

- Remote actions can be used to clear app data, ring, remotely launch apps, and more.
- Admins can remotely set and clear the work profile password.
- Admins can remotely lock or completely wipe the data in the work container.

VS

iOS REMOTE ACTIONS

- Admins can use remote actions to broadcast messages, lock, or ring iOS devices.
- Admins can remotely wipe the entire managed APFS volume from the iPhone.

ANDROID POLICIES & RESTRICTIONS

- Admins can deploy Wi-Fi and VPN configurations.
- File sharing via Bluetooth and external media can be limited.
- Restrictions can be enabled on screen capture, app runtime permission, accessibility, and more.
- Admins can prevent users from sharing location data with apps in the work profile.

VS

iOS POLICIES & RESTRICTIONS

- Admins can prevents corporate data from being saved on iCloud.
- Admins can deploy network configurations including Wi-Fi, per-app VPN, to BYO iPhones.
- Admins can configure corporate accounts including email, calendar, contacts, and more.
- Data usage can be tracked for managed apps on the iOS device.

hexnode

Visit hexnode.com to learn more

mdm-support@hexnode.com
partners@hexnode.com
US: +1-833-439-6633
International: +1-415-636-7555

References:
https://gs.statcounter.com/os-market-share/mobile/worldwide
https://www.cisco.com/c/dam/global/ru_ua/assets/pdf/byod-economics_econ_analysis.pdf
https://insights.samsung.com/2016/08/03/employees-say-smartphones-boost-productivity-by-34-percent-frost-sullivan-research/
https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY20Q3BringYourOwnDevice2.pdf