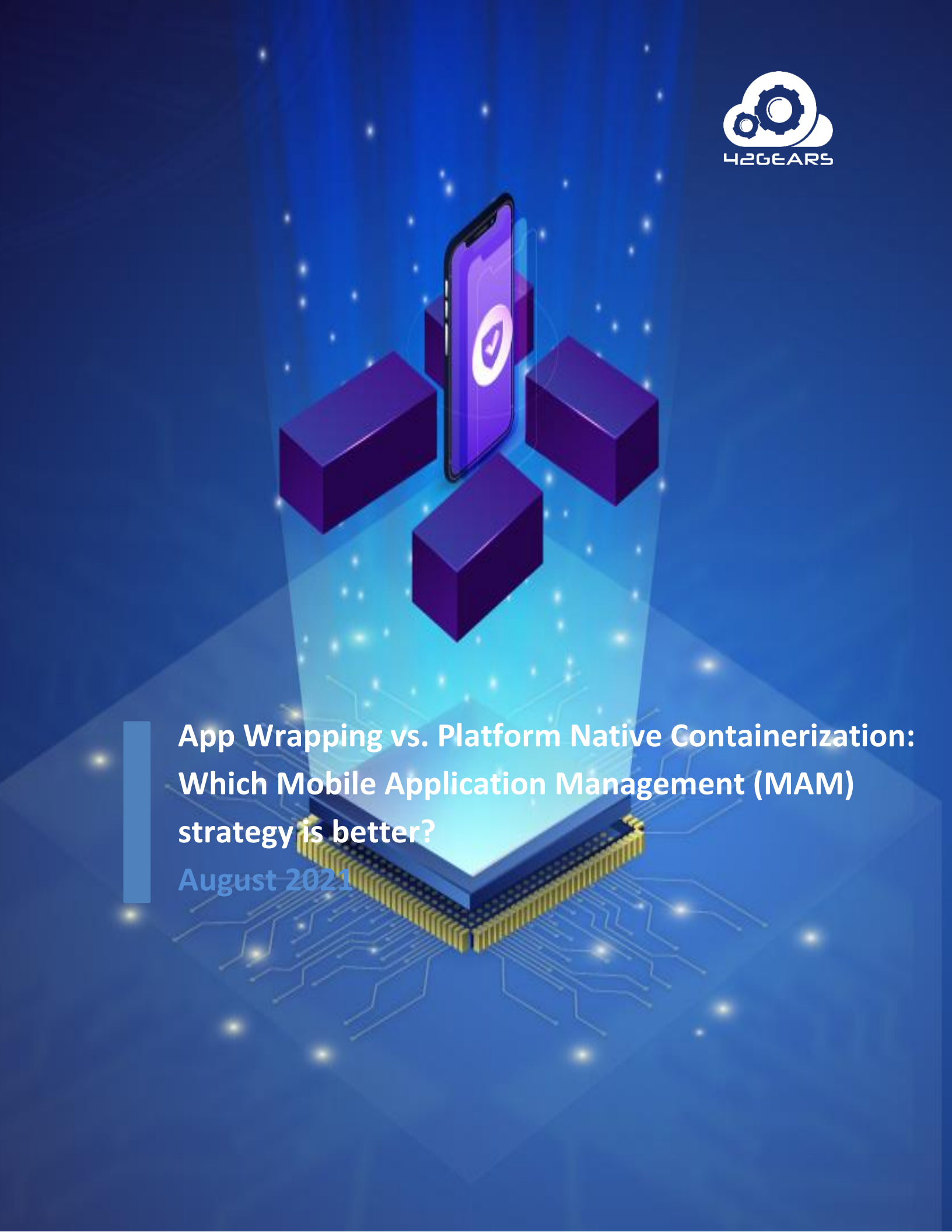

# App Wrapping vs. Platform Native Containerization: Which Mobile Application Management (MAM) strategy is better?

August 2021

# Table of Contents



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of 42Gears Mobility Systems

# App Wrapping vs. Platform Native Containerization: Which Mobile Application Management (MAM) strategy is better?

App wrapping and containerization are two major components of a Mobile Application Management (MAM) strategy. They both provide IT with granular control over managing mobile applications and separating corporate apps from personal apps. However, app wrapping, and containerization are aiming for the same thing in a different way.

## A. Why do we need app wrapping or containerization?

The first reason is the prevalence of Bring-Your-Own Devices (BYOD) in the workplace. As more and more organizations are adopting BYOD (Bring Your Own Device) strategy, keeping the corporate data secure has become a challenge. **According to research by Global Market Insights, Inc,[1] "the market value of BYOD is estimated to reach $367 billion by 2022.**

In a BYOD system, users are allowed to access corporate data, files, emails, or other sensitive information from their personal devices, which can make the corporate data vulnerable to various kinds of security threats.

The second reason is lack of full enterprise control over the personal devices. As personal devices contain personal apps and data, organizations cannot have full control over these devices, making it impossible to fully eliminate the threat of data breaches.

The third major reason is data compromised through malicious apps. NowSecure[2] did a review of 250 popular Android mobile apps from different industries, which revealed that more than 70% of these apps leaked personal information and put users at risk.

Naturally, this is a major concern for organizations because BYO devices also contain corporate data, and malicious downloads can put corporate data at risk. Therefore, we need app wrapping or platform native containerization to segregate corporate data from personal data and to make corporate data more secure.

[1] https://www.globenewswire.com/news-release/2016/03/22/822021/0/en/Bring-Your-Own-Device-BYOD-Market-size-worth-USD-366-95-Billion-by-2022-Global-Market-Insights-Inc.html

[2] https://www.nowsecure.com/blog/2019/06/06/test-of-250-popular-android-mobile-apps-reveal-that-70-leak-sensitive-personal-data/

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of 42Gears Mobility Systems

### *How data can be compromised on personally-owned devices*

There can be multiple means through which data breaches can occur on personally-owned devices:

- When the corporate data is accessed by personal apps present on the device.
- When corporate data is transferred from the managed devices to unmanaged devices.
- When email attachments present in a corporate email account are accessed via personal apps.
- When corporate data is downloaded from the company website using personal apps.
- When the user has taken a backup of corporate data into the personal account.

In order to overcome possible security vulnerabilities, such as the ones mentioned above, a proper Mobile Application Management (MAM) strategy should be in place. MAM manages the entire life-cycle of apps, including installing, updating, and uninstalling them. Plus, MAM helps in securing the data accessed by these apps, and taking remedial actions if apps display suspicious activity, such as removing the apps from the device.

Securing corporate data from vulnerabilities can be done using technologies like app wrapping and platform native containerization. Both the techniques help to achieve data security, but do so in different ways. We will explore all advantages and disadvantages of both.

## B. What is App Wrapping?

App wrapping is the process of adding an extra layer of security to the mobile applications on a device without affecting the core functionality of the app. App wrapping is offered by EMMs either via a MAM SDK or dynamic wrapping on already-compiled apps. This process helps to protect business data without altering the look and the functionality of an application.

### *Advantages of using app wrapping*

Some of the advantages of using App wrapping are as follows:

- **Platform native support is not required:** App wrapping functionality is implemented by EMM vendors irrespective of native support for containerization. It is independent of

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of 42Gears Mobility Systems

platform versions. App wrapping is useful for organizations with older versions of devices, as platform-native support for containerization is a recent offering.

- **Have management control on apps:** App wrapping empowers IT admins to control the security of enterprise apps, which includes encryption, restricting app access, deleting apps, and more. EMMs can offer capabilities beyond those available on native platforms, like preventing copy/paste from work to personal apps on iOS devices.

### *Disadvantages of using app Wrapping*

Some of the disadvantages of using App wrapping are as follows:

- **Lack of standard process**: As app wrapping is independent of platform versions, it is implemented by EMM vendors in their own way; hence, there is no standard process of doing it. Wrapped apps are tightly coupled with the EMM solution they were developed for, and are incompatible with any other EMM solution. Developers working with different EMM vendors follow different ways of configuring and securing the app through wrapping.
- **Lack of security**: App wrapping mostly works by intercepting Platform API calls made by the application and fulfilling them in ways which ensure data security and encapsulation. This methodology can often miss out on some system calls or fall behind the dynamic and ever-changing Platform APIs. This can result in leakages and insecure implementations.
- **Not supported by Google Play Store:** Wrapped applications are not supported by the Google Play Store; the reason is these apps can at any time be changed by EMM vendors, and there isn't a regular or standard process of doing it. This means wrapped apps can only be hosted on an EMM's private app store.
- **Risky implementation technique:** Some app wrapping implementation makes use of non-standard methods like using Private APIs or reflection. These methods can break in the context of some OS upgrades or give unexpected results.
- **No support for 3rd-party apps**: App wrapping generally involves rebuilding and re-signing applications. Of course, developers can only use the apps or source code to which they have access. This means other third-party apps will be out of reach and beyond their limits.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of 42Gears Mobility Systems

## C. What is Containerization?

Containerization[3] is the process of isolating work data from personal data while existing together in the same device. In this case, IT admins can only control work profiles without touching users' personal profiles, data, and apps. The enterprise apps will be seen with a work badge to keep them separate from personal apps.

Containerization allows management policies such as encryption, data sharing and more to apply on targeted apps and data. It helps to provide an extra layer of security to protect mobile apps and data from malware infections, or to prevent data from reaching unauthorized users. Also, it empowers admins to wipe business data in case a device is lost or stolen.

### *Advantages of Platform Native Containerization*

- **Native containerization is more secure:** As native containerization techniques are designed by the creators of each platform (Android, iOS, Windows), they are highly secure. Data encryption is done on the platform level which is hard to bypass.
- **Standard process:** Containerization is implemented through a standard process set by each platform; hence, different EMM vendors have no need to follow separate techniques.
- **Rich set of DLP features:** Platform native containerization on many platforms easily offers core functionalities like Disable Screenshot, Disable Copy / Paste, and Work-only VPN, which are otherwise challenging to implement independently.
- **Have full control:** Admins can have full control over the work containers. They can create an Enterprise Play Store, from which users can download managed apps. It will be entirely managed and controlled by the MDM.

### *Disadvantages of using Platform Native Containerization:*

- **Dependency on platforms:** Containerization is dependent on the support given by each platform or OEMs. EMMs have to fall back on alternate approaches like App Wrapping if no relevant platform or OEM provides support for containerization.

[3] https://www.cdw.com/content/cdw/en/articles/datacenter/how-containerization-can-have-a-big-impact-on-your-data-center.html

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of 42Gears Mobility Systems

- **Missing feature implementation:** EMMs are at mercy of OEMs and platforms for containerization features. If Platform vendors deem a feature not important and useful, EMMs won't be able to support it despite strong demand from the field. One such classical example is lack of support for preventing Copy/Paste across managed and unmanaged apps in iOS.

## *App wrapping vs Containerization*

So far, we have analyzed the pros and cons of app wrapping and containerization techniques.

Let's explore in detail what the perfect strategy for your business will be.

Corporate data security has become paramount with the increasing number of mobile apps. Using a non-standard technique such as app wrapping to secure workspace should not be the first choice. Wherever available, platform native containerization should be used. This should not be a challenge in the context of managing knowledge worker devices, as they typically own standard devices from leading manufacturers. These devices usually comply with platform features and support platform native containerization.

On the other hand, frontline workers and blue-collar workers may be more sensitive to device cost, meaning they may own poorly-supported non-standard devices from smaller vendors (e.g. non-GMS Android devices). For such devices, platform native containerization support might be absent, and hence, work data security based on app wrapping might be your best bet.

Additionally, enterprises need to comply with laws, and non-compliance may result in harsh consequences, and damage to a firm's reputation. As per copyright laws, it is illegal to modify a code written/published by others without their permission. In App wrapping, developers usually modify 3rd party apps, which can get the enterprise in legal trouble. On the other hand, platform native containerization manages apps without violating any laws as they are managed by industry leaders i.e., Google, Apple, and Microsoft.

In a report by the National Vulnerability Database[4], there is a mention about app wrapping techniques using HTTP resources in wrapper apps. It can make the apps vulnerable to MITM (man

[4] https://nvd.nist.gov/vuln/detail/CVE-2016-10671

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of 42Gears Mobility Systems

in the middle) attacks and also can cause remote code execution (RCE) vulnerabilities. In containerization, all data inside the container (including emails and files) are encrypted using military-grade encryption which makes the data unreadable, even on devices that are jailbroken. With containerization, not only is data-at-rest, but also any data transported over the network to and from the container, is encrypted.

## *Summary*

In a BYOD scenario, managing and securing enterprise applications are crucial while also preserving device owner's right to privacy at the same time. Platform native containerization has the ability to make this happen. Containerization empowers IT admins with granular control over enterprise apps and helps in achieving greater levels of data security.

42Gears MAM[5] (Mobile Application Management) helps enterprises to have full control over the work container and ensure corporate data security. 42Gears MAM supports all platforms including Android, iOS, Windows.

So, if you are looking for a reliable EMM or MAM solution to achieve better enterprise app management, Try 42Gears EMM[6] or MAM[7] solutions.

[5] https://www.42gears.com/white-papers/42gears-mobile-application-management-mam/
[6] https://www.42gears.com/solutions/enterprise-mobility-management/
[7] https://www.42gears.com/mobile-application-management/

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of 42Gears Mobility Systems