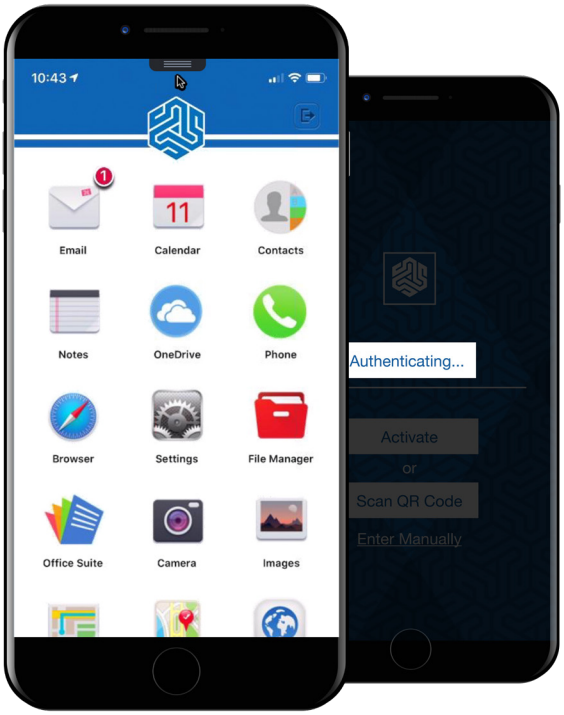
Containerization vs App Wrapping vs MDM

Many organizations have traditionally relied upon Mobile Device Management (MDM) to protect and manage devices by forcing password policies, restricting access to applications, and having the ability to wipe the device. As cyber-attacks become more sophisticated, this approach has failed to sufficiently secure the data being sought after on the device. Organizations looking to stay ahead of the threats need to incorporate advanced data encryption tactics to protect the sensitive corporate or government related data being accessed, used, and stored on employee's mobile devices. The two most common approaches are App Wrapping or Containerization.

Both Containerization and app wrapping can provide security, but containerization has several major advantages:

- Containerization is device and operating system independent and most importantly, does not require an MDM profile on the device – Personal devices are just as viable as corporate owned / managed devices.
- Application containerization provides a secure isolated environment on a mobile device that serves as a secure location for corporate/government information. It provides an entire workspace that allows interaction and data sharing between applications inside the workspace, while maintaining security.
- App wrapping solutions only work on individual apps resulting in significantly longer implementation cycles, significantly longer installation times, significantly increased attack surface and significant extra effort in the end-user experience due to log in – log out processes while moving from app to app.
- Containerization isolates work related email, files and apps from personal information and protects the privacy of the end-user



SyncDog offers a containerized solution that creates a vault for multiple applications and provides centralized management functionality for administrators.

The solution offers a FIPS 140-2 Certified, AES 256-bit encrypted, end-to-end mobile security solution. The modular solution enables organizations to custom fit their mobility policies and security measures and align them to the specific needs of the various roles and titles of their entire employee base — down to the individual user. It will no longer matter if the device is iOS or Android, Managed or Un-Managed, Corporate/Government Owned or personal (BYOD) — all can be supported through a single solution. SyncDog protects and manages the device, detects, and prevents malware/phishing and other intrusions, encrypts, and isolates all the corporate or government data/files/apps that are accessed by or stored on the device and offers a private app store for distribution of internal native or hybrid apps. SyncDog can be hosted in the cloud (SaaS), on premise, or hybrid. All from a single vendor, from a single download and centrally managed in a single administrative console.

+1.855.SYNCDOG (1-855-796-2364)
info@syncdog.com

1801 Old Reston Ave, Suite 301
Reston, VA 20190