TECHNICAL CONTAINER REQUIREMENTS TO ENABLE SECURE MOBILITY

CONTAINERS NEED TO PROTECT THE 3 C's OF SECURE MOBILITY

The Good Dynamics Secure Mobility Platform utilizes secure container technology designed from the ground up to protect the 3 C's of secure mobility: content, credentials and configurations. Whether your users are accessing data locally on the device, on your corporate network, or from a cloud service, the Good secure container helps keep the 3 C's from being discoverable on corporate- or personally-owned (BYOD) mobile devices, or being moved to personal apps or clouds.

Content	• Corporate data at rest, in transit, and in use • Regulated information, such as customer data, PII, etc. • Proprietary formulas, plans, processes
Credentials	• Username and passwords • Tokens and certificates • To the content on device and to backend systems accessed
Configurations	• Critical system data: VPN, WiFi, EAS, AD, LDAP, etc. • Passwords and other mobile policies and restrictions • Jailbreak/root detection policies

CRITICAL CONTAINER REQUIREMENTS TO ENSURE SECUIRTY OF THE 3 C's

When investigating container solutions, validate the following requirements to ensure your corporate content, credentials, and configurations are actually secured or risk potential data leakage and exposure to breach.

- The container should use a separate crypto module from the native OS cryptography.
- The container should utilize a FIPS 140-2 validated crypto module.
- The container cryptographic module should encrypt both data-at-rest and data-in-transit.
- The container should maintain file level encryption at all times (i.e., no unencrypted temporary files are created when a document is in use).
- The container should maintain encryption when files are being copied from one app to another (i.e. Open-In).
- The container should support at a minimum the following DLP controls:
    - Restricts Open In and Copy/Paste by policy
    - Prevents automated OS "App Snapshots"
    - Obfuscates stored file name in file systems
    - Prevents unencrypted copies during Open In
    - Prevents file sharing to Facebook and Twitter
    - Prevents AirDrop of files without utilizing Supervisor Mode
    - Encrypts all browser cache, bookmarks, cookies, and other sensitive data

- The container should protect any locally stored authentication credentials with its separate cryptography and not rely on native encryption.
- The container should support alternative authentication options that do not store backend credentials, such as passwords or certificates on the device (i.e., such as Kerberos or other IAM service providers).
- The container authentication framework should be extendable to add 2-factor authentication support as required.
- The container should not rely on device-wide VPN for backend system access.
- The container should provide dedicated secure transport for accessing backend systems.
- The container should not require additional VPN licenses or hardware for backend connectivity.
- The container should utilize proper certificate validation for HTTPS/TLS communications (i.e., certificate pinning).
- Each container should integrate jailbreak/root detection at container login and IT-defined intervals (i.e., not relying upon just the MDM agent).
- The container should be able to conduct jailbreak/root detection offline (i.e., airplane mode, no available connectivity).
- The container should use separate encryption from the native OS to encrypt and protect log files.
- The container should encrypt backup data with separate encryption from native OS (i.e. iTunes encrypted Backups, iCloud backups).

GOOD CONTAINER UNIQUELY PROTECTS YOUR CONTENT, CREDENTIALS AND CONFIGURATIONS

Mobile operating systems have unique security gaps that may expose a variety of attack vectors, such as Man-in-the-Middle (MITM), brute force, and forensic recovery. This can lead to corporate data loss or expose credentials and configuration information that can support attacks against back end systems. Ensure your mobile devices aren't providing unintentional access to this critical corporate information. The Good secure container supports all of the above requirements, thereby mitigating the potential risks exposed by relying on the native operating system alone.

In addition to security weaknesses in the native operating system, apps can also be potential sources of data leakage or exposed credentials and configuration data. Even cloud-based apps can be susceptible, for example, if corporate content is synched to local storage where they become dependent on device security controls. And there have been several highly publicized vulnerabilities and exploits whereby cloud services customers' credentials have been exposed. Native controls and MDM have limited ability to protect against apps and cloud services that do not enact enterprise grade security controls via container or other mechanism. The Good secure container secures cloud data stored in local apps while protecting credentials and configuration data that could be used to access cloud-based accounts and systems.

Click **here** to get more detailed information on Good's containerization, or click **here** to understand Good's security methodology and security certifications.

ABOUT GOOD

Good Technology is the leader in secure mobility solutions, providing the leading secure mobility solution across all stages of the mobility lifecycle for enterprises and governments worldwide. Good offers a comprehensive, end-to-end secure mobility solutions portfolio, consisting of a suite of collaboration applications, a secure mobility platform, mobile device management, unified monitoring, management and analytics, and a third-party application and partner ecosystem. More than 6,000 organizations in over 190 countries use Good Technology solutions, including FORTUNE® 100 leaders in commercial banking, insurance, healthcare, and aerospace and defense. Learn more at **www.good.com**.

Global Headquarters
+1 408 212 7500 (main)
+1 866 7 BE GOOD (sales)

EMEA Headquarters
+44 (0) 20 7845 5300

Asia / Pacific Headquarters
+1 300 BE GOOD