V-KEY

STRONGER WITH V-OS

FEATURES COMPARISON

V-OS App Protection is a SDK based solution to provide mobile app protection.

App Wrapping (a.k.a. codeless) based solution does not require modification of the mobile app's source code. Examples are DNP HyperTech CrackProof, Verimatrix.

	V-OS APP PROTECTION	APP WRAPPING BASED SOLUTION
APPROACH	SDK based solution requires mobile app developer to integrate SDK into mobile app source code by calling appropriate APIs.	Mobile app developer applies app protection to compiled app binaries (APK or IPA files) by uploading them to a service or processing them through a tool.
PROTECTION AREA	Mobile app developer focuses on the important area to be protected. • The protection is specific to the application logic • Adds about 2MB to app size (depends on features used) • Encrypted troubleshooting logs allow Customer Support to resolve issues	Solution automatically selects areas to be protected, which may include non-critical areas and may miss out critical areas.
USER EXPERIENCE	Mobile app developer has better control to provide optimal user experience. E.g. app developer can decide what message to display to user in different threat scenarios, when to use Secure Keyboard, etc.	Mobile app developer has no control over user experience changes imposed by the solution.

Content is based on publicly available information and provided only for information purposes.

FEATURES COMPARISON

	V-OS APP PROTECTION	APP WRAPPING BASED SOLUTION
SECURE CRYPTOGRAPHY	V-OS provides isolated execution environment to protect sensitive keys. Architecture is similar to GlobalPlatform's Trusted Execution Environment (TEE). It is a layer between device operating system and host application. Strong protection from brute force, dynamic, and static attacks. It is a proven approach which has passed multiple global pentests without any security breach.	Obfuscation and White Box Cryptography (WBC) are applied to the mobile app binaries. *Problems with obfuscation:* • Application size is increased significantly • Difficult to troubleshoot if problems are caused by obfuscation • Most obfuscation schemes can be easily defeated (e.g. by injecting faults) *Problems with WBC:* • Slower and requires more resources • Restricted to symmetric-key cryptography • DCA, DFA and SIFA have been successfully used to extract keys from WBC implementations.
DATA PROTECTION	V-OS stores sensitive information in Trusted Storage. Secure File IO SDK utilizes V-OS trusted environment to provide device bound protection to file, database and byte array.	Use of Obfuscation and White Box Cryptography (WBC) to protect data. See above for weaknesses of this approach.
MALWARE PROTECTION	Malware (with whitelist/blacklist) can be detected. Response to the detected malware can be customized.	Unable to detect malware.
DEBUGGER/EMULATOR DETECTION	Debugger/emulator are detected to prevent attacker from accessing sensitive runtime information.	Unable to detect debugger/emulator.

Content is based on publicly available information and provided only for information purposes.

FEATURES COMPARISON

	V-OS APP PROTECTION	APP WRAPPING BASED SOLUTION
CLIPBOARD CONTROL	V-OS App Protection provides protection on native apps against unintended data leakage in copy/paste buffer. This feature could be configured remotely and updated on runtime.	Unable to control the clipboard.
REMOTE ADMIN TOOL DETECTION	RAT are detected to prevent attacker from accessing sensitive information remotely.	Unable to detect RAT.
ROOT/JAIL BREAK DETECTION	Rooted/jailbroken devices are detected. Profile can be configured to quit the app or continue running. App is still protected in a compromised device.	Mobile app is not protected in a compromised device. Mobile app cannot run in rooted/jailbroken devices.
APPLICATION TAMPERING	Detects whether an app has been re-signed or tampered.	Prevents tampering with application.
HOOK DETECTION	V-OS App Protection detects hook.	Unable to detect hook.
SWIZZLE DETECTION	V-OS App Protection detects Objective-C method swizzling.	Unable to detect swizzling.
KEY LOGGING	Secure keyboard to protect against capturing sensitive data entered by the user.	Unable to protect against key logging.

Content is based on publicly available information and provided only for information purposes.

FEATURES COMPARISON

	V-OS APP PROTECTION	APP WRAPPING BASED SOLUTION
NETWORK PROTECTION	SSL pinning and optional mTLS (Mutual Transport Layer Security) to mitigate Man-in-the-middle attack.	Unable to provide mTLS.
DEVICE BINDING	V-OS creates device fingerprint (DFP) based on the device information. DFP is one of the parameters to derive keys to protect the runtime environment.	Unable to provide device binding.
TIME FENCING	Enable/disable mobile app usage during a specific time period of a day. Useful for scheduling a server maintenance.	Unable to provide time fencing
OVER-THE-AIR (OTA) UPDATE	Profile configuration, malware signature, V-OS can be updated over the air (OTA). Response to the attack/malware can be modified via OTA. Latest malware signature is downloaded to protect the mobile device. New V-OS features can be added without downloading the host application.	Unable to be updated over-the-air.
THREAT INTELLIGENCE	Collects device threat information and sends them to backend App Protection Server for analysis and/or decision making.	No threat intelligence.

Content is based on publicly available information and provided only for information purposes.