V-OS MOBILE APP PROTECTION

Mobile App Protection SDK
Mobile App Shield

V-KEY

Connect, Deploy, and Get Protected in Minutes

V-Key's V-OS Mobile App Protection is a multi-layered, mobile-first solution specifically designed to prevent attackers from gaining insight into your source code and modify or extract valuable information from it. Built on top of V-Key's patented V-OS Virtual Secure Element as its ultra-secure foundation, V-OS Mobile App Protection protects your mobile applications with its proven Runtime Application Self-Protection technology (RASP) from the ever-evolving matrix of malware and threats running on Android, iOS and HarmonyOS – even on rooted or jail-broken devices. Shield your apps from reverse engineering, tampering, API exploits, and other attacks that can put your business, your customers, and your bottom line at risk.

Available in two formats as a full-featured SDK **(Mobile App Protection SDK)** or as a light-weight app wrapper **(V-OS App Shield)** that can secure an app in minutes.

Mobile App Protection Features (SDK)

- RUNTIME APPLICATION SELF-PROTECTION (RASP) BUILT IN
- EMULATOR AND HOOKING DETECTION
- DEVICE AND FILE SYSTEM INTEGRITY CHECKS
- SECURE ANTI-KEYLOGGER KEYBOARD
- SMS HIJACKING PROTECTION
- CODE OBFUSCATION FOR PROTECTION AGAINST REVERSE ENGINEERING
- OVERLAY AND SCREEN MIRRORING PROTECTION
- SECURE CRYPTOGRAPHIC FUNCTIONS FOR BOTH DATA-AT-REST AND DATA-IN-USE
- APP INTEGRITY CHECKS AGAINST TAMPERING
- NETWORK INTEGRITY CHECKS AGAINST MAN-IN-THE-MIDDLE (MITM) ATTACKS ON DATA-IN-TRANSIT

Designed to operate in untrusted operating systems and app environments, the Mobile App Protection SDK gives App developers freedom to design and build the best user experience possible on Android, iOS and HarmonyOS devices without compromising security. The SDK comes out-of-the-box with myriad configurable options for various threat categories, responses and policies that can be easily updated over-the-air as new threats evolve. An intelligent administrative dashboard provides active threat intelligence that can prevent Java hooking attempts, generate compliance reports, and verify the effectiveness of your current mobile security strategy.

WHAT WE DO

V-Key is a software-based digital security company whose technology powers security solutions that deliver the highest level of defence and control for digital identity, user authentication, access and authorisation -- without compromising the user experience. It is trusted by government, banking, and mega-app clients across the region to connect people, organisations, and devices everywhere by securing the global digital economy.

OUR MISSION

To provide a secure Universal Digital Identity to power trusted digital services globally.

V-Key provides trusted, reliable, and secure Digital ID services that enable people to truly and safely participate in the modern economy.

FOR MORE INFO ON MOBILE APP PROTECTION

Contact insidesales@v-key.com

V-OS VIRTUAL SECURE ELEMENT · V-OS APP IDENTITY
V-OS MOBILE APP PROTECTION · V-OS MOBILE SMART TOKEN · V-KEY SMART AUTHENTICATOR

info@v-key.com   www.v-key.com

V-OS App Shield Comparison vs Mobile App Protection SDK:

FEATURES / FUNCTIONALITY	SOLUTION	
	V-OS App Shield	V-OS Mobile App Protection (SDK)
Cloud-based Integration	✓	
No-code Integration	✓	
Reverse Engineering Protection	✓	✓
Runtime Attack Protection	✓	✓
Regular OTA Updates	✓	✓
Fully customisable threat responses		✓
Strong Encryption of specific data/keys		✓
Advanced Protection		✓

Obfuscation Solutions vs V-OS Mobile App Protection

Most in-app protection vendors implement one or more of the following: Obfuscation, Runtime Application Self-Protection (RASP), Whitebox cryptography. All these, on their own, can be easily by-passed, or suffer from code lifting. A virtual secure element like V-OS has tamper protection capabilities that cannot be by-passed and is not susceptible to code lifting attacks.

	Typical Obfuscation Solutions	V-OS App Protection
Integration approach	Automated application of obfuscation based on configuration file	SDK integration provides better control over usage of features and flexible user experience
App size	Increased significantly after obfuscation	Adds about 2MB to app size (depends on features used)
Supportability	Difficult to troubleshoot if problems are caused by obfuscation	Encrypted troubleshooting logs allow Customer Support to resolve issues
Security	Most obfuscation schemes can be easily defeated	Critical code (defenses and crypto) are strongly protected by V-OS through isolation, which is proven through FIPS 140-2 and CC EAL3+ certifications
Threat intelligence	No ability to collect threat information from endpoints for analysis	App Protection Server collects threat intelligence from all endpoints, which can be analyzed or fed into other systems such as fraud detection or SIEM

V-OS App Shield

V-OS App Shield is a simple yet powerful codeless protection solution that can be deployed in three easy steps and does not require any modification of the app's source code. For the Basic App Shield service, just upload the APK or IPA file (step 1) to the cloud-based App Shielding platform. V-Key applies Code obfuscation and App shielding (step 2). Then simply download the protected APK or IPA file (step 3). The Premium Shield package includes V-OS App Protection server access in V-OS Cloud, CI/CD/DevSecOps integration and advanced shielding options. Currently available on Android operating systems only.

Automatically Apply V-OS App Protection Features

CI / CD / DevSecOps Integration

- App Protection Profile
- Secure Keyboard (for password fields)
- Device Binding
- Secure File IO for Specific Files/DB
- Anti - Screenshot
- String & Constant (e.g., API Keys) Externalisation and Encrytion
- Reports: Permissions, Protections Applied, etc.,

THE V-OS VIRTUAL SECURE ELEMENT

At the heart of V-Key's product suite is V-OS, the world's first Virtual Secure Element to be FIPS 140-2 (US NIST), achieve FIDO security targets, and be Common Criteria EAL3+ certified. It has also been accredited by the Infocomm Media Development Authority of Singapore (IMDA). V-OS creates an isolated virtual environment within mobile applications to safely store cryptographic keys and other important information.

V-OS VIRTUAL SECURE ELEMENT • V-OS APP IDENTITY
V-OS MOBILE APP PROTECTION • V-OS MOBILE SMART TOKEN • V-KEY SMART AUTHENTICATOR

info@v-key.com   www.v-key.com