V-Guard Mobile Application Protection

KEY BENEFITS

What

- Mobile application intrusion detection and protection system
- Mobile application embedded framework SDK of highly secure developer APIs

How

- V-Guard uses V-Key's patented V-OS to secure sensitive processing and data for mobile software applications
- Ensures your mobile application integrity when deployed to high-risk customer mobile devices
- Seamless mobile application integration for both public and enterprise mobile applications
- Notify V-Key's V-Track server on all mobile application activations and threat events

Why

- Protect mobile applications from both known and unknown threats
- Secure application data and safeguard user privacy even if the mobile device is lost or compromised
- Provide complete visibility via V-Key's V-Track server

Achieving Real-Time Mobile Application Protection

Mobile devices today contain full-fledged operating systems that support a wide variety of features that can be leveraged by mobile applications to provide a rich user experience. However, these features can be exploited by malicious applications, or malware, to compromise user information and exploit implicit trust in the mobile phone. This insecurity of mobile phones limits the use of these ubiquitous platforms for transactions or storage of user information requiring a higher level of security, including financial transactions and sensitive communications.

V-Key has developed a highly secure framework, V-Guard, that integrates with mobile applications to secure them against advanced persistent threats, including hackers, trojans, and rootkits. V-Guard is built on top of V-Key's patented V-OS to offer tamper-proof security for applications, ensuring the integrity of customers' and employees' mobile devices and mobile applications. Mobile applications protected with V-Guard can now be used as trusted applications, securing the user's sensitive information and transactions even if the mobile device itself is lost or compromised.

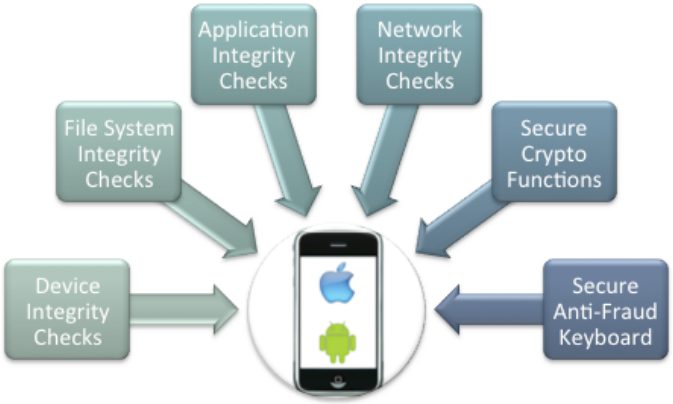
>> V-Guard Mobile Application Protection

Multi-Layered Security Features

V-Guard implements multi-layered security mechanisms to help secure the mobile application. These include; binary code morphing, anti-reverse engineering, trojan detection mechanisms, and device integrity checks, as well as tamper-detection and response mechanisms. These mechanisms have been developed based on V-Key's extensive research into mobile attack vectors and best-available defenses.

V-Guard allows mobile application developers to secure data and safeguard end users' privacy, such that an attacker with control of the underlying software environment is unable to steal information from the application or user.

V-Guard also gives mobile application developers secure replacements for unsafe native functions, including a secure virtual keyboard and number pad for password, credit card, and PIN entry.



For more information

For more information, contact **info@v-key.com** or visit **www.v-key.com**.

SPECIFICATIONS

Security Features

- Run-time threat detection with configurable protection controls
- Device integrity checks for malware such as keyloggers
- File system integrity checks to detect backdoors and rootkits
- Application integrity checks protect against tampering
- Network integrity checks guard against man-in-the-middle attacks on data-in-transit
- Secure cryptographic functions guard your data-at-rest
- Replacements for insecure native functions with V-Guard's highly secure developer APIs
- Multi-layered checks and anti-tamper mechanisms

Trusted Mobile Middleware

- V-OS patented mobile Virtual Secure Element
- Tamper-proof virtual layer ensures app cannot be hacked

Platforms

- Apple iOS and Google Android, both natively and with middlewares such as PhoneGap

V-Key Inc
72 Bendemeer Road, #02-20 Luzerne, Singapore 339941
Tel: +65 6471-2524
E-mail: info@v-key.com

RED HERRING GLOBAL WINNER 100

SiTF AWARDS2012 Awarding the finest in ICT innovations