V-KEY
STRONGER WITH V-OS

V-OS App Protection

Mobile Digital Identity, Authentication and Authorization

Stronger with V-OS

Virtual Secure Element

Building on the industry-leading patented V-OS Virtual Secure Element, V-Key has developed a highly secure framework that integrates with mobile apps to secure them against advanced persistent threats, trojans, and rootkits.

Protection with Threat Intelligence

V-OS secures sensitive processing and data, ensuring app integrity when deployed, and safeguarding user privacy even if the device is lost or compromised.

- ◆ Device integrity checks for malware
- ◆ File system integrity checks to detect backdoors and rootkits
- ◆ App integrity checks against tampering
- ◆ Network integrity checks against MITM attacks on Data-in-Transit
- ◆ Secure Cryptographic functions for both Data-at-Rest and Data-in-Use
- ◆ Secure Anti-Fraud Keyboard

Threat Intelligence Security Management

Designed as the Mobile Threat Command and Control system, enterprises can configure security policies to manage attack response and control.

- ◆ Collect Real-time App Threats
- ◆ OTA Policy Updates
- ◆ Extensive RESTful web services
- ◆ Integrate easily with MDMs, SIEMs, and other Threat Analytic Engines for seamless management

STRONGER WITH V-OS

- Mobile Identity
- V-OS App Protection
- V-OS Smart Token
- V-OS Messaging
- V-OS Face Biometrics
  V-OS eKYC

BENEFITS

Multi-layered Security
Binary Code Morphing, Anti-reverse engineering, trojan detection mechanisms, Tamper response mechanisms.

Application Controls
Limit users on How, When, and Where they use your applications, including Geo-fencing or enforcing time limits.

Threat Response Policies
Set policies on how apps should react to threats

Android and iOS Support
Small footprint on mobile platforms.

V-OS APP PROTECTION FEATURES AND SPECIFICATIONS

Robust App Protection solution secured by the anti-fraud, anti-malware
V-OS Virtual Secure Element

V-OS App Protection server provides a number of policy controls that administrators can use.

Add trusted TLS / SSL Servers for data-in-transit protection. Customize how the application will respond to mobile threats.

- Real-time information on App Threats detected by mobile applications
- Threat forensics for which mobile apps are being attacked from where, when, and which attack vectors
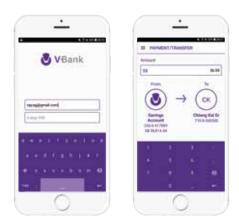- Issue individualized V-OS cryptographic modules for identity and authentication

Platforms

OS: Red Hat Enterprise Linux (RHEL)

Server: JBoss EAP, WebLogic

Database: MySQL, MariaDB, Oracle, Microsoft SQL Server

V-Key implements secure keyboards against keylogging in order to provide defense-in-depth against this common attack on mobile applications. For additional threat protection and intelligence, the solution also scans for keylogging techniques using a combination of heuristic checks and signatures.