Data Sheet

Mobile Runtime Application Self-Protection (RASP)

Security gaps are often found in mobile applications, raising concerns about protecting in-app transactions on Android and iOS platforms. Strengthening safeguards against on-device malware threats is essential to enhance fraud prevention efforts across these applications.

Complete Visibility and Protection

iVerify Mobile Runtime Application Self-Protection (RASP) offers threat visibility and real-time protection on devices. It uses SDK integration and proprietary advanced threat telemetry to defend against advanced threats targeting the device, allowing application vendors to prevent app access on compromised devices.

Key Benefits

- **Real-Time Threat Monitoring** - Continuous visibility into threats during runtime through a centralized dashboard enables teams to make timely, informed security decisions.
- **Reduce Fraud Risks** - Protect against advanced mobile threats that could hijack accounts to prevent unauthorized financial transactions.
- **Malware Defense** - Safeguard sensitive personal and financial information from being compromised by advanced threats during in-app processing and viewing.
- **Full Visibility** - Real-time insights into emerging threats help app teams remain informed about the latest security trends, keeping apps secure.

Why iVerify RASP for Mobile Security

Implementation:

- Utilizes SDK integrated into the mobile application
- Monitors phone behavior to detect threats, including runtime attacks, data interception, and user interaction exploits
- Operates in real-time with minimal changes to the application's code

Threat Response:

- Policy-defined actions trigger immediate detection response
- SDK alerts the host app with detailed, actionable forensics
- Enables real-time threat containment and response

Threat Monitoring and Analysis:

- Actively monitor risks using a threat dashboard
- Provides data to analyze and enhance protective measures
- Supports customized threat responses or callback actions

Policy and Scalability:

- Updated threat policies in real time without new release
- Scalable and efficient for apps with large user base

Key Detection Capabilities to Prevent On-Device Abuse

RASP is implemented using an SDK integrated into the mobile application. The SDK can monitor the phone's behavior and detect potential security threats, including runtime attacks, data interception, and user interaction exploits, in real-time with minimal changes to the application's code.

A policy-defined response triggers immediate on-device action when a threat is detected. The SDK alerts the host app, providing detailed, actionable forensics, enabling the app to respond in real time to contain the threat.

With the threat dashboard, security teams can actively monitor risks and respond as needed. This data also helps development and security teams analyze threat patterns and strengthen protective measures. App teams can choose from pre-configured threat responses or customized callback actions. Importantly, threat policies can be updated in real time without requiring a new app release, making it scalable and efficient for large user bases.

Essential Detections to Prevent Runtime Threats

- Hooking Frameworks
- App Tampering
- System Tampering
- Privilege Escalation Detection
- Device Security Disabled
- Insecure Device Settings
- Actively Exploited Android Versions
- Actively Exploited iOS Versions

Detect Risk, Threats & Attacks

- Malware
- Tampering
- Screen Overlay
- Screen Sharing
- Privilege Escalation
- Accessibility
- Permissions Network
- Traffic Interception

iVerify.

iVerify believes users shouldn't have to sacrifice privacy for security. Our easy-to-deploy solution provides fleet-wide iOS and Android security telemetry without requiring a management profile on the device. This lets users keep their personal data private and secure their mobile devices from advanced malware, vulnerabilities, and targeted attacks.

Request more information or a demo at iverify.io/contact