Lookout + Trustonic Partnership Brief

Enhancing mobile security for payment and banking applications

Mobile apps – the new hacker battleground

Mobile apps have become a key part of everyday life to manage everything from booking travel to handling finances. Service providers and financial companies increasingly rely on these mobile apps to deliver innovative consumer experiences and increase brand engagement. However, the rise in adoption of mobile is creating a corresponding rise in cyber threats focused on iOS and Android apps and devices. Malicious attackers are now targeting financial apps on mobile to steal login credentials to bank accounts and transaction platforms by leveraging malicious apps, banking trojans, and mobile phishing to compromise customer accounts and commit fraud, which creates a need for both software and hardware-backed security solutions for sensitive operations.

Most enterprises and banks have some mobile security in place but lack a holistic solution because the general assumption is that mobile is more secure by nature than web or other channels. However, credentials and data can be compromised on mobile just as easily, and once malicious actors have that information, they can use it across both web, mobile, and other platforms to initiate an account takeover and other fraudulent activity.

Lookout provides the visibility and security necessary to ensure devices are healthy enough to access an organizations internal and consumer apps, and together with Trustonic's Trusted Application Protection (TAP), developers can leverage advanced application protection to secure critical mobile apps for digital banking, payments, mPOS, and mobileID. Lookout and Trustonic work side-by-side to provide the ideal solution by providing mobile device security, secure storage, and the secure transaction environment required for a mobile transactional environment.

App Risk Posture

Security and risk visibility into all devices across the mobile app user base

Custom Remediation

Define remediation workflows to mitigate data compromise and risk of reputation damage

Speed to Market

Frictionless deployment of secure mobile apps with a simple lightweight SDK

Hardware Isolation

Execute sensitive parts of application and store customer data within the TEE

Advanced Threat Detection

Zero-day and compromised device detection leveraging large data sets

Compliance and Privacy

No PII is collected ensuring alignment with aspects of compliance standards

Lookout App Defense SDK

The Lookout App Defense solution allows developers to protect mobile apps using an embeddable lightweight SDK for both Android and iOS. Once the SDK is integrated into the app, it connects to the Lookout Security Cloud, which enables threat detection fed by data from over 170 million devices and 70 million analyzed mobile apps.

Organizations and developers can access security telemetry generated by Lookout App Defense to mitigate risks their app faces based on the severity and type of threat. The SDK has existing integrations with security tools such as SIEM and risk rating models via the Lookout Event Feed API, which provides a feed of raw security event telemetry. Overall, the SDK can help you reduce the risk of fraud and data compromise, comply with standards such as GDPR and PSD2, and actively protect customers and enterprises by identifying potential threats present on the user device running the mobile app.

About Trustonic

The Trustonic Secure Platform (TSP) is integrated into more than one billion devices today. TSP provides devices with a hardware protected environment for applications. Trustonic is the industry's only provider of these advanced capabilities at scale, and the only vendor whose mission is to open access to the capabilities to third-party developers. Service providers across a broad range of verticals use Trustonic's development tools to develop and deploy trust enhanced services. Specifically, Trustonic's Trusted Execution Environment (TEE), which is embedded in over 1.7 billion mobile devices, provides hardware/software protection to enable secure trusted operations. Trustonic TEE can protect biometric keys, user credentials, and sensitive transactions on the device enclave to protect confidential information.

Contact the Teams

Lookout®

www.lookout.com/products/app-defense

appdefensesales@lookout.com

TRUSTONIC

http://www.trustonic.com/

sales@trustonic.com