

Lookout App Defense SDK

Advanced mobile app protection against customer data compromise and fraud

Threat detection powered by 180M+ devices and 90M+ apps

Lookout has the industry's largest mobile dataset, which ensures that the protection deployed into both your internal and consumer mobile apps is fed by the latest security data, threat trends, and protection policies.

The most mobile security patents in the industry

Lookout has over 130 patents dedicated solely to mobile. This number increases significantly year-over-year, showing our commitment to continued investment in security R&D.

Unmatched device compromise detection capabilities

Lookout goes beyond the reach of traditional security tools and techniques to detect device compromises. In most cases, cyber criminals resort to advanced jailbreak and rooting techniques, including persistent and non-persistent elevation of privileges, that circumvent typical detections in place.

Advanced malware detection capabilities for malicious apps

Detect both known and new malware via machine-learning backed auto-conviction capabilities and shared intelligence with Google, Apple, Microsoft, and other leading members of the cybersecurity community. Examples of detection include Pegasus, BancamarStealer, Cerberus, Gustuff, Monokle, WannaLocker, WannaHydra, AgentSmith, and others.

Custom remediation workflows based on classifications

Gain visibility into risk across your entire customer base with mobile App Risk Posture and malware classification based on severity, intent, and other threat characterizations. Create custom threat mitigation and remediation to make your app self-protecting

Robust anti-tampering capabilities

Protect your app from malicious actors that may leverage screen overlays, app re-packaging, fake keyboards, hooking frameworks and code injection, and other covert exploits that could compromise customer data

Extensive end-to-end mobile app protection partnerships

Lookout has partnered with Promon, which provides app shielding and anti-tampering to ensure coverage of extensive security concerns, Buguroo, which provides an anti-fraud solution, and Trustonic, which provides a Trusted Execution Environment (TEE).

Lightweight SDK with simple deployment

The SDK is optimized for performance to minimally impact devices and not interrupt or block app functionality. The cloud-first, device-assisted architecture minimizes the need for updates as new threats are detected, and Lookout threat telemetry easily integrates with SIEM and anti-fraud systems via REST APIs.