OneSpan

Datasheet

Break the attack chain with

Threat Protection SDK

Stop modern attacks with on-device threat detection

Protect mobile banking apps with on-device detection of malware, unsafe networks, and suspicious user-interaction patterns.

Protect mobile banking apps from sophisticated device- and network-based attack techniques with a lightweight, client-side set of SDKs that help teams detect compromised devices, reduce exposure to high-risk activity, and respond faster to device takeover, remote attack tools, and adversary-in-the-middle (AITM) atacks.

Designed as an additional, on-device defense layer for mobile app shielding Threat Protection SDK complements existing back-end controls and risk engines rather than replacing them.

Why Threat Protection SDK?

Mobile banking attacks now extend beyond traditional malware to include device compromise, session manipulation, and tactics designed to exploit trusted user behavior. Threat Protection SDK helps banks detect these risks earlier, protect customer sessions, and enhance security operations with on-device intelligence that supports faster, more informed response.

Proactively defend against advanced mobile app attacks

Threat Protection SDK helps identify compromised devices, unsafe networks, and suspicious user activity before attackers can manipulate banking sessions or trigger fraudulent actions. It enables your security team to detect:

- Known malware/banking trojans
- Remote attack attempts
- Sideloaded or untrusted apps
- Insecure network conditions
- Suspicious clipboard activities
- Abnormal app-switching patterns

These capabilities help interrupt attack chains earlier, protect customer funds, reduce operational and security risk, and support your organization's security and compliance objectives.

Meet growing regulatory and compliance requirements

Threat Protection SDK is purpose-built for organizations that needs a lightweight, client-side-only solution to help meet key regulatory expectations for detecting device- and network-based threats on mobile endpoints. Support mobile security and fraud control requirements across global markets, including guidance from:

- Monetary Authority of Singapore (MAS)
- Hong Kong Monetary Authority (HKMA)
- Taiwan's Financial Supervisory and Mobile Security Alliance (MSA)
- Reserve Bank of India (RBI) and National Payment Corporation of India (NPCI)
- Bank Negara Malaysia

Accelerate time-to-value with lightweight SDKs

Embed on-device protection quickly into existing mobile banking apps with minimal disruption. The client-side only integration approach helps teams comply with data privacy requirements and respond faster to emerging threats without disrupting user experience or development cycles.

Threat Protection SDK unifies critical mobile threat signals, spanning device, malware, network, and user-interaction risk, into one on-device defense layer, helping banks close security gaps and enhance mobile app shielding across their mobile portfolios.

Highlights

- **Strenghten in-app protection**
  Add an on-device detection layer to your existing mobile app security stack to identify device, malware, network, and user-interaction threats earlier.
- **Meet key regulatory expectations faster**
  Use lightweight, client-side SDKs to help address mobile security and device-threat detection requirements across multiple jurisdictions.
- **Gain richer threat visibility**
  Spot high-value signals on malware, remote attack tools, sideloaded apps, unsafe networks, and suspicious interaction patterns directly from the device.
- **Deploy with less friction**
  Integrate SDKs into existing Android and iOS apps with minimal changes, preserving user experience while improving security coverage.

How does Threat Protection SDK work?

Threat Protection is a suite of lightweight, client-side SDKs embedded directly into your mobile banking apps to provide on-device threat protection, real-time prevention, and seamless reporting. When a violation is detected, the SDK will immediately flag the threats and report telemetry to your security team, enabling you to block compromised devices before attackers can manipulate banking sessions or trick your customers into unintended actions.

1. Malware detection SDK: The SDK analyzes the cryptographic signatures of installed apps and packages against a list of known malware provided by the bank. It also detects RAT indicators such as accessibility-service abuse and unauthorized remote-control activity, and it identifies apps installed outside officiel or trusted distribution channels.

2. Network security SDK: The SDK monitors the device's active network connection for insecure Wi-Fi, VPN usage, and proxy-related risks. It returns network security status through real-time APIs and change listeners, enabling the app to detect network changes and respond when users connect through potentially unsafe conditions.

3. Threat Signal SDK: The SDK monitors user interaction patterns for signs of device abuse or malicious activity without interrupting normal app use. It generates non-blocking threat signals from clipboard activity and suspicious background-to-foreground app switching, enabling the app to warn users, log events, or trigger adaptive authentication while preserving an optimal user experience.

Product specifications

	Android	iOS
Malware Detection SDK Detect known malware through signature-based analysis, including RAT activity and sideloaded apps that may indicate device compromise or abnormal account activity.		
• Signature-based malware detection	✓	
• RAT detection	✓	✓
• Sideloading detection	✓	✓
Network Security SDK Detect insecure network conditions, VPN usage, and proxy-related risks to help identify potential interception threats.		
• Insecure network detection	✓	✓
• VPN connection detection	✓	✓
• Proxy detection	✓	✓
Threat Signal SDK Detectsuspicious clipboard activity and abnormal app-switching patterns without interrupting the user experience.		
• Clipboard analysis	✓	✓
• App switch analysis	✓	✓

Supported platforms

Android

- Android 7 (API level 24) or later
- Target Android 15 (API level 35)
- Support for 16 KB page sizes

iOS

- OS support:
  - Malware Security SDK: iOS 15 or later
  - Network Security SDK: iOS 15 or later
  - Threat Signal SDK: iOS 16 or later
- Swift 5 or later
- Xcode 16 or later

About OneSpan

OneSpan is a global leader in digital security, trusted by thousands of enterprises across 100+ countries—including more than 60% of the world's 100 largest banks— to safeguard digital accounts, secure financial transactions, and prevent fraud. Our award-winning solutions provide passwordless authentication, digital transaction security, and advanced mobile application protection, helping organizations meet the highest security standards and global compliance requirements. As cyber threats grow more sophisticated, OneSpan delivers cutting-edge technology to safeguard customers, mitigate risks, and ensure trust in every digital interaction.

Learn more at
OneSpan.com/security

Contact us at
OneSpan.com/contact-us