

# Promon Insight™

Trusted threat telemetry for mobile apps



# Promon Insight™

Close the gap between detection and action in mobile app security



Mobile apps are constantly under attack, often invisibly, whether by humans or AI. From rooting and jailbreaking to emulation, hooking, and screen scraping, attackers are actively targeting your apps and your users. These threats are increasingly automated, adaptive, and fast, outpacing what traditional tools can detect. Yet most organizations can't see these attempts because their tools rely on data from potentially compromised devices.

**Promon Insight™ changes that.**

By collecting runtime telemetry directly from SHIELD-protected apps, Insight delivers clean, structured, and privacy-conscious security data. It allows security, fraud, and SOC teams to detect threats, investigate incidents, and take action based on accurate, tamper-resistant data.

With privacy and data control built in, Insight is the missing layer between mobile threat detection and informed, timely response.

**Platforms**

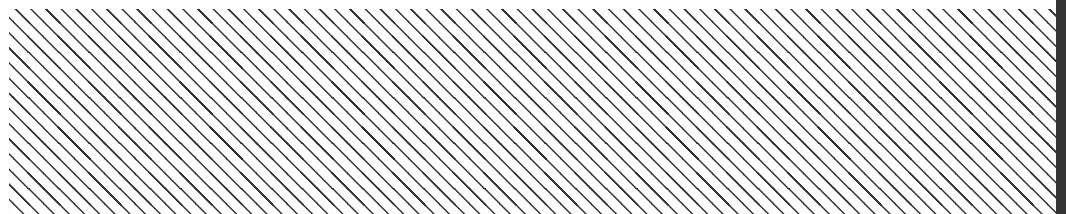
-  iOS
-  Android

**Architectures**

- Android:** armeabi-v7a, arm64-v8a, x86\_64
- iOS:** arm64-v8a

# Key benefits of Promon Insight™

- ✓ **Faster forensic investigations**  
Detailed, timestamped event data from real user devices helps your teams quickly understand what happened and why.
- ✓ **Expose hidden fraud signals**  
Detect and forward high-risk behaviors like hooking, screen readers, and emulators to your SIEM or fraud platform.
- ✓ **Simplified compliance**  
Support internal and external audits with runtime integrity signals and structured forensic data, built with GDPR and CCPA in mind.
- ✓ **Seamless integration**  
Export structured data to your SIEM, fraud systems, or Promon's dashboard in JSON or Protobuf. Works in cloud, hybrid, or on-prem setups.
- ✓ **Privacy-first custom enrichment**  
Add custom session IDs or user data to tie events to business context, without ever sharing PII unless explicitly configured.



# Real-world problems solved today

## **Forensic analysis**

Use Insight data to reconstruct what happened in a fraud or breach scenario. Forward events like debugger use, untrusted keyboards, or rooting indicators to your SOC to determine if and how your app was involved.

Who benefits: Fraud analysts, SOC teams, compliance leads

## **App threat telemetry**

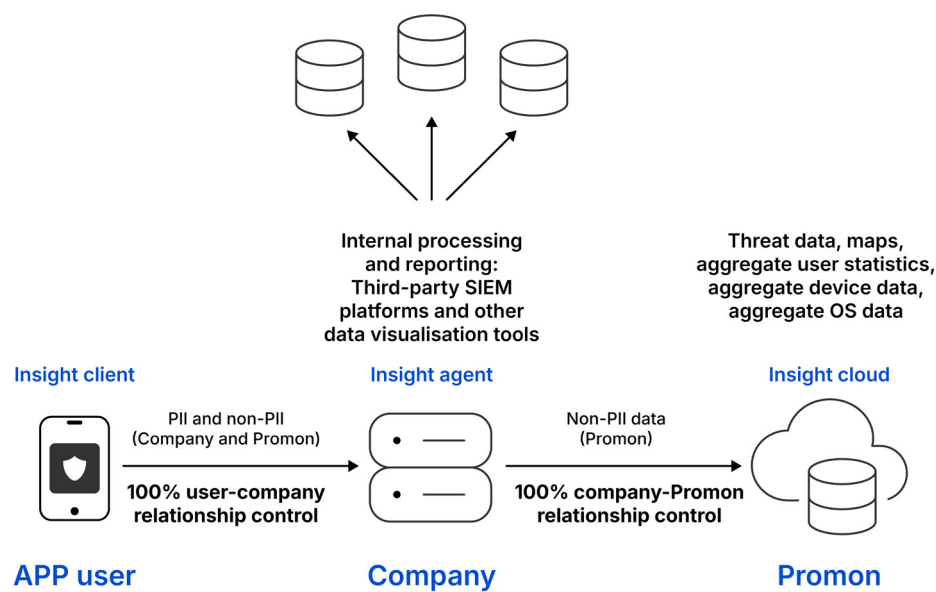
Capture SHIELD-detected threats like hooking, jailbreaking, or runtime manipulation—and route them to your systems for visualization and analysis. Get structured insight into the types of threats blocked by SHIELD.

Who benefits: Security teams, product owners, CISOs, security solution providers, and researchers



# Built on Promon Trust Architecture

Promon Trust Architecture ensures a secure, fully controlled relationship between organizations, their users, and Promon.



## Deployment options

Dashboard access is only available via Promon cloud. On-prem customers can forward data to their own tools for visualization.

Data sent to	PII	Non-PII	Dashboard access
Promon Cloud only	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Customer on-prem only	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> *
Promon and Customer	PII processed on-prem only	Non-PII sent to Promon cloud dashboard	Available for non-PII

\* Data fed into customer’s SIEM or fraud systems can be visualized there for analysis.

**What data does Insight collect?**

PII is never collected or sent unless explicitly enabled. Custom data is processed on-device and under customer control.

Type	Examples
App & device metadata	App version, OS version, SHIELD variant
Threat events	Rooting, jailbreaking, hooking, screen readers, emulators
Evidence data	(Severity-tagged event metadata)
Metadata	Timestamps, device instance ID (non-PII), agent ID, error logs
Custom data (optional)	Session IDs, fraud case IDs—configured by customer

PII is never collected or sent unless explicitly enabled. Custom data is processed on-device and under customer control.

# PROMON

## About Promon

Promon leads the way in proactive mobile app security. For 19 years, we've been making the world a safer place by securing any app, on any device—in no time at all. Today, we protect over 2 billion users, secure 13 billion monthly transactions, and safeguard \$2.5 trillion in market cap. Promon is headquartered in Oslo, Norway, with offices in more than 15 countries around the world.

## Would you like to talk to an expert?

Mobile app security is crucial to preserve and improve your business reputation. Request pricing or talk to an expert to learn more today.

[Book a meeting »](#)

[promon.io](https://promon.io)

**Promon AS**  
Cort Adelers Gate 30  
0251 Oslo  
Norway