Promon Insight™
Trusted mobile app security analytics

Promon Insight™ equips you with actionable, evidence-backed threat intelligence to reduce business and security risks. By seamlessly integrating with Promon SHIELD® for Mobile, it provides deep insights into app, device, and geographical risk profiles—enabling you to benchmark against industry and regional standards.

Built on the Promon Trust Architecture, Insight ensures a secure, fully controlled environment compliant with data protection laws. Enhance fraud detection, improve threat visibility, and accelerate data-driven decision-making across your security teams and business leaders.

Compatibility and support

Platforms

- iOS
- Android
- Linux
- Windows
- select Unix servers

Architectures

Mobile
Android: armeabi-v7a, arm64-v8a, x86, x86_64
iOS: arm64-v8a

Server CPU architectures
Linux: linux/amd64, linux/arm64, linux/riscv64
macOS (Darwin): darwin/arm64, darwin/amd64
Windows: windows/arm64, windows/amd64

Mobile apps are prime targets for cyberattacks like rooting, jailbreaking, hooking, phishing, and unauthorized access—posing significant risks to businesses and users.

With 67% of smartphone users worried about data security and the average data breach costing $4.88 million in 2024, the stakes have never been higher.

Promon Insight™ helps you navigate these challenges effectively. Analyzing telemetry data from your applications delivers near-instant, evidence-backed threat intelligence to detect anomalies like fraud attempts or malware attacks before they escalate. This proactive approach enables you to address vulnerabilities promptly, enhance app security, comply with regulations like GDPR and CCPA, and provide a safer experience for users. By cutting through false positives, Promon Insight™ lets your security teams focus on genuine threats and make faster, data-driven decisions.

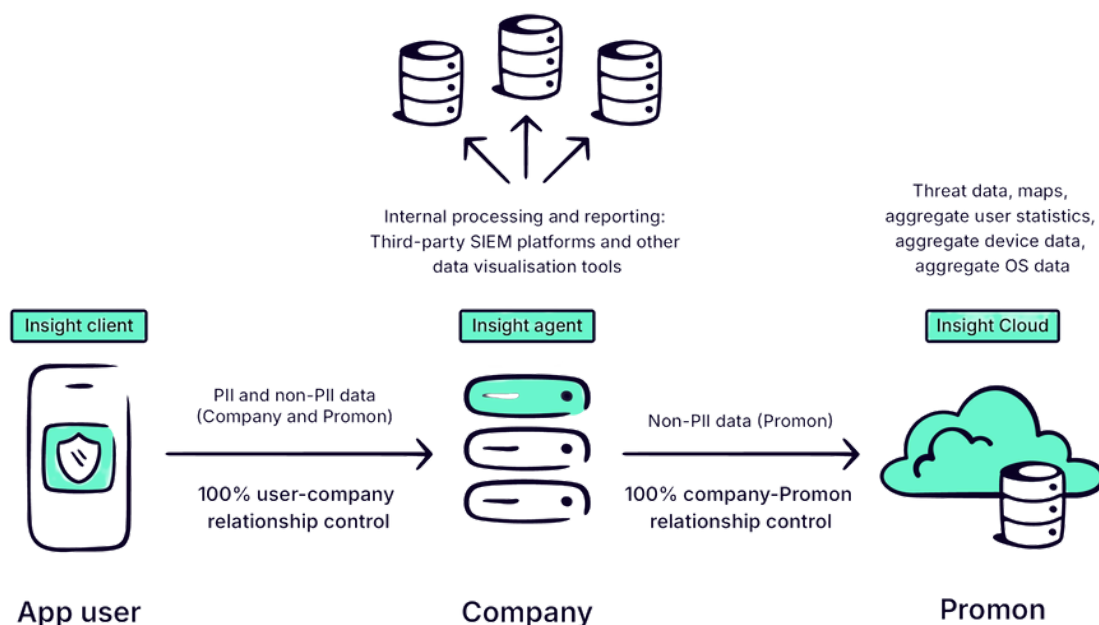# Benefits of app security analytics with Promon Insight™

✓ **Actionable, security-specific analytics**
Quickly identify and address security events like rooting, jailbreaking, runtime integrity breaches, and screen recording before they become critical. Insight provides near-instant, evidence-backed threat data, empowering your team to act faster on issues unique to your mobile apps.

✓ **Easy executive reporting**
Facilitate transparent executive reporting for better communication and faster decisions. With filters for operating systems, regions, and device manufacturers, stakeholders gain clear insights into app health, user activity, and threat levels. Ready-made dashboards and seamless integration with existing SIEM tools enhance collaboration between security teams and business leaders.

✓ **Complete control and privacy**
With Insight's on-premises implementation, you can maintain full control over your client-server architecture. Customize configurations, manage security settings, and tailor data flow to meet your needs. Privacy-focused by design, no user PII is sent to the Promon Insight Cloud. You can enrich data sets with PII while keeping complete control over personal data, ensuring compliance with GDPR and CCPA.

✓ **Reduce false positives**
Sifting through countless alerts—many of them false positives—is a major challenge. Promon Insight™ uses advanced threat signals enriched with evidence data to minimize false positives and improve detection accuracy, allowing your security teams to focus on real, actionable threats.

Top threats Filter ⌄ ...

Threat	Risk ⇕	Volume
Hooking Framework	High	11,743
Emulator Detected	High	1,251
Native Code Hook	High	535
Screen Reader	Medium	25,4
Rooted/Jailbroken	Low	535
Untrusted Keyboard	Low	132
Runtime Integrity	Low	132
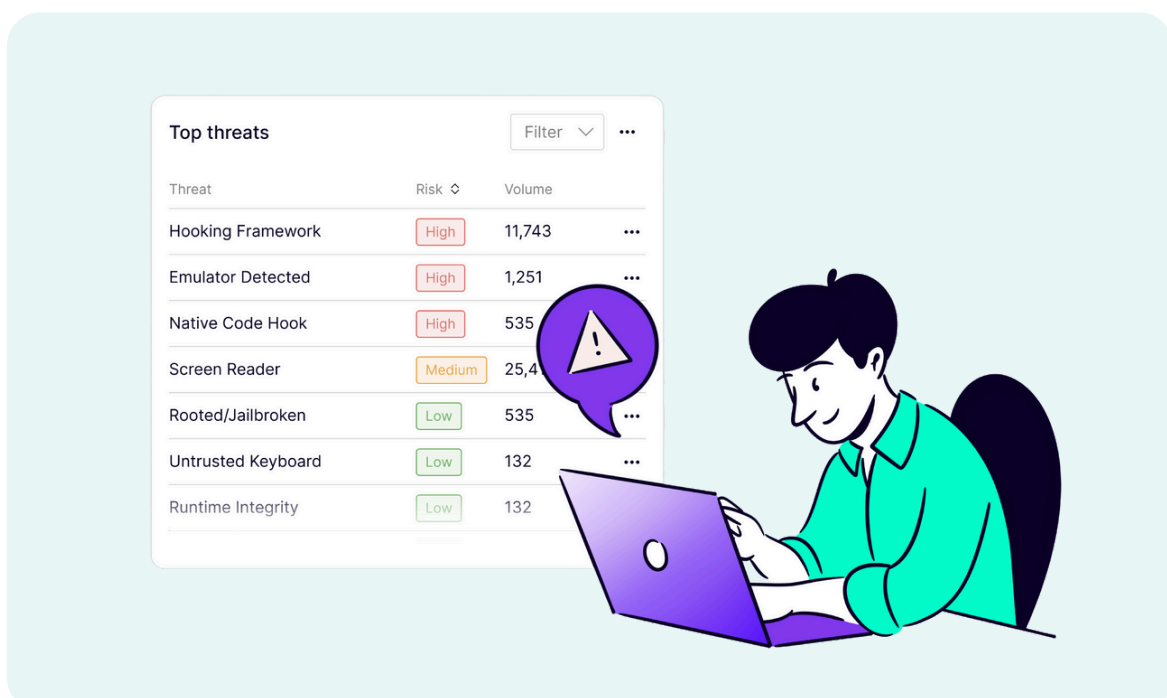
✓ **Prevent fraud**
Continuously monitor mobile app activity to detect unauthorized or fraudulent transactions, ensuring compliance with regulations like PSD2. Promon Insight™ identifies anomalies such as suspicious geolocations, enabling swift responses to safeguard sensitive payment data and reduce fraud risk.

✓ **Prevent intrusion**
Quickly identify and analyze suspicious activities and attack patterns across your entire install base. Stop intrusions before they escalate. Leverage security telemetry data to gain insights into unauthorized access attempts and fine-tune your intrusion detection systems, improving your overall security posture.

✓ **Forensic analysis**
Investigate security breaches with comprehensive forensic tools. Use app data to reconstruct events, identify the attack's root cause, evaluate its impact, and prevent future incidents. With the average cost of a data breach reaching $4.88 million in 2024, forensic analysis is essential to guard against future incidents.

Promon Trust Architecture

Internal processing and reporting:
Third-party SIEM platforms and other data visualisation tools

Threat data, maps, aggregate user statistics, aggregate device data, aggregate OS data

Insight client — **Insight agent** — **Insight Cloud**

PII and non-PII data (Company and Promon)
100% user-company relationship control

Non-PII data (Promon)
100% company-Promon relationship control

App user — Company — Promon

Promon Trust Architecture is the foundation of Promon Insight™'s app security analytics that ensures a secure, fully controlled relationship between organizations, their users, and Promon.

Promon Insight™ for your industry

Healthcare

Ensure data privacy and regulatory compliance, particularly for apps outside HIPAA coverage, and prevent unauthorized data harvesting.

Gaming

Detect cheating attempts and protect virtual goods through detailed activity insights.

E-Commerce

Monitor and ensure transactions are secure against bot-driven credential-stuffing attacks.

Finance and banking

Detect and prevent fraudulent transactions fast, safeguard user authentication, and quickly generate compliance reports.

Streaming

Prevent piracy and unauthorized access and understand the device and regional risk profiles.

👉 What data does Promon Insight™ collect?

The data collected will change over time with the evolving threat landscape, device and OS evolution. Initially, the data Insight collects will fall into the following categories:

1. Install-base data: Device manufacturer and model, operating system, version and architecture, app name and version, SHIELD version, etc.
2. Threat detections: jailbroken, rooted, untrusted keyboard, screen reader, emulator and hooking, etc.
3. Evidence data: data that validates the level of evidence behind the detection.*

Future capability

The data collected by Insight is carefully selected according to privacy laws such as the GDPR or CCPA. As Insight is based on the Promon Trust Architecture, custom data, which can be classified at PII data, will never be sent to the Insight Cloud. You will have the flexibility to send back any type of data you want without having to worry about privacy or compliance.

About Promon

Promon is the leader in proactive mobile app and SDK security. We make the world a little bit safer, one app at a time. Since 2006, some of the world's most impactful companies have trusted Promon to secure their mobile apps. Today, more than two billion people use a Promon-protected app. Promon is headquartered in Oslo, Norway, with offices throughout the globe. Mobile app security is crucial to preserve and improve your business reputation. Request pricing or talk to an expert to learn more today.

Learn more

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