OneSpan

Mobile Threat Insights and Response

OneSpan Next-Gen App Shielding

Real-time visibility and control over mobile app threats

Mobile applications are no longer attacked only at runtime. Modern threats combine device compromise, app cloning, API abuse, adversary-in-the-middle attacks, and automated fraud, evolving continuously across millions of devices and environments.

OneSpan's Next-Gen App Shielding extends in-app protection with cloud-based threat insights, transforming real-time telemetry into clear visibility, contextual understanding, and orchestrated response across the entire mobile ecosystem. Instead of isolated detections, security teams gain insights they can act on, instantly, consistently, and at scale.

Why threat insights are critical for mobile apps

Without centralized threat insights:

- Attacks remain fragmented across individual app instances
- Compromised devices continue accessing backend APIs undetected
- Security responses are delayed, inconsistent, or impossible to audit
- Compliance teams lack the contextual evidence required by regulators

OneSpan Next-Gen App Shielding converts millions of security events into actionable threat insights to enable faster decisions, smarter automation, and controlled escalation.

OneSpan's mobile threat insights & response platform

Next-Gen App Shielding augments mobile in-app protection with three cloud-based threat insights modules, enabling continuous monitoring, interpretation, and response across all protected applications.

Key capabilities:

- Real-time mobile security insights derived from app telemetry
- Centralized visibility into attack types, affected devices, and OS versions
- Policy-driven and adaptive response orchestration
- Manual, automated, or fully programmable response models
- Alignment with regulatory and compliance frameworks (PCI-MPoC, eIDAS 2)

TraceBoard

Human-supervised threat insights. Monitor, investigate, and respond through a real-time security console.

DeviceAttest

No-code automated enforcement. Policy-driven responses without technical expertise or code changes.

BuildAPI

Programmable threat integration. Embed insights directly into backend systems via REST and streaming APIs.

Three threat insights modes

Next-Gen App Shielding supports three complementary threat insights modes, allowing organizations to choose how insights are consumed and acted upon, depending on security maturity and operational needs.

TraceBoard: Human-supervised threat insights

TraceBoard provides a human-supervised threat insights experience, giving security teams real-time visibility into mobile attack patterns and individual incidents — all from a single web console.

What teams gain:

- A consolidated view of mobile threat insights across all apps and app versions
- Contextual breakdown by attack type, device, OS, and geography
- Drill-down into individual app instances and sessions
- Insight-driven response actions: **app lock, step-up authentication, or remote data wipe**

Best suited for:

- **Security Operations Centres (SOC)** requiring full visibility and control
- **Fraud and risk teams** investigating mobile-driven abuse
- **Regulated organizations** that require traceability, auditability, and human-in-the-loop decision-making

DeviceAttest: No-code automated threat insights

DeviceAttest turns threat insights into automated decisions, without requiring code or mobile security expertise. Security policies run continuously, enforcing responses the moment a threat is detected.

What teams gain:

- Policy-based automated responses driven by real-time threat insights
- Instant enforcement actions triggered without manual intervention
- Continuous device and app instance attestation
- Insight-driven enforcement aligned with security and compliance policies
- Compliance support for emerging standards such as PCI-MPoC and eIDAS 2

Best suited for:

- **Compliance and security teams** that need enforcement at scale without engineering overhead
- **Organizations adopting PCI-MPoC or eIDAS2** requiring automated attestation
- **Mobile product teams** looking for policy-driven security without code changes

BuildAPI: Programmable threat insights

BuildAPI enables organisations to embed Next-Gen App Shielding threat insights directly into their backend systems, supporting advanced response orchestration and enterprise integrations.

It is available in two variants, designed for different operational needs.

BuildAPI: Rest

Built for backend developers who need to trigger specific security actions, manage cryptographic keys, and integrate mobile threat detection directly into server-side logic and application workflows.

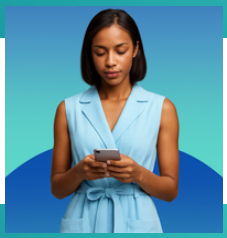
What it delivers:

- REST APIs to query threat insights and app/device trust status
- Programmatic triggering of security actions: block, step-up, revoke, isolate
- Cryptographic key management as a service
- Tight integration into backend workflows and application logic

Best suited for:

- **Backend and platform engineering teams** building custom security logic
- Risk-based access control and decision engines
- Highly customized security and fraud response workflows

BuildAPI delivers mobile threat intelligence your way, via REST for backend security logic, or streaming for real-time SIEM and SOC visibility.



BuildAPI: Streaming

Designed for Fraud and SOC teams that need to ingest a constant flow of security events into monitoring systems for real-time visibility and proactive threat correlation.

What it delivers:

- Continuous streaming of mobile security events
- Seamless ingestion into SIEM, SOC, and monitoring platforms
- Real-time correlation of mobile threats with enterprise security signals
- Proactive detection of large-scale or coordinated attacks

Best suited for:

- **Fraud teams** monitoring behavioral anomalies at scale
- **SOC teams** operating real-time security monitoring
- **Organisations with SIEM-centric security architectures**

From threat signal to action, at every stage of your security journey

Most platforms detect. OneSpan Next-Gen App Shielding responds.

Whether your team is building the first layer of threat visibility, automating compliance enforcement, or embedding mobile security into enterprise-grade workflows, Next-Gen App Shielding meets you where you are, and scales with you.

- Human-supervised insights for visibility and investigation (TraceBoard)
- No-code automated enforcement to meet compliance and scale requirements (DeviceAttest)
- Fully programmable, insight-driven orchestration through APIs and streaming (BuildAPI)

Ready to see it in action?

Discover how OneSpan Next-Gen App Shielding can protect your mobile ecosystem — from the first threat signal to the final response.

Request a demo

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