Better Together: Mobile EDR + App Risk Intelligence

Complete mobile risk visibility across every device and every app, without invasive controls.

The Mobile Security Gap

Mobile is the most under-secured endpoint in the enterprise, and it carries corporate credentials, sensitive data, and authentication for nearly everything else. Employees authenticate, collaborate, and handle regulated data on phones that generate no alerts and feed no investigation workflows.

Two distinct risk layers go unaddressed: the device (zero-click exploits, smishing, SIM swap, compromise) and the apps running on it (vulnerable components, SDK exposure, insecure data handling, and unreviewed AI tools). Traditional MDM and MTD tools were built for neither.

A Unified Approach to Mobile EDR and App Risk Intelligence

iVerify and NowSecure close the mobile security gap together: iVerify detects threats at the device and OS level (the spyware, smishing, and compromise activity that conventional tools miss), while NowSecure continuously analyzes the apps themselves for vulnerabilities, risky SDKs, and data exposure.

One platform, two layers of risk, finally correlated. You get complete mobile visibility across managed and BYOD fleets, without invasive controls

iVerify Enterprise *(Device Layer)*	**NowSecure (*App Layer*)**	**Combined Outcome**
Kernel-adjacent telemetry across iOS & Android	Continuous mobile app risk analysis	Unified device + app visibility
Behavioral detection of mobile compromise	Vulnerable & high-risk app detection	Richer investigation & remediation context
Smishing and SIM swap detection	SDK exposure & insecure configs	Faster identification of mobile exposure
Runtime mobile threat visibility	Privacy & compliance risk assessment	Stronger posture for managed + BYOD
Real-time alerts and SOC integration	App supply-chain / component analysis	Better governance & policy decisions
Device risk scoring & investigation	OWASP MASVS-aligned intelligence	Coverage MDM/MTD/EDR alone miss

Why the Combination Wins

One platform, integrated directly	NowSecure-powered app intelligence runs inside iVerify Enterprise evaluated alongside device telemetry in the same workflows. No standalone tooling, no fragmented visibility.
Correlated, not siloed signals	App risk is correlated with system-level device and network signals for a holistic view across the attack chain, something neither MDM nor legacy MTD was designed to do.
Continuous, not point-in-time	Approval is a one-time decision; apps keep changing. Approved apps are continuously monitored for new permissions, data flows, and behavioral changes.
The AI app blind spot, covered	Visibility into AI application usage across the fleet, so security teams can govern an emerging and fast-growing source of data leakage.
BYOD without invasion	Full app visibility across personal and managed devices, collecting only the security telemetry needed. No personal data, no usage logs, no enrollment friction.
Compliance built in	App risk continuously mapped against OWASP, NIAP, and frameworks including GDPR and HIPAA, supporting audit readiness without manual periodic reviews.

See It in Action

Watch our on-demand webinar to see how iVerify and NowSecure work together to deliver complete mobile security visibility, with a live demonstration of the integration.

Watch On-Demand →

Where Legacy Tools Fall Short

Category	Design For	The Gap It Leaves
MDM / UEM	Policy enforcement, configuration control, device wiping	Manages the device, not the apps on it. No continuous app risk scoring or compliance mapping
Mobile Threat Defense (MTD)	Basic app scanning and surface signals like jailbreak or network inspection	No deep analysis of app vulnerabilities, cryptography, or privacy; no behavioral monitoring of approved apps
Endpoint / EDR	Traditional endpoint detection and response	Operates above the OS layer on indirect signals. Misses risk from app behavior, third-party code, and AI integrations

Who It's For

- Highly regulated industries with continuous compliance needs, like financial services, healthcare, government & public sector
- BYOD-first organizations needing deep app visibility without compromising privacy or enrollment rates
- Organizations with high data sensitivity, where a single app compromise could trigger a catastrophic data leakage event
- Security engineers, SOC analysts, and IT/security leaders responsible for managed and BYOD mobile fleets

How It Works

1. **Deploy**	Deploy the iVerify agent fleet-wide across iOS and Android in minutes alongside an existing MDM/MAM, or standalone.
2. **Detect**	Apps are continuously analyzed via SAST, DAST, IAST, and APISec for vulnerabilities, privacy issues, behavioral changes, and compliance risk, then correlated with OS-level telemetry.
3. **Respond**	The platform alerts security teams to risky or non-compliant apps, enabling policy enforcement and targeted remediation.

Built on Industry Leadership

- NowSecure is the industry leader in mobile app security testing: 4M+ app assessments, 600+ automated tests per assessment across security, privacy, compliance, and supply chain
- App risk coverage spans both Google Play and the Apple App Store
- iVerify's threat research is recognized at the highest levels of the industry. The team observed and caught two exploit frameworks operating in the wild — Coruna and DarkSword — engaged in mass exploitation of mobile devices including iOS, investigated in partnership with Google's Threat Analysis Group. That same caliber of research earned iVerify a distinction no other mobile security company holds: a place in OpenAI's inaugural Trusted Access for Cyber Programs group.
- Standards-aligned: OWASP MASVS, NIAP, GDPR, HIPAA, and more

Get Started Today

See how combined device telemetry and app intelligence surface real mobile risk across a fleet. Request a demo at iverify.io/request-demo