iVerify. Enterprise

Mobile EDR for the Modern Threat Landscape.

OS-level visibility. Behavioral Baselining. Alerts your SOC can trust.

Mobile devices now sit at the center of enterprise identity and access workflows, used to access SaaS applications, approve MFA requests, communicate internally, and maintain persistent access to business systems. But unlike laptops and servers, mobile devices often operate with little visibility into compromise, credential theft, exploit activity, or identity abuse.

iVerify Enterprise changes that. Delivering true Mobile EDR, built specifically for mobile devices, it provides continuous OS-level telemetry, behavioral detection, and high-fidelity threat visibility across iOS and Android without invasive controls or mandatory MDM enrollment.

Key Benefits

OS-Level Mobile Visibility

Continuous telemetry collection & behavioral analysis to uncover exploit activity, credential theft, & compromise that MTD & MDM platforms miss.

Rapid Detection & Response

High-fidelity alerts, device risk scoring, investigation history, & telemetry streamed directly into existing SOC & incident response workflows.

Privacy-First Architecture

Built to minimize data collection while delivering enterprise-grade detection & response capabilities across personal & corporate devices.

Mobile-Native Threat Defense

Detect & respond to smishing, SIM swap activity, malicious applications, credential theft, & zero-click exploit campaigns.

Mobile App Risk Intelligence

Continuous visibility into installed mobile applications, risky SDK exposure, insecure configurations, & vulnerable software.

Flexible Deployment Options

Deploy iVerify Enterprise in cloud, hybrid, or on-prem environments to align with enterprise security, compliance, & operational requirements.

Workforce-Scale Mobile Protection

Protect managed & BYOD fleets without compromising employee privacy or requiring invasive device management controls.

Enterprise Security Operations Integration

Integrate mobile telemetry & alerts directly into SIEM, SOAR, identity, & SOC workflows through open APIs, webhooks, & real-time reporting.

Why iVerify

iVerify helps organizations close the mobile visibility gap with Mobile EDR, built specifically for the realities of modern enterprise infrastructure.

Unlike legacy mobile security approaches that focus primarily on device posture or malware signatures, iVerify delivers behavioral detection, OS-level visibility, and operational workflows designed to address modern mobile threats targeting enterprise identity, access, and communications.

Trusted by enterprises, governments, and privacy-focused organizations globally, iVerify has helped uncover and publicly document some of the most advanced mobile exploit activity observed in commercial environments.

SOC 2 Type 2 ■ **GDPR** ■ **ISO 27001:2022** ■ **TrustArc - TRUSTe**

Built for Modern Mobile Threats

Mobile EDR & Threat Detection

- Continuous OS-level telemetry across iOS and Android
- Behavioral detection for exploit activity and credential theft
- Detection of advanced mobile compromise, including Pegasus, Coruna, Predator, and DarkSword
- High-fidelity alerts integrated directly into SOC workflows
- Unified fleet visibility, device history, and investigation context
- Seamless integration with major UEM/MDM platforms for simplified enterprise deployment
- Approved Microsoft MTD partner

SmishGuard: Mobile Social Engineering Defense

- Detection of link-based and linkless smishing attacks
- Protection across SMS, messaging platforms, and browsers
- Sender reputation analysis and phishing infrastructure blocking
- DNS-level enforcement (SecureDNS) without invasive VPN routing
- Privacy-first architecture designed for BYOD environments

SIM Swap Detection

- Near real-time monitoring for SIM swap indicators
- Continuous monitoring to detect identity-focused attacks before MFA abuse occurs
- Carrier-confirmed verification workflows
- Immediate alerts delivered directly to security teams

Stop Mobile Threats Before a Breach.

Request a demo at:

iverify.com/request-demo