AI-Accelerated Exploit Protection

Technical Solution Brief

Protect enterprise mobile devices as AI accelerates vulnerability analysis, exploit adaptation, and offensive research.

Maintain Device Trust as Exploit Timelines Accelerate

AI-assisted tooling is making it faster to analyze vulnerability research and build upon existing offensive techniques, reducing the time available for defenders to assess exposure and deploy mitigations. For a growing share of exploitation, patching now happens after compromise, not before it.

iVerify Enterprise provides continuous operating system-level visibility throughout this window, helping security teams identify exposed devices, detect evidence of compromise, investigate suspicious activity, and make informed device trust decisions while remediation is underway.

Protect Across the Exploit Response Lifecycle

1 Identify Exposure

- Assess device posture and operating system versions
- Identify devices affected by emerging vulnerabilities
- Prioritize risk using mobile threat intelligence

2 Detect Compromise

- Continuously assess mobile device integrity
- Analyze security-relevant OS telemetry and system artifacts
- Identify suspicious behavior associated with exploitation and compromise

3 Investigate with Evidence

- Review the evidence supporting detections
- Analyze historical security telemetry
- Correlate mobile findings with identity, endpoint, and cloud events

4 Respond & Validate

- Inform device trust and access decisions
- Escalate significant findings to deeper forensic analysis
- Validate device security following remediation

See What Existing Controls Can't

MDM / UEM	PATCH STATUS	IDENTITY	→	IVERIFY
Compliant	Current	Authenticated		⚠ Suspicious OS behavior detected

A device can satisfy compliance and authentication requirements while still requiring further investigation. iVerify provides supporting operating system telemetry and system artifacts that help analysts determine whether suspicious activity represents a meaningful change in device trust.

What iVerify Adds to Your Existing Security Stack

EXISTING INVESTMENT

MDM / UEM

IVERIFY

Evidence about whether the mobile OS is behaving as though it has been compromised

EXISTING INVESTMENT

Patch Management

IVERIFY

Visibility into exposed devices while remediation is underway, regardless of patch status.

EXISTING INVESTMENT

Identity & Conditional Access

IVERIFY

Device integrity signals that can inform access decisions

EXISTING INVESTMENT

SIEM / SOAR

IVERIFY

Mobile OS-level telemetry that can be correlated with enterprise security events

Technical Capabilities

OS-Level Device Integrity

Continuous analysis of security-relevant operating system telemetry and system artifacts across iOS and Android to identify suspicious behavior and evidence of compromise.

Evidence-Based Investigation

Detections include supporting evidence analysts can validate, with historical telemetry for investigation and escalation to iVerify Threat Hunter IR for advanced mobile forensics.

Enterprise Security Integration

Integrate mobile findings into SIEM, SOAR, identity, and conditional access workflows, with REST API support and exportable security telemetry for automation and custom workflows.

Threat & Application Intelligence

Use mobile threat intelligence to prioritize emerging threats, with NowSecure Mobile Application Risk Intelligence (MARI) providing additional visibility into application and SDK risk.

Privacy-Conscious by Design

Security visibility without inspecting employee content.

iVerify focuses on security-relevant telemetry and does not require organizations to inspect employees' personal messages, emails, photos, or other private user content to identify mobile security threats.

Detect Compromise Before Compliance Gives You False Confidence

iVerify Enterprise extends your existing mobile security architecture with the operating system-level visibility, evidence, and integrations needed to respond as exploit timelines accelerate.

Book a demo →