iVerify.

BYOD Security

TECHNICAL SOLUTION BRIEF

Achieve meaningful security visibility across your entire BYOD fleet without invasive controls or legal exposure.

Securing a BYOD Workforce Means Solving Four Problems at Once

BYOD creates a structural conflict: employees resist device management on personal phones, but traditional mobile security depends on exactly that kind of access. Security teams are left choosing between limited visibility, controls employees won't adopt, or the cost of a company-owned device program.

01

Resistance to Surveillance

Employees rightly resist invasive monitoring and full device management on personal phones, pushing usage toward shadow IT or leaving devices under-secured.

02

The Uninstrumented Fleet

That resistance leaves a BYOD fleet that carries corporate credentials and MFA apps but no security visibility, creating an exposed entry point attackers can reach.

03

The Legal Imperative

Growing privacy regulation limits how organizations can collect and monitor data on employee-owned devices. Over-monitoring creates its own legal exposure.

04

Attacks Target Access, Not Ownership

Exploits, credential theft, and session hijacking target the device as an access point into enterprise systems, whether it's corporate-owned or personal.

Where Existing BYOD Approaches Fall Short

None of the tools already in most security stacks solve all four problems at once. Each was designed for a narrower job.

APPROACH	DESIGNED FOR	WHERE IT FALLS SHORT ON BYOD
MDM / UEM	Full policy enforcement and configuration control, including data wipe and asset tracking.	High control over personal devices often leads to low adoption and employee friction.
Mobile Threat Defense (MTD)	Application scanning and network protection.	Doesn’t confirm whether the device itself has been compromised.
Containers	Isolating corporate apps and data within an application boundary.	If a zero-click exploit compromises the OS, the attacker can still reach core device capabilities regardless of the container.

SOLVED PROBLEM BY PROBLEM

The iVerify Approach

iVerify is a Mobile EDR that decouples security visibility from device management and invasive data collection, answering each BYOD problem directly rather than trading one risk for another.

PROBLEM 1 Resistance to Surveillance

iVERIFY'S ANSWER

Privacy-First Deployment

Deploys with MDM, with MAM, or fully standalone, with no full device enrollment and no invasive permissions. Employees keep control of their device; security teams still get visibility.

PROBLEM 2 The Uninstrumented Fleet

iVERIFY'S ANSWER

Kernel-Adjacent Telemetry

Continuously evaluates kernel-adjacent telemetry and OS log artifacts to detect compromise, closing the gap MDM can't reach and MTD can't see deep enough into.

PROBLEM 3 The Legal Imperative

iVERIFY'S ANSWER

Data Minimization by Design

Collects no PII, browsing history, messages, or photos. Focuses strictly on device integrity and threat telemetry, nothing more than security requires.

PROBLEM 4 Attacks Target Access, Not Ownership

iVERIFY'S ANSWER

Identity-Layer Response

Feeds device risk signals directly into identity providers (Okta, Entra ID), so access decisions are based on device trust, not who owns the device.

How iVerify Secures BYOD

iVerify extends EDR-level protection to BYOD while keeping a minimal, privacy-respecting footprint.

1 Deployment

- Installs fleet-wide across iOS and Android with minimal user action
- Works with MDM, with MAM, or fully standalone
- No dependency on full device enrollment

2 Detection

- Continuously monitors device integrity in the background
- Flags behavioral anomalies, indicators of compromise, and zero-click exploitation
- Surfaces risk without ever inspecting personal content

3 Response

- Routes device risk signals into identity providers for conditional access
- Revokes access at the identity layer the moment risk is confirmed, with no remote wipe of a personal device required
- Escalates significant findings into existing SIEM, SOAR, and XDR workflows

Privacy-Conscious by Design

Security visibility without inspecting personal content.

iVerify focuses on kernel-adjacent telemetry and device integrity signals, not personal activity. The platform does not collect PII, browsing history, messages, or photos to identify mobile security threats on a personal device.

Organizations deploy iVerify Enterprise to:

- Fully embrace BYOD productivity without expanding the security gap
- Close the blind spot unmanaged devices create on Tier-1 corporate systems
- Minimize legal exposure by collecting only what security requires
- Increase employee adoption of mobile security
- Enforce Zero Trust access decisions on unmanaged endpoints
  Extend EDR-level protection to every device without buying it

Built for Teams Balancing BYOD and Risk

- Organizations with high BYOD adoption across the workforce
- Teams subject to strict privacy regulation (GDPR, CCPA, and similar)
- Security teams building toward Zero Trust maturity
- Enterprises facing low adoption of existing mobile security tools

Secure Every Device Employees Actually Use

Learn how iVerify Enterprise gives security teams full BYOD visibility without the privacy tradeoff.

iverify.com