

Every layer of mobile risk, detected, triaged and resolved.

Mobile EDR, app vetting, secure DNS and managed threat hunting in one subscription.

Mobile devices sit at the center of enterprise identity and access, yet securing them usually means stitching together MDM, a legacy MTD tool, a DNS filter and a manual app review process, with no one on staff who can read a mobile diagnostic log. **iVerify Complete brings the device, app and network layers together with the analysts who act on what they find.**

Four layers, one subscription

Device, app, network and human coverage, from one partner.

Unparalleled mobile visibility

Kernel-adjacent telemetry and behavioral detection that legacy MTD and MDM tools cannot access.

Privacy-first for BYOD

No mandatory MDM, no VPN routing, built to minimize data collection.

What's included

01 · DEVICE LAYER

iVerify Enterprise

Mobile EDR with SmishGuard and SIM swap detection. Continuous kernel-adjacent telemetry and behavioral detection across iOS and Android.

- Detects advanced compromise, including Pegasus, Predator, Coruna and DarkSword
- SmishGuard catches link-based and linkless smishing and vishing; SIM swap detection flags MFA bypass attempts
- Conditional access via Okta and Entra ID, with alerts streamed to SIEM, SOAR and SOC workflows

02 · APP LAYER

App Vetting powered by NowSecure

Continuous app risk intelligence that runs inside iVerify Enterprise, correlated with device telemetry.

- Automated risk scoring for apps on managed and BYOD devices; approved apps monitored for new permissions, data flows and behavior changes
- Visibility into AI app usage across the fleet
- Mapped against OWASP MASVS, NIAP, GDPR and HIPAA, backed by 4M+ NowSecure app assessments

03 · NETWORK LAYER

Secure DNS powered by threatER

threatER EnforceDNS uses iVerify's mobile telemetry to block malicious domain resolution in real time.

- Protection on corporate networks, home Wi-Fi and cellular, without VPN routing
- Cuts off smishing links and command-and-control (C2) callbacks before a payload is delivered
- Unified audit trail of mobile DNS activity, including devices off the corporate network

04 · HUMAN LAYER

Managed Threat Hunting

iVerify's mobile threat hunters and forensic analysts turn alerts into verdicts, with no in-house mobile forensics expertise required.

- Analysts triage alerts and confirm true or false positives, guided by a simple in-app workflow for end users
- IR Mode forensic collection preserves evidence before legacy extraction tools can delete it
- IOCs from each investigation feed back into detection across your protected fleet

From first signal to malware sample

Every real compromise iVerify catches moves through the same four phases. With Complete, each one is covered.

01

Anomaly detection

Continuous monitoring combines device signals, cross-signal correlation, behavioral baselines and iVerify’s threat intelligence to uncover novel threats. Integrated conditional access then automatically restricts access to corporate data.

SECONDS FROM INFECTION

02

Triage

Security teams use in-platform tooling to investigate alerts and confirm true or false positives, pulling extra diagnostic data through a guided in-app workflow when needed. iVerify threat hunters are always on call for additional expertise and support.

MINUTES FROM INFECTION

03

Investigate

First-party forensic tooling collects additional device data to assess scope and impact, preserving logs and artifacts for further analysis.

HOURS FROM INFECTION

04

Traditional forensics

A full forensic acquisition with industry-grade tools works to recover samples. New IOCs sweep the fleet.

DAYS LATER

When you buy iVerify, you don't just buy software. You buy a security outcome.

Coverage at a glance

Dots mark primary coverage, colored by layer

Threat or need	Enterprise	App Vetting	Secure DNS	Threat Hunting
Zero-click exploits and mercenary spyware				
Fileless malware and device compromise				
Smishing links and phishing domains				
SIM swap and MFA bypass				
Risky, vulnerable or non-compliant apps, including AI apps				
C2 callbacks on corporate, home and cellular networks				
Alert triage, forensics and incident response				

Already running iVerify Enterprise?

Complete builds on the deployment you already have. App vetting runs inside iVerify Enterprise, Secure DNS draws on the telemetry your agent already collects, and iVerify analysts stand behind every critical alert. Ask your account team or partner about upgrading.

Proven research, verified controls

The team behind public disclosures of the Coruna and DarkSword exploit frameworks, the latter with Google. Approved Microsoft MTD partner.

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

Stop mobile threats before a breach.

See iVerify Complete in action.

Request a demo at iverify.com