Threat Hunter IR

Mobile Forensic Data Acquisition for Incident Response

Retrieve the OS-level diagnostic data your security team needs to investigate suspicious mobile activity, validate potential compromise, and support incident response.

How Threat Hunter IR Works

1 Check for Known Indicators

Scan for known IOCs, spyware artifacts, and signs of compromise.

2 Acquire Forensic Data

Retrieve OS-level diagnostic data, logs, telemetry, and process metadata from supported mobile devices.

3 Investigate and Respond

Analyze collected evidence to validate findings, determine scope, and support incident response activities.

Key Benefits

Deploy in Any Environment

Operate in disconnected, remote, or highly regulated environments without requiring internet connectivity during collection.

Gain Deep Mobile Visibility

Move beyond surface-level indicators with forensic evidence that helps analysts validate suspicious activity and reconstruct attack timelines.

Integrate with Existing Security Operations

Support cloud, hybrid, and fully on-prem deployments while integrating with SIEM, SOAR, EDR, and MDM workflows.

Acquire Mobile Forensic Data Anywhere

Retrieve OS-level diagnostic data, telemetry, logs, and process metadata directly from iOS and Android devices without complex deployment requirements.

Preserve Privacy While Investigating

Collect only the forensic data necessary for security investigations, helping balance investigative visibility with user privacy.

Accelerate Incident Response

Collect, package, and process the data needed to move from suspicion to evidence and support investigation workflows.

Better Together: Threat Hunter IR + iVerify Enterprise

iVerify Enterprise tells you where to look. Threat Hunter IR helps you uncover what happened.

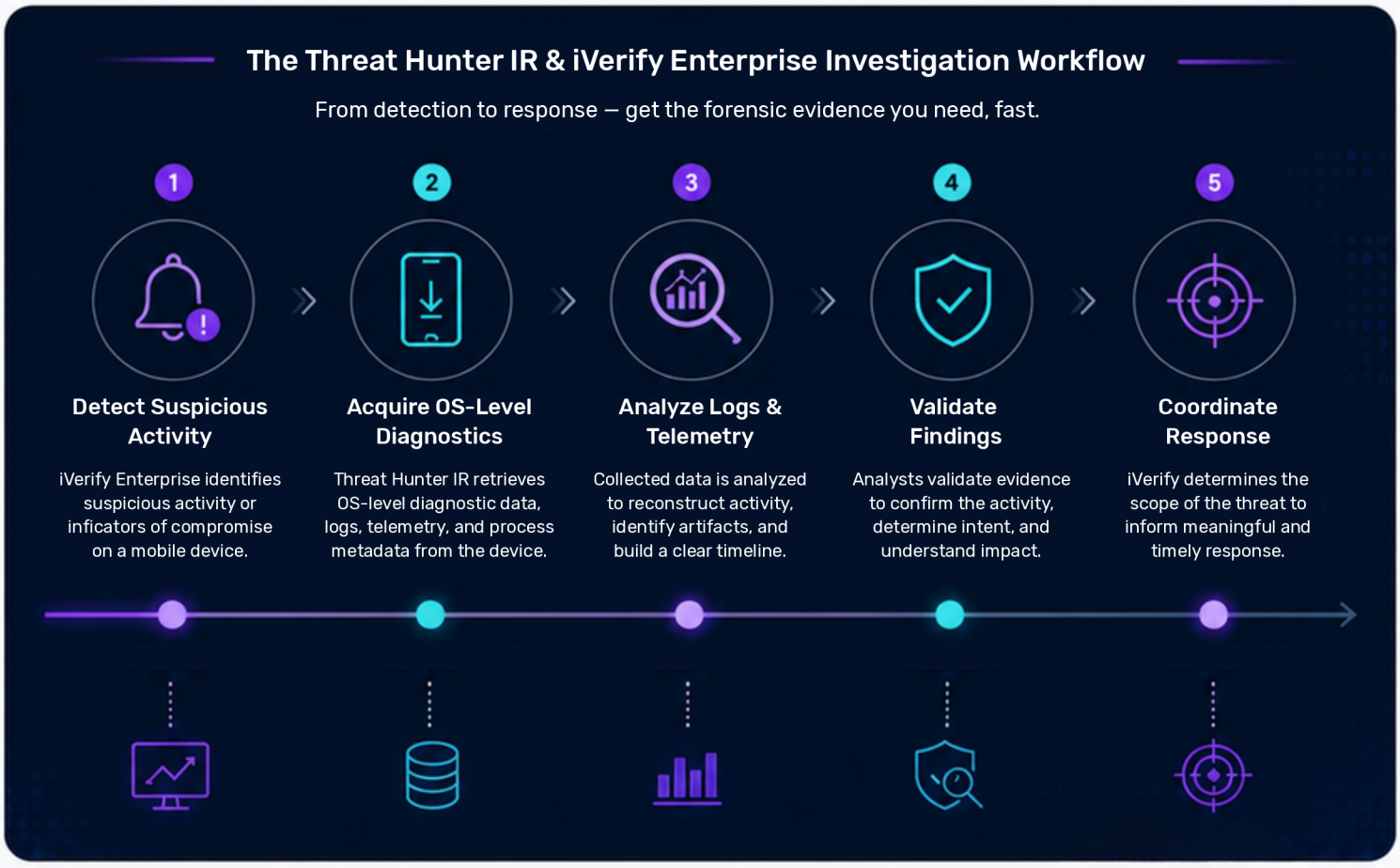
iVerify Enterprise continuously monitors iOS and Android devices for suspicious activity, behavioral anomalies, indicators of compromise, and emerging mobile threats. It provides security teams with ongoing visibility into mobile risk across managed and unmanaged devices, helping identify devices that may require further investigation.

When suspicious activity is detected, Threat Hunter IR retrieves the OS-level diagnostic data, telemetry, logs, and process metadata needed to validate findings, understand the scope of activity, and support incident response.

While Threat Hunter IR can be used independently to support mobile forensic investigations, organizations using both solutions benefit from continuous monitoring combined with on-demand forensic depth.

Where Threat Hunter IR Delivers Value

- Mobile incident response investigations
- Investigating devices flagged by iVerify Enterprise
- Executive protection programs
- High-risk traveler assessments
- Mobile forensic readiness programs
- Compliance and forensic audits
- Security operations in disconnected environments



Acquire. Investigate. Respond with Confidence.

Request a demo at:

iverify.io/request-demo