Data Sheet

Mobile Threat Detection Scan Capabilities

For iVerify Enterprise Solutions

Protect your mobile fleet from advanced zero-day vulnerabilities, spyware, and other threats with continuous and point-in-time behavioral hunting that analyzes heuristic threat data, diagnostic logs, process metadata, and malicious adversarial signatures.

SCAN TYPE	DESCRIPTION
Background Scanning/Continuous Monitoring	Scans occur in the background, conducting the following: • File-based IOCs • Biometrics enabled and trusted • Screenlock enabled • OS version • iVerify app version • Lockdown mode enabled (iOS only) • Security patch version (Android only) • Work profile enabled (Android only) • Play integrity enabled (Android only) • Side-loading disabled (Android only) • Developer mode disabled (Android only) • Android Debug Bridge disabled (Android only)
Forensic Scan iOS Sysdiagnose	End users must initiate scans manually and share the sysdiagnose with iVerify via in-app guides. The scan does **not** include sensitive personal data such as passwords, browsing history, messages or any app content like photos or emails. • Unified logs • Crash Logs • Configuration Profiles • Power and Battery Information • Network Status & Statistics • System Configuration • App Metadata • Diagnostic Settings and Preferences • Process Lists and Process Metadata
Forensic Scan Android Bug Report	End users must initiate scans manually and share the bug report with iVerify via the in-app guides. The scan does **not** include sensitive personal data such as passwords, browsing history, messages or any app content like photos or emails. • Logcat Information • Power and Battery Information • Verified Boot State • Network Status & Statistics • Apps and App Metadata • Diagnostic Settings and Preferences • Process Lists
Extended Protection	Continuously collected and uploaded data includes: • Process lists • Unified logs • Crash logs • Installed app lists and metadata • Sysdiagnose automatic upload, if triggered