High-Risk Travel Protection

Technical Solution Brief

Protect executives and employees before, during, and after high-risk travel with continuous mobile threat detection and enterprise visibility.

High-Risk Travel Requires a Different Security Model

High-risk travel exposes employees to mobile-specific threats—including targeted phishing, malicious networks, device compromise, and physical access—that are often invisible to traditional endpoint security. iVerify provides continuous mobile telemetry that helps organizations establish device trust before travel, monitor risk during travel, and assess devices before reconnecting them to corporate resources.

Protect the Entire Travel Lifecycle

1 BEFORE TRAVEL

Establish trusted baseline

- Verify device integrity before departure
- Identify existing compromise indicators
- Detect jailbreaks or rooted devices
- Validate security posture against organizational policy
- Ensure devices begin travel from a known-good state

2 DURING TRAVEL

Continuously monitor for mobile threats

- Detect mobile phishing and smishing attacks
- Identify suspicious device behavior
- Monitor device integrity changes
- Alert security teams to elevated device risk
- Provide continuous visibility throughout travel

3 AFTER TRAVEL

Determine whether devices remain trusted

- Reassess device integrity
- Review detections and telemetry collected during travel
- Investigate suspicious activity using historical evidence
- Determine whether devices can safely reconnect to corporate resources
- Support incident response when compromise is suspected

Travel Threat Coverage

TRAVEL THREAT	IVERIFY CAPABILITY
Mobile phishing (Smishing)	Detects malicious SMS and mobile phishing attacks
Device compromise	Identifies indicators of compromise and elevated device risk
Jailbroken or rooted devices	Detects reduced device integrity
Risky applications	Identifies applications that increase organizational risk
Suspicious configuration changes	Detects changes affecting device trust
Unsafe device posture	Continuously evaluates device security posture
Emerging mobile threats	Threat intelligence-driven detection capabilities
Post-travel validation	Reassesses device trust before reconnecting to enterprise resources

Technical Capabilities

Device Integrity Monitoring

Continuously evaluate device health to identify changes that may indicate compromise or reduced trust.

INCLUDES:

- Device integrity verification
- Jailbreak and root detection
- Security posture assessment
- Configuration change monitoring
- Device risk scoring

Mobile Threat Detection

Detect mobile-specific threats that frequently target travelers.

COVERAGE INCLUDES:

- Smishing and mobile phishing
- Malicious applications
- Suspicious configuration profiles
- Unsafe device settings
- Emerging mobile threats informed by iVerify Threat Intelligence

Enterprise Security Visibility

Provide security teams with actionable telemetry rather than isolated alerts.

CAPABILITIES INCLUDE:

- Continuous device telemetry
- Investigation timeline
- Risk prioritization
- Alerting for security operations
- Historical security evidence for investigations

Flexible Enterprise Deployment

Designed for organizations with diverse mobile environments.

SUPPORTS:

- Corporate-owned and BYOD devices
- No MDM dependency
- Cloud-managed deployment
- Rapid enterprise rollout
- Scalable across global workforces

Security Architecture

Data Collection

- Device security posture
- System security signals
- Device configuration
- Application metadata
- Network-related security observations
- Device integrity indicators

Detection Methodology

- Behavioral analysis
- Device posture evaluation
- Threat intelligence
- Policy-based assessment
- Security event correlation

Enterprise Privacy

iVerify focuses on security telemetry rather than employee content. The platform does not require organizations to inspect personal messages, emails, photos, or other private user content in order to identify mobile security threats.

Why organizations use iVerify for high-risk travel

Organizations deploy iVerify Enterprise to:

- Establish trusted mobile devices before travel
- Improve visibility into mobile-specific attacks
- Support executive protection programs
- Continuously monitor mobile risk throughout travel
- Accelerate investigation of suspected compromise
- Reduce uncertainty when devices return from high-risk locations
- Strengthen Zero Trust initiatives with mobile device trust signals

Protect mobile devices wherever business takes your organization.

Learn how iVerify Enterprise helps security teams establish device trust before, during, and after high-risk travel.

iverify.io/request-demo