

## Solution Brief

# iVerify Enterprise

Elite Mobile Threat Defense for BYOD and corporate-owned devices

Mobile malware is commercialized on an industrial scale, yet millions of mobile devices connected to enterprise services remain defenseless. Whether a phishing message appears to come from the CEO or trusted institution – or whether the attacker uses zero-click capabilities – too many of us will fall victim to malware that can pose disastrous outcomes. Yet, mobile security solutions remain stuck in the past, relying heavily on technologies that generate privacy concerns and lack meaningful mobile device security capabilities. iVerify is here to change that.

## Key Benefits

- Extend threat protections to every device with access to your enterprise data
- Defend against corporate espionage, IP theft, physical security incidents, and ransomware
- Real-time threat detection and device integrity checks
- Secure browsing and DNS checks
- Detailed and constantly updated protection guides help employees become better security citizens while protecting your digital assets
- All this, without invading user privacy



The image shows a screenshot of the iVerify dashboard interface. The dashboard has a dark header with the iVerify logo, user information (Acme Corporation, Tianna Fuller), and a '+ Add Users' button. Below the header, there's a 'Dashboard' section with a filter dropdown set to 'All Operating Systems' and an action dropdown set to 'select users to enable options'. The main content area is a table with columns: Name, Access Code, Threat Detected, Signs of compromise, Version, and Added. A red callout bubble points to the 'Threat Detected' column, and another points to the 'Signs of compromise' column. A yellow callout bubble points to a row with a version of '2.1' and a warning icon. A blue callout bubble points to the 'Version' column. A green callout bubble points to the 'Added' column. A red callout bubble points to the 'Threat Detected' column. A blue callout bubble points to the 'Signs of compromise' column. A yellow callout bubble points to a row with a version of '2.1' and a warning icon. A blue callout bubble points to the 'Version' column. A green callout bubble points to the 'Added' column.

Full API for webhooks, SIEM Integration, and Onboarding/Offboarding Automation

Full Role-Based Access Control

Compromise Details

Multiple SSO and MDM Integrations

Guide Completion Details and Custom Training Policies

Gently Nudge Users to Update Patches

Full Dashboard Data Export to Enable Reporting

iVerify is the first mobile threat hunting company tackling sophisticated device-layer threats while respecting user privacy. iVerify Enterprise™ provides mobile threat defense in the form of iOS and Android telemetry monitoring that protects users' privacy and deploys rapidly. Perfect for BYOD fleets, and even more powerful when paired with MDM to instantly remediate compromises. iVerify also offers additional protections against social engineering with our universally acclaimed mobile security guides, as well as tools to help users secure the network layer.