vijilan
IT Security: Enabled

THREATDEFEND™ MOBILE

The breach doesn't care which device it's on. Neither do we.

Powered by CrowdStrike Falcon® for Mobile

Mobile is the blind spot in almost every security program we walk into. Phones and tablets carry the same email, the same SaaS access, the same MFA tokens as laptops — but most organizations have zero detection, zero containment, and zero visibility on them. ThreatDefend™ Mobile closes that gap by extending Vijilan's 24/7 SOC and SIEM correlation onto every iOS and Android device in your fleet.

AT A GLANCE

- What it is: Fully managed mobile threat defense for iOS and Android, delivered as a new module of ThreatDefend™.
- Engine: CrowdStrike Falcon® for Mobile, deployed and operated by Vijilan.
- Who runs it: Vijilan's 24/7 SOC — same analysts, same playbooks, same SLAs as your endpoints.
- How it's sold: Channel-exclusive through MSPs, MSSPs, and VARs. Bundled into ThreatDefend™ tiers.
- Coverage: iOS 16 and later. Android 9.0 and later. Managed and BYOD.

The Problem

The Blind Spot Nobody Owns

Ask any security leader who owns mobile in their environment and you'll get three answers: IT, the MDM vendor, or "the user." None of them are correct, and none of them are watching.

Mobile is now a primary attack surface

- Smishing and mobile phishing have overtaken email phishing in many sectors — and most MDM tools can't see, let alone block, a malicious URL tapped from a text message.
- Stolen session tokens harvested from a compromised phone bypass MFA on cloud apps without ever touching the corporate network.
- Rooted Androids and jailbroken iPhones inside the fleet silently expand the attack surface for months before anyone notices.
- Personal apps with excessive permissions exfiltrate contact lists, calendars, and clipboard data — including pasted passwords and one-time codes.
- Hostile networks at airports, hotels, and conferences strip TLS and inject payloads, and the user never knows.

Why MDM isn't the answer

MDM and UEM solve a configuration problem. They enforce passcodes, push apps, and wipe lost devices. They were never built to detect adversary behavior, hunt for indicators of compromise, or correlate a suspicious mobile login with a phishing email that hit the same user 90 seconds earlier.

That is a SOC problem, not an IT problem — and that is the gap ThreatDefend™ Mobile is built to fill.

The Capabilities

What ThreatDefend™ Mobile Actually Does

Four capability pillars, all delivered as a managed service. You don't run the console. You don't tune the policies. You don't get a flood of alerts. You get outcomes.

1. Mobile Phishing Defense

Blocks malicious URLs, domains, IPs, and file hashes the moment a user taps. Stops smishing, malicious QR codes, and credential-harvesting pages before the page renders. Surfaces repeat-offender users so you can target awareness training where it matters.

2. On-Device Threat Detection

Detects jailbreaking on iOS, rooting on Android, OS integrity tampering, malicious profiles, unauthorized apps, and risky configurations. Every detection mapped to MITRE ATT&CK for Mobile so the report makes sense to auditors and CISOs alike.

3. Zero Trust Posture Signal

Continuous device-posture evaluation feeds your conditional access policies. A compromised phone loses access to email and SaaS automatically. For Android, Vijilan also leverages Device Trust signals from Android Enterprise — including on unmanaged BYOD.

4. Privacy by Design

We monitor corporate apps, not personal life. No SMS content, no email body, no browsing history, no photos. Employees get protection. The company gets defensibility. HR gets a story that doesn't blow up in a town hall.

The Vijilan Difference

One SOC. Every Surface.

Most mobile security vendors stop at the device. They send you an alert and walk away. We don't sell a tool — we sell a service, and the service is what happens after the alert.

Cross-domain correlation in our SIEM

Every signal from Falcon for Mobile streams into Vijilan's SIEM alongside telemetry from your endpoints, identities, and cloud applications. That's where the real work happens. A single suspicious event on a phone is a ticket. The same event, correlated against four other signals, is a confirmed compromise — and we contain it before your team finishes their coffee.

Mobile Signal	+ Identity	+ Endpoint	+ Cloud
User taps phishing link on iPhone	Same user logs in from new geography 4 min later	No corresponding laptop session	Mailbox rule created in M365 to auto-forward and delete
VERDICT **Business Email Compromise in progress. Vijilan SOC kills the session, revokes tokens, isolates the device, deletes the forwarding rule, and notifies the client — automatically.**			

Every signal from Falcon for Mobile streams into Vijilan's SIEM alongside telemetry from your endpoints, identities, and cloud applications. That's where the real work happens. A single suspicious event on a phone is a ticket. The same event, correlated against four other signals, is a confirmed compromise — and we contain it before your team finishes their coffee.

What the SOC actually does

Detects
24/7 monitoring of every Falcon for Mobile signal with Vijilan's custom detection rules layered on top of CrowdStrike's native logic.

Triages
Praxis AI Engine auto-enriches each alert with MITRE ATT&CK mapping, IOC context, and historical user behavior before a human ever sees it.

Investigates
Cross-correlates mobile activity against your full Vijilan telemetry — endpoint EDR, identity, M365, Google Workspace, AWS, Azure.

Contains
Direct action on the device, the identity, and the cloud session. We don't just tell you what happened — we stop it from continuing.

Reports
Service Excellence cadence, monthly executive summary, full audit trail in the Partner Portal.

Where It Fits

The Vijilan Stack

ThreatDefend™ Mobile is a module of ThreatDefend™, our fully managed CrowdStrike Falcon stack. It is available in every ThreatDefend™ tier and can also be deployed as a standalone add-on for ThreatRespond™ clients who already run another XDR but want mobile coverage from Vijilan.

Capability	Essential	Advanced	Premium	Elite
Phishing & malicious URL defense	✓	✓	✓	✓
Jailbreak / root / OS integrity detection	✓	✓	✓	✓
Cross-correlation with identity & cloud	–	✓	✓	✓
24/7 SOC active containment on mobile	✓	✓	✓	✓
Mobile threat hunting & quarterly review	–	–	✓	✓
Zero Trust posture integration	–	–	✓	✓
Custom IOA development for mobile	–	–	–	✓

Pricing is per-device and follows the ThreatDefend™ tier the client is already subscribed to. Pricing is available exclusively through the Vijilan Partner Portal — no public price list, ever.

Deployment

Days, Not Quarters

CrowdStrike's mobile agent was built for scale. We built the deployment process around it so partners can roll this out across a client base in days, not quarters.

01	02	03
Scope & Activate Partner kickoff. We confirm device inventory, MDM/UEM in use, BYOD posture, and target rollout schedule. Tenants provisioned same day.	Zero-Touch Push App distributed through your existing UEM or via direct enrollment for BYOD. No user setup. Activation is automatic and silent.	SOC Cuts Over Mobile telemetry flows into the Vijilan SIEM. SOC playbooks updated. First-week tuning call to baseline normal behavior in your fleet.

Most clients are fully covered within 5 to 10 business days from contract signature. The Day 7 Service Excellence Call covers the Partner Portal walkthrough, escalation path, and reporting cadence — exactly as it does for the rest of ThreatDefend™.

Frequently Asked

Questions Partners Actually Ask

Q. Will it drain the device battery or eat data?
No. The Falcon for Mobile agent is engineered for near-zero impact on battery and bandwidth. Users won't notice it's there. Help desks won't get tickets about it.

Q. Does it work on personal devices (BYOD)?
Yes. Both iOS and Android support unmanaged deployment. We never see personal apps, messages, or browsing history — only corporate-designated apps and security signals.

Q. What does it see, and what doesn't it see?
It sees: malicious URLs, device posture, OS integrity, app installation events from corporate-managed apps, jailbreak/root status, network attacks. It does not see: SMS content, email content, photos, personal app usage, location tracking, or browsing history.

Q. Can it replace our MDM?
No, and that's a feature, not a bug. MDM enforces configuration. ThreatDefend™ Mobile detects and responds to threats. The two are complementary. Most clients keep their existing Intune, Jamf, or Workspace ONE and bolt us on alongside.

Q. How does it integrate with ThreatRespond™ for clients on a non-Falcon EDR?
ThreatDefend™ Mobile can be deployed as a standalone add-on for ThreatRespond™ clients. Mobile signals still flow into the Vijilan SIEM and correlate with their existing endpoint telemetry — we just don't run the EDR side on Falcon.

Q. What about the rule that only one product per environment can be deployed?
ThreatDefend™ Mobile is a module, not a separate product environment. It pairs cleanly with either ThreatRespond™ or full ThreatDefend™. Your client picks one EDR/XDR posture; the mobile module attaches to it.

Q. How is this priced?
Per-device, per-month, channel-only, surfaced exclusively in the Partner Portal. There is no public price list and there never will be.

Get Started

Bring ThreatDefend™ Mobile to Your Clients

Mobile is the cheapest gap a partner can close right now. The agent installs silently, the SOC carries the operational load, and the conversation with the client is short.

Existing Partners

Add the Mobile module from the Partner Portal. Provisioning is same-day.

OPEN PARTNER PORTAL

New to Vijilan

Apply to the partner program. NFR licenses available for qualifying MSPs.

BECOME A PARTNER

Live Demo

Twenty minutes. Real fleet. Real SOC console. Walk away knowing what your clients are missing.

BOOK A DEMO

Endpoints. Identities. Cloud. Now Mobile.

Four surfaces. One SOC. One SIEM. Zero blind spots.