iVerify.

PARTNER DATASHEET

iVerify Partner Program for MSPs and MSSPs

Close your customers' mobile blind spot. Grow a new managed service.

Add Mobile EDR to your portfolio and deliver OS-level detection, investigation, and response for the iOS and Android devices your customers already run their business on.

Your customers monitor laptops and servers around the clock, yet the phone in every employee's pocket holds their email, MFA apps, session tokens, and access to cloud systems. Most security stacks still treat it as unmonitored. The iVerify Partner Program gives MSPs and MSSPs the platform, multi-tenant tooling, and expert backing to turn that gap into a recurring, high-value service.

The opportunity: mobile is the endpoint your customers aren't watching

Mobile exploitation has gone mass-market. The DarkSword iOS exploit kit, disclosed by iVerify researchers with Google Threat Intelligence Group, and the Coruna kit show nation-state grade tooling now in the hands of criminal groups. These attacks inject into trusted processes, run in memory, and clean up after themselves, so a fully patched, compliant phone can still be compromised.

Most customer environments can't see it:

- **MDM enforces policy, not detection.** It reports OS versions and passcodes, not active exploitation or token abuse.
- **Legacy MTD relies on jailbreak checks and signatures** that modern zero-click exploits sidestep.
- **Desktop EDR stops at the laptop.** Mobile is often a checkbox in a broader platform bundle.
- **Identity attacks start on the phone.** Smishing, vishing, and SIM swaps are common paths to MFA bypass and account takeover.

1.07
per 1,000 consumer iOS devices showed signs of spyware

0
known Apple Threat Notifications on devices hit by DarkSword

75%
of detections were criminal groups, not state-sponsored actors

Source: iVerify Advanced Mobile Threat Report 2026

For partners, that gap is the opportunity: a service your customers need, that their current stack doesn't deliver, and that extends the SOC and managed detection work you already do.

What you can deliver: complete mobile security as a service

iVerify covers the full mobile attack chain, from the first smishing text to device-level exploitation, so partners can offer one service instead of stitching together point tools.

From first signal to security outcome

Every detection moves through four stages. Speed matters, because modern attacks erase their traces fast.

01	**Anomaly detection**	Continuous monitoring combines device signals, cross-signal correlation, behavioral baselines and iVerify's threat intelligence to uncover novel threats. Integrated conditional access then automatically restricts access to corporate data.	SECONDS FROM INFECTION
02	**Triage**	Security teams use in-platform tooling to investigate alerts and confirm true or false positives, pulling extra diagnostic data through a guided in-app workflow when needed. iVerify threat hunters are always on call for additional expertise and support.	MINUTES FROM INFECTION
03	**Investigate**	First-party forensic tooling collects additional device data to assess scope and impact, preserving logs and artifacts for further analysis.	HOURS FROM INFECTION
04	**Traditional forensics**	A full forensic acquisition with industry-grade tools works to recover samples. New IOCs sweep the fleet.	DAYS LATER

Your customers don't just get software. They get a security outcome, delivered by you and backed by iVerify.

Capability	What your customers get
iVerify Enterprise	Continuous kernel-adjacent telemetry and behavioral detection on iOS and Android for zero-click exploits, fileless malware, and spyware
Threat Hunter IR	On-demand forensic acquisition and investigation, with cloud, hybrid, or fully on-prem deployment
Managed mobile threat hunting	iVerify's analysts triage signals into verdicts, backed by a record of finding Pegasus, Predator, and DarkSword
SmishGuard	Protection against smishing, vishing, and linkless attacks across SMS, RCS, WhatsApp, and Signal, using Secure DNS with no VPN required
SIM swap detection	Carrier change and SIM swap risk signals to help stop MFA bypass and account takeover
Conditional access	Okta and Entra ID integrations that block a risky device from corporate apps, no MDM required
Threat intelligence	Mobile threat research, malware analysis, and risk-based prioritization
Integrations	Webhooks and an open API for SIEM, SOAR, MDM, and IAM workflows, plus NowSecure app risk intelligence

Built for BYOD and managed fleets. iVerify doesn't require MDM or a management profile and is designed to collect minimal data. It doesn't read texts, emails, photos, or browsing history, which makes it easier for your customers' employees to accept on personal phones. Deployment is lightweight and fleet-wide across iOS and Android, including zero-touch enrollment through an existing MDM where one is in place.

Program benefits

BUILT FOR HOW YOU DELIVER SERVICES

Multi-tenant management portal:
manage every customer from one console, with single-click provisioning, real-time dashboards, user-level reporting, and analytics on scans, vulnerabilities, and threat timelines.

Fast proof of value:
provision customer assessments quickly to show what is already on a fleet before the contract is signed.

Flexible commercials:
customizable customer requirements and quarterly usage-based billing.

Expert backing:
a dedicated partner support team, plus access to iVerify's mobile threat hunters and forensic analysts when an investigation needs to go deeper.

BUILT TO GROW YOUR BUSINESS

Three partner tiers: Bronze, Silver, and Gold

Deal registration

Sales and technical training

Co-marketing opportunities

Solution packages

PACKAGE
Business
WHAT'S INCLUDED
iVerify Mobile EDR with SmishGuard smishing protection and end-user sysdiagnose uploads

PACKAGE
Enterprise
WHAT'S INCLUDED
BYOD or managed device deployments, plus managed threat hunting, incident response, and forensics

PACKAGE
Government
WHAT'S INCLUDED
Self-hosted cloud and white-label options, available on request and subject to minimum contract values

Add-ons Premium Support | Threat Intelligence | Onsite Threat Hunting Training

Who the program is for

MSSPs and MDR providers
adding mobile telemetry and threat hunting to an existing SOC service

MSPs
offering managed mobile security alongside endpoint, identity, and device management

Security consultations and IR firms
that need mobile forensics for high-stakes client engagements

Where it fits best: customers with BYOD fleets, executives or staff exposed to targeted attacks, and regulated sectors such as financial services, government, healthcare, and technology.

How it works

01
Apply:
complete the partner interest form and meet the iVerify partner team.

02
Onboard:
get access to the multi-tenant portal, plus sales and technical training.

03
Prove value:
run a customer assessment to surface real findings on a live fleet.

04
Deliver and grow:
deploy across customers, register deals, and build co-marketing programs with iVerify.

iVerify is a pioneer in mobile EDR, providing security teams kernel-adjacent visibility into mobile devices, closing a gap that's persisted while laptops and servers have long had full EDR. iVerify detects, investigates, and responds to the threats mobile devices face today: fileless malware, spyware, smishing, malicious applications, and enterprise credential theft. iVerify's solutions make secure mobile productivity possible, letting employees work confidently from their phones without putting the business at risk.

Become an iVerify partner.

Complete the partner interest form at iverify.com/msp-mssp and our team will be in touch.

iverify.com All Rights Reserved.