Closing the SIM Swap Visibility Gap

Detect phone number compromise before it becomes account takeover

Phone numbers form part of the enterprise identity layer, used for SMS-based MFA, voice one-time passcodes, password resets, account recovery, help desk verification, banking approvals, and other high-value authentication moments. But when a phone number is transferred to an attacker-controlled SIM or eSIM, that trust model breaks.

Most mobile security stacks are built to detect risks on the device, including jailbreaks, root access, malicious apps, risky configurations, malware, and suspicious network activity. Those signals matter, but they do not confirm whether the phone number associated with that device is still under the user's control.

In a SIM swap attack, the user's device may still appear patched, enrolled, compliant, and free of obvious malware while the attacker receives the SMS codes, voice calls, and recovery messages intended for the legitimate user. The attacker may never need to touch the device itself. That makes SIM swap a different kind of mobile security problem. It is not always a device compromise. It is a compromise of the phone number as an identity factor.

iVerify SIM swap detection helps security teams close this gap with passive, carrier-confirmed detection built into iVerify Enterprise

Why SIM Swap Matters to Enterprise Security

SIM swap attacks are especially dangerous because they give attackers temporary control over a trusted identity channel. Once they control the phone number, they can attempt to convert that access into broader account compromise.

Common follow-on activities include:

- Account takeover
- MFA bypass
- Password reset abuse
- Recovery flow hijacking
- Help desk impersonation
- Executive impersonation
- Banking or crypto account compromise
- Lateral movement through linked accounts and services

The attack often depends on speed. The longer an attacker controls the number without detection, the more opportunities they have to intercept codes, reset passwords, abuse recovery workflows, and access additional accounts. Early detection changes that dynamic, allowing security teams to respond while the attacker is still trying to turn phone number control into account control.

Why Traditional Approaches Fall Short

SMS heartbeats create noise
Some systems send scheduled SMS messages to check whether a number is still reachable. But SMS delivery can fail for benign reasons, including roaming, coverage gaps, carrier delays, or temporary connectivity issues. This can lead to false alarms, alert fatigue, and unnecessary costs.

User self-reporting is too slow
Some organizations rely on employees noticing they have lost cellular service and reporting the issue to IT. But users may not notice quickly, especially when their device remains connected to Wi-Fi and common apps continue to work.

MDM checks are not enough
MDM tools may be able to determine whether a SIM is present on a device. But SIM presence does not prove that the original phone number is still assigned to that SIM.

Carrier confirmation is often missing
The carrier is the authoritative source for whether a SIM-to-subscriber binding has changed. Without that validation, security teams are left interpreting incomplete signals.

iVerify's Approach

Passive detection. Carrier-confirmed alerts. SOC-ready context.

iVerify SIM Swap Detection is included with iVerify Enterprise and can be enabled by administrators for supported managed-device environments.

Once enabled, the iVerify mobile agent passively samples cellular state from OS-exposed telephony APIs. These signals are evaluated for recognizable SIM swap patterns, with no single signal treated as conclusive on its own. When iVerify detects a combination of signals consistent with SIM swap activity, the platform queries the user's carrier to confirm whether the SIM associated with the phone number has been reassigned. If the carrier confirms the swap, iVerify generates an alert for the SOC.

There are no SMS heartbeats, no user prompts, no additional end-user permissions, and no reliance on the user noticing something is wrong. The result is a high-confidence, carrier-confirmed alert that security teams can act on quickly.

How iVerify Help Security Teams Reduce Risk

Reduce account takeover exposure
Identify phone-number compromise before attackers can fully exploit it across authentication, recovery, and help-desk workflows.

Improve MFA risk management
SIM Swap Detection does not replace phishing-resistant MFA. Organizations should continue moving toward stronger authentication methods such as FIDO2. But many enterprises still rely on SMS or voice-based verification in some systems, recovery flows, or high-risk workflows. iVerify provides a safety net during that transition.

Give SOC teams a signal they did not have before
SIM swap activity is often invisible to traditional mobile security tools. iVerify adds a carrier-confirmed signal tied to a known managed device.

Reduce mean time to detect
Instead of waiting for a user to report lost service, iVerify can alert security teams within minutes of carrier-confirmed SIM swap activity, depending on device state and scan timing.

Reduce triage burden
Alerts include the context that analysts need to act quickly, including device, phone number, carrier, detection context, carrier confirmation, and timestamp.

Response Actions Enabled by SIM Swap Detection

When a SIM swap alert is confirmed, security teams can quickly initiate response actions such as:

- Suspend active sessions
- Reset MFA factors
- Lock high-value workflows
- Review recent password reset attempts
- Escalate to help desk or identity teams
- Verify high-risk user activity
- Monitor linked accounts for suspicious access
- Trigger incident response playbooks

This helps limit the attacker's ability to turn phone number control into broader enterprise compromise.

Built for Enterprise Mobile Security

iVerify SIM Swap Detection is part of iVerify Enterprise, the mobile endpoint detection and response platform built to help organizations identify and respond to real-world mobile threats.

By adding carrier-confirmed SIM swap visibility to broader mobile security telemetry, iVerify helps organizations protect a critical identity layer that is often overlooked: the phone number attached to the employee's mobile device.

Ideal for Organizations That Need To

- Protect executives, administrators, and high-risk users
- Reduce account takeover and MFA bypass risk
- Strengthen mobile identity security
- Improve SOC visibility across managed mobile fleets
- Support migration away from SMS and voice-based authentication
- Detect phone number compromise without SMS heartbeats or user friction

Close the SIM Swap Visibility Gap

Request a demo to learn how iVerify SIM Swap Detection helps protect managed mobile fleets.