iVerify. SIM Swap Detection

Detect SIM swap before it becomes account takeover

SIM swap attacks give adversaries control of one of the most trusted identity factors in the enterprise: the mobile phone number.

Once a number is transferred to an attacker-controlled SIM or eSIM, the user's physical device may still appear clean, compliant, patched, and enrolled while the attacker can begin receiving SMS codes, voice calls, and account recovery messages intended for the employee.

iVerify SIM Swap Detection helps security teams close this visibility gap with passive, carrier-confirmed SIM swap detection. Included with iVerify Enterprise and enabled by administrators, SIM Swap Detection monitors device-level cellular signals and validates suspected SIM swap activity through carrier confirmation before alerting the SOC.

The result is a high-confidence signal security teams can act on quickly, without relying on SMS heartbeats, user self-reporting, or additional end-user permissions.

Why It Matters

Even as organizations move toward phishing-resistant MFA, SMS and voice-based one-time passcodes remain embedded in many enterprise, financial, administrative, and recovery workflows.

That creates risk for:

- Account takeover
- MFA bypass
- Password reset abuse
- Recovery flow hijacking
- Executive impersonation
- Banking, crypto, and high-value workflow compromise

Early detection reduces the attacker's window of opportunity. Instead of discovering a SIM swap after the user notices lost service or after an account has already been compromised, security teams receive an actionable alert they can use to lock workflows, reset MFA, suspend sessions, or trigger incident response.

Deployment Options

Available as part of iVerify Enterprise, deployment uses the existing iVerify app and current enterprise alerting workflows. Once enabled, telemetry begins flowing automatically from the device on the next scan cycle. End users do not need to take any additional action, approve new permissions, or interact with prompts.

How It Works

iVerify SIM Swap Detection is designed for managed mobile fleets. It uses a multi-stage detection flow to identify when an employee's mobile number may have been transferred to an attacker-controlled SIM or eSIM.

1. Device Signal Collection

The iVerify app collects a scheduled snapshot of cellular state from OS-exposed telephony APIs. No new end-user permissions are required.

2. Signature Detection

iVerify evaluates a combination of device-level signals for recognizable SIM swap patterns. No single field is treated as conclusive on its own because individual signals can have benign explanations in isolation.

3. Carrier Validation

When device telemetry suggests SIM swap activity, iVerify queries the relevant carrier to confirm whether the SIM-to-IMSI binding has changed within a recent window.

4. Alert Generation

If the carrier confirms the swap, iVerify generates an alert containing relevant context such as the device, phone number, carrier, detection trigger, and confirmation timestamp.

5. SOC Response

Security teams can use the alert to initiate response actions, including session suspension, MFA reset, account recovery review, help desk verification, or high-risk user escalation.

Key Capabilities

Passive On-Device Telemetry

Uses OS-exposed telephony signals from the device, with no SMS heartbeats, user prompts, or additional app permissions.

SOC-Ready Alerts

Alerts are delivered through existing iVerify workflows, including the portal, email, webhook, API, or SIEM integrations, depending on customer configuration.

Carrier-Confirmed Detection

Validates suspected SIM swap activity with the carrier before generating an alert, reducing noise and giving SOC teams a higher-confidence signal. Available for Microsoft Intune-managed devices on Verizon or T-Mobile as of June '26. *Additional carrier and MDM support on the roadmap.*

Designed for Low-Noise Response

Because alerts are generated after carrier confirmation, analysts can focus on response instead of investigating incomplete device-state indicators, heartbeat failures, or delayed user reports.

Why iVerify is Different

Legacy SIM swap approaches often rely on indirect signals or user interaction. SMS heartbeats can fail because of roaming, coverage gaps, carrier delays, or delivery issues. User self-reporting depends on the employee noticing a problem, which may take hours, especially if the device is still connected to Wi-Fi. MDM-level checks may identify whether a SIM is present, but they do not necessarily confirm whether the phone number has been transferred away from that SIM.

iVerify takes a different approach by combining passive device telemetry with carrier confirmation. This gives security teams a direct signal tied to a known managed device and validated against the authoritative source of whether a swap has occurred.

SOC Benefits

- **Reduce Mean Time to Detect:** Alert security teams quickly after confirmed SIM swap activity, depending on scan timing and device state.
- **Reduce Triage Burden:** Provide analysts with the context they need to understand what happened, which device is affected, which carrier is involved, and when confirmation occurred.
- **Improve Account Takeover Response:** Enable security teams to act before phone number control turns into full account control.
- **Strengthen MFA Risk Management:** Support organizations that still rely on SMS or voice-based authentication and recovery flows while they move toward phishing-resistant MFA.

Close the SIM Swap Visibility Gap

Request a demo at:

iverify.io/request-demo