EINPRESSWIRE

iVerify Launches SIM Swap Detection To Thwart Common Social Engineering Attack

Near-real-time SIM swap detection for BYOD and managed-device environments addresses critical mobile visibility problem

iVerify logo

BELFAST, NORTHERN IRELAND & NEW YORK, NY, UNITED STATES, March 11, 2026 /EINPresswire.com/ -- iVerify, the leader in advanced mobile endpoint detection and response (EDR) solutions today announced near-real-time SIM swap detection for BYOD and managed-device environments to address a critical visibility problem that leaves SOC teams blind to SIM swap.

Multi-factor-authentication systems are architected to put mobile at their nexus making them a prime target for entry into business networks. Despite this, and the wealth of information they hold, phones remain largely unprotected. This blindspot means SOC teams often find out a SIM swap happened after a costly incident has occurred and 90% of the time the user isn't aware either.

Account takeover via SIM swap is a popular tactic among cyber criminal groups who use the technique to bypass multi-factor authentication and intercept recovery flows. According to a Cifas report, mobile phone accounts were implicated in 48% of 2024 account takeover incidents with SIM swap attacks surging 1,055% from the prior year. SIM swap was involved in some of 2025's biggest breaches leveraging compromised account access to escalate privilege and/or move laterally into corporate networks enabling ransomware deployment, data theft and other nefarious activities.

Current solutions, such as heartbeat SMS and user-driven flows that require heavy end-user interaction, are ineffective, proven by the volume of breaches that started through SIM swap in the past few years. Enterprises need early warning before attackers exploit the swapped number.

“Mobile phone numbers are linked with a variety of high-value personal and corporate accounts, from banking apps to MFA flows, making them attractive to cyber criminals,” said Rocky Cole, cofounder and COO of iVerify. “For companies looking to guard against SIM swap attacks, there isn’t a scalable solution that covers the dozens of telcos active in an enterprise. The landscape is fragmented, carrier-based protections require every employee to enroll and third-party solutions add layers of bureaucracy that frustrate end users. Businesses need a novel solution that can overcome these challenges and that’s exactly what we’ve built.”

iVerify’s SIM swap detection works by monitoring a set of device-level cellular signals to detect anomalies in network behavior. When a potential indicator of a SIM swap is observed, such as an unexpected change in signal characteristics, the platform automatically queries carrier APIs through an integration with Cinch to verify whether a SIM change has occurred. This verification step ensures a zero false-positive outcome. Scans run continuously every 15-30 seconds, and if the carrier confirms a SIM swap, administrators are alerted automatically without requiring any action from the end user.

SIM swap detection, which will be available in Q2 of 2026 for both iOS and Android, requires MDM enrollment and is available for devices running on Verizon and T-Mobile.

To learn more about SIM swap detection, visit www.iverify.com.

About iVerify

iVerify is a pioneer in mobile endpoint detection and response (EDR) solutions, providing advanced protection against the real threats mobile devices face. The company's comprehensive security platform safeguards organizations from fileless malware, smishing, malicious applications, ransomware operations, and breaches resulting from credential theft. iVerify's solutions span from consumer to enterprise and government sectors, offering both privacy-focused BYOD protection and enterprise-grade security capabilities to ensure every device in the workplace is secure.
For more information, please visit: www.iverify.com.

Monika Hathaway
iVerify
email us here