Solution Brief

Robust Mobile Threat Intelligence with VIP Advanced Device Reputation

Problem

Increasing losses from customer account takeover fraud on mobile channels

Solution

Robust threat intelligence paired with seamless authentication

Benefits

- Excellent security hygiene
- Minimized potential for fraud
- Frictionless user experience
- Uniform authentication experience across channels
- Simplified management, no security gap

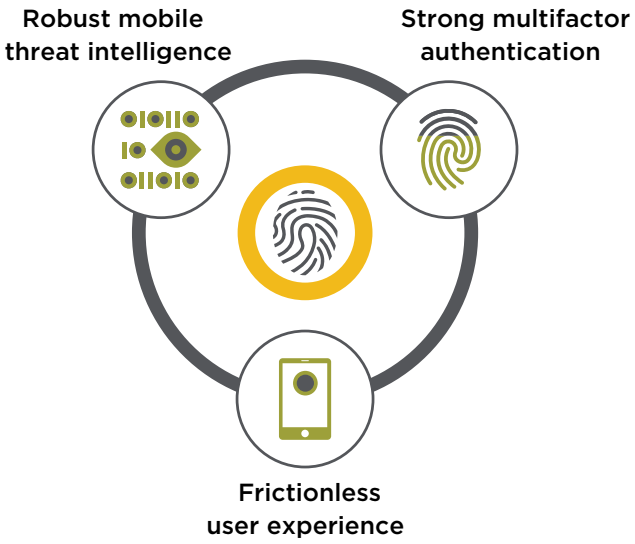
Introduction

According to Javelin Strategy & Research's 2018 Identity Fraud Study, fraud losses from account takeover (ATO) attacks rose to over $5 billion in 2017; that's a 120 percent increase from 2016. The shift towards digital channels, especially mobile, has given cyber criminals the means to orchestrate more sophisticated and complex attacks. Stolen credentials, phishing schemes, malware, man-in-the-middle attacks, mobile SIM swapping—these are all techniques used by cyber criminals to exploit consumers and infiltrate incomplete security defenses. To combat this threat, organizations need robust mobile threat detection and strong multifactor authentication, all while preserving the user experience. Enter Symantec Validation and Identity Protection (VIP). The Symantec VIP platform supplies three critical components needed for a strong ATO defense strategy.

Robust Mobile Threat Detection

Incorporating the VIP software development kit (SDK) with your mobile application provides unparalleled insights into mobile security threats. Powered by the Symantec Global Intelligence Network (GIN), the world's largest civilian cyber threat intelligence database, VIP identifies cyber threats that can compromise digital channels. The Symantec GIN correlates threat intelligence from nine trillion lines of telemetry across endpoints, web, and emails to achieve unequaled detection of new threats. Take advantage of critical new mobile threat intelligence extracted from the GIN to gain powerful insights into device risk, network risk, configuration anomalies, and cyber threats. Create risk profiles of every mobile user to strengthen your security posture and guide your authentication strategy—all while giving your low-risk customers a seamless experience.

Figure 1: VIP at a Glance



Device Risk Signals

Key insights:

- O/S Type and Version
- Upgradability Status
- Running O/S with Known Vulnerability (CVE)
- VIP Access or SDK Version
- Debugger

Why they matter: Cyber criminals exploit loopholes in out-of-date software. It's important you evaluate the device and ensure it's up to date with the latest software version and not operating with any known O/S vulnerabilities.

Network Risk Signals

Key insights:

- SSL Strip
- SSL MiTM
- Content Manipulation
- ARP Spoofing
- DNS Spoofing
- Access Point Reputation

Why they matter: The network a customer uses to connect to your organization can introduce critical vulnerabilities, paving the way for man-in-the middle (MiTM) and other attacks. These insights pierce that veil to ensure a safe, secure connection.

Configuration Anomalies

Key insights:

- No Passcode
- Untrusted Profile
- Touch ID Safety Detection
- Untrusted certificate
- Developer option enabled
- Unknown sources enabled
- Storage encryption disabled

Why they matter: Interrogating the mobile device for configuration anomalies provides key insights into whether the device may be susceptible to being physically controlled by another user.

Cyber Threat Intelligence

Key insights:

- Malware Detected
- Malware Details
- Vulnerability Detected (KRACK)
- Compromised Device (Jailbroken/Rooted)

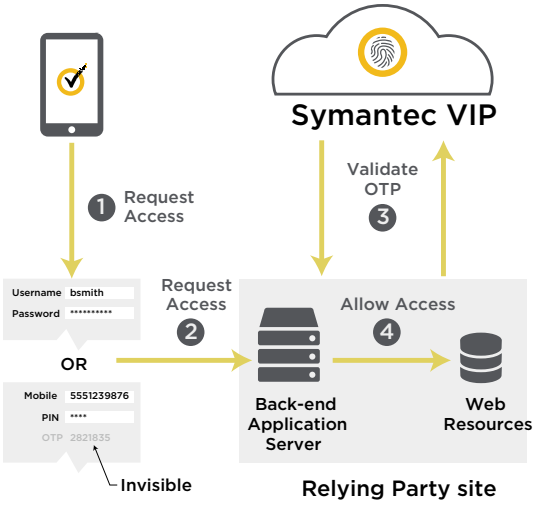
Why they matter: A recent Symantec data study showed a strong correlation between device reputation and fraud risk; the least reputable devices were 3x more likely to be associated with identity fraud.

Strong Multifactor Authentication—and a Seamless User Experience

To protect mobile applications, many organizations default to biometrics (such as touch ID) and SMS one-time passcodes. These capabilities provide a layer of protection but alone are not sufficient to stop sophisticated ATO attacks. Cyber attack methods are constantly evolving, and technologies such as SMS are not foolproof.

Symantec VIP empowers organizations with unequaled multifactor authentication technology. VIP registers, provisions, and validates the mobile device securely, and does so without impacting the customer experience. For example, rather than transmit a one-time-passcode through nonsecure SMS channels, VIP embeds this capability within your mobile application. The code is validated behind the scenes, all completely transparent to customers. The result is a highly secure and friction-free authentication experience. Using this process throughout the customer lifecycle promotes continuous customer trust.

Figure 2: VIP Validation Process



1. User logs into mobile app embedded with VIP
2. Client's back-end app server validates user's credentials
3. VIP service validates the OTP (along with credential ID)
4. Upon approval, user gets access to application

Summary: Improved Threat Detection and Frictionless Strong Authentication

Today's consumers have zero tolerance for friction-filled experiences—especially in the mobile channel. Fortunately, you can partner with Symantec to make intelligent, riskbased decisions that ensure highly secure-yet-seamless interactions with customers across channels. The latest enhancements to the Symantec VIP SDK further drive cyber threat insights into the mobile realm.

Next Steps

For more information on how Symantec VIP can help secure your mobile strategy, visit the Symantec VIP page.

For more information, visit VIP Enterprise.

SED-VIP-SB100 March 16, 2020