

The TAG logo consists of the letters 'TAG' in a bold, white, sans-serif font, centered within a solid blue rectangular box.

TAG

SPECIAL ANALYST REPORT

TOP FIVE MOBILE APP SECURITY VENDORS

2025 - 2026

The Approov logo features a stylized graphic of colored dots (pink, green, yellow) above the word 'approov' in a lowercase, white, sans-serif font, all contained within a black rectangular box.


approov



SPECIAL ANALYST REPORT

TOP FIVE MOBILE APP SECURITY VENDORS – 2025-2026

PREPARED BY THE TAG ANALYST TEAM

www.tag-infosphere.com

LEAD ANALYST: DR. EDWARD AMOROSO

Chief Executive Officer, TAG Infosphere¹

Research Professor, NYU²

eamoroso@tag-cyber.com

Version 1.0
2025

This TAG Analyst Report features the TAG Top Five vendor Approov in the area of Mobile App Security for 2025–2026 based on TAG’s evaluation criteria..

Approov focuses on API security for mobile apps, ensuring secure communication between apps and their backend services. Its solution includes mobile app attestation to verify app integrity and block unauthorized or tampered apps from accessing APIs. Approov seamlessly integrates into existing mobile applications, offering protection against API abuse, bot attacks, and unauthorized access without requiring changes to backend APIs.

¹ TAG Infosphere provides research and advisory in cybersecurity, artificial intelligence, and climate science/sustainability for enterprise teams, government agencies, public policy lawmakers, academic researchers, and commercial vendors. See <https://www.tag-infosphere.com/>.

² NYU’s Center for Cybersecurity (CCS) is an interdisciplinary academic center in which leading edge cybersecurity research, teaching, and scholarship are directed into meaningful real-world technology, platforms, and policies. See <https://www.cyber.nyu.edu/>.

INTRODUCTION

Mobile applications have become essential to modern life, enabling users to access services, manage personal data, and conduct transactions conveniently. However, their ubiquity has also made them a primary target for cyberattacks. Mobile app security is critical to protect sensitive user information, ensure privacy, and prevent unauthorized access to personal and corporate data. The increasing integration of mobile apps with Internet of Things (IoT) devices, cloud services, and financial systems further underscores the need for robust security.

Mobile app security faces unique challenges due to the diversity of devices, platforms, and development environments. Fragmentation in operating systems, such as Android and iOS, requires developers to tailor security measures to specific platforms, increasing complexity. Additionally, mobile devices often operate in untrusted environments, such as public Wi-Fi networks, where attackers can intercept communications. The prevalence of third-party libraries and APIs in app development introduces supply chain vulnerabilities, and many applications fail to implement secure coding practices, leaving them exposed to risks such as SQL injection and reverse engineering.

Mobile applications are susceptible to a range of threats, including malware, phishing attacks, and unauthorized access through weak authentication protocols. One prominent risk is mobile ransomware, where attackers encrypt user data and demand a ransom for decryption. Another is insecure data storage, where sensitive information, such as login credentials or payment details, is improperly stored in plain text. Man-in-the-middle (MitM) attacks on unsecured communication channels can allow attackers to intercept and manipulate data exchanged between apps and servers.

Developers and organizations can adopt several strategies to secure mobile applications. Implementing robust encryption for data storage and transmission is crucial to protecting user information. Using strong authentication mechanisms, such as multi-factor authentication (MFA), can prevent unauthorized access. Regular security assessments, including penetration testing and code reviews, can help identify and address vulnerabilities. Moreover, secure development practices, such as minimizing permissions, avoiding hardcoded credentials, and using obfuscation techniques, can reduce the risk of exploitation.

As mobile applications continue to evolve, so too will the methods used to secure them. Emerging technologies, such as artificial intelligence (AI) and machine learning, are playing a growing role in detecting and mitigating threats in real time. Regulatory frameworks like GDPR and CCPA are driving increased attention to data protection, pushing developers to prioritize privacy by design. The integration of advanced technologies like biometric authentication and secure enclaves will further enhance mobile app security.

EVALUATION CRITERIA

The process for calculating a TAG Navigator to determine the aggregate CVR for a cybersecurity vendor involves ten factors. How these factors are used has evolved and is now associated with a common, normalized interpretation and scoring that is being used in various sectors including cyber insurance as a basis for reviewing the effectiveness of a vendor in reducing the cyber risk of buyers. The ten factors are as follows:

1. Company Stage: This references where a given vendor currently resides in the corporate lifecycle. At one end of the scale are the start-ups driven by founding teams. Mature public companies with experienced management are at the other end of the scale.

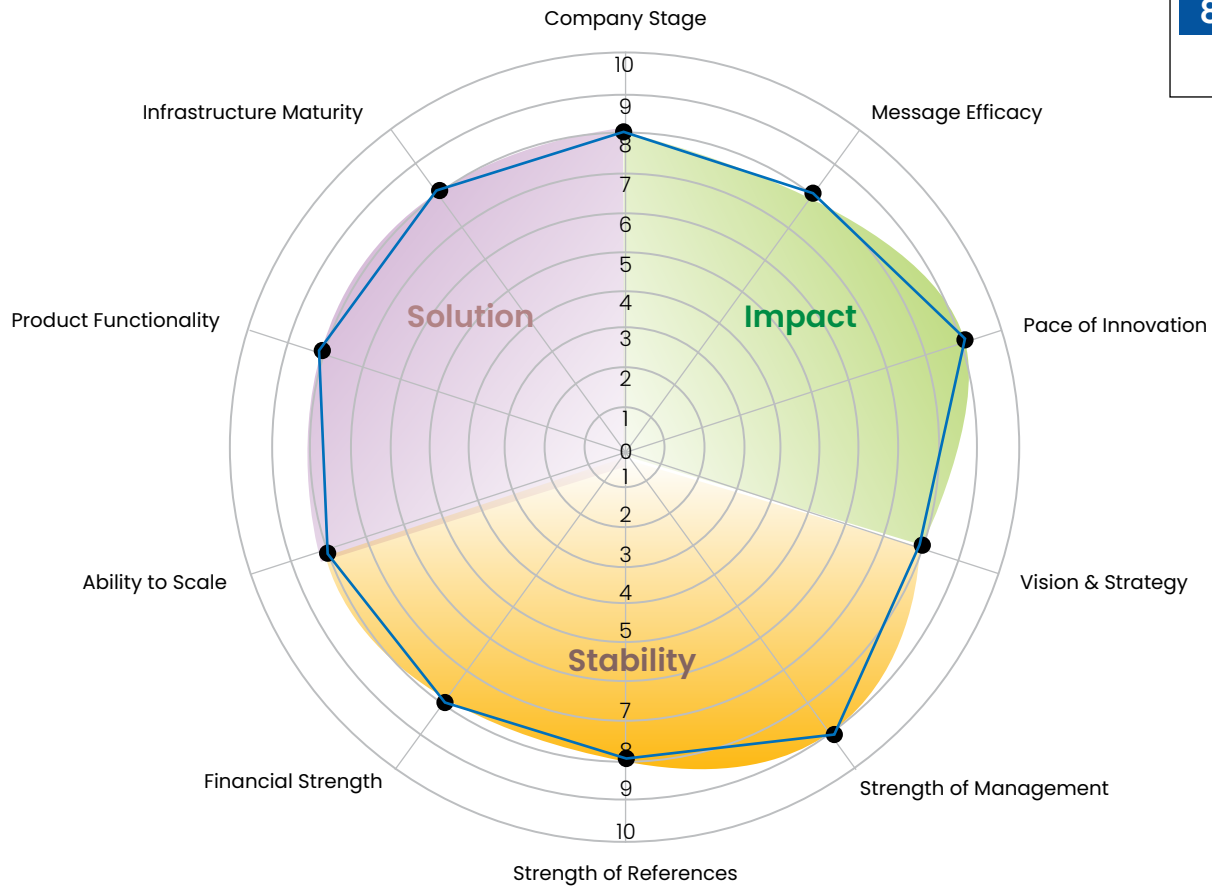
- 2. Message Efficacy:** This involves the vendor's marketing and value proposition message. At one end of the spectrum is an unclear description focused mostly on features. At the other end is a strong message of what solution is being addressed and why.
- 3. Pace of Innovation:** This involves how rapidly the vendor is innovating. At one end of the scale are the vendors innovating at an impressive pace. At the other end of the scale are companies who slow innovation in favor of scale.
- 4. Vision and Strategy:** This addresses whether the vendor articulates their role and purpose. At one end of the scale are vendors developing a future vision. At the other end of the scale are vendors who describe a clear vision and strategy for their company.
- 5. Strength of Management:** This references whether a strong management team exists. At one end of the spectrum are companies with new managers in their first leadership roles. At the other end are companies with a mature, experienced leadership team.
- 6. Strength of References:** This involves the references who can vouch for a vendor. At one end of the scale are new vendors with virtually zero customers and at the other end, we find vendors with massive global customer bases.
- 7. Financial Strength:** This addresses the company's funding, revenue, and profitability. At one end of the spectrum are companies with weak near-term financial prospects. At the other end are well-funded or public companies with growing revenue and profits.
- 8. Ability to Scale:** This addresses whether the solution can be provided to a large base. At one end of the spectrum are companies that struggle to support new customers. At the other end are companies with a platform that can handle rapid growth.
- 9. Product Functionality:** This references whether the solution addresses the needs of its customers. At one end of the spectrum are companies with a prototype. At the other end are companies with a working solution that is thoroughly used and supported.
- 10. Infrastructure Maturity:** This references whether the company is sufficiently protecting user data and ensuring proper support for customer security. New vendors are usually challenged in this area and often do not have security teams in place.

More information on these ten factors that comprise the set of criteria used in rating cybersecurity vendors is available on-demand from TAG. Research as a Service (RaaS) customers can review the justifications for ratings through their TAG RaaS portal account. They can also obtain more detailed guidance on roughly 4700 commercial cybersecurity vendors. Information on TAG RaaS subscriptions can be obtained at <https://www.tag-infosphere.com/>.

TAG TOP FIVE NAVIGATOR
MOBILE APP SECURITY PLATFORM
 TOP-TIER VENDOR PROFILE

APPROOV

10
 ▲
CVR
RATING
8.2
 ▼
 0



Approov enhances mobile app security by focusing on API security and mobile app integrity. Its mobile app attestation technology verifies that only genuine, untampered apps can access APIs, protecting backend systems from unauthorized or rogue applications. By embedding lightweight SDKs into apps, Approov enables seamless attestation processes without compromising app performance or user experience.

Approov's solution protects against a range of threats, including man-in-the-middle (MitM) attacks, API abuse, and bot-driven exploits. It ensures that only authenticated apps can interact with APIs by leveraging secure tokens, which are dynamically generated during the attestation process. This approach prevents attackers from using unauthorized apps or emulators to exploit backend services.

Approov also helps protect secrets and enhance service continuity and incident response, even when third-party APIs are affected. Because of the unique way Approov can get attestation information about the device and the application, API keys can be delivered just in time to the application but only when the device and app are verified as genuine and unmodified. In this way, secrets are always secure and never appear in your code. Certificates, pins, and API keys can easily and immediately be updated across all deployed apps. In this way, if secrets are ever stolen from cloud repositories or acquired through other means, or if a third-party API used by your app changes keys, they can immediately be rotated without any service interruption and without having to update apps.

Methodology: The TAG Navigator uses 10 factors to assess vendor's solutions. Each factor represents a key aspect of the solution's value and has been deemed by TAG as a reasonable predictor of its success in the discipline. TAG's Cyber Vendor Ratings (CVR) factors are rated on a scale of 1-10. The solution analyzed above has been selected by TAG as a top-tier solution within the discipline.

The TAG logo consists of the letters "TAG" in a bold, white, sans-serif font, centered within a solid blue rectangular box.

SPECIAL ANALYST REPORT

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to provide on demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, and artificial intelligence.

tag-infosphere.com



ABOUT APPROOV

Approov provides advanced mobile app and API security, ensuring only genuine, untampered apps can access backend services. Its dynamic runtime protections prevent bot attacks, reverse engineering, and data breaches, safeguarding sensitive data across all mobile ecosystems.

approov.com