TAG

OVERVIEW AND ASSESSMENT OF MOBILE APP SECURITY START-UP APPROOV

DR. EDWARD AMOROSO,
CEO, TAG
RESEARCH PROFESSOR, NYU

approov

TAG

OVERVIEW AND ASSESSMENT OF MOBILE APP SECURITY START-UP APPROOV

PREPARED BY THE TAG ANALYSTS

LEAD ANALYST:
DR. EDWARD AMOROSO, CEO, TAG,
RESEARCH PROFESSOR, NYU

This independent analyst report on cybersecurity company Approov is intended for use by existing or prospective users of the company's mobile app security platform, as well as by investors, researchers, or other stakeholders interested in learning more about this vendor. The work reported below was done by the TAG analyst team with consultation from Approov as well as discussions with enterprise teams knowledgeable of mobile app security.

INTRODUCTION

Approov is a mobile app security platform that currently addresses the growing concern of API abuse, mobile app tampering, and unauthorized client access in distributed environments. Originally founded in 2002 by a UK-based firm known as CriticalBlue, the platform has since evolved for use by organizations operating in finance, healthcare, retail, automotive, and other sectors where mobile app integrity and API security are mission-critical.

Industry veteran Ted Miracco took the helm as CEO in late 2022 with a clear goal of expanding Approov's reach into the important U.S. market for dynamic run-time mobile app protection. Under Ted's leadership, in August 2025 Approov closed an

[1] *CriticalBlue, before shifting its focus to mobile app and API security with the launch of Approov, was initially dedicated to code optimization and microprocessor design technologies for the semiconductor industry.*

additional £5 million (US$ 6.7 million) funding round. The investment was spearheaded by the Investment Fund for Scotland, managed by Maven Capital Partners, with participation from Souter Investments, as well as existing investors Lanza techVentures and Scottish Enterprise. This funding milestone enables Approov to bolster its Research & Development team in Edinburgh, driving the creation of advanced technologies to secure mobile applications and APIs against evolving threats, including those powered by AI.[2]

It's worth noting that despite the rapid growth of mobile traffic, now a dominant share of global internet usage, mobile app security has often received less focused attention from CISOs compared to traditional web security. This gap persists even as sensitive information such as healthcare records, financial assets, and digital credentials increasingly flow through mobile APIs that are inadequately protected by legacy approaches.

A key aspect of TAG's interest in Approov has been its shared view that such focus is inconsistent with growing concerns that should be raised about poor mobile app security. Tag advises enterprise clients in this area and views improved mobile app security as an urgent management consideration, one that demands increased attention on reducing the associated risk. This report should reflect that view.

MOBILE APP SECURITY MARKET

The mobile ecosystem presents a unique challenge because users tend to view the App Stores from Google and Apple as being sufficient gatekeepers of security and trust. This is at least partially true. We are pleased that both large companies have done an acceptable job in demanding higher quality code and more secure execution environments for their operating systems (as opposed to earlier generations of insecure Windows execution.)

But the reality is also that the App Stores from Apple and Google provide only a superficial level of vetting. In practice, they do little to ensure protection of the backend APIs, where the most valuable assets reside. HIPAA-regulated data, digital banking credentials, vehicle access controls, and even tokenized rewards, for example, are all accessible via exposed API calls that are often insufficiently shielded from abuse.

This false sense of security is compounded by industry reliance on static defenses such as code obfuscation.[3] These techniques, while helpful in deterring basic reverse engineering, are increasingly easy to defeat using modern AI-driven de-obfuscation tools or real-time binary manipulation. Worse, they offer an insufficient practical means of monitoring or responding to threats dynamically at runtime.

Global trends in regulation are also entering the picture. Enterprises now operate in a multi-market environment, where apps may be sideloaded (or the device can contain sideloaded apps), and the use of alternative operating systems such as HarmonyOS or non-GMS Android variants is increasing. Upcoming regulatory changes, including the EU Digital Markets Act (DMA) and the Competition and Consumers Bill (DMCC) are forcing mobile teams to consider stronger security for app deployments.

OVERVIEW OF THE APPROOV PLATFORM

The purpose of Approov is to ensure that only untampered, authorized versions of mobile apps running in trusted environments are allowed to access protected backend APIs. Such functional requirement is viewed by our team at TAG as being not only desirable for mobile app security, but increasingly essential. Compliance and regulatory frameworks should be adopting and including such controls immediately.

[2] *TAG has worked with Approov for two years in a research and advisory capacity, including generation of research publications such as this one: https://approov.io/info/apple-and-google-suppress-innovation-in-mobile-app-security-why-it-matters.*

[3] *We see this technique emerge during TAG review sessions with commercial security vendors addressing mobile app risk. Here is a typical report on this method from Symantec: https://www.security.com/threat-intelligence/spyware-obfuscation-static-analysis.*

Approov accomplishes such control through a combination of runtime integrity verification, device environment checks, dynamic secret delivery, and token-based authentication. The platform is delivered as a software development kit (SDK) integrated into the mobile application, coupled with a cloud-based service responsible for evaluating app authenticity and issuing tokens in real time.

MOBILE APP INTEGRATION

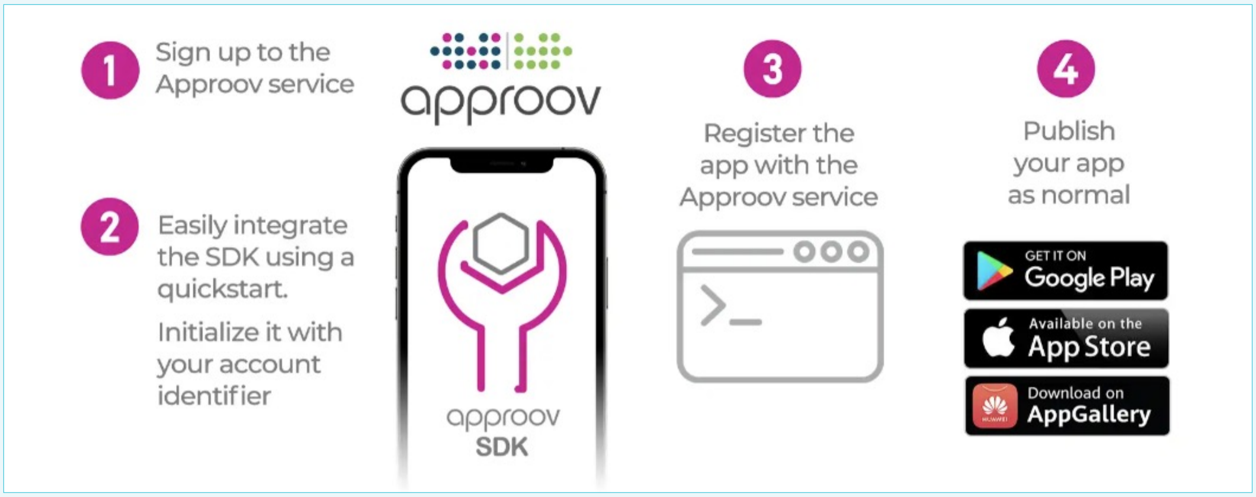
1 Sign up to the Approov service
approov
2 Easily integrate the SDK using a quickstart.
Initialize it with your account identifier
approov SDK
3 Register the app with the Approov service
4 Publish your app as normal
GET IT ON Google Play
Available on the App Store
Download on AppGallery

Figure 1. Ease of Mobile App Integration Using Approov

Approov offers run-time security, where adding Approov to an iOS or Android mobile app is easy. It involves a wide range of platforms supported using the Quickstarts process as depicted in Figure 1 above.

When an application protected by the Approov platform starts, it initiates an attestation process to confirm its legitimacy. This process involves the app sending a challenge to the Approov cloud service, which in turn analyzes the binary fingerprint of the application and inspects runtime conditions, such as whether the device is rooted, jailbroken, emulated, or exhibiting signs of instrumentation. Readers will note these familiar device problems as being consistently present in mobile environments.

This approach by Approov reflects a modern philosophy, one that is consistent with the trend toward zero trust design devoid of a protective perimeter. Specifically, what the approach here is that rather than building higher walls around the app itself, Approov focuses on defending the entire system of interaction, including the edge device, the app, the communication layer, and the APIs on the backend.

If the mobile app and its runtime environment pass the attestation checks, the Approov service issues a signed token, typically a JSON Web Token (JWT), which the app includes in subsequent API calls. These tokens are short-lived, and the backend verifies their validity before permitting access. This ensures that trust is continually reassessed at runtime, rather than assumed statically based on installation or package signing.

A feature of the Approov platform is its support for over-the-air (OTA) security updates, an essential capability in any environment where mobile attacks evolve quickly and traditional App Store-based patching is too slow. OTA delivery allows certificate pins, secrets, and even runtime policies to be updated without requiring a new app release or re-approval from distribution platforms. This increases resilience and enables real-time threat response.

APP ATTESTATION

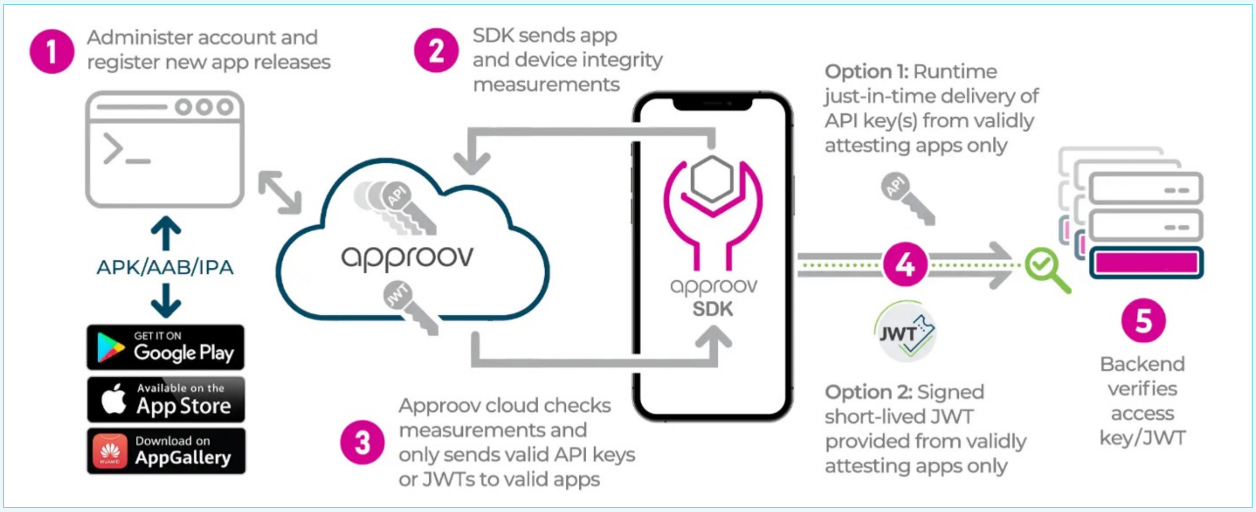
1
Administer account and register new app releases
APK/AAB/IPA
GET IT ON Google Play
Available on the App Store
Download on AppGallery
2
SDK sends app and device integrity measurements
approov
API
JWT
3
Approov cloud checks measurements and only sends valid API keys or JWTs to valid apps
approov SDK
Option 1: Runtime just-in-time delivery of API key(s) from validly attesting apps only
4
JWT
Option 2: Signed short-lived JWT provided from validly attesting apps only
5
Backend verifies access key/JWT

Figure 2. App Security Attestation Using Approov

App attestation is a validation method used to provide proof of authenticity for a given app and that it is running in a trusted device. The process using the Approov platform is depicted in Figure 2 above.

Approov also delivers API secrets only to verified instances of the mobile app. In contrast to static embedding, where secrets are often extracted by attackers, this method ensures that sensitive credentials exist only briefly and in verified environments. Similarly, certificate pinning is managed by the Approov service rather than hardcoded in the binary, thus allowing updates in response to certificate rotations or compromises, without requiring user intervention.

OPERATIONAL CONSIDERATIONS AND PLATFORM INTEGRATION

From an operational standpoint, Approov benefits from and encourages collaboration across app developers, DevOps teams, and backend engineers. The SDK is embedded during build-time, and mobile binaries are registered with Approov. JWT validation must be added to protected API endpoints, which can be accomplished with widely available libraries and Approov's helper tools.

The solution includes telemetry support for logging attestation failures, suspicious device profiles, and token validation issues. This visibility helps teams detect patterns such as geographic anomalies, bot-like behaviors, or use of cloned and modified apps in the wild.

SECRETS PROTECTION

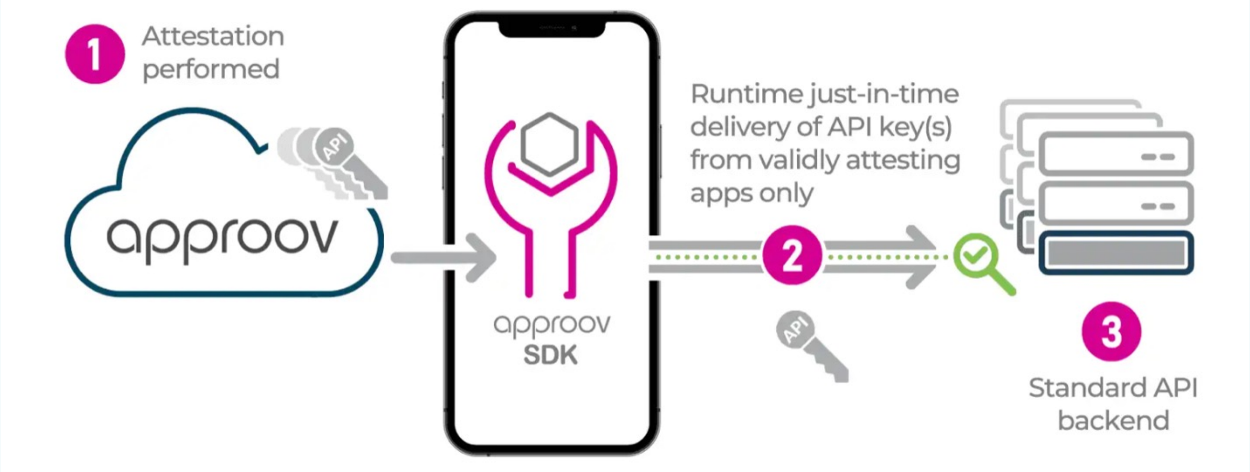
1
Attestation performed
approov
API
approov SDK
Runtime just-in-time delivery of API key(s) from validly attesting apps only
2
API
3
Standard API backend

Figure 3. Runtime Secrets Protection Using Approov

Approov supports runtime secrets protection whereby API keys and other secrets are removed from the app package in advance of them being shipped for download as shown in Figure 3.

The platform operates as a global SaaS offering, with attestation services hosted in the cloud, primarily on AWS. This architecture allows it to handle high-scale usage across geographies.

Approov does require an internet connection to validate the app's integrity. Offline, an attacker can analyze the application but can't access protected APIs or secrets. Any real attack must come online, and that's where Approov shines—by blocking access from tampered or unauthorized app instances in real time. It ensures your backend stays safe, regardless of what an attacker tries to do offline.

Pricing follows a usage-based model based on monthly active users, with enterprise plans available. Public documentation is extensive, and integration with modern mobile CI/CD workflows is supported.

MARKET PROSPECTS FOR APPROOV

Our bias toward improved mobile app security stems from our extensive experience across the TAG team in enterprise protection and telecommunications.[4] The belief is widely held across our TAG team that mobile security is under-estimated regularly and that residual risk exists in most enterprise IT and networking environments, regardless of the size, scope, or sector of the organization. This might help to explain our interest in Approov.

That said, we believe that Approov's long-term prospects rest on its ability to help buyers recognize this urgency in mobile security-related risk. One strategy we would recommend for Approov to follow in its global marketing efforts is to emphasize the disparity between mobile usage, which dominates traffic globally, and the relatively modest level of enterprise security investment which has been allocated to protecting mobile environments.

[4] The lead author for this report (Amoroso) served for many years as the Chief Information Security Officer (CISO) at AT&T, where he led efforts to drive mobile security into the enterprise IT and network ecosystem.

REAL-TIME THREAT INTELLIGENCE

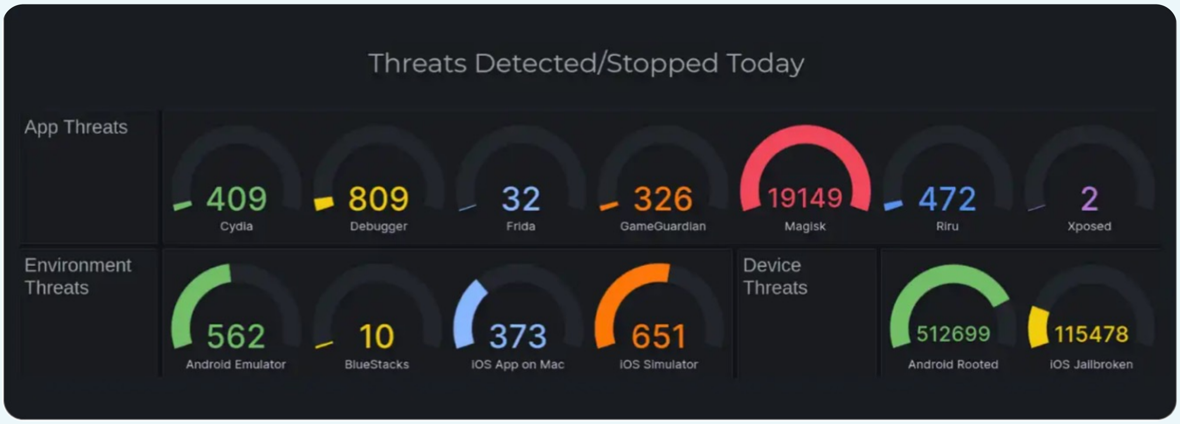

Figure 4. Real Time Intelligence Dashboard Reporting

Approov offers a live feed of telemetry from running mobile apps and the associated threats. This is provided via a dashboard for easy review and action (see Figure 4).

It should be reinforced to enterprise decision makers that the modern mobile threat surface now includes sideloaded apps, alternative operating systems, multiple device types, and an expanding mix of app distribution models, all of which erode traditional trust assumptions. These attributes of the mobility ecosystem introduce risk that conventional controls and frameworks will do nothing to reduce.

This is not just a challenge in North America and Europe. Mobile growth is fastest in Latin America, the Middle East, Africa, and Asia, where users rely on devices from Xiaomi, Vivo, OPPO, and Huawei, often outside the Apple and Google duopoly. In such cases, securing mobile apps requires a strategy that accounts for all platforms, regions, and store ecosystems. Approov's support, including non-GMS Android and HarmonyOS, is a differentiator.

CLOSING REMARKS

It should be evident from our comments above that we recommend Approov as a strong cybersecurity partner for anyone involved in the development, test, delivery, and execution of mobile apps. The company delivers a layered, OTA-updated, runtime-verified mobile security platform that is aligned with zero-trust. It addresses inadequacies in static defenses, illusions of App Store gatekeeping, and operational needs for scalable, developer-friendly integration.

Readers are encouraged to reach out to the TAG team for additional information on mobile app security, or any other aspect of modern cybersecurity or artificial intelligence-based products, vendors, or issues. TAG Research-as-a-Service (RaaS) customers can reach out through their portal account. And readers are also strongly encouraged to connect directly with the Approov team for discussions, guidance, and a demonstration of their fine product.

We look forward to hearing from you.

ABOUT TAG

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