SOLUTION BRIEF

Complete Protection for Mobile Apps and APIs

Key Benefits of the Approov Solution

- Positive app authentication
- Blocks all forms of API abuse
- Runtime secrets protection for 3rd party APIs
- Protection from Man-in-the-Middle attacks
- Tamper detection & jailbreak/root detection
- Confidence that the client environment is always secure
- Elimination of API keys & secrets from mobile code
- Dynamic management of security policies, certificates & secrets
- Cross platform support for iOS, Android & HarmonyOS
- Support for non-GMS Android devices
- Compliance with regulatorystandards
- Real-time analytics for control & compliance
- Easy integration & operation

Mobile Apps Leak Secrets and Their APIs are Exposed

Mobile apps are now a critical element of B2B and B2C businesses worldwide. However apps can be analyzed, understood, cloned or copied, and the environments they run in can be hacked, rooted, instrumented and manipulated to interfere with the operation of an app.

Hackers can intercept or manipulate financial transactions, steal credentials to use in ransomware attacks, target APIs with fake apps and bots, or simply aim to stop the operation of the service. Mobile apps and their APIs must be protected using a zero trust approach at runtime.

Traditional Approaches are Insufficient and Hard to Maintain

Backend Application Security: Traditional server-side solutions such as a WAF or Bot Mitigation solutions rely on known patterns and involve constant maintenance and updates to keep up with the latest attack vectors. In addition, they don't effectively detect scripts impersonating mobile apps or have visibility to devices.

Obfuscating Code or Hiding Endpoints: Obfuscation may slow down attackers, but it cannot prevent determined adversaries from reverse engineering an app. Likewise, simply hiding API endpoints offers no real security—it only creates a false sense of protection. Real protection comes from continuous runtime authentication, which ensures only verified app instances can interact with backend systems.

Transport Level Security: Deploying TLS provides an encrypted channel between the mobile app and the server but TLS can be bypassed by software on the client. Certificate pinning can prevent MitM attacks. However, devops teams often push back on this best practice, citing concerns about performance and availability, meaning traffic is exposed.

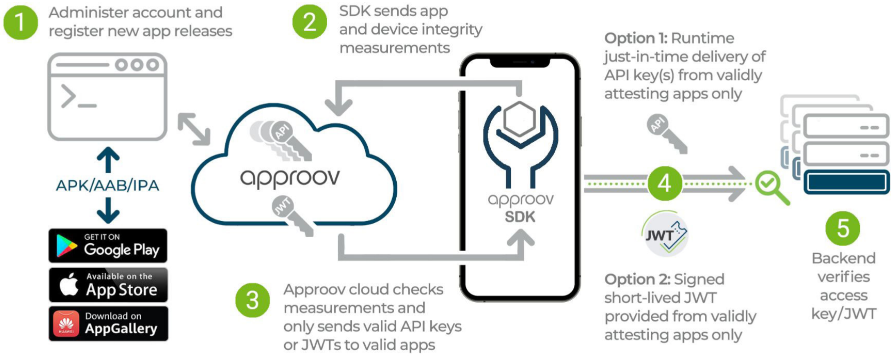
Mobile Application Security Testing (MAST): Using Mobile Application Security Testing before deployment relies on known vulnerability databases and predefined attack patterns and doesn't detect currently unknown "zero-day" exploits or business logic issues in APIs.

Approov Protection for Mobile Apps and APIs

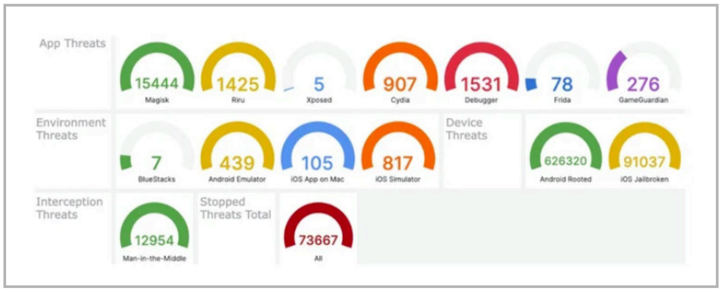
Approov Mobile Security provides a comprehensive multi-factor, end-to-end mobile app and API security solution that prevents any manipulation of the app, device or communications channel to the backend, and removes secrets from your app code. Only safe and approved apps can successfully use your APIs. Bots and fake or tampered apps are all easily turned away and PHI is protected.

Approov also implements over-the-air management of security policies as well as dynamic management of secrets such as API keys and certificates, delivering them just-in-time to the app, and only when the app and client are known to be safe. This eliminates the need for app upgrades when changes are required.

How Approov Protects Your Mobile Apps and APIs


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

- **Positive app authentication:** Approov ensures that traffic destined for your API is indeed coming from the legitimate mobile app and not a third-party tool. This ensures synthetic traffic generated by Bots and other API clients is eliminated while no valid app traffic is rejected.
- **Protection from Man-in-the-Middle attacks:** Approov makes sure best-practices for TLS are applied correctly all the time, ensuring all API calls are protected and man in the middle attacks are eliminated. Approov ensures certificate pinning is implemented correctly, eliminating the concern over apps being blocked when problems arise with a certificate.
- **Confidence that the client environment is always secure:** Even if your app's authenticity checks out, it may still be running in a compromised environment. Approov detects rooted/jailbroken devices, apps running in debuggers or on emulators, or malicious instrumentation frameworks manipulating your apps.
- **Elimination of API Keys and secrets from mobile code:** Approov implements secure dynamic management of secrets such as API keys. These no longer need to be stored in the app code. Such secrets are delivered just-in-time to the app, and only when the app and client are known to be safe.
- **Dynamic management of security policies, certificates and secrets:** Approov's security layers operate frictionlessly for your users. Secure over-the-air capabilities update security policies, deliver enhancements, upgrade or rotate certificates, blacklist specific devices, rotate API keys for managed or third-party APIs, or deregister specific app versions: all without the need to change the app.



- **Live analytics for control and compliance:** App attestation traffic monitoring and security failure analytics are available. Alerts can be set for changes in volume of attestation traffic or spikes in app integrity failures. Anonymized data provides information on the cause of the security failures and information about the app, device, and network environments.
- **Easy integration and operation:** Easy SDK integration in the app is combined with industry standard token checks at the backend. Approov integrates easily and seamlessly with your Identity and Access Management (IAM) solution. A wide range of existing mobile platforms and backend service integrations are provided. A unified command line interface provides easy DevSecOps integration into your existing developer and operations infrastructure.

Contact us for a free technical consultation - our security experts will show you how to protect your revenue and business data by deploying Approov Mobile Security
https://approov.io/info/contact

approov