approov
mobile security

SOLUTION BRIEF

Protecting Mobile Healthcare Apps and APIs

Key Approov Capabilities

Positive app authentication to eliminate automated traffic on your APIs

Systematic protection from Man-in-the-Middle attacks

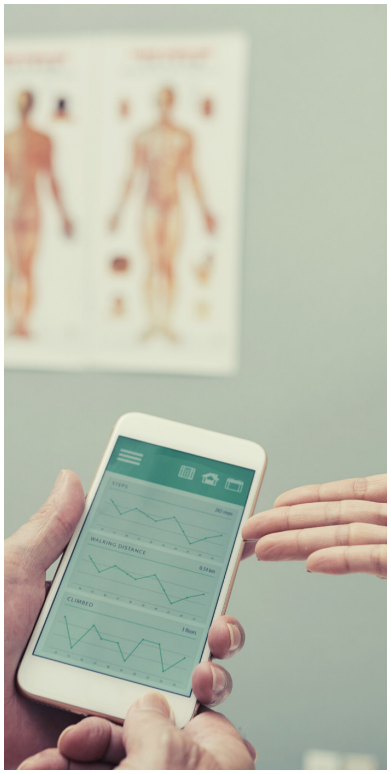
Confidence that the client environment is always secure

Elimination of API Keys and Secrets from Mobile Code

Dynamic management of security policies, certificates and secrets without requiring app release updates

Live analytics for control and compliance

Ease of Integration And Operation



Mobile Healthcare Apps are Being Adopted Rapidly but Their APIs are Exposed

The use of mobile healthcare apps is proliferating rapidly, driven by the massive spike in the demand for virtual healthcare. These apps are used by practitioners for all aspects of treatment and practice management, and by patients to control and access healthcare data. In addition, government regulations are pushing to drive patient ownership of data and innovation through interoperability.

Because of these trends, mobile healthcare applications and the APIs they access are at the heart of the new healthcare ecosystem. However, they must be protected in order to prevent unauthorized access to Personal Health Information (PHI) and to ensure HIPAA compliance in this highly regulated industry.

PHI is the most valuable data on the dark web making Healthcare apps and their APIs a prime target for cyber-criminals.

Traditional Approaches are Insufficient and Hard to Maintain

Signature-based approaches: 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, most are heavily reliant on browser fingerprinting which is not relevant with mobile apps and they don't effectively detect scripts impersonating mobile apps. In general, it is good practice to eliminate as much traffic as possible before it hits the backend.

Anti-tampering: Good development discipline and taking steps to protect your mobile app code from tampering or reverse engineering should always be employed. However, secrets required to attack your APIs can be acquired by hackers from other channels, so protecting the app code must be part of a broader security program that also focuses on protecting the mobile API and the critical assets on the server from bad actors who are imitating your app.

Transport Level Security: Deploying TLS certainly provides an encrypted channel between the mobile app and the server. 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. You can't depend on patients and healthcare professionals being on secure networks, and if your TLS is not managed properly third parties can steal secrets and manipulate your 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 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.

Approov adds additional security controls to the SMART/FHIR framework and makes it easy to demonstrate HIPAA operational controls are in place to protect your APIs.

Key Benefits of the Approov Solution

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.

"Getting the app and API protection wrong in the MV Medic app was not an option. The recent LGPD legislation means that our healthcare institution customers could suffer from significant fines if we didn't meet our security goals."

– Tiago Calado, Software Development Manager, MV

Contact us for a free technical consultation: www.approov.io