

Vitality Safeguards Mobile Health Data and API Access with Approov



"Approov gives us strong, reliable assurance that only genuine instances of our app are talking to our APIs. That's absolutely essential when we're protecting sensitive health data and rewarding healthy behavior. The integration was clean, the support was excellent, and we now have a mobile API security model we can trust."

— Peter Paddock, Digital and Mobile Solutions Architect, Vitality

A Healthier Society Depends on Secure, Trusted Data

[Vitality](#) isn't a traditional insurer. As a pioneer of the shared value insurance model, Vitality rewards customers for healthy lifestyle choices—from steps walked to workouts completed and heart rate zones maintained. Its mission is to make people healthier and to enhance and protect their lives.

This unique model is only possible because of the seamless integration between the Vitality mobile app, wearable devices like Apple Watch, and a backend platform that processes vast amounts of behavioral and biometric data every day. But the more value this ecosystem delivers, the more attractive it becomes to malicious actors.

Vitality needed to ensure that every digital interaction—from earning rewards to submitting activity data—was coming from a genuine, untampered mobile app running on a secure device, not from scripts, bots, or compromised apps.

The Challenge: Authenticating Mobile and Wearable App Traffic

With a growing base of highly engaged users and increasing integration with consumer health devices, Vitality faced several challenges:

- Ensuring API access only from genuine apps.
- Preventing mobile API abuse and reward fraud.
- Maintaining data integrity across iOS, Android, and Apple Watch.
- Securing high-value personal health data from interception or manipulation.

One area of particular importance was Apple Watch, where a flagship program allows members to earn a subsidized device by staying active. Since user activity directly drives financial rewards, accurate and tamper-proof data submission is fundamental to the fairness of the program.

In parallel, health and wellness data has become one of the most lucrative forms of stolen data on the dark web, often fetching more than financial records due to its value in insurance fraud, identity theft, and targeted scams.

Why Approov? Proven Mobile API Threat Mitigation

Vitality selected Approov Mobile App Attestation to provide a robust and scalable solution for verifying the authenticity of every mobile API request.

With Approov, Vitality can:

- Ensure only official, untampered apps on genuine devices communicate with backend APIs.
- Detect rooted, jailbroken, or emulated environments.
- Support cross-platform protection, including seamless integration for Apple Watch apps.
- Dynamically deliver secrets or API keys only to trusted app instances.

This provides zero trust for mobile apps—ensuring that even if a device is compromised, backend systems are not.

Results: Trustworthy Data, Protected APIs, and Reward Integrity

Since adopting Approov, Vitality has dramatically strengthened its mobile API security posture:

- API requests are cryptographically verified to come from authentic apps.
- Data from wearable integrations like Apple Watch is trusted and secure.
- Attempts to spoof apps or run them in compromised environments are automatically blocked.
- Backend systems receive only validated traffic, reducing fraud risk and increasing confidence in rewards distribution.
- Vitality protects sensitive health data in compliance with data protection standards, while raising the bar against API abuse.

Looking Ahead: Scaling Secure Engagement Without Compromise

As Vitality continues to expand its offerings across digital wellness, fitness, and healthcare services, Approov is a critical enabler—ensuring that trust, security, and data accuracy scale with innovation.

With a mobile-first strategy and a strong culture of digital excellence, Vitality's use of Approov ensures its app remains not just a key engagement channel—but a trusted, secure gateway to healthy living.

"Our business model depends on accurate, trustworthy data from our members' mobile apps and devices. Approov ensures that data is genuine and hasn't been tampered with, which protects our rewards program, maintains fairness, and builds trust with our customers." – Peter Paddock, Digital and Mobile Solutions Architect, Vitality



Approov protects your revenue by ensuring that only your own mobile apps—running in safe environments and communicating over secured connections—can use your APIs and backend resources. Botnets, malicious scripts, tampered and fake apps are blocked.

Find out more about Approov Mobile Security: www.approov.io