Analyst Guide: Securing Mobile Apps

An Intellyx Analyst Guide for Approov

By Jason Bloomberg and Eric Newcomer, Intellyx

Table of Contents




Introduction

High-level Mobile apps are now the center of your business strategy - why is it not the case for security also? Instead of being an afterthought, it should be the key security focus.

Your threat surface isn't made up of holes. It's made up of devices – devices in the hands of bad actors. You may put your app on users' devices, but the bad guys control the devices in their possession – including the apps, the data, and everything else. Protecting the back-end is insufficient. Obfuscation is a mere bump in the road for hackers. You need to rethink mobile security.

By Jason Bloomberg

Managing Director
Intellyx

Why Isn't Mobile at the Center of your Cybersecurity Strategy?

Part 1 of the Securing Mobile Apps Series

A FOCUS ON USER AUTHENTICATION (INCLUDING MULTI-FACTOR AUTHENTICATION) IS NOT ENOUGH TO PUT MOBILE AT THE CENTER OF YOUR CYBERSECURITY STRATEGY. ALSO NECESSARY: DEVICE, APPLICATION, AND CHANNEL INTEGRITY AS WELL AS SECURE API ACCESS.

Digital transformation has been with us for over a decade now, and most enterprises have made significant progress toward achieving its customer-facing goals.

Realigning siloed organizational models to better meet the needs of customers, employees, and others is no easy task – and indeed, companies have achieved varying levels of success.

While digital transformation is more about such organizational change than technology, tech unquestionably plays an important enabling role. In particular, mobile applications are central to many organizations' digital strategies.

Mobile-first thinking, in fact, now pervades discussions of digital transformation. Mobile devices are now ubiquitous, and mobile apps are both widely accepted and enormously powerful.

While such mobile-first digital strategies are the norm, mobile-first *cybersecurity* strategies are not. Instead, cybersecurity becomes more of an afterthought than an integral part of the digital strategy.

While it's true that mobile apps are among the various endpoints that bad actors might use to breach the organization, but as endpoints, they are on the periphery of the cybersecurity strategy.

As a result, there is a strategic disconnect within most enterprises: mobile is at the center of their digital strategy but peripheral to their cybersecurity strategy. Shouldn't mobile be at the center of their cybersecurity strategy as well?

Five Reasons Why Mobile-First Digital Strategy Should Drive Mobile-First Cybersecurity Strategy

Digital strategies are customer-focused. Since today's customer typically interacts with organizations via mobile apps, it's no surprise that digital strategies depend upon mobile-first technology strategies.

Here are five reasons why this logic should extend to cybersecurity strategies as well.

1. *Organizations must understand how mobile-first impacts the organization's threat surface.* The threat surface reflects all the possible points of compromise a bad actor might use to penetrate an organization's cybersecurity defenses. As endpoints, mobile apps are on this threat surface.

   The apps themselves, however, are not the whole story. Also on the threat surface: the device itself, the channel (network connection), the security credentials on the device, and the services mobile apps might access via APIs. In other words, each mobile app puts at least five holes in the threat surface, not just one.

2. *Every app is a front door to the back end.* Organizational silos may hinder digital strategies, but they offer a measure of compartmentalization that affords some security protection—even though such protections inevitably focus on back-office services alone.

   In a digital world, the mobile app connects directly to back-end services. In other words, every app is a front door to the back-end that bad actors are hoping to exploit.

3. *The more digital an organization is, the more important putting mobile at the center of the cybersecurity strategy becomes.* For some organizations, mobile apps are only one part of a diverse digital strategy. In other cases, the mobile app becomes the primary point of interaction between customers and the company – making mobile the central cybersecurity concern for the organization.

4. *Bad actors control their own devices.* You wouldn't intentionally hand over a corporate laptop to a malicious hacker – but the same bad actors own their own devices. As a result, they have complete control over the device – its hardware, operating systems, and network functionality.

   This control is intentional, as organizations want to afford customers the freedom to use any devices they like and empower them via their mobile apps. However, empowering customers means empowering the bad actors as well.

5. *Self-protection is a digital priority*. Organizations may not control users' devices, but they can control their apps – as long as they don't cede that control to bad actors. Yet existing mobile device management (MDM) technologies don't work for consumer users and fall short even in the enterprise.

It is essential for digital and cybersecurity strategies to align as organizations increasingly depend upon mobile apps. In fact, it makes even more sense to say that the digital and cybersecurity strategies should be two sides of the same coin.

As a result, the necessary protection is most effective if it resides in the app itself. In other words, app self-protection becomes a digital as well as a security priority.

For all these reasons and more, it is essential for digital and cybersecurity strategies to align as organizations increasingly depend upon mobile apps. In fact, it makes even more sense to say that the digital and cybersecurity strategies should be two sides of the same coin.

Separating the two generally leads to a lack of attention to cybersecurity as digital priorities command the attention of corporate leadership – to the long-term detriment of the organization. Don't let this mistake happen to you.

The Intellyx Take

This article is the first in a four-part series focusing on aligning mobile cybersecurity with digital priorities.

Next up: a closer look at secrets. Not only do bad actors steal mobile app credentials, but we all depend on our smartphones to support two-factor authentication. How do we protect our secrets in a mobile world?

Third in the series: putting your eye on the device. Cybersecurity depends upon visibility, as bad actors seek to hide in the shadows. How should an organization go about establishing visibility at the device level?

Wrapping up the series: certificate pinning. Organizations use mobile apps to terminate TLS sessions as any endpoint does – but there are many hops between phone and back-end, and TLS is a point-to-point protocol, giving bad actors the ability to mount man-in-the-middle attacks. We'll explore how certificate pinning is the solution.

By the end of the series, we'll have laid out the roadblocks to putting mobile at the center of your digital strategy – and how vendors like Approov can overcome them.

By Eric Newcomer

CTO & Principal Analyst
Intellyx

"Mobile First" is for Mobile Secrets, Too

Part 2 of the Securing Mobile Apps Series

Organizations, such as the Citi Consumer Bank when I was head of security architecture there, adopt a "mobile first" approach to application development.

"Mobile first" means first developing a mobile application that delivers a great customer experience, and later focusing on developing other customer facing applications (such as a web app).This is because of the growing importance of mobile applications in attracting new customers and retaining existing customers. But this also means a growing importance in securing mobile devices, as well.

Organizations should really consider prioritizing their cybersecurity programs on mobile devices. Often mobile security is viewed more as a part of the overall security program - an important part of course – but not often as the first priority.

Because mobile application adoption rates continue to grow, and mobile devices are connecting to more and more server-side APIs, it makes sense to consider prioritizing security on the mobile app.

What does "mobile first" mean for cybersecurity?

Generally speaking, it means making sure you lock down your mobile apps before you make sure you lock down your server apps.

Most organizations take the opposite view, and not surprisingly, because the server apps and the data they manage represent an organization's crown jewels.

However, the greater use of mobile devices means a greater risk of an incident or breach involving the APIs that access these server apps.

It's understandable that many organization's security policies focus primarily on protecting the server-side apps.

However, a mobile device has the secret key to the front door, as it were – the key to the server-side APIs.

The more mobile devices become part of daily life, the more they become significant sources of risk to those server-side apps.

Switching the focus from the server-side to the mobile device

"Mobile first" typically emphasizes the customer experience. After all, that's how consumers tend to judge a business such as a bank these days.

However, a good customer experience relies upon the responsiveness of the server-side APIs that exchange data to and from the mobile app. Any trouble with these APIs, such as a delayed or missing response, and the app is in trouble - no matter how smooth the UX.

And because of the growing number of server-side APIs, the security exposure is also growing. Many of these APIs are not locked down properly.

These APIs often don't have usernames and passwords and their access keys may be all too easily stolen from mobile device files, server-side files, or mobile application source code (which can be decompiled to retrieve them).

The risk of unprotected APIs

As mentioned previously, great customer experiences depend on great APIs. That's why there is so much investment in the industry now on solutions for API design, API analytics, API management, API testing, and of course API security.

But how do we know all the APIs are really secure? As much as half of them are not even protected with usernames and passwords.

Many organizations may view the challenge of protecting mobile application secrets as a mobile only challenge or think about it in the context of how best to deliver a great user experience (i.e. focusing only on secrets visible to the user).

But a secret isn't a secret if everyone knows it, or more importantly if anyone can access it easily.

Protecting mobile device secrets

API keys are the secrets that can open locked doors to server-side data. That makes them the most important secrets a mobile device holds.

Furthermore, organizations often assign privileged accounts to APIs. Hackers breaking into privileged accounts are the ones who create massive breaches and incidents.

The attack surface of the mobile device is constantly growing because of the explosion of APIs accessible via the Internet. Not protecting API keys is like putting all your money in a safe place in the home but not locking the front door.

The attack surface of the mobile device is constantly growing because of the explosion of APIs accessible via the Internet. Not protecting API keys is like putting all your money in a safe place in the home but not locking the front door.

Ironically, the same people who would never consider exposing a database secret often don't think as much about protecting mobile device API secrets.

What can you do about it?

Manage API keys independently from mobile device applications, for a start, the way you would think about managing database secrets independently from server-side apps.

Lock up API keys in a secrets vault stored in the cloud. Take the API keys out of the mobile app code and manage them independently and access them dynamically as needed, "just in time."

Maintain, update, and cycle them safely, with strong governance. Replace them immediately if anyone steals them.

Use a solution such as Approov Runtime Secrets which allows API keys and other secrets to be completely removed from the app package shipped to the app store.

Instead, deliver secrets securely to valid app instances at runtime, improving the security posture and significantly enhancing operational flexibility.

The Approov service delivers secrets "just-in-time" to the app only at the moment they are required to make an API call, and only when the app and its runtime environment has passed attestation.

Stolen secrets can immediately be rotated without any service interruption and without having to update the apps.

The Intellyx Take

As the ecommerce balance shifts more and more to mobile devices, it makes more and more sense to think about mobile device secrets the same way we think about server-side secrets, such as database usernames and passwords, and improve how we protect mobile device secrets, especially API keys.

But for mobile devices it's not yet common practice, although it probably should be. API keys are quickly becoming one of the most important protection mechanisms for mobile apps and for APIs in general.

Yet all too often these sensitive and important APIs are not given the protection they deserve and require to avoid incidents and breaches.

A solution such as the one from Approov that stores API keys securely in the cloud and downloads them to the mobile device on demand only when needed goes a long way to closing this important security gap.

By Jason Bloomberg

Managing Director
Intellyx

Why Hackers Love Phones – Keep your Eye on the Device

Part 3 of the Securing Mobile Apps Series

MAINTAINING A CORPORATE CYBERSECURITY POSTURE MEANS LOCKING DOWN ITS THREAT SURFACE – ALL POINTS OF POTENTIAL COMPROMISE THAT 'BLACK HAT' HACKERS MIGHT USE TO PENETRATE THE CORPORATE NETWORK. OF ALL THESE POINTS OF COMPROMISE, AMONG HACKERS' FAVORITES ARE SMARTPHONES AND OTHER HANDHELD DEVICES. EVERY DEVICE IS AN OPEN DOOR FOR HACKERS, AS THEY ARE REPLETE WITH VULNERABLE APPS THAT CONNECT TO BACK-END SERVICES AND NETWORKS.

Hacking corporate assets via smartphones is surprisingly easy. Many anti-hacking security tools are useful hacking tools themselves in the wrong hands. Familiar security approaches like TLS encryption and code obfuscation are dead simple to get around.

Clearly, cybersecurity professionals must make a special effort to secure the devices in the hands of their employees, users, and the general public. The first step to this protection is to understand the risks.

Hacking Phones 101

Hacking individual users' phones to steal their data or login credentials is bad enough. But the big prize for mobile device hackers is the ability to use the phone to access corporate assets, typically in the cloud.

Bad actors love to hack phones for this purpose. One of the main reasons they love handheld devices so much is because they have their own – and in most cases, it's easy for them to download and install corporate applications on them.

Given the device is physically in the hands of the hackers, they can do what they want with it, including jailbreaking (on iPhone) or rooting (on Android). Both jailbreaking and rooting mean bypassing any vendor controls on the phone, enabling the hacker to run any apps or tools that they want.

For example, a hacker can run a tool like mitmproxy that gives them the ability to compromise the network security on the device, thus bypassing TLS encryption – opening the corporate backend to attack.

Hackers can also reverse engineer the apps on the device. Since they have full control of the devices in their possession, it's a simple process to poke around inside the inner workings of an app to discern any secrets it may have.

Sometimes the attackers go after other users' phones as well. Hackers have access to numerous tools like Burp Suite and Frida that ostensibly provide security teams with the ability to test mobile device defenses – but also give bad actors all the information they need to compromise users' devices.

It may also be possible for the bad actor to jailbreak or root other users' devices, thus bypassing any security controls on those devices – unbeknownst to the users.

Once hackers have control of an app on users' phones, they can interfere with the operation of it and other apps, thus diverting ad revenues, compromising personal data, or perhaps worst of all, stealing API keys.

With stolen API keys the hackers can build scripts to attack back-end corporate services – with corporate security none the wiser.

The cybersecurity team will have implemented various protections – but they may not be up to the task of dealing with mobile device vulnerabilities.

For example, static and dynamic application security testing (SAST and DAST, respectively) are important components of any corporate cybersecurity strategy – but simply aren't up to the task of protecting handheld devices.

Given the fact that hackers control their own devices, checking the software binaries on the device won't slow them down. Obfuscating JavaScript also falls short because bad actors can simply run a deobfuscation tool.

Approov continually secures the devices at runtime by managing the behavior of applications as they run (rather than looking at the software itself). In addition, Approov continuously monitors the back-end APIs that apps interact with.

Relying upon any security built into iOS or Android is also insufficient, as hackers can jailbreak or root a device – bypassing those controls and letting them install any malware they like.

It's even possible for hackers to compromise apps as they are running by inserting malicious code at runtime – code that will bypass any tool that checks the apps before they launch.

Securing Devices – What Works

There's only one approach that can mitigate the risks inherent in mobile devices: *continuous end-to-end runtime checking*.

This continuous runtime checking begins on the devices themselves. Dynamic Runtime Application Self Protection (RASP) from Approov, for example, verifies trust on the device, thus mitigating threats as they evolve in real-time.

Approov continually secures the devices at runtime by managing the behavior of applications as they run (rather than looking at the software itself).

In addition, Approov continuously monitors the back-end APIs that apps interact with, as well as the network channel between the devices and back-end services running in the cloud.

Security admins and developers can also configure the level of RASP for specific applications. For example, it may be acceptable for some games to run on rooted or jailbroken phones – while a financial services app developer may want to block all modifications to the device environment.

The Intellyx Take

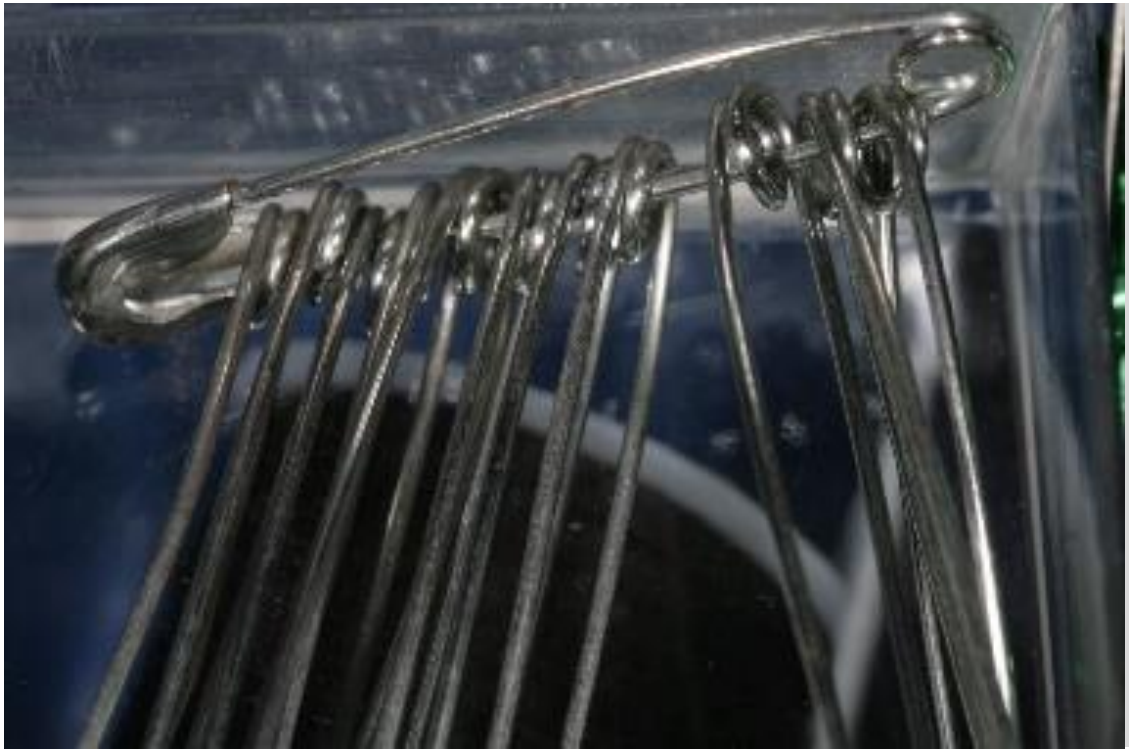
As with other parts of the cybersecurity landscape, mobile device security requires constant vigilance.

New threats appear daily, and the hacker community is always looking for new attacks to attempt. As a result, any mobile device protection must constantly be on the lookout for new threats, rolling out updates promptly as necessary.

It's also important to remember that mobile device attacks are constant, dynamic, and often ingenious. Hacking tools – and security tools that turn into hacking tools in the wrong hands – are plentiful and often free.

And for every 100 junior hackers satisfied with using existing tools to target known weaknesses, there is always one expert hacker crafting new, never-before-seen attacks.

Mobile device protection, therefore, must itself be constant, dynamic, and ingenious – and Approov fits the bill.



By Eric Newcomer

CTO & Principal Analyst
Intellyx

Dynamic Certificate Pinning for Secure Mobile Communication

Part 4 of the Securing Mobile Apps Series

A "man in the middle" (MitM) attack is one of the most serious types of attacks on the Internet. An MitM attack has the capability to divert or copy an entire flow of messages and steal login credentials, bank account numbers, credit card numbers, social security numbers, and generate denial of service attacks.

It's the main reason HTTPS is so widely used to securely encrypt HTTP traffic and help prevent such an attack.

The legacy of unsecure Internet traffic is why many people (such as my mother for example) still don't trust websites and mobile apps to keep their credit card and banking transactions safe.

Encrypting traffic using Transport Layer Security (TLS), as HTTPS does, prevents many MitM attacks, but of course cybercriminals are always upping their game and finding new ways to launch profitable MitM attacks.

Limitations of Encryption to Defeat MitM Attacks

TLS is the most popular encryption solution, standardized by the Internet Engineering Task Force (IETF).

TLS exchanges certificates between a client and server to set up a trusted connection and agree on specific encryption ciphers.

The client then uses a public key to encrypt the message before sending it to the server. The server uses a private key to decrypt the message. This solution works well to guard against basic MitM attacks because attackers can't easily decipher the encrypted messages.

But attackers have found ways to spoof certificates and steal keys. Furthermore, while HTTPS ensures that your data is encrypted, it can't validate that the communicating parties are actually both the client and server sides of your app.

As they say, however, when attackers find a new way to break in, a new solution is developed to prevent it. It's an arms race, but for every new threat there's a new protection following close behind.

Handling Mobile App Vulnerability to MitM

Mobile apps on Android and iOS primarily use HTTP just as websites do. And are therefore vulnerable to the same types of MitM attacks. And use HTTPS to help prevent them.

But mobile apps differ from web apps in some key ways. The operating system environments are different, the way apps are distributed is different, and the programming language code is often different.

Therefore, the environment in which mobile apps run benefits from additional protection against MitM attacks specific to mobile environments.

One such additional protection is certificate pinning for the public keys that encrypt the messages. The pinned certificate is loaded into the mobile application so the app can confirm that the server it communicates with is the correct one before sending data to it.

Certificate pinning also has a vulnerability, however, which is that certificates expire and older mobile apps, or mobile apps that are not kept up to date, may not work because they use expired certificates that the server won't recognize.

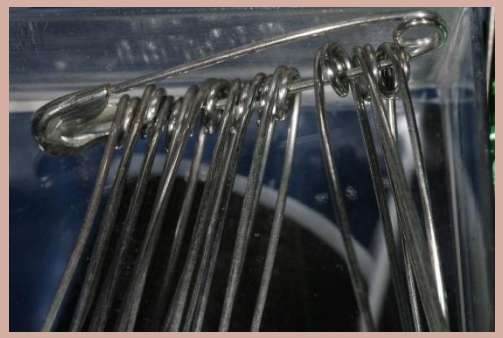
Dynamic Cert Pinning Solution

Dynamic certificate pinning solves the problem of certificates expiring, and also increases the protection level of the encryption since it makes it harder for an attacker to steal a key that might enable an MitM attack.

Dynamic certificate pinning updates allow the app to handle certificate changes without requiring a code update, and ensures a mobile app always connects to a trusted server whose certificate matches an up to date set of certificate codes.

Certificate pinning is easier to implement for mobile apps than for web apps because there is a secure channel through the app store for releasing the app code, including the certificate pinning configuration, making it a better solution for mobile apps.

Certificate pinning allows mobile applications to restrict communication only to servers with a valid certificate matching the expected pin value. The connection is terminated immediately if communication is attempted with any server that doesn't match the expected value.



Dynamic certificate pinning updates allow the app to handle certificate changes without requiring a code update, and ensures a mobile app always connects to a trusted server whose certificate matches an up to date set of certificate codes.

The pin is not usually a copy of the entire certificate, but typically a hash of the certificate, or some key identifying attributes of the certificate. The mobile app ships with the pin and will only connect if it sees the expected certificate.

Updating the pin information for dynamic pinning can be challenging, however. You have to get the pin information for every single pin that you want to include for every app domain the app talks to and dynamically load it into the app.

On top of that you have to handle the process of generating the exact format for the XML file that contains the pins for loading into the apps.

So even though there is now some solid platform support for dynamic pinning, the configuration part is tricky, especially if you're not familiar with certificate management.

That's why the mobile security vendor, Approov, has made available to the community a tool to take the hard work out of generating and maintaining dynamic cert pinning information.

The Intellyx Take

Distributed applications are vulnerable to MitM attacks, especially those using the public Internet, which is basically every mobile application.

MitM attacks have been successfully used to steal login credentials, bank account numbers, social security numbers, and to take over servers with denial-of-service attacks. You really don't want to deploy a mobile app that is vulnerable to MitM attacks.

Encrypting network traffic provides a basic protection against MitM attacks. But encryption techniques are not foolproof. The artifacts of encryption are vulnerable to theft – including encryption keys and the certificates used to establish trusted connections.

Dynamic certificate pinning addresses these additional challenges by storing and updating information in the mobile app that allows the app to know when it's communicating with a fake endpoint.

If you want to get started with static certificate pinning, though, the free Pinning Generator Tool from Approov makes it simple to generate and maintain pinning configurations to improve protection for your mobile apps. However, static certificate pinning is more challenging to set up and maintain, than dynamic.

About the Analysts

Jason Bloomberg is the founder and managing director of enterprise IT industry analysis firm Intellyx. He is a leading IT industry analyst, author, keynote speaker, and globally recognized expert on multiple disruptive trends in enterprise technology and digital transformation.

He is #14 on the *Top 50 Global Thought Leaders on Cloud Computing 2024* and #10 on the *Top 50 Global Thought Leaders on Mobility 2024*, both by Thinkers 360. He is a leading social amplifier in Onalytica's *Who's Who in Cloud?* for 2022 and a *Top 50 Agile Leaders of 2022* by Team leadersHum.

Mr. Bloomberg is the author or coauthor of five books, including *Low-Code for Dummies*, published in October 2019.

Eric Newcomer is CTO and Principal Analyst at Intellyx, a technology analysis firm focused on enterprise digital transformation. Eric is a well-known technology writer and industry thought leader, and previously held CTO roles at WSO2 and IONA Technologies, as well as Chief Security Architect and CISO roles at Citigroup and Credit Suisse.

About Intellyx

Intellyx is the first and only industry analysis, advisory, and training firm focused on customer-driven, technology-empowered digital transformation for the enterprise. Covering every angle of enterprise IT from mainframes to cloud, process automation to artificial intelligence, our broad focus across technologies allows business executives and IT professionals to connect the dots on disruptive trends. Read and learn more at https://intellyx.com or follow them on X at @intellyx.

About Approov

Approov is an essential component of mobile application security for major global organizations that serve millions of users annually. These organizations operate in various sectors, including eCommerce, financial services, healthcare, automotive, and gaming. Approov offers a comprehensive runtime security solution, known as RASP (Runtime Application Self-Protection), designed specifically for mobile apps and their APIs. This solution is unified across multiple platforms, including iOS, Android, and HarmonyOS.

Approov serves as a formidable defense, thwarting automated attacks and preventing the manipulation of mobile platforms by compromised or unauthorized apps. Its efficacy lies in its ability to block unauthorized access attempts originating from scripts, bots, and counterfeit or tampered apps.