



## Continuous discovery and analysis of your mobile applications

Organizations are increasingly using their mobile channels to connect with their customers and employees, promoting an incessant development of new mobile applications from different departments and business areas and with multiple software companies.

Therefore, it's normal that organizations don't have a full view of all their apps and versions, thus losing control of their mobile channel. This results in critical vulnerabilities and other breaches of security with the organization's apps, increasing their exposure to potential attacks.

mASAPP gives organizations a real and updated view of the security status of their full mobile channel, giving them back the control. It can automatically discover all the apps published in official and non-official markets that are somehow related with an organization, even the ones that the organization is unaware of.

mASAPP analyzes them in real time and continuously identifies new security risks, which makes them easier to correct.

## Discover and analyze all of your organization's apps automatically and non-stop, identifying security risks



### Discovery

An innovate proposal to autonomously discover applications.



### Vision

Continuously analyze and identify vulnerabilities and other security risks.



### Thoroughness

Non-stop in-depth analyses, including static, dynamic, library and backend testing.



### Precisión

Helps to identify and correct security breaches by delivering actionable information.



### Immediacy

Powerful Big Data engine to classify, search and analyze from millions of apps.

## Benefits

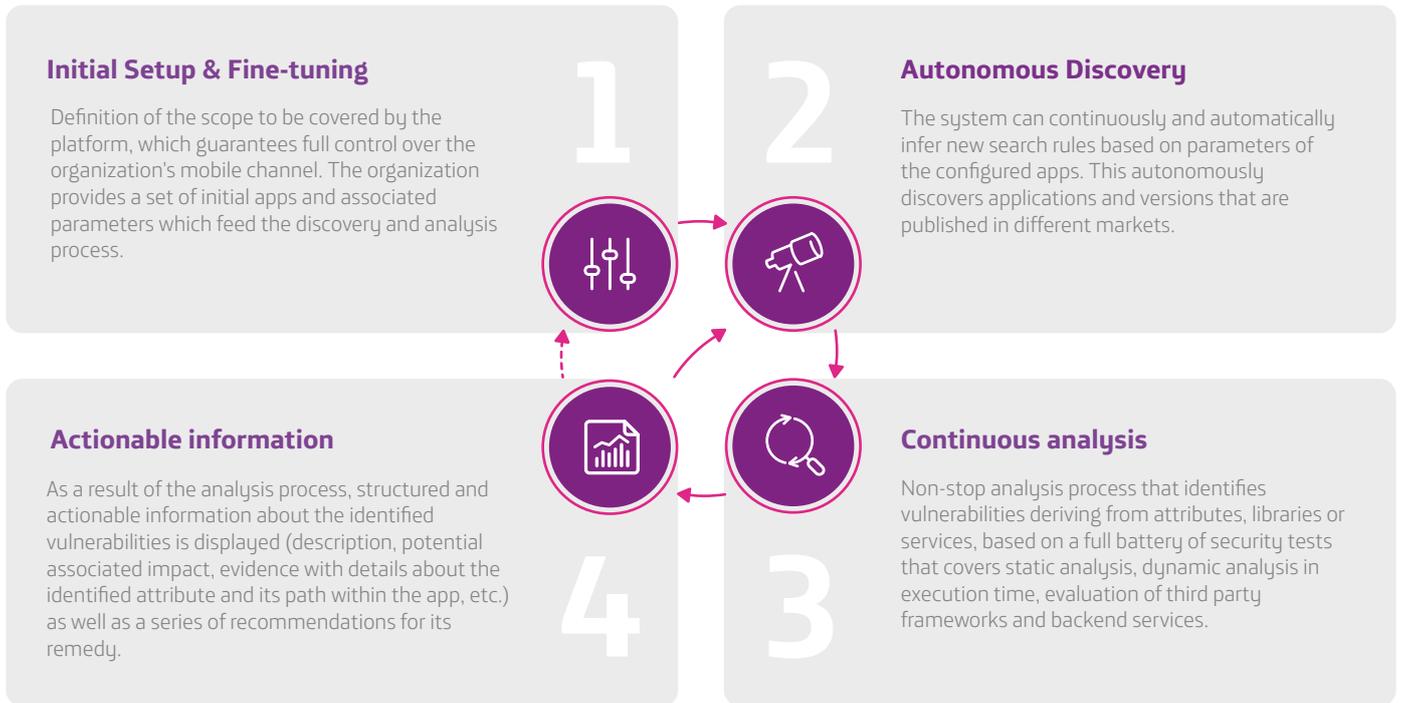
- **Comprehensive and centralized view** of the security status of all your published apps, continually identifying new vulnerabilities using non-stop security analyses.
- **Full control** over your mobile ecosystem thanks to the proactive discovery system and automatic identification of all your applications, including new versions of existing apps and those that have been taken off the market. Including those that the organization had forgotten about or was unaware of: Shadow App.
- **Traceability** over the lifecycle of your mobile apps. This simplifies the identification and monitoring of new vulnerabilities that could arise, making it easier to effectively remedy and correct them.
- **Accesible.** Does not require technical or source code knowledge to identify vulnerabilities in analyzed applications.

## Target group

- Organizations with a digital presence that need to regain control over their official mobile applications and require a solution that provides them with a continuous and updated view of their entire mobile channel.
- Entities whose customers and employees actively use the mobile channels activated by the organization and which need to continuously know the security risks of the apps.
- Organizations that implement an SDLC process and need to monitor their developed applications to identify future vulnerabilities that could arise over time.

## How it works

mASAPP provides visibility and control over your mobile channel based on a continuous lifecycle of discovery and analysis of applications, structured into four main phases.



## mASAPP within our value proposition

In order to adapt to the client's specific needs and requirements, mASAPP can be acquired as a module within the Vamps service, or within the "Risks on the mobile channel" solution from the CyberThreats service. Both services are managed and operated by Telefónica.



### Vamps

Provides an overview of the vulnerabilities to which the organization's assets are exposed, including mobile apps. It can be used to quickly manage their correction to reduce exposure time.



### CyberThreats

Provides visibility and context on the security status of your full mobile ecosystem, identifying security breaches in your apps, whilst detecting and removing third party applications aimed at somehow damaging your organization.