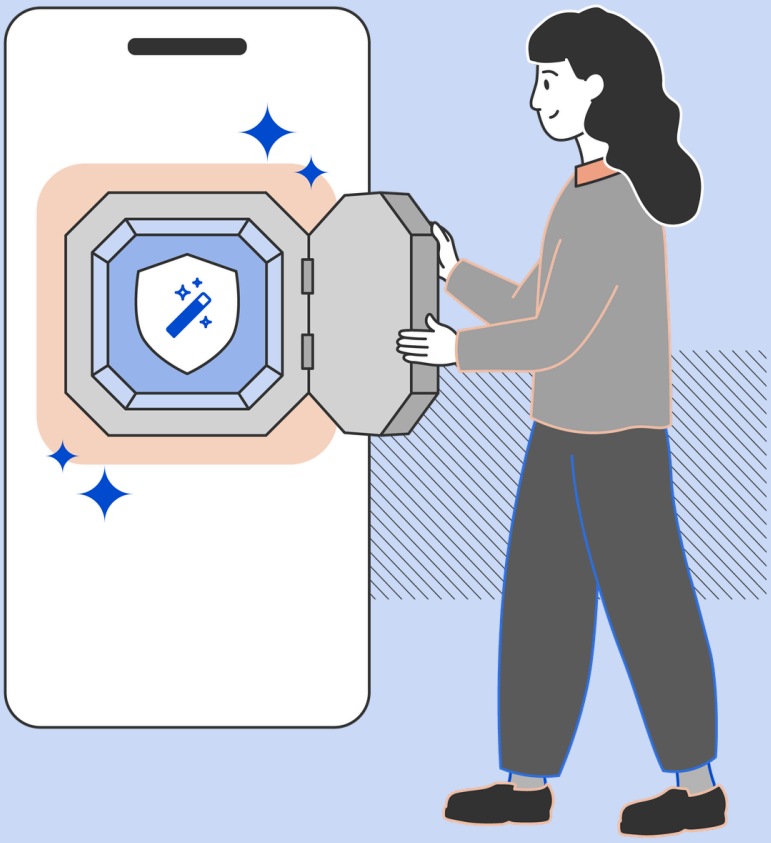
PROMON

Promon AI Protect™

Protect the AI model inside your app



Promon AI Protect™

Protect the AI model inside your app. Encrypted in the package. Bound to your app.

More mobile apps now ship AI models in the app package, such as classifiers that detect cheating, score fraud or recognize images. Left unprotected, the model sits in the APK as a plain file, under its own name. Anyone who unzips the package can copy it, study it or change it.

Promon AI Protect™ changes that.

An add-on for Promon Shield for Mobile™, it keeps the model encrypted in the package and bound to your app, alongside Shield's runtime protection.



What you can do with Promon AI Protect™

Remove the plain file

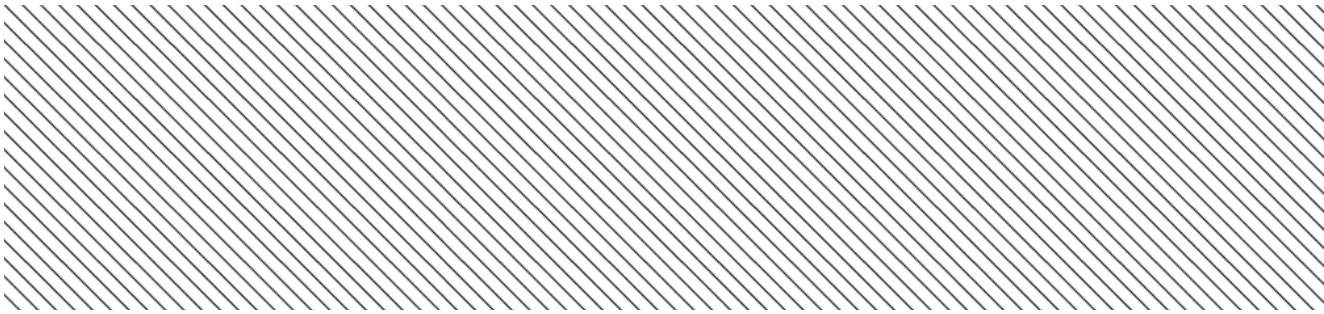
The model is encrypted and renamed, so it cannot be recognized in the package.

Bind the model to your app

The key is tied to your app's ID, so a copied file cannot be decrypted in another app. Everything is checked for tampering when the model loads.

Pair it with Shield

While the app runs, the model is decrypted in memory, where Shield for Mobile's runtime protection applies.



Protect the models worth extracting



Mobile games

Make it harder for cheat developers to extract your anti-cheat and bot-detection classifiers, study them, and tune their cheats and bots until nothing gets flagged.



Banking and fintech

Raise the cost for fraudsters who extract and reverse engineer your on-device fraud-scoring model to learn which signals to spoof.



Vision and audio features

Encrypt the models your team trained or fine-tuned, so a competitor who unzips your APK finds an encrypted file, not a model to clone into their own app.

The result?

Your model encrypted in the package, bound to your app, and protected by the vendor that already protects the rest of your app.

Requirements and integration

AI Protect fits Android apps that bundle and load their own TensorFlow Lite (LiteRT) models, up to about 100 MB. It requires Promon Shield for Mobile. Your developers make one small change to how the app loads the model, and Shielder or Integrator encrypts it in the build they already run. It does not protect large language models, stop prompt injection, or prevent model theft by querying the model.

How many copies of your AI model are out there?

One in every install of your app. Make sure each one is encrypted and bound to your app. **See Promon AI Protect™ in action today.**

Book a meeting »

PROMON

About Promon

Promon leads the way in proactive mobile app security. For 20 years, we've been making the world a safer place by securing any app, on any device—in no time at all. Today, we protect over 2 billion users, secure 13 billion monthly transactions, and safeguard $2.5 trillion in market cap. Promon is headquartered in Oslo, Norway, with offices in more than 15 countries around the world.

Would you like to talk to an expert?

Mobile app security is crucial to preserve and improve your business reputation. Request pricing or talk to an expert to learn more today.

Book a meeting »

Copyright 2026, Promon AS. All rights reserved. We reserve the right to introduce modifications without notice.