



# Mobile Application Protection Suite

**Build secure, compliant and fraud-resistant mobile apps for Indonesia**

zScan • zShield • zKeyBox • zDefend • zConsole — now hosted in an Indonesian data centre

**OJK & UU PDP ALIGNED**

**DATA RESIDENT IN INDONESIA**

**Presented by SecureCentral — Authorised Zimperium Partner, Asia Pacific**

Australia • New Zealand • Singapore • Malaysia • Indonesia



**Authorised APAC Partner**

Local pre-sales, deployment and first/second-line support in-region.

[info@securecentral.com.au](mailto:info@securecentral.com.au)

[www.securecentral.net](http://www.securecentral.net)

# What we will cover today

A 20-minute view of the mobile app risk, the platform, the proof and the next step

01

## The Indonesian mobile risk picture

Mobile-first banking, e-wallets and the fraud economy targeting them

02

## Zimperium MAPS platform

zScan, zShield, zKeyBox, zDefend and zConsole across the app lifecycle

03

## Data sovereignty for Indonesia

zConsole hosted in-country to meet OJK and UU PDP expectations

04

## Competitive battle card

Guardsquare, Appdome, V-Key, Promon, Build38, Digital.ai

05

## Customer proof

Global and regional organisations protecting apps with Zimperium

06

## Engagement with SecureCentral

PoV plan, commercial model and next steps

# A mobile-first economy — and a mobile-first target

Digital banking, e-wallets, lending and government services are delivered almost entirely through apps

## #1

channel for banking in Indonesia is the mobile app — branch and web are now secondary

## Android

dominates the installed base, with high sideloading and modified-APK exposure

## OJK

expects banks to manage IT risk end-to-end, including the customer-facing app

## UU PDP

No. 27/2022 imposes personal-data obligations with material penalties

## What attackers actually do to Indonesian apps

- **Repackaged / modded APKs** — cloned banking and e-wallet apps redistributed through unofficial stores and chat groups.
- **Banking trojans & overlays** — credential and OTP theft via accessibility abuse and screen overlays.
- **Rooted, emulated & hooked devices** — Frida, Magisk and emulator farms used for bonus abuse and account takeover.
- **Key extraction** — static keys and tokens lifted from the binary to forge transactions.
- **Social-engineering "APK kiriman"** — victims installed malicious APKs sent via WhatsApp disguised as invitations or invoices.

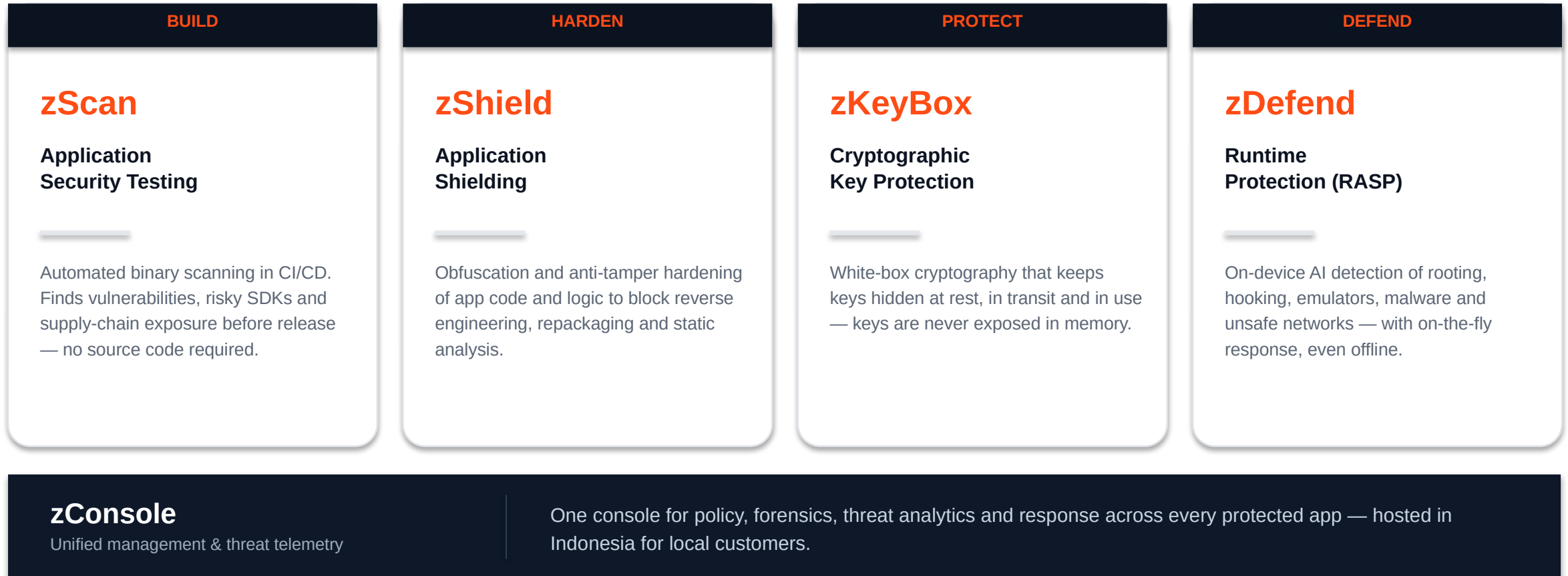
## The business impact

- ▶ Direct fraud loss and reimbursement cost
- ▶ Regulatory exposure with OJK and Bank Indonesia
- ▶ Brand and trust damage amplified on social media
- ▶ Engineering time lost to forensic investigation
- ▶ App-store takedowns and release delays

Threat patterns summarised from Zimperium zLabs public research and SecureCentral field experience in the region.

# Zimperium MAPS — protection across the app lifecycle

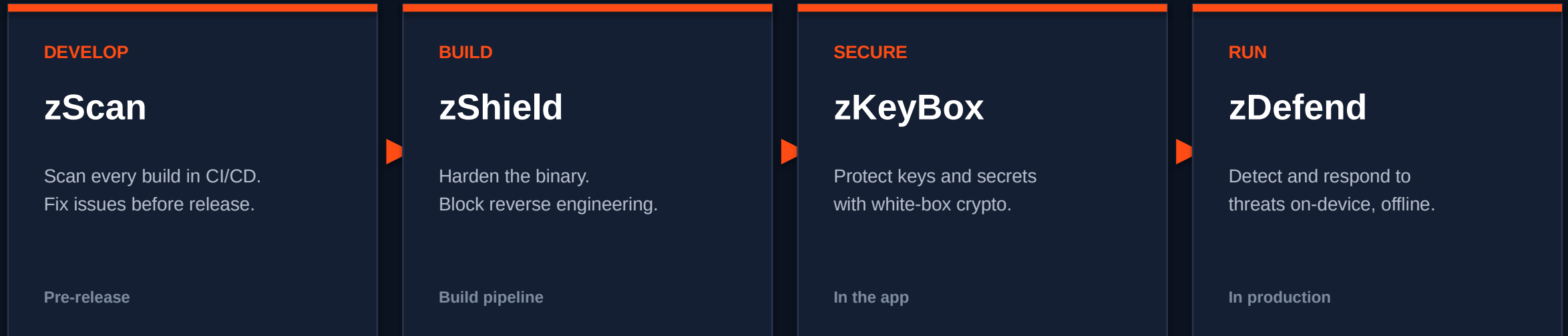
The only complete platform purpose-built to protect mobile apps from development through runtime



Source: [zimperium.com/maps](https://zimperium.com/maps) — product scope and descriptions as published by Zimperium.

# Shift left, stay protected at runtime

One platform, one console, one vendor — from the first build to every device in the field



## Fewer vulnerabilities shipped

Security testing runs on every build, not once a year before pentest.

## Fraud blocked at the edge

Compromised, hooked or emulated devices are detected before the transaction.

## Evidence for the regulator

Per-app forensics and threat telemetry in zConsole, retained in-country.

# What each module does — and the outcome it buys you

Modules are licensed individually or as the full suite; all report into a single zConsole

| Module   | Core capability                                                                                                | Typical Indonesian use case                                          | Outcome                            |
|----------|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|------------------------------------|
| zScan    | Automated binary & SBOM scanning, AI-assisted triage of third-party SDK risk                                   | Pre-release gate for mobile banking / e-wallet releases              | Release faster with fewer findings |
| zShield  | Code obfuscation, anti-debug, anti-tamper, integrity checks for iOS & Android                                  | Stop cloned and repackaged APKs circulating outside Play Store       | Repackaging made uneconomic        |
| zKeyBox  | White-box cryptography; keys protected at rest, in transit and in use                                          | Protect transaction signing keys, QRIS and payment credentials       | Keys survive a rooted device       |
| zDefend  | RASP SDK: root/jailbreak, hooking (Frida), emulator, malware, network & phishing detection, OTA policy updates | Block account takeover, bonus abuse and overlay trojans in real time | Fraud stopped before it posts      |
| zConsole | Unified policy, threat analytics, forensics, SIEM/SOAR integration                                             | In-country hosting for OJK data-residency expectations               | Auditable, local evidence trail    |

**Deployment note:**

zDefend integrates as an SDK (native and hybrid frameworks). zShield and zKeyBox apply at build time, so typical first integration is measured in days of developer effort, not months. SecureCentral provides the integration workshop locally.

# zConsole is now hosted in an Indonesian data centre

Addressing OJK expectations on electronic system and data placement for financial institutions



## Hosted in Indonesia

- **In-country zConsole** — the management console and its threat, forensic and policy data are hosted in an Indonesian data centre.
- **Data stays onshore** — app telemetry and threat events generated by Indonesian customers are processed and retained locally.
- **Built for OJK** — supports data-placement and electronic-system obligations that apply to banks, multifinance, insurers and fintech lenders.
- **Audit-ready** — local evidence, logs and reporting that can be produced for OJK, Bank Indonesia and internal audit.
- **Local latency** — faster console performance and response for Jakarta-based SOC and fraud teams.

## Regulatory drivers we map to

### POJK 11/POJK.03/2022

IT implementation by commercial banks — IT risk management, electronic system and data placement, third-party assurance.

### OJK & BI cyber-resilience guidance

Controls for digital banking and payment channels, including customer-facing application security.

### UU PDP No. 27/2022

Personal data protection obligations, breach notification and accountability for data controllers.

### PCI MPoC / PCI DSS

Where the app accepts card payments on COTS devices; MAPS is used in ready-to-use PCI MPoC packages.

Regulatory references are provided as context for discussion; customers should confirm applicability with their own compliance and legal teams. Hosting location confirmed with Zimperium and SecureCentral at time of writing.

# Zimperium MAPS vs the in-app protection field

Guardsquare • Appdome • V-Key • Promon • Build38 • Digital.ai — internal sales guidance



| Capability                        | Zimperium MAPS             | Guardsquare         | Appdome             | V-Key           | Promon              | Build38             |
|-----------------------------------|----------------------------|---------------------|---------------------|-----------------|---------------------|---------------------|
| App shielding / obfuscation       | Yes — zShield              | Yes — core strength | Yes — no-code build | Partial         | Yes — core strength | Yes                 |
| Runtime protection (RASP)         | Yes — zDefend, AI engine   | Yes — RASP checks   | Yes — policy driven | Yes — vOS focus | Yes                 | Yes                 |
| Security testing in CI/CD         | Yes — zScan binary + SBOM  | Limited             | Limited             | No              | No                  | Limited             |
| White-box key protection          | Yes — zKeyBox              | Partial             | Partial             | Yes — vKey core | Partial             | Partial             |
| Device-side threat intelligence   | Yes — zLabs + on-device ML | Rules-based         | Rules + signals     | Limited         | Limited             | Limited             |
| Unified console across modules    | Yes — zConsole             | Multiple consoles   | Yes                 | Yes             | Yes                 | Yes                 |
| MTD (device) from same vendor     | Yes — Zimperium MTD        | No                  | No                  | No              | No                  | No                  |
| Indonesia-hosted management plane | Yes — ID data centre       | Not offered locally | Not offered locally | Regional        | Not offered locally | Not offered locally |

Positioning in one line:

Point tools protect one stage of the lifecycle. MAPS covers testing, hardening, key protection and runtime in a single platform — and Zimperium is the only vendor in this set that also secures the device with MTD, giving Indonesian banks one supplier, one console and one support path.

Comparison reflects publicly available vendor positioning and SecureCentral field experience as at the date of this deck. Verify current vendor capability before external use.

# Head-to-head talk tracks

How to win the conversation when each competitor is in the deal

## Guardsquare

Their pitch: Strong obfuscation heritage (DexGuard / iXGuard).

**We say:** Hardening is only half the problem — a protected binary still runs on a rooted, hooked or malware-infected phone. MAPS adds on-device runtime detection with threat telemetry and OTA policy updates without an app-store release.

## Appdome

Their pitch: No-code build-time plug-ins, fast to adopt.

**We say:** Fast to switch on, but protection is applied as a build service. MAPS gives you an engineering-grade SDK, deep forensics per device and shared intelligence with Zimperium MTD — plus in-country hosting.

## V-Key

Their pitch: Regional presence; virtual secure element and key focus.

**We say:** Strong on keys, thinner on lifecycle. MAPS matches key protection with zKeyBox white-box crypto and adds CI/CD security testing, shielding and RASP in one console.

## Promon

Their pitch: SHIELD app hardening with good banking references.

**We say:** Overlaps on shielding; limited security testing and no device-side MTD story. MAPS consolidates four controls and a single evidence trail for OJK reporting.

## Build38

Their pitch: T.A.K platform, app shielding and trust services.

**We say:** Smaller research footprint. Zimperium zLabs publishes continuous mobile threat research that feeds the on-device engine — detection improves without you shipping a release.

## Digital.ai / others

Their pitch: App-protection within a broader DevOps suite.

**We say:** App protection is one line in a large portfolio. Zimperium is mobile-only, with a dedicated mobile research team and the deepest mobile telemetry set in the market.

# Trusted by financial institutions worldwide

Representative global enterprise customers of Zimperium's mobile security platform



## FINANCIAL SERVICES & PAYMENTS

Banks, card networks, wallets, brokers and insurers rely on Zimperium to protect mobile apps and devices.

Logos sourced from Zimperium's "Representative Global Enterprise Customers" sales material. Use only in Zimperium-approved contexts.

# Across every mobile-dependent industry

Automotive, manufacturing, technology, healthcare, energy, entertainment and professional services



## AUTOMOTIVE



## MANUFACTURING



## TECHNOLOGY



## HEALTHCARE & PHARMA



## ENERGY & UTILITIES

Zimperium protects more than 300 enterprise customers and public-sector organisations globally, including defence and government agencies.

Logos sourced from Zimperium's "Representative Global Enterprise Customers" sales material.

# Where MAPS is deployed in the Indonesian market

Named references are available under NDA through SecureCentral and Zimperium

## Tier-1 & digital banks

Mobile banking super-apps protecting transaction signing, OTP flows and account opening.

## E-wallets & QRIS payments

Wallet apps and QRIS acceptance apps defending against emulator farms and bonus abuse.

## Multifinance & P2P lending

Lending apps hardened against repackaging and identity fraud at onboarding.

## Insurance & health apps

Claims and policy apps protecting personal data under UU PDP.

## Government & public services

Citizen-facing identity and service apps requiring onshore telemetry.

## Retail, airlines & logistics

Loyalty, booking and driver apps protecting points, fares and route data.

## A note on Indonesian customer logos

Zimperium does not publish a named Indonesian customer list, and several local deployments are contractually confidential. Rather than show logos we cannot substantiate, this slide describes the segments in which MAPS is deployed locally. SecureCentral will supply approved Indonesian reference logos, case studies and reference calls on request — confirm the current approved list with Zimperium before any external use.

# Recognised leadership, measurable return

Independent analyst recognition and customer-reported outcomes



## Leader

SPARK Matrix™ In-App Protection Platform, 2026

## \$1.3M

fraud prevented in six months (customer reported)

## 95%

of malware fraud blocked in a banking deployment

## \$17.5M

total benefits in a logistics deployment

“Zimperium continues to solidify its position as a formidable Leader in the App Protection Platform market ... giving enterprises everything they need to build secure, compliant, and fraud-resistant mobile apps.”  
**SPARK Matrix™: In-App Protection Platform, 2026**

“Mobile applications face distinct threats — such as device loss/theft or on-device malware — that differ from those targeting web applications.”  
**Gartner, How to Avoid Common Cybersecurity Pitfalls in Mobile App Development**

### Mobile-only focus

Zimperium does nothing else. zLabs research feeds the detection engine continuously.

### On-device AI detection

Works offline, no cloud round-trip, no user data leaving the handset.

### Apps and devices

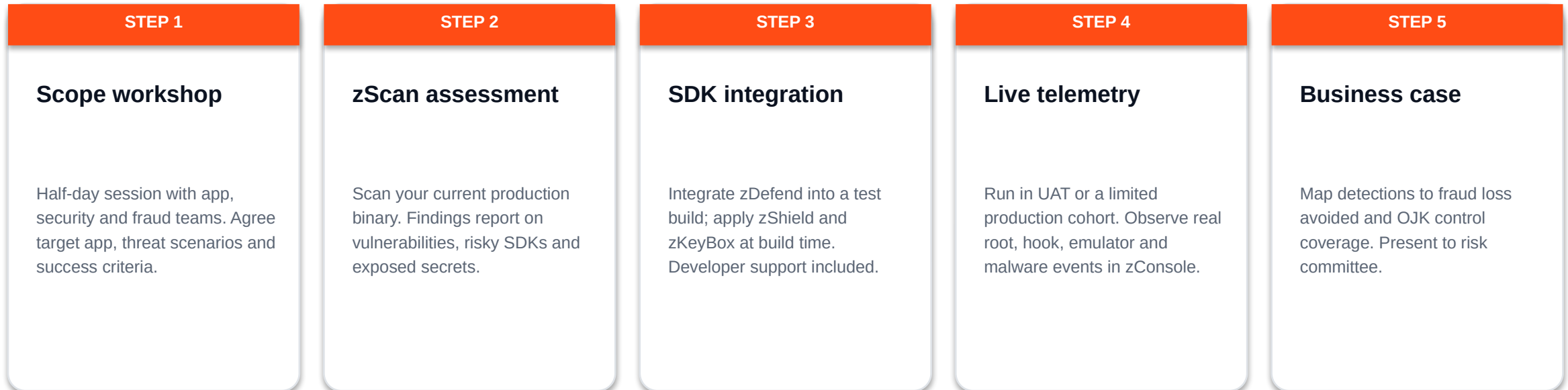
MAPS plus MTD from one vendor — the full mobile attack surface.

### Local delivery

SecureCentral provides Indonesian pre-sales, integration and support.

# A proof of value you can run on your own app

SecureCentral runs the evaluation locally, in Bahasa Indonesia and English



## What you get at the end

A findings report on your real app, live threat telemetry from your real users, and a costed proposal — with licensing, integration effort and local support all quoted by SecureCentral.

## Commercial model

Annual subscription per protected app, by module. Bundle pricing for the full suite and for MAPS + MTD. Local invoicing and IDR options available through SecureCentral's Indonesian reseller network.



# Secure every app. On Indonesian terms.

- ▶ Complete lifecycle protection — test, shield, protect keys, defend at runtime
- ▶ zConsole hosted in an Indonesian data centre for OJK-aligned data residency
- ▶ One vendor for apps and devices, delivered and supported locally

[BOOK A SCOPE WORKSHOP](#)

[REQUEST A zSCAN](#)



**Authorised Zimperium Partner — Asia Pacific**

## Talk to us

[info@securecentral.com.au](mailto:info@securecentral.com.au)

[sales@securecentral.com.au](mailto:sales@securecentral.com.au)

+61 (2) 8004 5099

[www.securecentral.net](http://www.securecentral.net)

Australia • New Zealand • Singapore  
Malaysia • Indonesia