ARMMADA

ZIMPERIUM®

Mobile Application Protection Suite (MAPS)

Aplikasi Mobile adalah Aset Utama—Sudahkah Aman dari Ancaman Siber?

Di era digital, perusahaan FSI seperti bank, fintech, asuransi, dan penyedia dompet digital menjadikan aplikasi mobile sebagai jalur utama layanan dan transaksi.

Ketergantungan ini membuat aplikasi semakin rentan menjadi target serangan siber, dan tanpa perlindungan yang kuat, risikonya dapat merugikan perusahaan maupun nasabah.

Risiko Nyata yang Mengintai Aplikasi Mobile

Dengan data sensitif dan transaksi besar yang diproses setiap hari, aplikasi mobile di sektor finansial menjadi sangat rentan dieksploitasi oleh pelaku siber. Teknik serangan yang harus diwaspadai meliputi:

- Reverse engineering — membongkar kode untuk mencari celah atau memanipulasi fitur
- Overlay attack — aplikasi palsu yang menutupi aplikasi asli untuk mencuri kredensial
- Cloning — pemalsuan aplikasi dan distribusi bajakan yang telah dimodifikasi
- Emulasi dan rooting/jailbreak — memungkinkan aplikasi berjalan di lingkungan tidak aman
- Runtime hooking dan injection — memodifikasi perilaku aplikasi saat dijalankan

Regulasi Semakin Ketat, Keamanan Aplikasi Harus Siap

MAPS siap membantu perusahaan memenuhi standar keamanan global seperti OWASP MASVS, GDPR, PSD2, serta regulasi lokal di sektor finansial. Seiring meningkatnya pengawasan dari otoritas seperti OJK, Bank Indonesia, dan regulator global lainnya, penguatan kontrol keamanan pada aplikasi mobile kini menjadi hal yang wajib untuk:

- Menjaga kerahasiaan, integritas, dan ketersediaan data nasabah
- Mencegah fraud dan akses yang tidak sah
- Memastikan transparansi dan kemudahan audit

Perlindungan Aplikasi = Investasi pada Reputasi

Satu insiden keamanan dapat membuat kepercayaan nasabah runtuh. Dampaknya bukan hanya pada reputasi brand, tapi juga pada loyalitas pelanggan dan potensi sanksi hukum. Dengan perlindungan menyeluruh dari MAPS — sebelum, saat, dan setelah aplikasi digunakan oleh pengguna akhir, risiko terhadap reputasi dan kepercayaan dapat ditekan sejak awal.

Zimperium is proudly distributed by PT Global Infotech Solution
Prince Center Building, 11th Floor, Jl Jenderal Sudirman Kav 3-4
Jakarta Pusat DKI Jakarta, Indonesia 10220
www.global-infotech.co.id / www.armmada.co.id

Email: info@armmada.co.id

infotech

ARMMADA

ZIMPERIUM®

Zimperium: Proteksi Menyeluruh untuk Aplikasi Mobile

Satu platform. Empat lapisan proteksi.

Semua terintegrasi untuk mendukung praktik DevSecOps secara end-to-end. Apa saja yang dilindungi oleh Zimperium MAPS?

- **zScan** – Analisis keamanan kode sejak tahap pengembangan
- **zShield** – Hardening dan obfuscation untuk cegah rekayasa balik dan pembajakan
- **zKeyBox** – Keamanan aset kriptografi dalam aplikasi
- **zDefend** – Proteksi real-time saat aplikasi dijalankan (RASP)

Teknologi On-Device Machine Learning

Zimperium tidak bergantung pada cloud untuk deteksi ancaman—semua analisis dilakukan langsung di perangkat, dengan akurasi tinggi dan respons real-time.

Cocok untuk lingkungan yang membutuhkan low latency, privasi tinggi, dan tidak selalu online.

Dipilih dan Dipercaya oleh Lembaga Keuangan Global dan Lokal

Kepercayaan institusi di berbagai negara membuktikan keandalan Zimperium dalam melindungi aplikasi mobile di industri finansial.
Zimperium telah digunakan oleh:

- Bank besar di Indonesia, Singapura, dan Malaysia
- Fintech unicorn dan perusahaan asuransi digital
- Organisasi dengan regulasi ketat di sektor publik dan militer

Zimperium MAPS memberikan proteksi yang tertanam langsung di dalam aplikasi ("baked into the app") melalui SDK, bukan sekadar ditempel dari luar seperti jaket tambahan (metode wrapping). Metode Integrasi ini membuat perlindungan menjadi jauh lebih kuat, ringan, dan tidak mengganggu pengalaman pengguna. Sangat ideal untuk aplikasi publik atau B2C yang memiliki kebutuhan keamanan tinggi dan tidak boleh kompromi terhadap performa. SDK memberikan feedback real-time dan kontrol granular (misalnya memblokir aksi tertentu jika mendeteksi ancaman)

---

ecovadis · KAN Komite Akreditasi Nasional LSSM-075-IDN · IAS IAF ISO 27001:2022 · QACS IAF IAS ISO 20000-1:2018

infotech