Mobil Uygulamalarınızı Tamamen Koruyun!

EndCrypt Nedir?

EndCrypt, mobil uygulamalarını kolayca kendi kendini koruyan bir uygulamaya dönüştürebilen beyaz kutu (White box) teknolojisi tabanlı bir mobil uygulama güvenlik çözümüdür. Ağ veya işletim sistemi yerine doğrudan uygulamaya entegre edilmiş kullanıma hazır bir SDK'dır (yazılım geliştirme kiti).

EndCrypt yalnızca uygulamaları dinamik olarak korumakla kalmaz, aynı zamanda sıfırıncı gün ve diğer geniş kapsamlı siber saldırıları (kötü amaçlı yazılım, veri sızıntısı, izinsiz giriş, kurcalama, tersine mühendislik vb.) algılar ve bu tür siber saldırılar için aksiyon alır.

Yönetim ve HSM Entegrasyon yetenekleriyle birlikte EndCrypt, yeni bir bakış açısı getirerek pazarda kendini benzerlerinden farklı, mobil uygulama sahiplerine katma değeri yüksek bir siber güvenlik çözümü olarak tasarlanmıştır. HSM ile entegre uygulama içi güvenlik çözümleri, uygulamaların her zamankinden daha güvenli çalışmasını sağlamaktadır.

In-App-Security kategorisinde yer alan EndCrypt, gelişmiş yeteneklerinin yanısıra dijital güvenlik alanında da getidrdiği yeniliklerle öncü olmayı hedeflemiştir.

Koruma
(Sıkılaştırma Yetenekleri)

- Kod Gizleme (Code Obfuscation)
- Beyaz-Kutu Kriptografi (White-box Cryptography)
- Kaynak Şifreleme (Resource Encryption)
- Cihaz-Uygulama Bağlanması (Device App Binding)
- Tersine Mühendislik (Reverse Engineering)
- Çok Faktörlü Kimlik Doğrulama (Multifactor Authentication)
- Ortadaki Adam Man-in-the-middle (MITM)
- Çalışma Süresi Boyunca Uygulamanın Kendini Koruması (Runtime App Self Protection)
- Clickjacking Koruması
- Kod Enjekte Edilmesi Saldırıları (Code Injection)

Tespit
(Kurcalamaya Karşı Koruma Yetenekleri)

- Emulasyon Tespiti (Emulation Detection)
- Hata Ayıklama Tespiti (Debugging Detection)
- Ayrıcalık Yükseltme Tespiti (Privilege Escalation Detection)
- Jailbreak / Root Detection
  İz Kaydı Toplama (Fingerprinting)
- Repackaging Tespiti (Repackaging Detection)
- Cihazın Klonlanması (Cloning of The Device)
- Kurcalamaya Karşı Koruma (Anti-tampering)
- Kancalama Tespiti (Hook Detection)
- Overlay Tespiti (Overlay Detection)
- Anti-bot

Aksiyon
(Proaktif Tepki Yetenekleri)

- Ekran Görüntüsü Almayı Engelleme Kontrolü (Anti-screenshot Check)
- Bütünlük Kontrolleri (Integrity Checks)
- Keylogging Engelleme (Anti-keylogging)
- Risk Analizi / Atak Telemetrisi (Risk Analysis / Attack Telemetry)

Yönetim ve Katma Değerleri

- HSM Entegrasyonu ile güvenliğin donanımsal seviyeye taşınabilmesi
- Güvenli Anahtar Saklama
- Güvenli Kanal
- Hassas Veri Güvenliği Onay ve İzleme (Attestation And Monitoring)
- Kurulum Sertifika Kontrolü
- Şifrelenmiş Veritabanı
- Kaynak Kurulum Kontrolü
- Güvenli Kütüphanelerin Kullanımı
- Anahtar Yönetim Sistemi