企業級資安解決方案

GSS IT & Security

Info Security Products Guide 2020 GLOBAL EXCELLENCE GOLD ★★★★★ Info Security Products Guide

finalist 2019 SC Awards Finalist

GOLD THE GOLDEN BRIDGE AWARDS BEST 2018 BUSINESS WORLD 2018 Golden Bridge Award

FIPS VALIDATED 140-2 FIPS 140–2

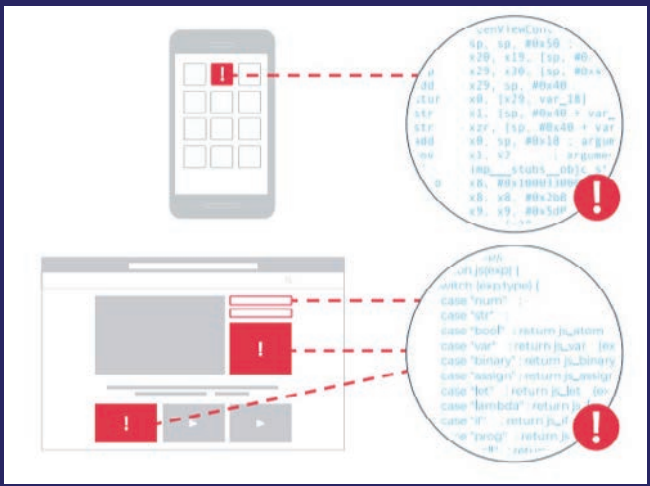
ARXAN

應用程式防護領導品牌

04

Arxan for APP

手機應用程式 (APP) 的使用率在各行各業中持續成長，同時也提供了攻擊者更多元的攻擊方式。使用者皆可以在應用程式商店取得應用程式，並於危險的環境中執行。如今，駭客廣泛利用這種傳播環境，並將其攻擊擴展到行動應用程式上，通過竊取使用者身份、智財權或通過存取後台系統來獲取利益。從 Accenture Consulting 公司近期發布的報告顯示，超過 60% 的行動銀行應用程式恐遭逆向工程攻擊。

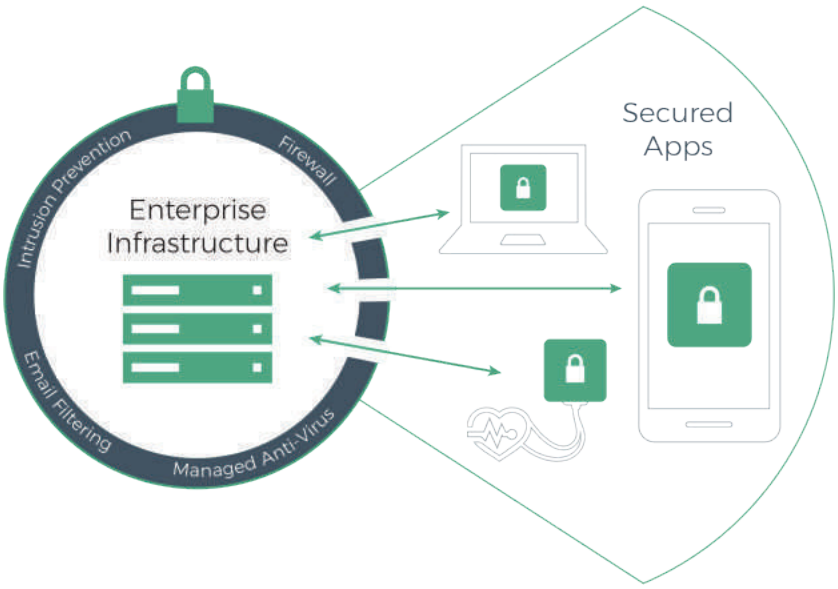


駭客通常由逆向工程進行攻擊，反組譯後可取得應用程式關鍵演算法、金鑰、API 存取權限及敏感資料，並瞭解如何篡改程式。為了應對這些威脅，必須對應用程式進行防護，以確保應用程式安全。

應用程式原始碼防護

Arxan Code Protection 採用數十種專利防護技術 (Guards) 來強化應用程式，可彈性調整細部的防護機制，以兼顧應用程式之效能及安全性。

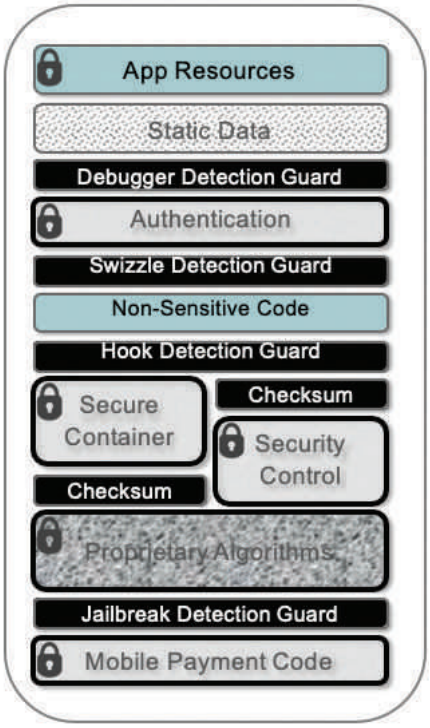
Arxan 所提供的 Guards 分為靜態及動態防護，靜態防護如混淆及字串加密等。動態防護如 Root/Jailbreak、模擬器偵測及防篡改等。防護方式簡單快速，只需將所有的 Guards 撰寫設計於防護文件 (GuardSpec) 中，並將原先的 APK 及 IPA 與 GuardSpec 一同建置後即完成防護，過程中不需要修改任何一行程式碼，而且防護可以在幾分鐘內完成。Arxan 的防護方式對於軟體開發生命週期的影響很小，並且可以快速地整合到 DevSecOps 流程中。整合後，每次的建置會自動套用 GuardSpec-- 無需花費額外的人力即可持續確保應用程式的安全性。



結合 Arxan Threat Analytics(威脅分析平台) 模組，一旦部署完畢，就可以在短期內利用防禦策略處理已識別的威脅，例如：鎖定帳戶存取、禁用應用功能。長期的修正方法可以包括通過程式碼、資料和金鑰加密來加強保護，以便對特定的威脅進行補救。

Arxan 金鑰與資料防護

Arxan 白箱加密技術可以通過混淆和加密來隱藏重要的金鑰，透過靜態和動態金鑰來防護敏感資料。Arxan 支援所有主要的加密演算法，只需微調部分的程式碼調整即可確保金鑰的安全性。



Arxan for Android 特色

- 防護方式簡單快速，並能整合到 DevSecOps 流程中。
- 針對應用程式防護，無需修改程式碼。
- 針對靜態攻擊時，提供多種靜態防護 Guards，例如：混淆及字串加密等防護機制，可避免應用程式遭受逆向工程攻擊。
- 針對動態攻擊時，提供多種動態防護 Guards，例如：Root、模擬器偵測及防篡改等防護機制，可避免應用程式於不安全環境下運行。
- 可整合 Arxan Threat Analytics(威脅分析平台)，提供即時威脅分析和攻擊預警，同時也可整合至 SIEM。

零信任是一個概念，其核心組織不應該信任其周邊內外的任何內容，而是在授予存取權限之前驗證任何嘗試連接到系統的內容

Arxan for iOS 特色

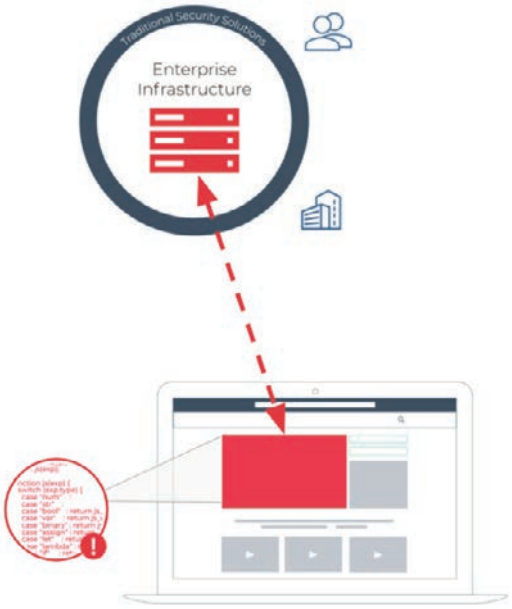
- 防護方式簡單快速，並能整合到 DevSecOps 流程中。
- 針對應用程式防護，無需修改程式碼。
- 針對靜態攻擊時，提供多種靜態防護 Guards，例如：混淆及字串加密等防護機制，可避免應用程式遭受逆向工程攻擊。
- 針對動態攻擊時，提供多種動態防護 Guards，例如：Jailbreak、模擬器偵測及防篡改等防護機制，可避免應用程式於不安全環境下運行或遭到攻擊。
- 可整合 Arxan Threat Analytics(威脅分析平台)，提供即時威脅分析和攻擊預警，同時也可整合至 SIEM。

Arxan for Web

目前估計約有 95%的網站是使用 JavaScript 語言進行開發。JavaScript 可透過在 Client 端瀏覽器進行部分驗證計算方式，以達到有效提高效能並增加使用者體驗。即使 JavaScript 帶來諸多優點的同時，也存在一個致命的問題：程式碼安全性。

JavaScript 安全性問題

JavaScript 為直譯式之程式語言，若無針對程式碼進行保護，很容易遭攻擊者攔截和分析。攻擊者可透過未防護的程式碼來竊取憑證並攻擊後台系統。使用 JavaScript 的應用程式很容易受到靜態應用程式分析（閱讀明確的應用程式程式碼）和動態應用程式分析（使用偵錯程式來追蹤程式碼的運行方式）。一旦了解與後台溝通的程式邏輯，駭客就可以以此找尋驗證的弱點或以非法存取後台系統的方式進行攻擊。為了保護整個 IT 系統，企業還需要保護客戶端 Web 應用程式並防止它們成為攻擊媒介。



從安全角度來看，應將客戶端瀏覽器中的所有程式碼視為在零信任環境中運行，並應採取安全措施來保護敏感資料及重要程式邏輯。例如：當應用程式被逆向工程時，資料存取方法使用 API（例如：支付表單或憑證驗證）則易於暴露。這些攻擊可能暴露客戶資料並洩露後端資料。

透過觀察 Web 應用程式與後台系統間的互動資訊，衍生出其他形式的攻擊。其中最值得注意的是有針對性的惡意程式碼攻擊，例如：竊取憑證的 Man-in-the-Browser（MitB）惡意軟體。攻擊者可依據使用者輸入內容以及驗證資訊，客製化設計相對應的惡意軟體，以竊取用戶憑證並存取其帳戶。

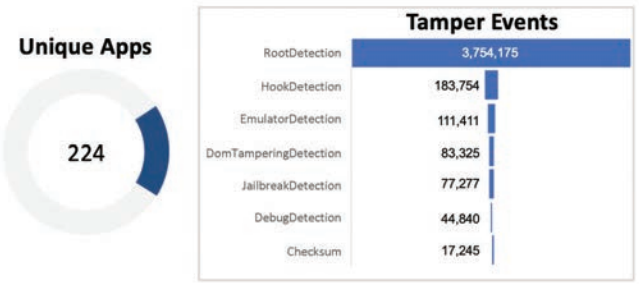
Arxan for Web 特色

- 針對靜態攻擊時，提供多種靜態防護 Guards，例如：混淆及字串加密等防護機制，可避免應用程式遭受逆向工程攻擊。
- 針對動態攻擊時，提供多種動態防護 Guards，例如：debug 模式偵測及防篡改等防護機制，可避免於不安全環境下運行或遭到攻擊。
- 即時警報，程式被嘗試分析甚至篡改時，通知企業並立即執行反應動作，如關閉攻擊者帳戶或更新程式碼來進行保護
- 針對應用程式防護，無需修改程式碼
- 可整合 Arxan Threat Analytics(威脅分析平台) 提供的即時威脅檢測和攻擊預警，可自行串接 SIEM 工具。

Arxan Threat Analytics

保護應用程式極為重要

保護應用程式的需求逐漸提升，尤其是對於網路銀行、支付、電子商務、醫療裝置、娛樂和遊戲等產業。保護公司應用程式之商業邏輯和客戶資料，可有效防止品牌受損、財務損失、智慧財產權盜竊和政府罰款。然而，應用程式商店及電子商務網站所提供超過四百萬款的應用程式中，大部分的 APP 沒有因應逆向工程威脅進行防護，並且無法警告企業其 APP 遭受攻擊的能力。

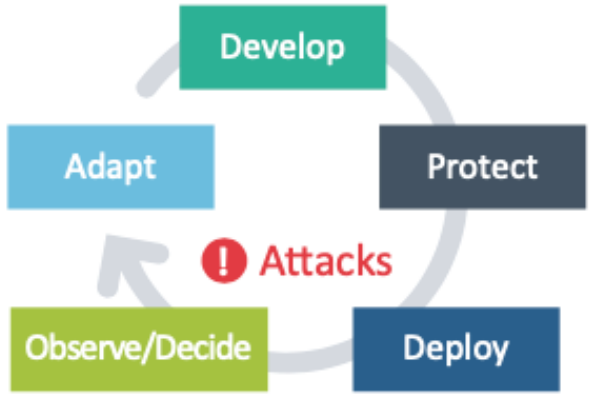


傳統開發所面臨的挑戰

為了防止惡意攻擊者，企業需要的關鍵是掌握應用程式攻擊如何發起、何時發起以及從何處發起。完美的程式以及傳統軟體的保護方式皆無法有效的防範惡意的攻擊者。傳統的應用程式保護方案，開發者無法了解應用程式發佈後所面臨的威脅。由於保護強度不足且無法在發生攻擊時警示企業，讓攻擊者有機可乘。目前，企業僅能在損害造成之後應對。

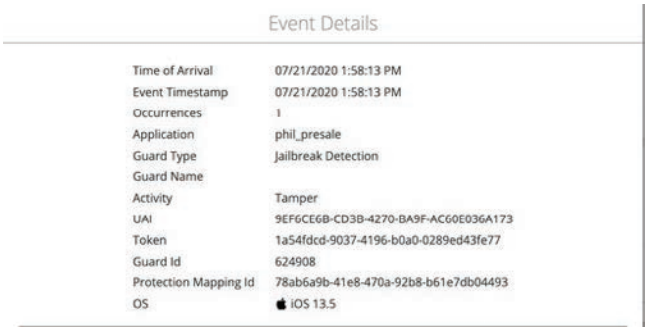
因應挑戰而生的解決方案

Threat Analytics 是 Arxan 提出的威脅分析解決方案，可整合其他 Arxan 的防護產品，並提升能見度，藉由威脅分析，可以掌握駭客攻擊方式及位置，同時針對這些攻擊可以再補強防護機制。Threat Analytics 可即時向客戶提供風險資料，使其能夠採取適當措施。



企業可以在應用程式發佈後即時提供攻擊資訊。當遭遇攻擊進行時，能提供應用程式所遭受攻擊的資訊，並警示以便企業採取應對機制。Threat Analytics 所提供的威脅告警，可以協助企業自行驗證防護強度是否需要進行調整，如以下問題：

- 我的應用程式防護是否足夠？
- 何時應針對已知威脅更新應用程式？
- 是否可識別不良行為者並採取適當措施以保護企業？



提供關鍵威脅情報

- **即時且可行動化的資訊 –** 檢視應用程式安全性以瞭解應用程式執行狀態以及遭受攻擊的時間
- **透過驗證建立信心度 –** 在應用程式發佈後提供運作報告以瞭解其所在的威脅環境
- **安全報告 –** 保護資料之安全性，可透過瀏覽器存取並且容易與 SIEM 和 BI 平台整合
- **掌握威脅趨勢 –** 透過數十億個受 Arxan 保護的應用程式中所蒐集的資料，可以即時掌握攻擊趨勢

Arxan Threat Analytics 整合

Arxan for Android 或 iOS

Arxan 可有效為行動應用程式提供高效的防護。可以將保護整合至開發後程式碼中，並與現今的快速開發環境相容。Arxan 應用程式保護可阻止攻擊並在裝置遭入侵和發生攻擊時發出警報。

Arxan for Web

Arxan for Web 提供快速且安全的防護，防護 JavaScript 和網頁程式碼，防止竄改並發出攻擊警報以阻止用戶端威脅，以免它們被用來取得客戶憑證和重要的資產。

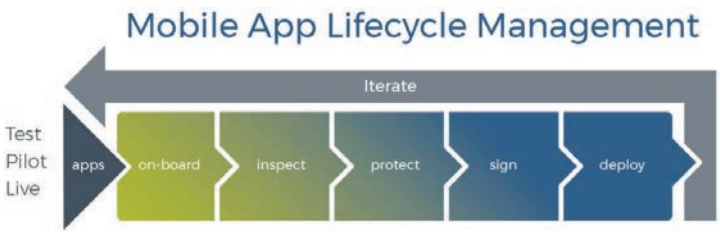
除了基本的應用程式防護，應用程式部署管理也是非常重要的。應用程式部署皆需納入安全性、分析和管理策略三大面向。Apperian 提供企業建立以企業商標為名的應用程式商店，向用戶提供經過審查的應用程式，達成最大限度地掌控應用程式分配情況及使用者採用率。

Apperian 增強功能允許 IT 團隊實施權限管理以達成有制度的應用程式級別管理、應用程式使用率分析、應用程式層級 VPN、撤銷應用程式、禁用複製 / 貼上、Jailbreak 檢測等。

Apperian 應用程式管理

為了簡化業務營運，企業內部使用的應用程式 (APP) 在員工、承包商和合作夥伴的非託管設備上運行。企業部署不安全的應用程式與在不信任環境中運行應用程式一樣，對企業構成重大的威脅。

這種威脅，導致應用程式管理困難，難以去尋找有效且安全部署行動應用程式的方法。為解決此問題，企業需要採用三階段應用程式管理方法。



About Arxan Technologies

Arxan 是全球值得信賴的領導者，提供業界最全面的應用程式保護解決方案，與找尋保護應用程式以及為擴展企業安全部署應用程式的組織合作。 Arxan 目前在許多行業有著保護超過 10 億個應用程式實例，包括金融服務、行動支付、醫療保健、汽車、遊戲和娛樂。 該公司成立於 2001 年，總部位於北美，在中東和非洲和亞太地區設有全球辦事處。欲了解更多訊息，歡迎至 www.arxan.com 或在 Twitter 上關注 @Arxan。

GSS IT & Security

ARXAN　Checkmarx　WhiteSource　kryptowire

imperva　digital.ai　AVC Application Vulnerability Correlation　APPERIAN MOBILE APP MANAGEMENT

資安服務

GSS Galaxy Software Services 叡揚資訊

國家產業創新獎
卓越中堅企業獎

成立於 1987 年，是台灣資訊軟體業的領導廠商，於應用系統開發已有 30 多年經驗，以改善資訊安全、提高企業效能為使命，全方位引進國際前瞻領導性知名品牌產品，致力為各大企業及組織提供資訊安全解決方案、IT 效能管理軟體並提供專業技術、顧問及整合服務，優質服務累積廣大的客戶群，包含醫療業、政府國營事業、金融業、壽險業、電信業、交通運輸業、製造業、高科技業等等。未來也將持續引進國際頂尖資訊及技術，協助客戶完成數位轉型、堅守資訊安全防線，期許透過卓越的軟體與服務，帶領客戶透過 IT 創新提升企業產能及核心競爭力。

服務範圍

行動應用安全保護、源碼檢測服務、第三方元件檢測及管理、APP 黑箱檢測、工具使用建置及建議、SSDLC 整合、軟體 Coding 安全課程等，協助客戶提升應用系統安全強度，建立堅強資安防線。

台北總公司　10461台北市中山區德惠街9號5樓　Tel: +886-2-2586-7890
高雄辦公室　80453高雄市鼓山區明華路317號6樓　Tel: +886-7-5866195
www.gss.com.tw