ARXAN

應用程式防護領導者

04

在零信任環境中保護商業應用程式、保護客戶、商業和智慧財產資料的需求比以往任何時候都更大，並且應該成為每個企業的應用程式開發和部署策略的核心。保護應用程式和資料免受攻擊是防止品牌破壞、財務損失、智慧財產權盜竊和政府罰款的關鍵；傳統的網路安全是在防火牆或防火牆之後提供保護，但它們在對抗應用層的攻擊方面無效。

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。

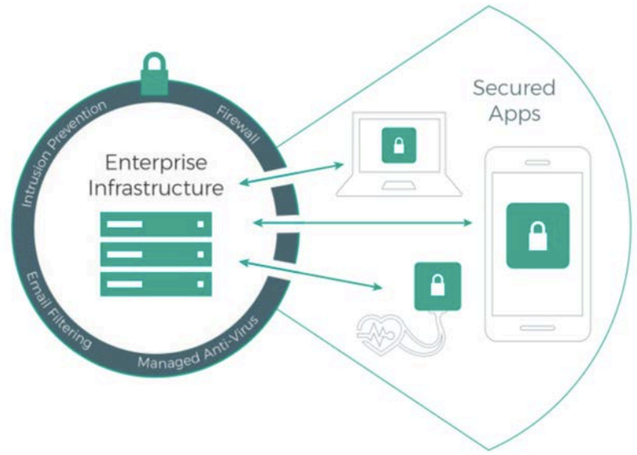
About Arxan Technologies

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，與尋找保護應用程式以及為擴展企業安全部署和管理業務關鍵型應用程式的組織合作。Arxan 目前在許多行業有著保護超過 20 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。

消費者的應用程式

與末端客戶直接互動，對於許多行業至關重要，如行動銀行、行動支付、連接醫療設備、娛樂和遊戲。只要公司的應用程式可以在”野生環境”存取，也就是直接下載或透過公開的應用程式商店，就可能遭受攻擊。應用程式是有價值的目標，因為它們擔任企業基礎架構的存取點。不良人士透過逆向工程來了解未受保護的應用程式程式碼。一旦程式碼被理解，不良人士可以插入惡意程式碼來竊取個人身份訊息（PII）和智慧財產權（IP），或透過暴露的密鑰及用於進行商業交易的 API 來攻擊企業。



Arxan 程式碼保護

專利的防護技術強化應用程式：使用專屬配置的防護網路方法可提供防篡改及自我修復措施，以實現執行期（Runtime）的應用程式自我保護安全（“RASP”）。

Arxan 威脅分析

提供獨特、即時可見的應用程式受攻擊資訊，如地點、時間以及攻擊的方式。威脅分析使企業能夠主動在攻擊完成或變得普遍之前，採取修正措施來應對應用程式攻擊與風險。

Arxan 白箱加密

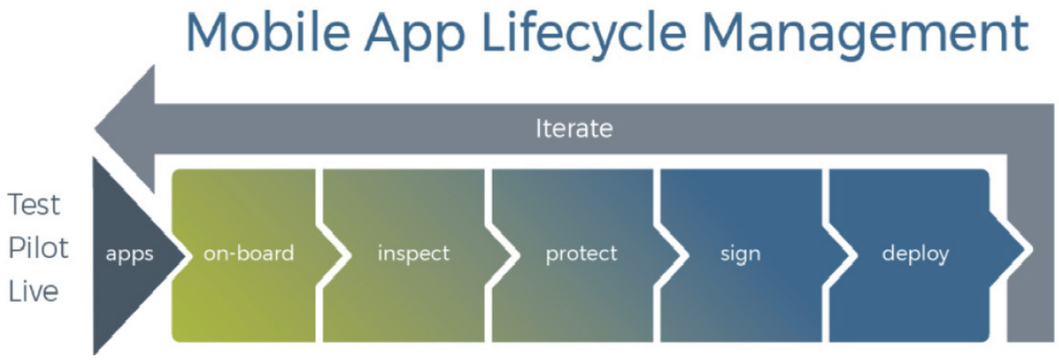
透過混淆和加密來隱匿關鍵金鑰和資料元素，從而保護靜態和動態金鑰以及應用程式的機敏資料。Arxan 支援所有主要的加密演算法和模式，只需要最小的程式碼空間以獲得最佳性能。

Arxan for JavaScript

保護基於瀏覽器的 JavaScript 應用程式並提供可配置的保護，允許開發人員決定每個應用程式所需的適當保護級別。Arxan 透過控制流（control flow）混淆和其他使惡意人士挫敗的技術，保護 JavaScript 免受逆向工程的影響。

企業生產力應用程式

為了簡化業務營運，企業生產力應用程式在員工、承包商和合作夥伴擁有的非託管設備上運行。組織部署不安全的生產力應用程式與任何在野生環境運行的應用程式一樣，對企業構成重大的威脅。這種威脅，導致持續性的管理困難，難以去尋找有效且安全部署行動應用程式的方法，來最大限度地採用和維護隱私而無需設備管理或註冊。為解決此問題，企業需要採用三階段應用程式管理方法。



Apperian 應用程式管理

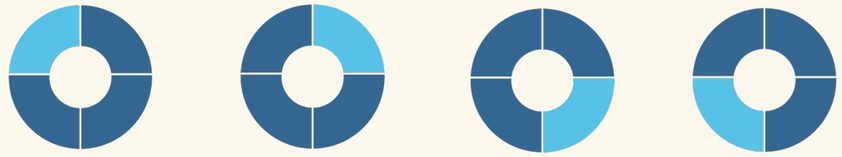
首先，應用程式需要正確地上架，以確保它們沒有惡意軟體和隱私風險。其次，客製和現成的應用程式需要包含安全性、分析和管理策略。

第二，不管是客製或現成的應用程式皆需透過封裝技術（App Wrapping）納入安全性、分析和管理策略。

第三，這些應用程式封裝器（App Wrappe）的增強功能允許 IT 團隊實施企業單一登入（SSO）以達成：應用程式級別有效且有制度的管理、應用程式使用率和分析、應用程式層級 VPN、撤銷應用程式、禁用複製 / 貼上、越獄（Jailbreak）檢測等。

最後，透過以企業商標為名的企業應用程式商店，向用戶提供經過審查與封裝的應用程式，達成最大限度地掌控應用程式分配情況及使用者採用率。

Arxan 企業解決方案



多層次的應用程式防護　視覺化＆智慧化　企業客戶的成功　進階威脅分析團隊

現代應用程式開發導致 API 威脅崛起

API 服務的出現讓開發人員能夠更快開發出行動和網路應用程式讓使用者使用。在網際網路流量的急劇變化中可以清楚看出 API 應用程式開發的普及程度目前有 83% 的流量與 API 相關，2014 年則為 40%。

並非所有 API 呼叫都合法

White traffic

用以進行業務的合法呼叫，佔所有 API 流量的大部。

Black traffic

明顯危險的呼叫，通常導向至網頁伺服器以突破網路安全層。常見的攻擊向量是使用蠻力技術（例如 DDoS 攻擊）或更集中的自動化憑證填充攻擊的機器人。

Grey traffic

可能危險的呼叫，但表面上看似合法。Grey traffic 難以識別，因為它可以利用遭竊的合法帳戶 ID 和 tokens 來獲得存取權限。

為何現代應用程式和 API 如此脆弱

任何公開發佈的應用程式都容易遭受逆向工程和後續攻擊，因為程式碼層級安全性不佳和編碼錯誤。API 攻擊的主要來源可能是無意間暴露 API 機密的行動和網路應用程式，包括 URL、tokens、加密金鑰和登入憑證。不幸的是，使企業面臨風險的行動和網路應用程式安全性下降的普遍程度勝過所應容許的程度。應用程式層級安全性漏洞使得對 API 進行二次攻擊成為可能，因為嵌入於應用程式的程式碼之資訊可提供關於 API 運作方式的藍圖。

- 25% 包含未編碼 API URL、API 金鑰及其他 API 機密的應用程式
- 60% 未遮罩資料庫參數或 SQL 查詢
- 74% 因應用程式遭入侵而經歷重大網路攻擊的組織
- 80% 執行弱通訊加密方法
- 97% 經過測試的行動應用程式缺乏任何形式的二進位保護
- 100% 遭 Magecart 入侵的網站缺乏原始碼保護

如何緩解 API 攻擊

現有的網路安全性解決方案解決某些 Black traffic 問題，但嘗試解決 Grey traffic 問題時有明顯差距。為了保護 API，安全性專業人士必須確認使用帳戶 ID 和 tokens 的流量是否確實合法。但如果應用程式經過逆向工程且 API 機密被揭露，則可使 Black traffic 看似合法，同時使用遭入侵的 API 機密執行後續攻擊。

Arxan In-App Firewall 可為用戶端 API 提供防護

在程式碼層級保護行動和網路應用程式以防止 API 資訊暴露

- 競合和動態二進位及原始碼保護，防止可能暴露 API 資訊的逆向工程
- 加密資料和金鑰以防止敏感資訊被攔截
- 及時偵測應用程式及其內容是否成為目標，以通知企業並自動觸發防禦措施

Arxan In-App Firewall 有助於防止資料竊取

為了替現有的網路和驗證防禦增加另一層網路應用程式安全性，Arxan 設計出應用程式內防火牆，允許受保護的網路應用程式只連線至授權的 API，防止從瀏覽器網路表單竊取客戶資料。

Arxan 應用程式保護的優點

Arxan 的所有保護功能旨在防止威脅行為者對應用程式的程式碼進行逆向工程，以及避免揭露可用來對後端系統進行後續攻擊的嵌入式資訊。Arxan 保護也可以整合至現今快速的 DevOps 環境而不會使 CI/CD 流程變慢。整合所有 Arxan 保護解決方案的關鍵功能之一，即能夠在任何行動或網路應用程式發佈後瞭解威脅態勢。

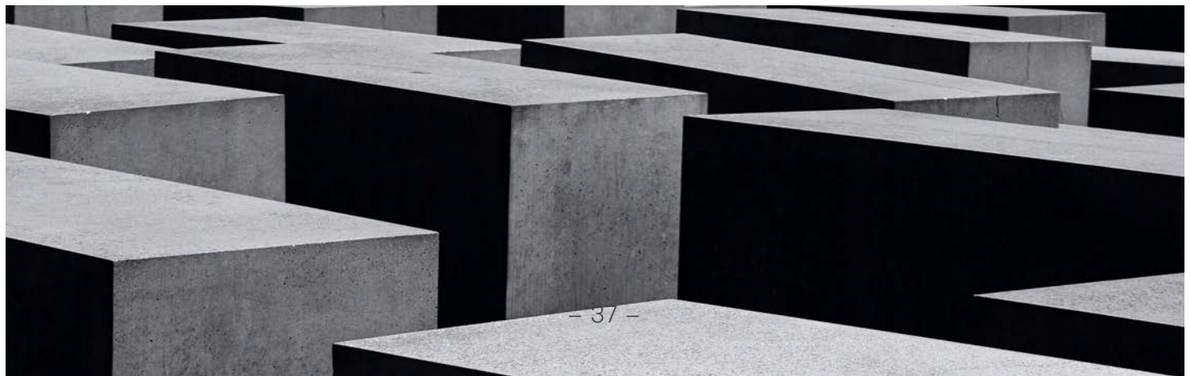
從瞭解行動應用程式上有多少 jailbroken 和 rooted 的裝置在運作，到即時得知是否有程式碼遭竄改，Arxan Threat Analytics 讓組織快速瞭解其應用程式所在的威脅環境。此功能整合於所有 Arxan 保護解決方案，提供關於所有受保護應用程式及其中嵌入之 API 狀態的即時現場情報。

Arxan 威脅分析的資料可以整合至現有的 SIEM、BI、WAF 或詐騙預防平台，有助於豐富已知的使用者資料，並且更全面地掌握何物、何處及何人攻擊您的應用程式。

Arxan 讓組織能夠關閉帳戶、使應用程式停用功能或存取權限以及在攻擊成功突破後端系統之前更新程式碼，以自動應對威脅。

全面的應用程式保護

Arxan 提供全面的應用程式層級安全性以防範各種威脅或實施企業應用程式治理 — 擴大企業信任範圍。Arxan 提供各種獲專利的安全性功能以保護處於風險中的應用程式，例如動態應用程式原則引擎、程式碼強化、混淆、白箱加密以及威脅分析。



Arxan for Web

開發人員希望構建具有快速，無縫用戶體驗的 Web 應用程式。實現該目標的最有效方法之一是使用 JavaScript，估計約佔所有網站的 95%。從單頁應用程式，漸進式網頁應用程式（PWA）開發項目，或透過將驗證過程推送到客戶端來簡單地提高性能，JavaScript 已成為有效提高性能和用戶體驗的共同點。但是，利用 JavaScript 為 Web 應用程式開發帶來了所有好處，它卻有一個主要問題：**程式碼安全性**。

JavaScript 安全性問題

JavaScript 是一種直譯型語言，這意味著除非採取額外步驟來保護程式碼，否則它很容易被截獲，查看和洩露。然後，可以使用此不安全的程式碼竊取用戶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（使用偵錯程式來了解程式碼的運行方式）。一旦設計了與 API 介面互動的程式碼，就可能會製造攻擊來識別弱點和存取後台系統。為了保護整個 IT 生態系統，組織需要保護客戶端 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或基礎架構存取點。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。這些攻擊可以暴露客戶資料，攔截和修改通訊，並洩露後端資料。

還可以使用 Web 應用程式如何與後台系統互動的資訊來製造其他形式的攻擊。最值得注意的是有針對性的惡意程式碼攻擊，例如旨在竊取憑證的 Man-in-the-Browser（MitB）惡意軟體。了解輸入發生的地方和驗證的位置可以為攻擊者提供設計惡意軟體所需的全部知識，以竊取用戶憑證和存取其帳戶。

在當今零信任世界中，保護客戶，業務和 IP 資料的需求比以往任何時候都要大。保護應用程式和資料免受攻擊是防止品牌破壞，財務損失，知識財產權盜竊，遊戲舞弊，重送攻擊，政府處罰等的關鍵。

防護 Web 應用程式

為了應對 JavaScript 應用程式的威脅，組織需要保護其應用程式程式碼。Arxan for Web 保護 JavaScript 程式碼，在危害後台關鍵資產之前，就已經在客戶端阻止威脅。 零信任是一個概念，其核心是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，驗證任何事情和所有嘗試連接到其系統的內容。

防護能力

透過混淆進行靜態防護，以保護"明確的" JavaScript 程式不被輕易理解

1

透過關閉瀏覽器或修復受攻擊的程式進行動態防護，以反應攻擊

2

即時警報，程式被嘗試分析甚至篡改時，通知組織並立即執行反應動作，如關閉攻擊者帳戶或更新程式碼保護

3

Arxan for Web 可在企業場所或透過雲端提供，並相容所有主要的開發框架。 而且，這兩種選項都可以保護編碼後的 JavaScript，而不會妨礙開發過程或時間表。

好處

防禦 JavaScript 程式碼攻擊以阻止應用程式分析，API 攻擊和惡意軟體。

即時偵測攻擊，使組織能夠通過以下方式回應攻擊
1. 禁用攻擊者的帳戶存取權限
2. 開發和更新混淆參數來重新部署程式碼

防護不會阻礙開發，因為是在完成開發程式碼後再進行防護，不管是在企業端或基於雲端，都可以順利、快速整合到現有開發流程和框架中。

Arxan 成功的客戶團隊幫助實施應用程式保護，以加快產品上市時間並在整個應用程式生命週期中發展保護。Arxan 的全球威脅團隊從多個途徑提供可操作的情報，以了解應用程式威脅環境，以便在威脅成為攻擊之前主動阻止它們。

從裡到外防護應用程式

Arxan 提供全面的應用程式級安全性，以防範一系列威脅或實施制度性的管理企業應用 – 擴大企業的信任範圍。Arxan 提供廣泛的專利安全功能，以保護在野生環境應用程式 – 例如動態的應用程式政策引擎、程式碼強化、混淆、白箱加密以及威脅分析。