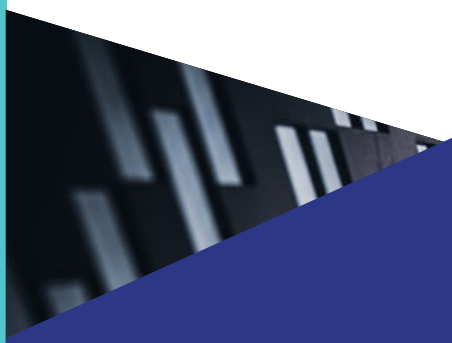
digital.ai

App & Web 防護

DevOps Dozen 2022
工具和服務獎獲得者

Info Security
Products Guide



產品簡介

應用程式 (Application) 添加 Digital.ai Arxan Protection 保護機制，防止惡意行為篡改您的應用程式。

當數位化轉型和全球流行病的爆發後，加速了更多軟體開發的需求，企業必須負責有效率的開發安全且操作方便的應用程式。在此之下，應用程式的其中一個挑戰是如何避免被繞過安全邊界。為了防止客戶數據、公司 IP 甚至金錢被盜，必須對應用程式進行混淆，提供防止篡改的方法。

大多數企業會面臨快速開發以滿足不斷變化的客戶、競爭、市場需求的壓力。敏捷開發的組織中應用程式可能每月發布兩次，甚至每天發布一次 APP。

因此，為您的應用程式提升安全性是非常必要的，但處於快速開發的壓力之下，可能會面臨以下問題：

01
沒有將安全性視為軟體開發流程的一部分。

02
將安全性視為麻煩與障礙。

03
想增加安全性但不知道從哪裡開始。

與此同時，資安長（CISO）面臨的主要挑戰是如何保護組織避免受到破壞，防止惡意行為與防止逆向工程和篡改其公司的應用程式。

挑戰

更快地開發更多應用程式的壓力

各種操作系統和程式語言的行動、桌面、網路所需的應用程式

如何避免應用程式被破解傳統安全措施

威脅行為者使用應用程式作為攻擊媒介

資安長面臨的另一個挑戰是維持客戶的滿意度。 如果建立防護所花費時間太長，而延遲了客戶需求的軟體交付，資安長將面臨客戶的抱怨。此外，如果資安長實施的安全控制在功能或速度方面對用戶體驗產生不利影響，資安長可能失去信譽。如果資安長不採取任何措施保護其公司開發的應用程式，則可能面臨違規風險，這將導致客戶數據、公司 IP 或收入遺失。此外，資安長通常是大型企業安全的公開代言人，因此當違規行為被公開披露時，他們的工作也將面臨風險。

Digital.ai APP Protection

以 DevOps 的速度構建安全軟體

Digital.ai APP Security 解決了軟體開發者和資安長面臨的挑戰，Digital.ai APP Protection 提供的最好的保護去避免惡意行為者繞過您的應用程式的邊界安全。

應用程式原始碼防護

Digital.ai APP Protection 在未受保護的程式碼與保護藍圖（Guard Spec）一起產生成受保護的應用程式。受保護的應用程式包含混淆的機器程式碼，這些程式碼依照最初設計的方式運行，但實際上威脅行為者無法讀取 – 即便將其透過反編譯程式後也無法解析。

可以根據需要在保護藍圖（Guard Spec）中設定自定義項和添加保護，或者您可以使用我們的自動配置選項的保護藍圖（Guard Spec）來自動混淆您的應用程式（不需要自定義或配置）。使用自動配置選項可以讓您更快地建立受保護的應用程式。

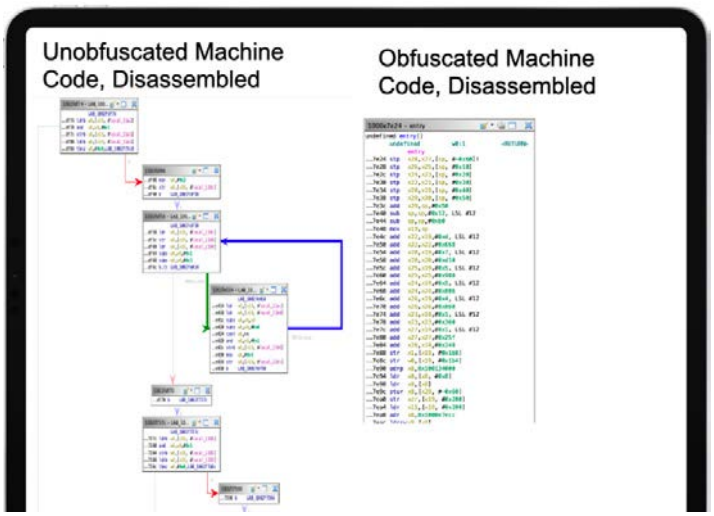
Digital.ai APP Protection 防篡改檢測技術

- 檢測應用程式何時在可能允許被篡改的不安全環境中運行，這些類型的環境典型範例是模擬器或已獲得 Root 權限 / 越獄 JB 設備。
- 檢測應用程式中的程式碼何時會被修改。
- 提供對應用程式於運行期間進行多種動態偵測。
- 在不安全環境中運行您的應用程式的嘗試的可見性。

結合 Digital.ai APP Aware（威脅分析平台）模組

- 如果威脅行為者試圖修改您的程式碼，將會收到警報。
- 提供有關發生竄改於什麼地方、設備、操作系統和瀏覽器上的詳細信息。
- 提供設備 IP 地址和威脅行為者的所在位置。
- 提供竄改發生的時間和檢測到的時間。
- 提供瀏覽器、該瀏覽器中的用戶代理、發生模組的 URL 以及被竄改的特定腳本的名稱。
- Digital.ai APP Protection 添加到應用程式中，不會減緩應用程式的開發過程或應用程式本身，同時還可以防止應用程式被用作攻擊媒介竊取您的 IP、客戶數據或收入。

在 Ghidra 中反彙編的應用程式碼



主要優勢：保護、監控、反應

通過開發過程將安全性嵌入到應用程式來進行保護

- 保護您的 Mobile APP、Web 和桌面應用程式中的程式碼、金鑰和數據
- 混淆程式碼以防止逆向工程，通過檢測不安全的環境和程式碼更改來防止篡改
- 快速整合軟體建置環境

監控有風險的應用程式

提供應用程式存在風險的可見性

- 可整合獨立報告或與現有安全營運中心的工具
- 產生安全報告
- 設定防護和保護的機制

通過偵測到威脅做出即時反應

營運時應用程式自我保護（RASP）自動即時防止威脅（可客製化反應）

- 強制升級認證
- 改變應用程式功能
- 關閉受到攻擊的應用程式

關鍵能力

APP Protection 特色	功能說明
Guard Network（縱深防禦）	確保威脅行為者必須同時拆除您設置的每項保護措施，才能通過 Guard Network 破解您的應用程式。
跨多個平台的應用程式安全支持	將安全性建構到 Mobile APP、Web 客戶端和桌面應用程式中。
跨多個操作系統的 APP Security 支持	為最廣泛的操作系統（包括 iOS、WatchOS、tvOS、Android、Mac、Windows 和 Linux 桌面）編寫的應用程式構建安全性。
跨多種開發語言的 APP Security 支持	為使用 C、C++、C#、Java、Javascript、HTML5 和 Kotlin 編寫的應用程式構建安全性
金鑰和數據保護	符合 FIPS 140–2 標準的私鑰白盒加密可確保您的通信安全。
提供對您的應用程式何時存在風險的可見性	Digital.ai 攻擊趨勢洞察與報告。
快速整合到您的軟體開發環境	無需額外增加建置環境，可在現有的軟體建置過程中自動建立安全防禦。
惡意軟體檢測	通過動態保護免受間諜軟體、鍵盤記錄程式和許多其他類型的惡意軟體的侵害。