digital.ai™ GSS Galaxy Software Services 叡揚資訊

第三年度

2025 應用程式安全威脅報告

分析現代應用程式的安全風險演變

內容

介紹

想像這樣一個情景：一個陌生人悄悄檢查你社區的房子，看看門是否鎖好。有些房子只是被遠遠觀察，有些沒鎖好門的則是被闖入，甚至被偷取重要物品。在最嚴重的情況下，這個人會把所有房子洗劫一空將所有值錢的東西拿走。

在 2025 年 1 月，Digital.ai 監控的用戶端應用程式中，有 83% 的「前門``」被「試探」（圖 1）。

這代表什麼？這些應用程式[1] 不是在不安全的環境中運行（例如已被 JB 或 root 的手機，或甚至在除錯器或模擬器中運行），要麼有人試圖找它的弱點。在最糟的情況下，它們甚至被人動手篡改過。

如果您社區 83% 的房屋都遭受到了這種的試探，想當然大多數屋主第一步肯定會立即採取行動：確認門鎖的狀態、加裝攝影機，甚至整個安裝防盜警報系統。

“威脅行為者不只是撬鎖，他們還系統性地檢查每扇數位大門，並且掌握了越來越複雜的先進技術。”

我們的數位世界正在以前所未有的速度擴張，同時也面臨持續增加的威脅。面對這些入侵風險，再加上資料外洩的成本可能高達 500 萬美元，企業不能再拖延，必須立即加固自己的數位資產。

隨著大量免費工具和 AI 技術的出現，威脅者現在可以輕而易舉地進行逆向工程、分析並大規模利用應用程式。這些威脅者不只是「撬鎖」，他們系統性地檢查每一個數位前門，並且手上掌握越來越先進的技術。

Digital.ai 的《2025 應用程式安全威脅報告》協助各組織為其數位資產築起更堅固的屏障。憑藉遍佈全球各產業的數百位客戶，Digital.ai 得以從獨特視角追蹤針對用戶端應用程式的攻擊。本報告在歷年基礎上進一步擴充，納入產業特定趨勢、地區差異，並從企業與使用者兩個視角進行新的分析。

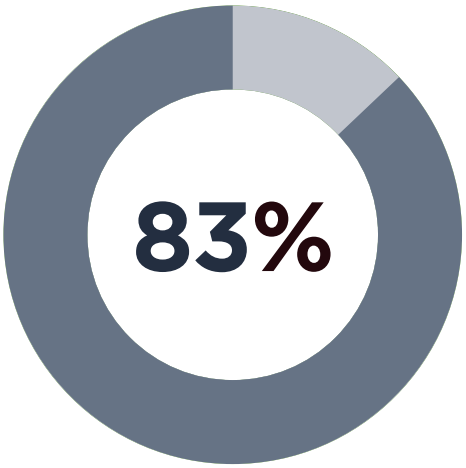


圖 1： 2025 年 1 月， 83% 的 Digital.ai 監控 的 客戶端應用程式受到攻擊

[1]「用戶端應用程式」指在使用者裝置（用戶端）上執行的應用軟體；（client-side app）

[2] 參考：https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

重要發現

1 用戶端應用程式攻擊上升

遭遇攻擊的應用程式比例自 2024 年 2 月的 65%，攀升至 2025 年 1 月的 82.7%；而行動平台更是攻擊的重點，iOS 達 88.1%、Android 更高達 90.4%（如圖 2 所示）。

2 更多 app 被更頻繁地上線

公司持續頻繁的向客戶提供新版本應用程式。這在行動應用程式領域最為明顯——2024 年，Apple 的 App Store® 和 Google Play™ 共提供了近 400 萬款應用程式，下載量高達 1,378 億次；桌面與網頁應用程式也依然受到歡迎。

3 威脅不再侷限於金融服務

雖然金融服務一直是主要攻擊目標，但最新數據顯示，電信業（91%）和汽車業（86%）也遭受了大量攻擊，顯示威脅正在跨行業擴散（如圖 3 所示）。

4 應用程式安全刻不容緩

企業必須優先強化對逆向工程和篡改的防護，確保安全措施能持續更新，以客戶。這種趨勢在移動應用程序中最為明顯應對日益擴大且演變中的威脅。已實施應用程式防護的企業，能領先應對越來越複雜的攻擊；而缺乏防護的企業仍然是易受攻擊的目標。

目前市面上已有一些簡單可實施的應用程式安全解決方案，能為企業提供非常有效的保護，不僅可節省數百萬美元、降低風險，還能增強最珍貴的資產——客戶信任。

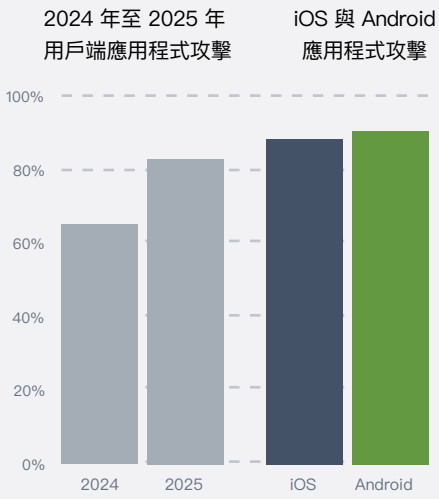


圖 2：不同裝置類型的用戶端遭攻 40% 擊比例

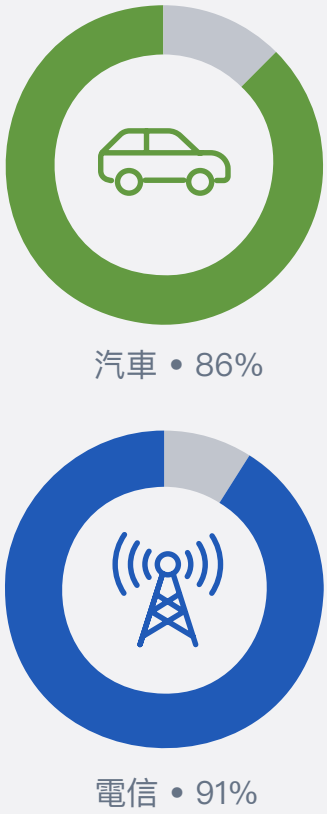


圖 3：2025 年電信和汽車行業遭受重大攻擊比例

3. https://42matters.com/stats

研究方法

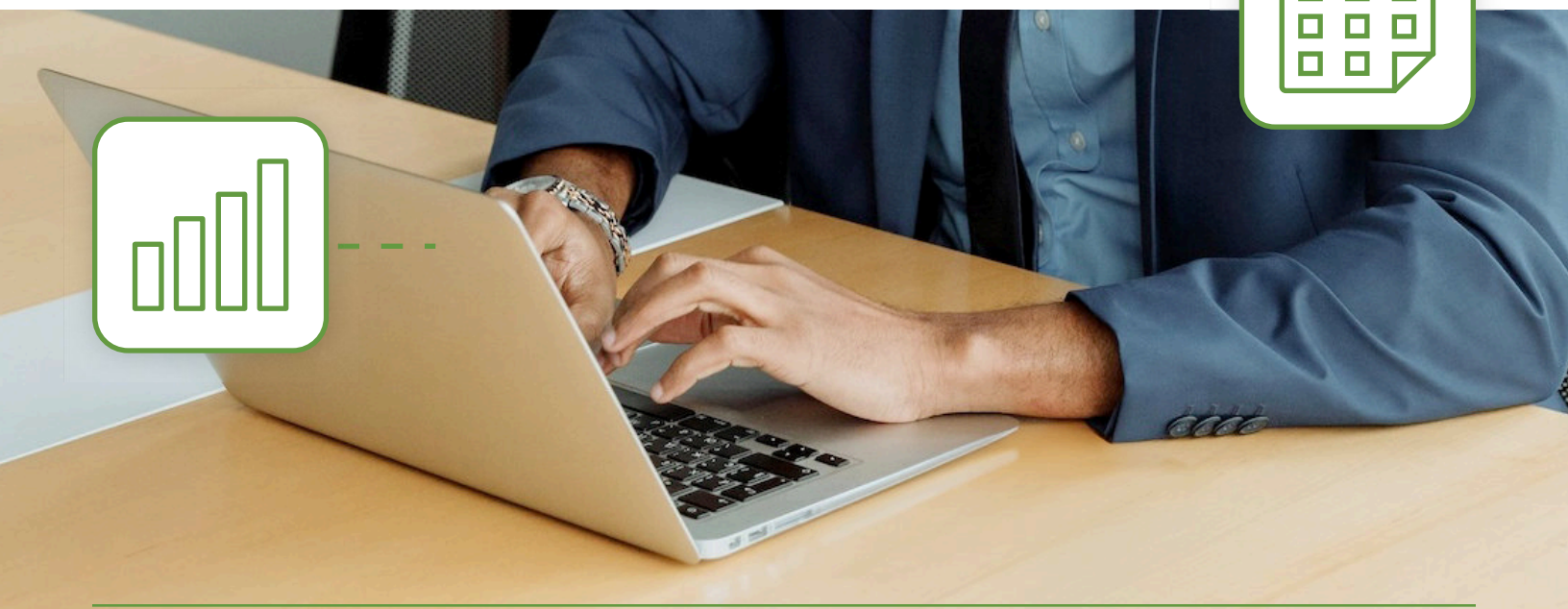
這份報告的數據來自 2025 年 1 月 1 日至 31 日期間，Digital.ai 部分應用程式安全產品客戶的使用情況。

Digital.ai 持續監控並保護這些受調查的客戶應用程式，抵禦來自全球、涵蓋各大產業的實際攻擊，產業包括銀行、媒體、電信、製造、遊戲以及網路安全等。

本報告所討論的攻擊類型（完整性、環境、以及工具注入）是由國際應用程式安全專業組織 OWASP® 所定義，並記錄在其《行動應用程式安全驗證標準》（MASVS）中。

想了解更多關於 OWASP® 與 MASVS 的資訊，可以參考此處。

4. “OWASP® 文字商標和 OWASP & Design 標誌是 OWASP Foundation， Inc. 在美國和其他國家/地區的註冊或未註冊服務商標。版權所有。嚴禁未經授權使用。



市場與產業趨勢

市場趨勢

從學校到全球企業，越來越多的組織正在打造自己的行動應用程式，以便在全球範圍內與顧客建立更緊密的聯繫，讓顧客能夠透過輕觸手機螢幕與其業務互動。

行動應用程式為組織提供了一個直接的、數據驅動的管道，可以即時蒐集資訊、個人化和增強客戶互動。行動應用程式已深入融入我們的生活、品牌以及與客戶的互動。**光是 Apple 的 App Store® 和 Google Play™ 商店 2024 年合計就提供了將近 400 萬款應用程式，下載量高達 1,378 億次。**

我們生活在一個「App 迷戀」的世界。但當企業和消費者都樂於接受這個趨勢時，威脅者更是樂在其中。資料外洩的成本已逼近 500 萬美元[6]，而任何上線的應用程式都有可能成為攻擊者的切入點。

誘因

應用程式對攻擊者來說是非常誘人的目標。隨著企業為了提高客戶參與度而將更多關鍵業務搬到客戶端平台，應用程式包含比以往更多的商業邏輯。這種轉變創造了一個不斷擴大的攻擊面，為那些懷有惡意的人帶來了巨大的潛在利益。

在 2025 年，不論是行動、網頁，還是桌面應用程式，都吸引了攻擊者異常高的關注。放眼全球、各行各業，攻擊者正以前所未有的頻率針對應用程式下手。光是今年 1 月，Digital.ai 監控的應用程式中，就有 82.7% 遭受攻擊。

現在的威脅者加上 AI 協助的攻擊，以及攻擊者之間願意更頻繁地分享手法與腳本，變得比以往更有效率，也更具規模。

“行動應用程式為組織提供了一個直接的、數據驅動的管道，可以即時了解、個人化和增強客戶互動。”

5. https://42matters.com/stats

6. https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

產業趨勢

Digital.ai 今年擴大了產業資料分析的覆蓋範圍，把電信、醫療保健和汽車行業應用程式攻擊情況也納入分析。即便你的組織不屬於這四大產業之一，這份報告依然具有參考價值，透過這些數據能看到整體應用程式市場的狀況 與演變 。

電信（Telecom）

電信產業持續以極快的速度發展。電信應用程式不斷把更多控制權和功能放到客戶端，例如帳號管理、數位錢包、以及裝置安全功能，這些都和攻擊趨勢的數據息息相關。同時，行動電信商越來越多地將 eSIM 啟用、網路切換和漫遊管理整合到其應用程式中，減少對實體 SIM 卡和實體門市的依賴。

這對於安全意味著什麼？

簡單來說，應用程式越多，攻擊面就越大。當電信應用程式成為存取內容、連線服務，甚至金融交易的關鍵入口時，它們自然也成為竊取憑證、詐騙，以及應用程式被操控的熱門目標。同時，5G 和邊緣運算（Edge Computing） 的普及也在擴大攻擊面。分散式運算雖然減少了單一中央瓶頸問題，但也增加了潛在的故障點與客戶端風險。

金融服務 （FinServ）

就創新速度而言，僅次於電信業的就是金融服務業。促成 FinServ 演進的一大關鍵，是將「金融功能與銀行即服務（BaaS）」整合到原本非金融的應用程式中。

越來越多的非金融公司（零售、科技、汽車業）正在將金融服務嵌入到他們的平台中，使金融服務更加分散化，同時也成為攻擊者的理想目標。

例如，電信公司可能在自家 App 提供支付功能；汽車公司可能提供購買維修或零件的功能。而傳統金融服務則加速導入生成式 AI 與預測分析以高度個人化銀行服務，這也使得客戶端銀行應用程式的使用範圍持續擴大。

“隨著電信應用程式成為內容、連接和金融交易的重要通道，它們也成為憑證盜竊、詐欺和應用程式操縱更具吸引力的目標。”

汽車（Automotive）

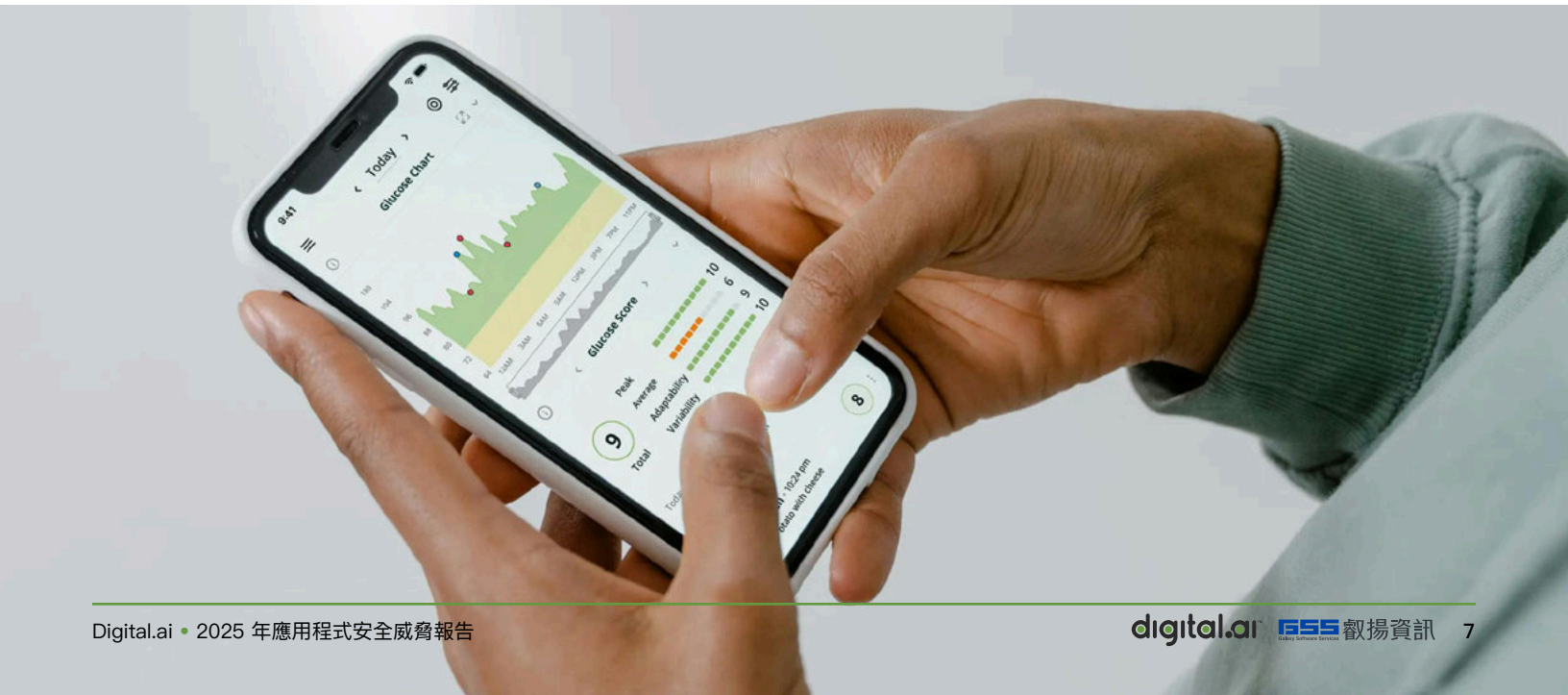
汽車產業競相把越來越先進的應用程式整合進車載系統，甚至在手機 App 裡加入解鎖、發動，甚至遠端維修的功能。汽車正從「硬體為核心」逐步轉型為「軟體定義車輛」。像是 OTA（無線更新）、AI 駕駛輔助、雲端連線車輛服務，如今正在快速成為業界標準，而不再是少數例外的功能。

這些進步同時也意味著更多攻擊機會。部分攻擊者可能只是好奇，想試試能不能從後座駕駛汽車；但也有攻擊者是帶著惡意，想要製造混亂甚至傷害並從中獲利。

醫療保健（Healthcare）

AI 驅動的診斷工具和虛擬健康助理正在改變病患照護的方式，尤其透過預測分析提升早期疾病偵測的能力。越來越多病患可以直接用手機取得這些健康資訊。同時，隨著數位健康平台的興起——例如遠距醫療、遠端病患監測、數位治療等快速普及——科技已將穿戴式裝置、行動健康追蹤 App 與雲端健康生態系統整合在一起。

不過要特別注意，這些醫療 App 都可能被逆向工程。有時候只是好奇的技術玩家病患，想修改自我照護方式；但在最糟的情況下，也可能遭到惡意攻擊者入侵，甚至造成病患傷害。



攻擊數據

本節匯總了各應用程式受到攻擊的可能性。在此內容中，彙整、呈現了由 Digital.ai 應用程式安全性產品保護和監控的所有產業、地理位置和平台的整合資料。

如前所述，82.7% 的應用程式在 2025 年 1 月遭受了攻擊，比 2024 年增加了 27%（圖 4）。

為什麼會這樣？主要有三個原因：

1. **工具普及化：**反編譯工具像 Frida、Ghidra 現在隨處可得，還有一大群社群玩家在分享技巧，讓攻擊門檻大幅降低。

2. **AI 助攻：**現在很多威脅者開始用生成式 AI，不只惡意程式產得更快，還能更快看懂程式碼進行原始碼分析。

3. **攻擊面變大：**App 越來越多，平台越來越廣，等於提供了更多練兵場。不論是白帽或黑帽駭客，都可以透過實際操作來累積經驗。

“所有行業的攻擊率都激增。無一倖免——過去較少受波及的領域（如醫療與汽車）如今也面臨重大威脅。”

2025 年有什麼不同？

最大的差別就是所有產業的攻擊率都大幅上升。沒有任何一個產業能倖免。甚至像以前比較少被盯上的醫療和汽車業，現在也都成為重點目標。

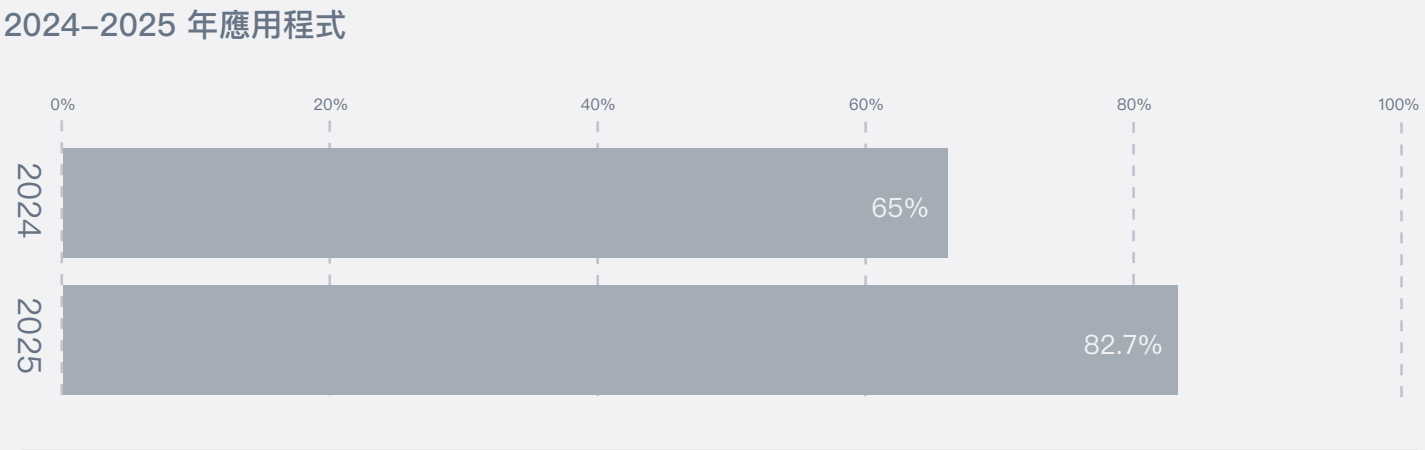


圖 4：2024 年至 2025 年間，用戶端應用程式攻擊增加了 27%

各產業受攻擊情況

金融服務和遊戲應用程式歷來是最易受攻擊的行業。然而，由於今年的數據有限，遊戲並未被包含在我們的分析中。

電信與汽車應用程式遭遇的攻擊頻率已接近以往金融服務的程度。一些產業的監管變嚴格，增強了安全控制機制，這部分可能也促進了攻擊偵測與通報數量增加。

金融產業 – 應用程式的被攻擊率為 87.5%（圖 5A）。

攻擊者的目標主要是數位銀行、金融科技、支付平台，常見手法包括：竊取交易數據、反編譯驗證機制、自動化詐欺、中間人攻擊、API 漏洞利用。雖然有像歐盟支付服務準則修正案 (PSD2) 的法規要求，但駭客還是能繞過身份驗證和多因子驗證。

醫護產業 – 78.5% 的受監測應用程式遭遇攻擊（圖 5B）。

因為醫療產業快速數位化，像遠距醫療、病患管理 App、穿戴式裝置，都帶來新的攻擊面。主要威脅有：病患資料竊取、鎖定醫療 API 的勒索攻擊、遠端監控系統被操控。美國的《健康保險流通與責任法案》（HIPAA） 和歐盟的《通用資料保護規範》（GDPR） 等嚴格法規推動了更強的安全性，並提高了攻擊的可見性，讓攻擊事件更容易被發現、記錄、回報。

汽車產業 – 應用程式的受攻擊率為 86%（圖 5C）。

「軟體定義汽車」高度依賴手機 App 來進行遠端控制、車聯網（telematics）以及 OTA 更新，這也讓它們成為攻擊者眼中的高價目標。攻擊者可能嘗試操控遠端解鎖、濫用充電設施的支付系統，甚至攔截車輛的控制數據。目前車聯網生態系的資安防護仍不夠一致，其中 API 更經常暴露在遭到竄改的風險之下，特別需要引起重視。

電信產業 – 應用程式的攻擊率最高，達到 91%（圖 5D）。

雖然我們在電信產業的樣本數相對較少，但有幾個因素顯示，電信依然是威脅行為者的主要攻擊目標。隨著 行動身分管理、電信帳單支付，以及 eSIM 啟用 等功能被整合進電信 App，這些應用的價值不斷提升，也更具吸引力。同時，SIM 卡交換詐騙（SIM–swapping fraud）、假冒電信 App，以及 API 濫用 仍是常見的攻擊手法。隨著電信業者採取更嚴格的資安措施，他們可能比管制較少的產業更容易發現並通報攻擊事件。

整體來看，今年所有產業的攻擊數量都有上升，而電信已經超越金融服務，成為攻擊最頻繁的領域。而醫療與汽車應用 也同樣成為主要目標。隨著法規日益嚴格，更強的安全措施將有助於 提升攻擊偵測能力，讓企業更清楚掌握自身面臨的風險。

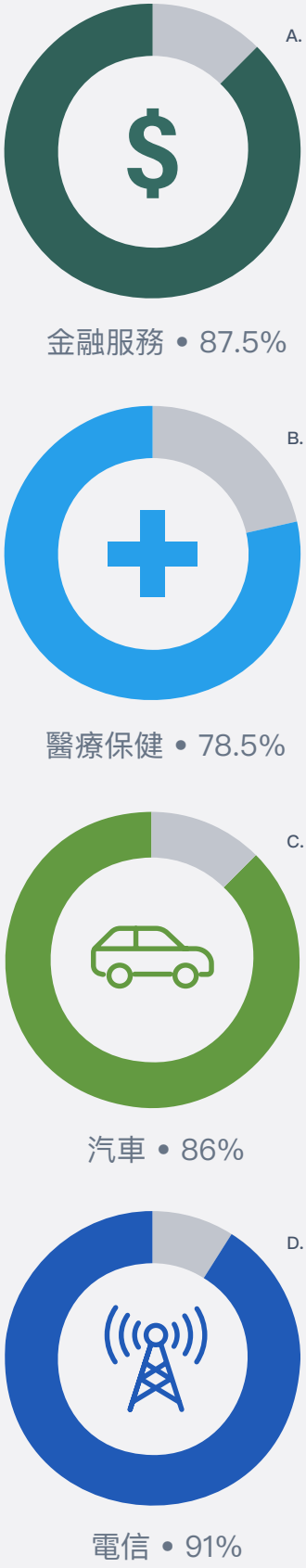


圖 5 （A–D）：2025 年對所有行業的客戶端應用程式的攻擊都有所增加

攻擊可能性：Android 與 iOS

在 2025 年，行動應用程式的攻擊率依然居高不下：Android™ 平台的受監測應用有 90.4% 遭到攻擊，iPhone® 應用則有 88.1%。雖然歷史上 Android 一直是主要目標，但隨著 iOS 攻擊事件增加，雙方的差距正在縮小，這可能與越獄（jailbreaking）及進階利用技術的提升有關。

為了因應這些新威脅，Digital.ai 改進了 越獄與 Root 偵測功能，因此回報的案例數量也相應增加。以下是依據攻擊可能信的分析：

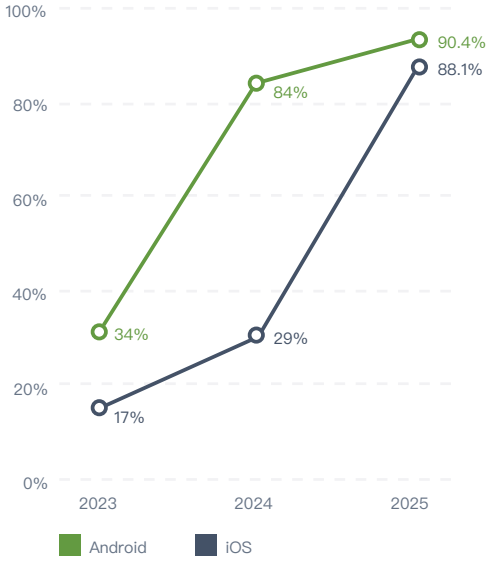


圖 6：2023 年至 2025 年間不同裝置的攻擊增加比較

環境攻擊（Environment attacks）：

指的是應用程式在不安全的環境下執行，例如裝置已 Root 或 JB 越獄。這類攻擊影響了 84.2%的 Android™ 應用 和 79.8% 的 iOS 應用（見圖 7）。隨著 Root 和 JB 越獄工具廣泛流通，平台本身的安全性持續被削弱。如果用「房子」來比喻，環境攻擊就像是有人轉一下門把，看看門有沒有鎖好。這不一定代表對方有惡意，但對「屋主」（也就是 App 擁有者）來說，這絕對是一個需要注意的警訊。

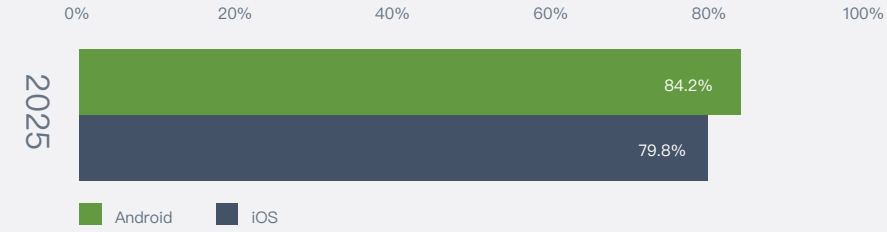


圖 7： 2025 年的環境攻擊

Instrumentation 攻擊

指的是動態修改程式碼，或利用像 Frida 這類的 hooking 框架進行操作。這類攻擊在 Android 上特別常見，攻擊率達 81.5%，而 iOS 則為 44%，幾乎是 iOS 的兩倍（見圖 8）。原因在於 Android 的開放架構讓應用在運行時更容易被操控，而 iOS 則有較強的內建限制。如果用「房子」來比喻，Instrumentation 攻擊比單純檢查門鎖更具侵入性。大致可以想像成：入侵者走進一扇未上鎖的門，仔細查看屋內財物，甚至可能做些筆記後，再從同一扇未上鎖的門離開。

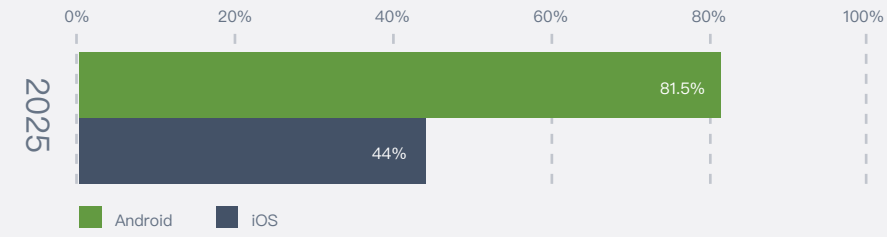


圖 8：2025 年的檢測攻擊

“雖然 Android 歷來更常成為攻擊目標，隨著 iOS 攻擊的增加，差距已經縮小。

完整性攻擊 (Integrity attacks)

指的是應用程式的程式碼被修改或重新打包。這類攻擊影響了 51.4% 的 Android 應用和 23.3% 的 iOS 應用（見圖 9）。Android 的應用分發模式以及第三方應用商店，讓攻擊者更容易散布被修改的應用程式；相對地，iOS 則因為 App Store 管控較嚴格而受到一定保護。如果用「房子」來比喻，Integrity 攻擊就像有人在房子裡動了東西，而且幾乎總是帶有惡意。他們可能會偷走電視、拿走一抽屜的珠寶，甚至破壞房屋財物。

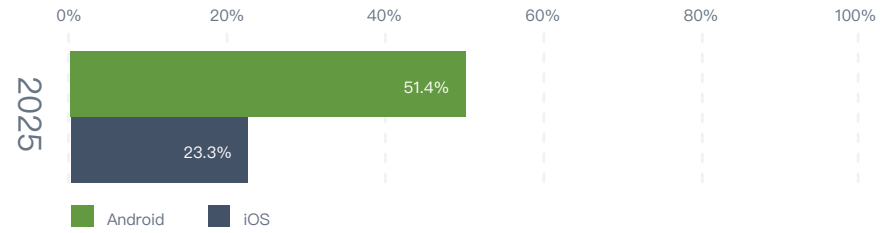
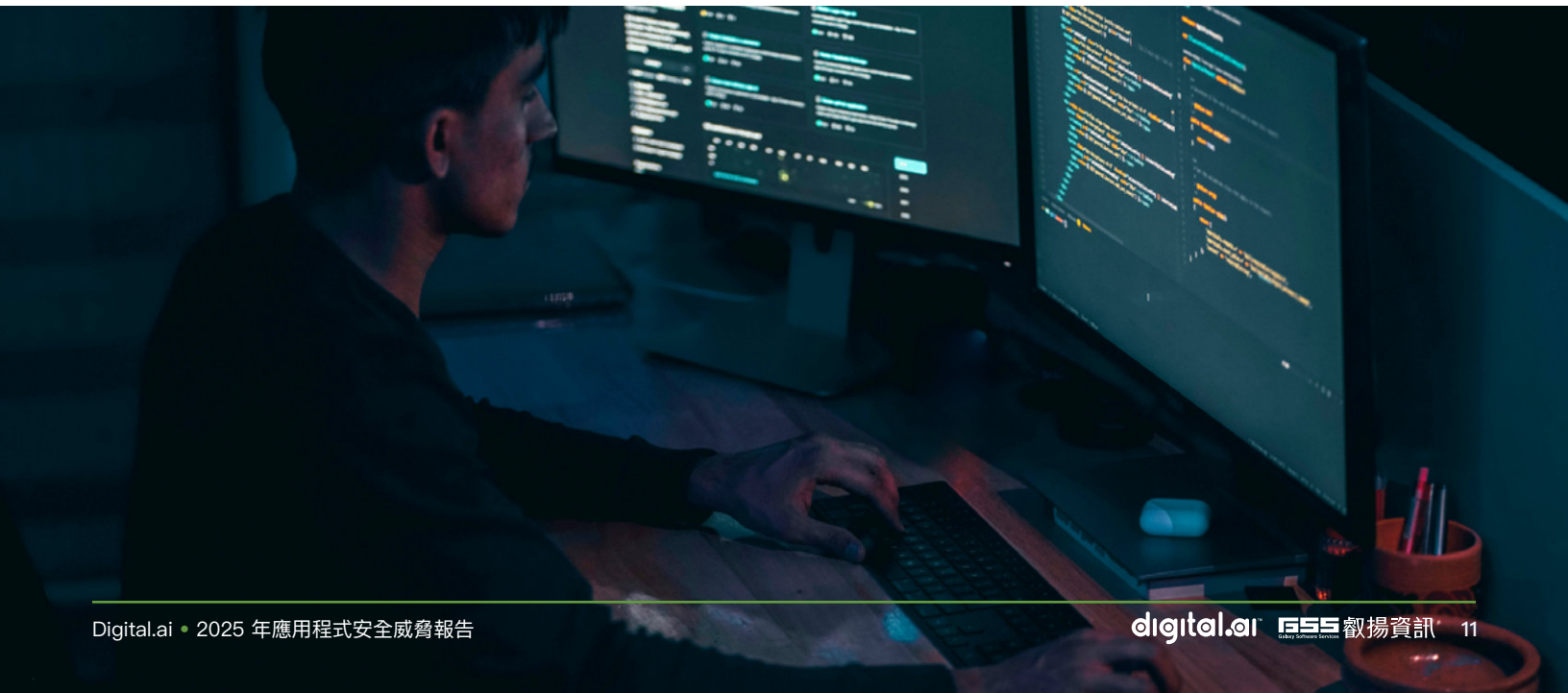


圖 9： 2025 年的完整性攻擊

> **“完整性攻擊相當於有人改變房子裡的東西，幾乎總是出於惡意。**

整體來看，兩個平台都面臨持續的威脅，但因為架構和安全政策不同，攻擊手法也有所差異。因此，企業需針對在這兩種不同作業系統上的應用程式，採取不同層級、不同類型的防護措施。



威脅觀點

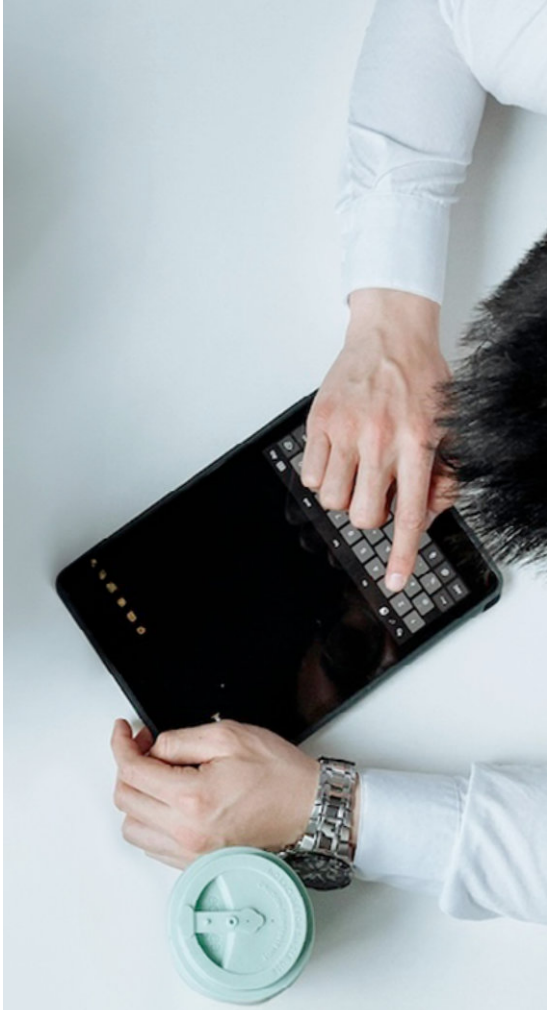
本節探討 Digital.ai 威脅評估中的關鍵細節，從企業端與最終使用者兩個角度，分析攻擊可能性，並重點關注 每個實際運行的 App遭受威脅的頻率 ，而不是 Digital.ai 客戶部署的行動應用數量。

企業視角（Enterprise Perspective）：

這種方法以開發行動應用的企業數量來衡量威脅。例如，如果兩家不同的企業各開發一個應用，而其中一個應用遭到攻擊，資料會顯示 50% 的企業應用受到攻擊。這種方式關注的是受影響應用占這些企業開發的應用總數的比例。

使用者視角（User-Level Perspective）：

這種方法則是從使用者暴露於安全事件的規模來衡量威脅。假設這兩個應用各有 1,000 萬名使用者，總共 2,000 萬個應用實例，如果其中有 40 萬個實例遭到攻擊，資料會顯示 2% 的應用實例被攻擊。這種方式可以從整體使用情況來了解威脅全貌，呈現「在實際使用環境中」的攻擊影響。



雖然 企業端的觀點 很有參考價值——

它凸顯出即便只有一個應用被入侵，也可能影響整個組織。但**如果進一步觀察被攻擊的應用實例總數，就能更全面地了解應用在哪裡、如何以及多頻繁地遭受攻擊。**

此外，使用者層級的攻擊統計也非常重要，因為這些攻擊可能嚴重破壞使用者信任，而使用者信任對企業來說至關重要。例如，如果攻擊事件被公開，或者使用者個別收到攻擊警告，他們對所互動的企業的印象就可能受到負面影響。

使用者層級觀點 （iOS vs. Android）跨作業系統版本

本節分析了今年一月期間，根據 Digital.ai 監控的所有應用實例所觀察到的使用者層級攻擊統計資料。

從企業與使用者兩個視角來看，以 OWASP® MASVS 的韌性分類來分析攻擊。以下是 2025 年觀測期間，依 MASVS 類別彙整的被攻擊 App 實例種類的大略占比：

- 整體攻擊：0.40%
- 不安全環境：0.35%
- 整體攻擊：0.40%
- 儀器：0.04%

Android™ 各版本的攻擊

Digital.ai 2024 年威脅報告的讀者希望看到不同行動作業系統版本的攻擊數據。最初的假設是，這些數據會呈現倒鐘型曲線（見圖 10）。

這個假設的原因是：舊版作業系統已經存在較長時間，研究人員有更多時間去發現漏洞，特別是那些可能讓攻擊者取得 root 權限的漏洞。而一旦設備被 root，它就更容易受到環境攻擊，進而增加完整性（integrity）和程式注入（instrumentation）攻擊的風險。相反地，最新的作業系統版本可能存在尚未被安全測試發現的漏洞，也常成為好奇使用者探索系統防禦能力的目標。

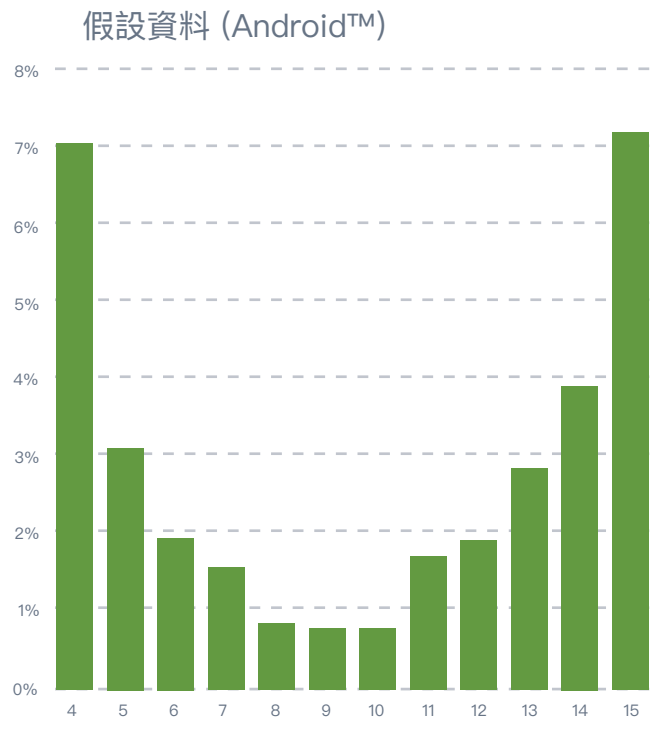


圖 10： 跨版本假設的攻擊百分比

然而，實際的數據顯示情況更複雜（見圖 11）。

Android 6 可能是一個異常值，因為曾有多次針對這個版本的局部攻擊被報告。排除這個版本後，數據呈現出鐘型曲線的趨勢：中間版本的攻擊頻率較高（Android 7、8、9、10、11），而兩端版本的攻擊頻率較低。造成這種現象可能有幾個原因：

1. **作業系統開發者逐步提升安全性**

   Apple 和 Google 等 OS 開發者持續改進系統安全。新版 OS 通常更難被攻破，因此攻擊者需要更高的技術創新。這種現象 在此部落格中進行了討論。因此，新版本在有效攻擊技術和工具尚未成熟之前，會吸引相當多的注意力。

2. **攻擊者希望開發能跨版本使用的工具**

   攻擊者傾向打造能在最多 OS 版本上運行的工具，但他們面臨的挑戰與應用開發者類似：支援舊版本越來越困難，取得舊設備的成本也逐漸提高，而維護這些舊設備的支持效益隨著使用者減少而下降。

iOS 應用在不同 iOS 版本上的攻擊情況

Apple® 裝置的攻擊趨勢與 Android™ 類似，但因為維護的版本較少，攻擊者和開發者需要支援的版本也相對較少。數據顯示，Apple 致力於讓所有使用者（包括潛在的攻擊者）都升級到最新的作業系統版本，這一點在觀察結果中很明顯。

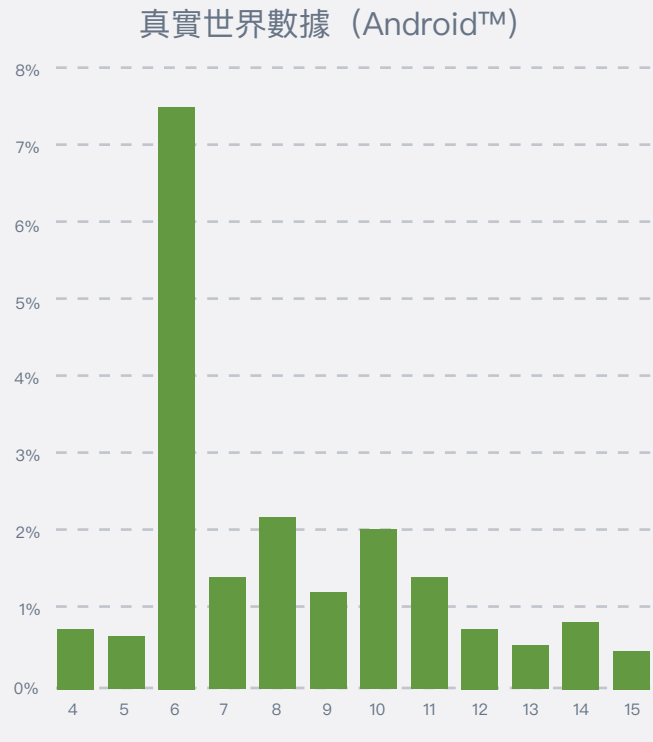


圖 11：跨版本的攻擊百分比

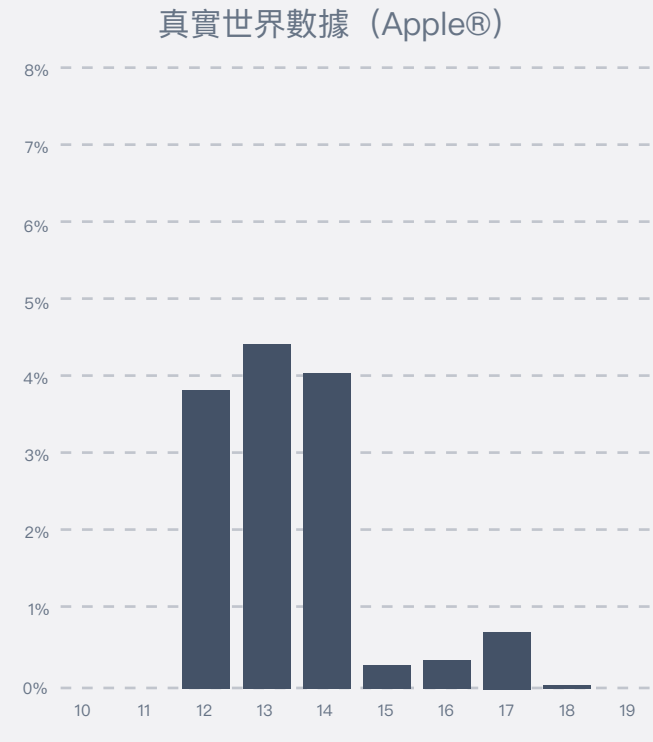


圖 12：跨版本的攻擊百分比

各地區攻擊率差異

攻擊率因地區而異，其中　EMEA（歐洲、中東及非洲）攻擊的比率最高，佔所有應用程式執行個體的 0.69%。其次是北美（0.64%）、拉美（0.58%）和 亞太（0.42%）（見圖 13）。

“更好的檢測和報告可以更清楚地了解威脅形勢。”

- EMEA（歐洲、中東及非洲）攻擊率較高，可能與其金融科技普及率高、監管要求嚴格有關。像 GDPR 這類法規提高了對隱私和安全的重視，使安全計畫更成熟，也提升了攻擊偵測能力。
- 北美攻擊率高，主要因為金融、醫療和科技公司集中。雖然企業在資安上投入不少，但高價值目標經常成為攻擊對象，整體風險仍然偏高，也因此這些投資是合理的。
- 亞太與拉美攻擊率較低，雖然看起來令人欣慰，但也可能因資安實務尚未成熟而缺乏可見性。監管環境 對攻擊可見性影響很大。EMEA（歐洲、中東及非洲）和北美擁有完善的資安法規，促使企業強化防護與偵測能力。相較之下，拉美和亞太的報告與資料安全要求不同，可能攻擊量相當，但威脅的可見性較低。

圖 13：按地區劃分的攻擊率

雖然 遭受更多攻擊並不是好事，但像 EMEA（歐洲、中東及非洲）和北美這類地區 較佳的偵測與通報能力，卻能讓我們對威脅情況有更清楚的了解。從這個角度來看，觀察到的使用者攻擊率較高，可能反而代表當地資安實務較成熟、防護和準備較完善。

監管框架影響網路威脅的偵測　EMEA（歐洲、中東及非洲）與北美洲受惠於已相當完備的資安法規與資料保護要求，這促使受管制的企業強化防護，也因此提升了攻擊偵測能力。相對地，拉丁美洲與亞太地區的實際攻擊量可能相近，但由於當地法規架構不同，對這些威脅的可見度較低。

這種看似矛盾的情況顯示：被偵測到的攻擊數較高本質上並不可取，但可能代表偵測與通報機制較完善。因此，通報數較低的地區（如拉丁美洲與亞太地區）未必更安全，而可能只是威脅偵測較不具可見度。從這個角度來看，EMEA（歐洲、中東及非洲）與北美洲相較於拉丁美洲和亞太地區可被視為處於較高的資安水準；此外，也可以說 電信產業 相較金融服務業在資安準備上更有優勢，因為其攻擊可見性更高。

惡意軟體

到目前為止，本報告討論的是一種非常特定的威脅，也就是財富 500 強公司（Fortune 500®）都在積極防護的威脅，同時也被 OWASP® 標示為對應用程式「韌性」的威脅。

然而，對最終使用者開發應用程式的企業來說，實際的威脅環境遠比這複雜，除了 OWASP 的 MASVS 中都有被標記清楚各種不同類型的威脅外。

其中一類額外威脅是在端點運行的惡意軟體（malware）。惡意軟體會對使用者造成多種問題，許多安全廠商都有製作了描述相關紀錄與報告。而本報告則專注於惡意軟體對 Digital.ai 客戶所開發應用的威脅。

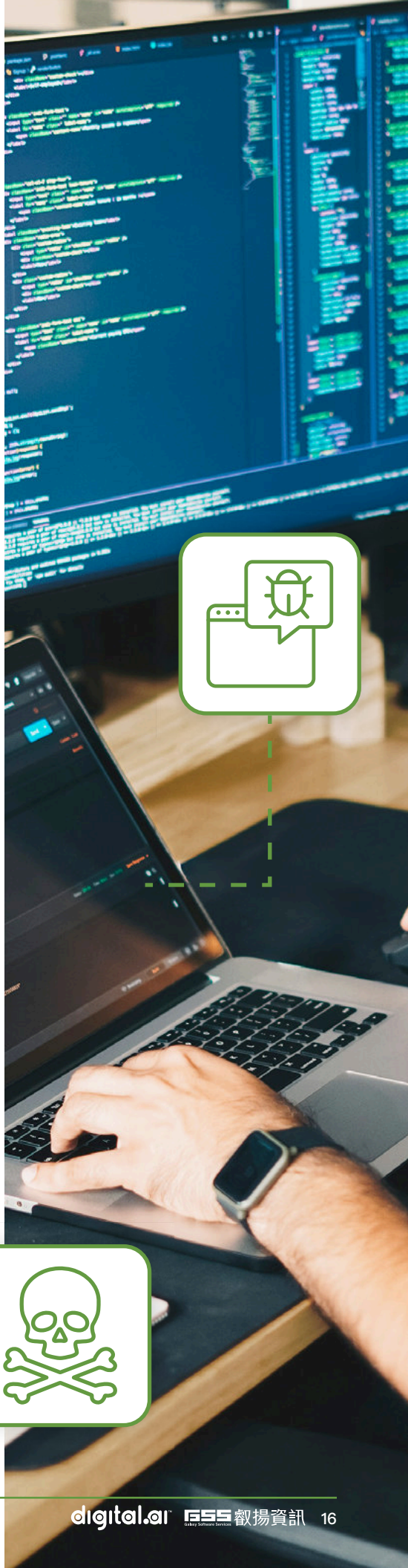
Digital.ai 用「惡意套件偵測（Malicious Package Detection）」的功能來追蹤這些惡意軟體。

根據今年 1 月的觀察，Digital.ai 發現 約 1.2% 的受監控裝置感染了某種惡意軟體，可以進一步分成以下幾類：

威脅等級	百分比
High	6.94%
Medium	10.65%
Low	83.77%

被歸類為高威脅等級的惡意軟體涵蓋多種類型，包括銀行木馬（banking trojans）、間諜軟體（spyware）、病毒（viruses）和蠕蟲（worms）。

作為應用程式的創建者，你的應用可能運行在一些同時也被惡意程式感染的 Android 裝置上。這些惡意程式有的看似無害，但也有可能造成嚴重危害。根據我們的研究，約 6.94% 的惡意軟體屬於高威脅，包括銀行木馬、間諜軟體、木馬、病毒與蠕蟲等。



結論

並不是每個檢查門鎖的人都是入侵者；例如，鎖匠可能只是想確認門鎖是否運作正常。然而，如果一個社區裡絕大多數的門鎖都被檢查過，住戶自然會想知道誰在檢查，以及他們的意圖為何。

應用程式的攻擊率已達到前所未有的水準：2025 年 1 月，有 82.7% 的受監控應用遭到攻擊，這凸顯了這些威脅的持續性和不斷演變的特性。

> **組織再也承擔不起不鎖門或依賴劣質門鎖的風險。**

雖然金融服務與電信仍然是主要攻擊目標，但隨著各產業採用行動優先和軟體定義生態系統，醫療與汽車應用也開始同樣面臨高風險。透過觀察 Android™ 與 Apple® iOS 平台的攻擊持續上升，可發現攻擊者利用運行時修改（runtime instrumentation）、環境操控（environment manipulation）以及完整性破壞（integrity compromise） 等手法來進行規避安全防護。而不同區域的攻擊率差異顯示，法規與資安成熟度可能會影響攻擊偵測能力，例如 EMEA 和北美的攻擊率通常高於 LATAM 與 APAC。

我們身處這個脆弱的「行動應用數位社區」中，企業再也不能放任門鎖不鎖或依賴低標準的防護。就像保護整個社區需要警覺的居民、堅固的防線以及先進的監控一樣，行動資安也必須採取多層、主動的防護措施。對於高階攻擊者而言，就像面對鍥而不捨的竊賊一樣——他們會探查每一個弱點。因此，企業必須部署先進混淆技術、防篡改措施、強加密、運行時保護，並進行持續監控，以加強數位防線，抵禦日益頻繁且精密的入侵行為。

Digital.ai 的應用程式安全解決方案提供具成本效益、易於實施、且非常有效的防護，以抵禦各種攻擊。隨著威脅持續演變，Digital.ai 不斷擴展防護能力、識別新興攻擊手法，並簡化部署流程——讓強而有力的應用程式安全不只是必要的，更是每個企業都能輕鬆取得的保障。

附錄

本報告的數據蒐集自 2025 年 1 月，涵蓋由 Digital.ai 所保護的 App；其客戶遍及全球、橫跨所有主要產業（銀行、媒體、電信、製造、遊戲與資安）。如有問題或建議，請聯絡：Daniel.Shugrue@digital.ai

為企業打造的 AI 驅動軟體交付平台。

- **整合與擴展**——整合工具、精簡應用程式交付，並可在任何環境擴展。
- **自動化與安全**——啟用可擴展的行動應用程式測試與安全機制。
- **降低風險**——藉由洞見威脅，確保應用程式的安全及品質。
- **最佳化與加速**——資料集中化，實現更快、更安全的交付。