行動裝置、應用程式和物聯網安全

保護全球資料和裝置

隨著國家支持的網路攻擊和網路惡意行為者急劇增加，我們相信我們的產品和服務只有在安全的情況下才能發揮作用。在 Google，我們比以往任何時候都更著重在保護民眾、組織和政府，透過分享我們的專業知識， 賦能社會，讓社會應對不斷變化的網路風險，且致力於推動網路安全的技術， 為每個人打造更安全的世界。

因此，我們必須保持領先地位，不斷改善我們的安全解決方案，以應對與日俱增的威脅情勢，特別是在保護所有連線裝置和應用程式方面，為消費者提供安全的環境，讓他們在使用的裝置上有代理權和選擇權。

挑戰

網路連線是有代價的

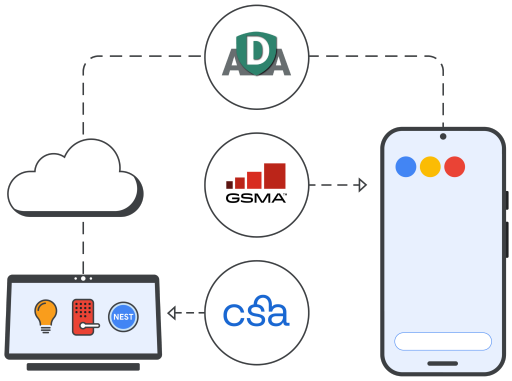
我們日常生活中的大部分時間都是在智慧型手機、應用程式和物聯網裝置上度過，花在網路上的時間越來越多，在此過程中也互相分享越來越多有價值的資料，例如銀行或醫療資訊。正因為如此，老練的網路犯罪分子比以往任何時候都更加鎖定這些裝置，以獲取敏感資訊。

更多裝置，更多資料，更多威脅

世界上現在估計有 170 億個物聯網裝置，從印表機到車庫門開啟器，每一個裝置都搭載了軟體 (有些是開源軟體)，很容易被駭客攻擊。[1] 整體而言，遭入侵的物聯網裝置數量在 2020 年幾乎增加了一倍。[2]

- 儘管我們的生活正與物聯網裝置建立密不可分的關係，但目前沒有評估連線產品安全品質的全球標準，使得消費者會做出缺乏根據的裝置安全決策。
- 消費者應有權擁有他們數位產品的透明度，就像他們有權知道自己購買的食品或清潔用品中含有哪些成分一樣。
- 行動裝置只是攻擊面向中的其中一個載體，裝置的互連性增加了對大規模安全透明性的需求。因此，連線裝置生態系統的安全與網路和系統的安全同樣重要。

我們與產業組織的合作



我們的解決方案

在 Google，我們透過行動裝置、應用程式和物聯網安全來提高連線裝置的安全性和透明度：

行動裝置安全

我們的開源作業系統 Android 利用分層安全方法來確保行動裝置的安全：

- 分層安全
  - 開機驗證、回滾保護和恢復出廠設定防護確保裝置上為最新、最安全的 Android 版本。
  - PIN 和生物認證可防止外部入侵。
  - 「尋找我的裝置」有助於定位裝置或者在裝置遭竊或遺失時將資料清除。
- 身分和密碼保護
  - 兩步驟驗證、手機作為安全金鑰和密碼管理器保護您的 Google 帳戶免受外部入侵。
  - 安全檢查和選用的進階保護能讓裝置安全流暢地運行。
- 反網路釣魚保護
  - Phone by Google 和 Messages by Google 有助於檢測並防止詐騙和網路釣魚攻擊。
  - Google 安全瀏覽保護全球超過 50 億台裝置。

應用程式安全

開箱即用的反惡意軟體能將惡意應用程式拒之門外，資料安全的資訊在下載應用程式時即能為使用者提供透明度。

- Google Play 商店: 機器學習檢測工具和人工分析師會先檢查所有應用程式後，才開放下載。資訊安全部分會說明應用程式所收集的資料類型，以及這些資料的用途。
- Google Play Protect: 每天掃描超過 1250 億個應用程式，並在檢測到安全風險時通知、刪除或停用。
- 應用程式防禦聯盟 (ADA): Google 與一流的行動裝置威脅檢測合作夥伴一同推出了應用程式防禦聯盟，透過共享情報和協調檢測來保護 Android 使用者免受潛在有害應用程式 (PHA) 的侵害。

物聯網安全

物聯網安全標籤清楚呈現了裝置上的隱私和安全措施，例如正在收集什麼資料。

- 我們堅持物聯網安全標籤方案的五個核心原則：即時標籤、評估方案、動態調整的安全基準、廣泛的透明度和採用獎勵。
- 我們正與連線標準聯盟 (CSA) 和 GSM 聯盟 (GSMA)合作，制定一個橫跨產業的認證計畫，以符合現有和未來的監管要求。

我們的原則

在 Google，我們應用 3 項核心原則來提高連線裝置的安全性和透明度：

深度防禦: 我們利用協同工作的多層安全架構來建構可平穩、有效運行的強大防禦系統。

公開與透明: 透明度是我們理念的關鍵。透過讓我們的平台使用者了解情況並分享知識，加強我們的防護機制，我們相信開源生態系統比封閉生態系統更安全。

Google 和我們生態系統的精華:
我們與 Google 和整個產業的專家團隊合作，協助保護數十億名使用者的安全。

應用程式

物聯網安全標籤：將控制權交到消費者手中

如果沒有既定的物聯網安全標籤，就沒有裝置製造商可以遵循的全球標準。使用者也無法了解他們的裝置是否有保護他們的資料。此產業需要齊心協力推動物聯網安全的發展，並將控制權重新交到消費者手中。我們正透過我們的流程和合作夥伴關係制定物聯網安全標籤計畫。

首先，我們投入外部安全研究，查明可能的漏洞 (Google Nest 參與了 Google 漏洞獎勵計畫，並為發現漏洞的非 Google 安全研究人員提供獎勵)。
從那時起，我們會在發布後至少五年內提供關鍵錯誤修補程式和錯誤修正。
我們在 2019 年及之後開發的所有裝置上都使用開機驗證，確保運行正確的軟體，且保護存取安全。例如，我們的 Google Nest 裝置使用產業認可的第三方安全標準進行驗證，例如 NIST、 ETSI 和 ISO 開發的標準。

這些標準和我們的安全軟體開發生命週期 (SDLC) 降低了消費者暴露於不良安全實踐的可能性，並為開放、更安全的網際網路鋪路。

我們的產業投資和里程碑

2007 **已建立安全瀏覽**，在使用者存取危險網站時主動提醒，現累計保護了超過 50 億台裝置。

2010 **已發布 Google 透明度報告**，顯示政府和公司的政策和行動如何影響隱私、安全和線上資訊存取。2018 年，我們特別針對 Android 新增了透明度報告。

2017 **已推出 Google Play Protect**，這是目前部署最廣泛的反惡意軟體解決方案，每天掃描 30 多億台裝置上超過 1250 億個應用程式。

2019 **已推出安全金鑰**作為 Android 的內建功能，並在 2020 年引入 iPhone。

2022 **已啟動 Google Play** 資料安全專區，向民眾提供有關應用程式如何收集、分享並保護使用者資料的更多資訊，並透過應用程式防禦聯盟開始實行第一個徽章系統，對已完成獨立安全審查的應用程式發放徽章。

2023 **密碼：無需密碼的未來**，在與 FIDO 聯盟和全球技術領導者一起推動開源標準十年後，透過擴展金鑰支援，正在開啟無需密碼的未來。

我們的方法

致力於開放、安全的數位世界

各個網路會出現更多裝置，裝置上會有更多資料，安全問題只會隨之加劇。我們正在透過產品開發、透明度標準和產業合作夥伴關係，將連線裝置推向安全的未來

我們產品戰略的基石是確保產品在預設情況下皆是安全的。安全瀏覽、Google Play Protect 和內建安全金鑰可保護行動裝置和應用程式，為我們的產品提供最高級別的安全防護。

我們在解決問題和分享連線裝置安全知識方面保持公開透明，從而達成安全營運大眾化。我們相信，採用我們的分層安全方法，開源生態系統能夠比封閉生態系統更加安全。

透過與 CSA、ADA 和 GSMA 的合作，我們努力推動網路安全領域的最新發展，為所有人打造更安全的網際網路和未來。

我們致力於提升連線裝置的安全標準，並為每個人、每個地方更安全的連線環境建立標準。
了解更多 Google 在連線裝置安全方面的進展: g.co/connecteddevicesafety

資料來源: [1] CNBC 網路報告，2023 年 1 月 9 日, [2] 什麼是物聯網攻擊？物聯網安全的來龍去脈，2021 年 7 月 20 日