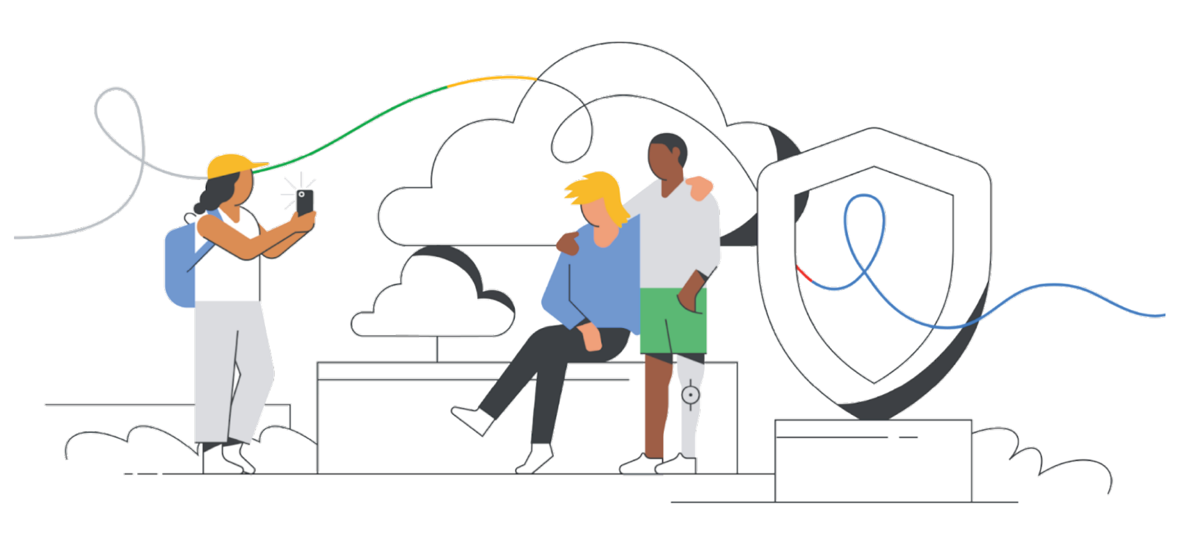
我們多年來的網路安全旅程

Safer with Google

Google 每天努力不懈，要讓每個人都能 安全 使用網路

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加著重在保護民眾、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。



歷久彌新，不斷創新

自 2004 年推出 Gmail 到 2022 年推出防護運算以來，Google 一直是網路安全技術的先驅，並在產品、平台和合作夥伴關係方面不斷創新，以消除各類威脅，透過以下方式為民眾、組織和社會創造更安全的未來：

- ✓ 開發安全的產品和平台
- ✓ 建立敏捷的安全團隊
- ✓ 促進計畫和夥伴關係
- ✓ 為創新和勞動力教育訓練提供關鍵資金

隨著民眾需求和網際網路發展的演變，我們將繼續走在新技術的前沿，減少不斷變化的網路威脅，確保 Google 帶給各位的每一天都更加安全。

2004 年，Gmail 垃圾信件防護

我們是最早建構 AI 驅動的電子郵件防護的公司之一。

99.9% 的危險和可疑電子郵件會由 Gmail 封鎖

2007 年，安全瀏覽

在 2020 年，我們在使用者存取危險網站時提醒他們，將這些線上保護措施發展為安全瀏覽強化防護功能，從而主動保護世界各地的裝置。

50 億台裝置擁有安全瀏覽 保護

2008 年，Google 密碼管理員

密碼管理員的推出讓登入變得更輕鬆、更安全，無須記住或輸入密碼，現在 50% 的跨平台 Chrome 登入都使用密碼管理員。

每天 檢查 10 億個密碼是否存在漏洞

2009 年，reCAPTCHA

我們制定詐騙和機器人程序管理解決方案，以阻止憑據填充和帳戶接管，並防止惡意軟體/假冒使用者的濫用活動。

為 500 萬個網站提供 防護

2010 年，零信任

在歷經極光行動 (一系列有組織的網路攻擊) 的危機之後，我們徹底改變了做法，建立安全預設架構，現在被稱為「零信任」。這個架構能確保出現更少的攻擊媒介、更少丟失資料的機會，以及對使用者所依賴系統進行更多控制。我們支持白宮在聯邦政府部門推行零信任模型的努力，並將其整合成 BeyondCorp Enterprise，供所有企業使用。

2010 年，威脅分析小組 (TAG)

在極光行動之後，我們成立了專門的專家團隊，負責檢測、分析並破壞政府支持的重大犯罪網路威脅。TAG 追查出北韓是 Wanna Cry 史上最大勒索軟體攻擊事件的源頭，最近也分享了來自印度、俄羅斯和阿拉伯聯合大公國的駭客僱傭生態系統的案例。

2010 年，Google Bug Hunters

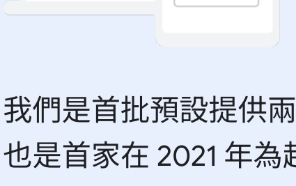
我們的漏洞獎勵計畫提供現金獎勵，吸引了高中生、律師、IT 專業人士和業餘愛好者來挑出 Google 產品中的錯誤。他們的動機各不相同，但使命不約而同都是找到未被發現的漏洞，以確保網路服務的安全。

自 2010 年起，支出了數百萬美元的獎勵

2010 年，紅隊

發起對抗性思維並破解 Google，幫助強化我們的防禦和加強發現漏洞的能力。他們的工作遍布全球，以跟上當前的威脅，改善安全控制，進行攻擊檢測/預防，並透過推動更新和更完善的框架來消除所有類型的漏洞。

2011 年，兩步驟驗證



我們是首批預設提供兩步驟驗證 (2SV) 的公司，也是首家在 2021 年為超過 1.5 億人自動啟用 2SV 的公司之一，提供安全簡便的登入方式。即使您的密碼遭竊，您的帳戶也會受到保護。

自推出 2SV 以來，遭攻擊的帳戶減少了 50%

2013 年，Project Shield

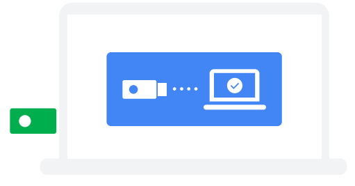
Project Shield 能識別威脅，並在安全社群和執法部門中做出回應，以保護 100 多個國家/地區中的新聞、人權組織、選舉網站、政治組織和競選活動免受分散式阻斷服務 (DDoS) 的攻擊。

目前在烏克蘭有 超過 150 個網站受到 保護

2014 年，Project Zero

一個致力於在網際網路上搜尋零時差漏洞的專門工作小組，包括軟體、硬體、Google 產品等方面，以確保安全和開放的網際網路。他們是第一批詳細介紹「熔毀」和「幽靈」漏洞的人，使開發人員能夠快速解決 CPU 漏洞，接著在整個軟體供應鏈中應用減緩措施。

2017 年，進階保護計畫 (APP)



為記者和政府官員等高知名度和高風險使用者提供額外的安全保護，包括安全金鑰。

超過 300 個聯邦競選活動受到 保護

2017 年，Google Play Protect

Google Play Protect 是全球部署最廣泛的行動裝置威脅防護服務，透過 Google 的機器學習不斷調整並改善，能自動掃描應用程式中的惡意軟體，以及替 Android 手機上的使用者付款加密。

每天掃描超過 1000 億個應用程式，找出惡意軟體

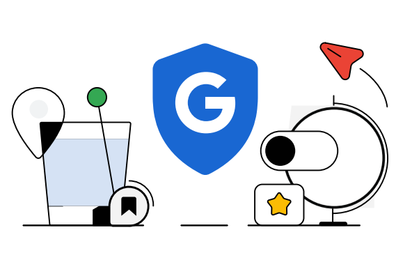
每日替 1.5 億名使用者的付款 加密

2018 年，Titan 安全金鑰

我們為需要端對端 Google 解決方案的使用者製作了 Titan 安全金鑰。這些金鑰符合 FIDO 標準，也可以在 Google 以外的其他地方使用。

2019 年，無密碼重新認證

擴展了我們在 Android 中的 FIDO 支援，因此使用者可以僅使用 PIN 或生物辨識無縫登入網站，無需密碼。



2019 年，Chronicle

作為我們核心基礎設施之上的專用層級，我們導入 Chronicle 以提供雲端安全，專為企業私下保留、分析並搜尋大量安全和網路資料而設計。

2021 年，投資進階網路安全

我們致力於加強網路安全，擴大零信任計畫，協助防護軟體供應鏈，並加強開源安全。我們承諾透過 Google Career Certificate 計畫，在 IT 支援和資料分析等領域訓練 100,000 名美國人。

投入 100 億美元，用於網路安全計畫

2021 年，Google 開源安全團隊 (GOSST)

GOSST 的成立是為了提高世界所依賴的開源軟體的安全性。我們與開源安全基金會 (OpenSSF) 合作，推出軟體工件供應鏈級別 (SLSA)，這是一個保護軟體供應鏈並為整個軟體生態系統實現長期安全性的框架。

投入 1 億美元，用於第三方開源安全操作，協助修復漏洞

2021 年，機密運算

針對關鍵的安全、安全和隱私，我們推出了 Google Cloud 機密運算，這是一項突破性技術，可在處理資料時對資料加密，從而使其在整個生命週期內保持安全，包括靜止或傳輸過程中。現在，即使是最敏感的資料也可以安全無虞地遷移至雲端。

2022 年，後量子密碼學標準化

著眼於未來，我們繼續開發下一代密碼系統，以防止公鑰密碼系統遭破解和數位通訊受到損害。美國國家標準與技術研究院選擇了 Google 參與的產品 (SPHINCS+) 進行標準化。

2022 年，防護運算

我們發布了防護運算，這是一個不斷發展的技術工具箱，改變了資料處理的方式、時間和地點，從技術上確保使用者的隱私和安全。我們透過資料足跡最小化、對資料進行去識別化和限制對敏感資料的存取來落實防護。這代表 Android 可以建議打字時的下一個字詞，同時保持對話的機密性。

2022 年，麥迪安和 Google Cloud

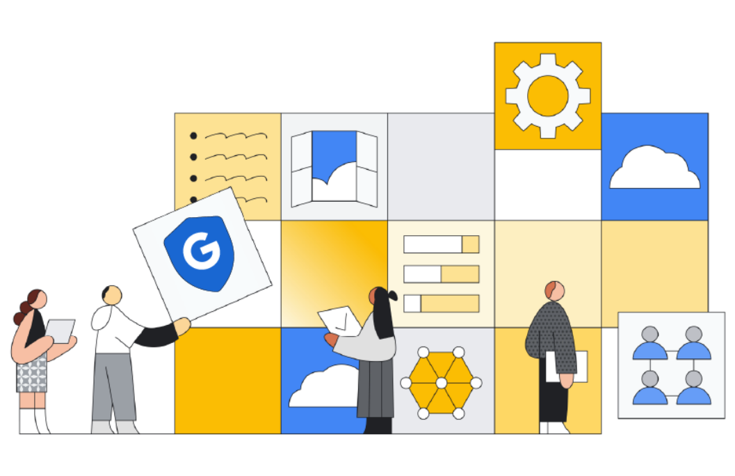
麥迪安與全球最大組織一起從事網路安全前工作，帶來即時、深入的威脅情報。結合 Google Cloud 的雲端原生安全產品，我們幫助企業和公部門機構在整個安全生命週期中受到保護。

2023 年，Passkey：無需密碼的未來

十多年來，我們一直在為無需密碼的未來奠定基礎。我們在 2013 年加入 FIDO 聯盟，以推動無需密碼世界的開放標準，而 2023 年以金鑰技術將我們對 FIDO 登入標準的支援擴展到 Android 和 Chrome，我們最終將擁有一個真正無需密碼的未來平台。

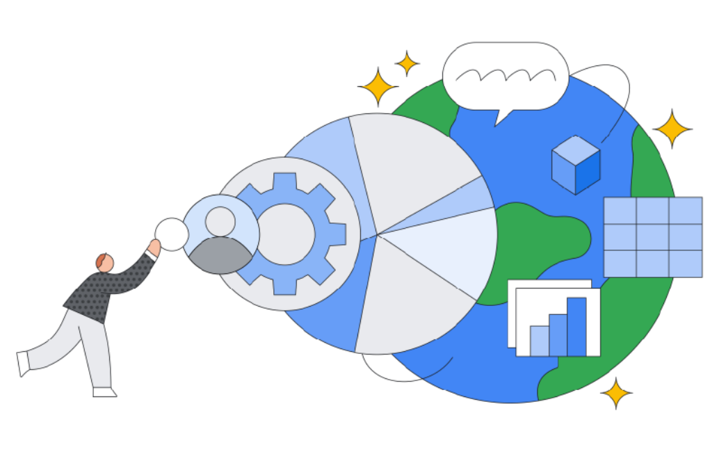
在技術範圍不斷擴大的時代，
對技術的信任是發揮社會真正潛力的關鍵。

在將安全知識付諸實踐的過程中，我們將繼續與個人、
企業和政府合作，保護他們的安全，
並推動網路安全的新紀元。



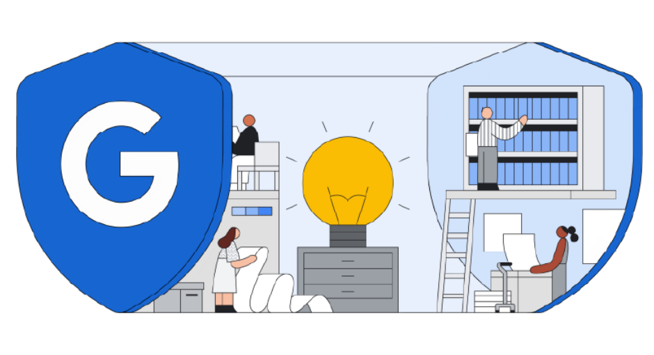
保護民眾、企業和政府

安全是我們產品策略的基石。
這就是為什麼我們所有的產品都具有內建防護，
在預設情況下是安全的。



賦予社會能力來應對不斷演變的網路安全風險

我們賦予社會能力，解鎖開源的潛力，
並與業界透明地共享我們的知識和專長，
以保持生態系統的安全。



推進未來技術

我們希望保護社會免受下一代網路的威脅。基於我們的 AI 專業知識，
我們正在設計下一波架構，以突破安全創新的界限。

Google 讓您的每一天都更加安全

前往 g.co/safety/cyber