Google Workspace

更安全的選擇

借鑑 Microsoft 重大網路安全事件，Google Workspace 是更安全的選擇。

目錄

內容提要

Microsoft 的資安問題層出不窮，近期一連串備受關注的事件更將客戶置於險境。其中一起事件就發生在 2023 年夏天，當時有個名為 Storm-0558 的組織入侵了美英兩國政府高官的帳戶，導致 22 個機構、500 多人及數萬封電子郵件的資料遭到竊取。美國國土安全部的網路安全審查委員會 (CSRB) 為此發布一份詳細報告，指出 Microsoft 的「一連串安全問題」[1] 是這起資料侵害事件的根本原因。這份報告詳盡揭示了 Microsoft 長期存在的系統性問題，以及「忽視企業安全投資與嚴格風險管理重要性的企業文化」[2]。

繼 Storm-0558 入侵事件後，2023 年 11 月 Microsoft 再次發生資料侵害事件，促使 CISA 發布 ED 24-04 緊急指令應對，而這次事件與上次僅相隔短短數月：「名為『午夜暴雪』(Midnight Blizzard) 的國家級網路駭客成功入侵 Microsoft 公司電子郵件帳戶，導致聯邦政府各民事執行單位 (FCEB) 與 Microsoft 之間的電子郵件通訊資料外洩。」[3]

Microsoft 屢屢遭遇資安危機，迫使企業與公部門機構尋求更好的替代方案。我們相信，Google Workspace 憑藉卓越的工程實績、深耕先進防禦措施的具體作為，以及將保護客戶安全視為重大責任的透明文化，是安全性更勝一籌的選擇。

這樣的信念是一次次實戰累積的經驗所鑄就。我們深知，任何機構都無法確保完全抵禦精明狡猾的攻擊者。事實上，這批政府資助的攻擊者早在 2009 年就攻擊過 Google，促使我們大規模採取安全改進措施，並獲得 CSRB 報告認可：「Google 也對基礎架構進行了全面安全檢修。」[4]

本白皮書簡要分享了 Google 安全策略的發展歷程，並詳細介紹 Google Workspace 的控管措施和安全防護優勢，包括 Gmail、Google 雲端硬碟、簡報、文件、Meet、Chat 等應用程式。

注意：本白皮書適用於 workspace.google.com 介紹的 Google Workspace 產品。內容是根據截至 2024 年 5 月的資料撰寫，反映當時現況。文中提及即將推出的功能，不代表確定具體的發布時間表。 Google 會持續加強客戶資料保護措施，因此相關的安全政策和系統可能在日後有所變動。本白皮書介紹的產品功能是否可用，取決於各個 Google Workspace 版本產品提供的授權。

Microsoft 資安問題模式

Microsoft 是如何被入侵的？

2023 年夏天，名為 Storm-0558 的駭客組織在中華人民共和國政府的資助下，成功入侵 Microsoft 系統並竊取了簽署金鑰，「這使得 Storm-0558 基本上取得了全世界所有 Exchange Online 帳戶的完整存取權」[5]。這起資料侵害事件導致美國高階政府官員的電子郵件帳戶遭到未經授權存取，包括負責國安事務的國務院、商務部、眾議院、駐中華人民共和國大使在內，全球另有 22 個機構與 500 多人受到波及。

Storm-0558 取得的簽署金鑰「作用是對遠端系統進行安全驗證，而這對任何雲端服務供應商來說，都是加密的關鍵要素」[6]。簽署金鑰就好比能打開飯店所有房間的萬能鑰匙，只要得到它，到哪裡都暢行無阻。由於在 Microsoft 系統中，不同類型的帳戶可以信任相同的金鑰，所以單一入侵事件可能同時影響到消費者、企業和政府帳戶。「截至本報告發布時，Microsoft 仍未得知 Storm-0558 取得簽署金鑰的方式和時間點」[7]。

CSRB 指出：「遺失簽署金鑰本身已是嚴重問題，但如果不清楚金鑰遺失的具體方式，影響將更加深遠，因為這表示受害公司無法確定自家系統是如何遭到入侵，相應的安全漏洞是否已補上。」[8] 綜觀各大雲端服務供應商發生過的事件，這是迄今為止影響最嚴重的資料侵害事件之一。CSRB 將這起事件描述為「價值不斐的間諜活動」[9]。

短短幾個月後，2023 年 11 月，另一個由俄羅斯政府資助的駭客團體「午夜暴雪」利用密碼噴灑攻擊，大舉入侵 Microsoft 公司的電子郵件帳戶，受害者包括高階主管、資安、法律和其他團隊[10]。該團體取得了美國政府官員的電子郵件通訊資料。Microsoft 在 2024 年 3 月表示，午夜暴雪從 2023 年 11 月發動的攻擊在歷經五個月後仍未結束，而 Microsoft 尚未提出解決問題的時間表：「最近幾週有證據顯示，午夜暴雪正利用當初從我們公司電子郵件系統竊取的資訊，獲取或試圖獲取未經授權的存取權，藉以進入公司部分原始碼存放區和內部系統。」[11]

這些入侵事件只是意外嗎？

這類攻擊的嚴重性不可小覷。發生地緣政治衝突時，外國攻擊者若能存取政府通訊資料和系統，就能利用這些資源進行間諜活動或攻擊重要基礎設施，可能對政府和民眾造成嚴重影響。

未能優先重視資安與風險管理

CSRB 對 Storm-0558 入侵事件的結論是「這次入侵原可預防，根本不應該發生」[12]，理由是「Microsoft 的安全文化不夠完善，需要徹底改革。尤其是，考慮到該公司在全球技術生態系統中的核心地位，以及客戶願意託付資料與營運的信任程度，這樣的要求十分合理」[13]。

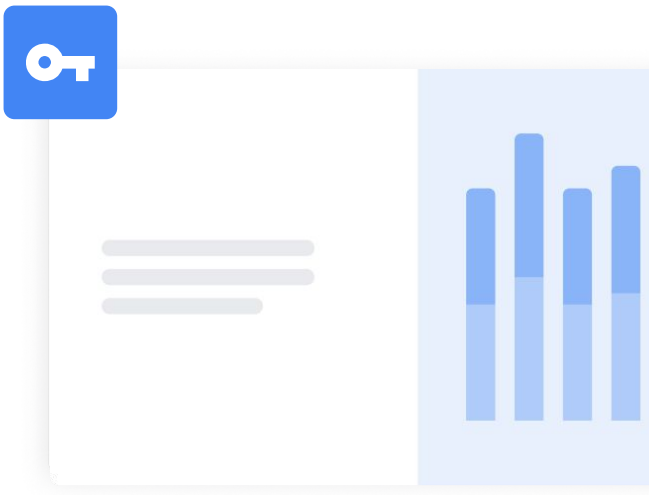
未能更正不正確的公開聲明

CSRB 也對 Microsoft 處理事件的方式表達嚴重關切，因為 Microsoft 在事件發生後「未能及時更正不正確的公開聲明」[14]，直到「委員會完成審查並反覆向 Microsoft 詢問更正事宜後」[15]，Microsoft 才予以更正。結果，「此次入侵事件後，Microsoft 客戶仍無法取得基本資訊，無力針對 Microsoft 雲端環境的安全性進行風險評估」[16]。

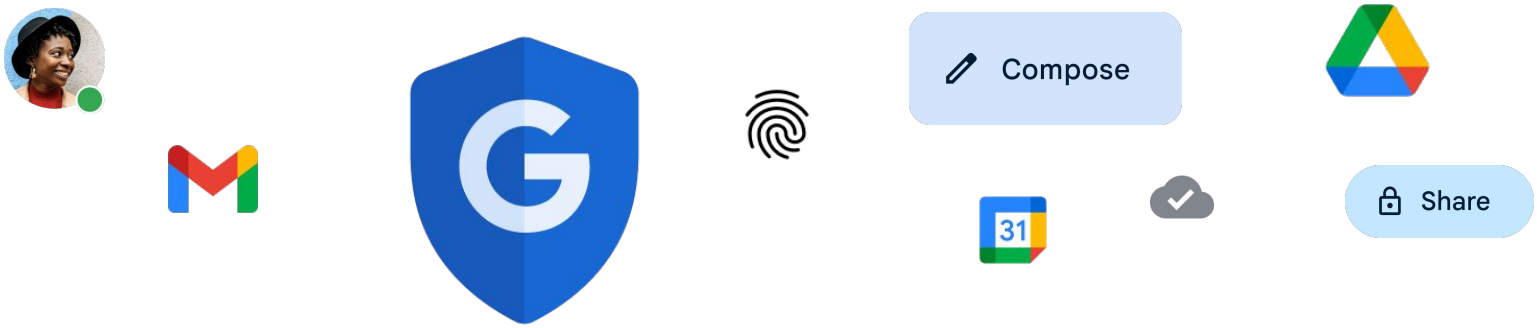
未能確認金鑰遺失途徑

事實上，由於 Microsoft 至今尚未找出根本原因，所以能否防止這類事件再次發生，仍為未知數。「儘管 Microsoft 曾於 3 月 12 日發布更新，但在委員會審查結束時，Microsoft 仍未找到包含 2016 年 MSA 金鑰的當機傾印檔，或金鑰曾被不當移動的任何證據」[17]。此外，「委員會評估，Microsoft 並未掌握 Storm-0558 取得 2016 年 MSA 金鑰的途徑」[18]。

即便任何機構都可能遇到精明狡猾的攻擊者，但證據清楚顯示，Microsoft 無法確保自身系統與客戶資料的安全。



Google Workspace
為您開拓更安全的道路



不同凡響，
更安全的解決方案

Google Workspace 是以業界最佳實務做法為基礎，根據嚴格的隱私權和安全性標準打造而成：

- 以瀏覽器為基礎的雲端優先技術會持續更新，且無需仰賴本機裝置、原生應用程式或電子郵件附件。
- 內建採零信任機制的控制選項、加密功能和驗證程序，讓人員可以在任何地方工作，無須使用 VPN。
- 防護體系遍布全球，能抵擋網路釣魚、惡意軟體、勒索軟體和供應鏈攻擊，妥善保護貴機構資訊安全，而且無須安裝外掛程式。Gmail 能阻止超過 99.9% 的垃圾郵件、網路釣魚內容和惡意軟體進入您的收件匣。Gmail 平均偵測到的惡意軟體數量是標準第三方防毒軟體的兩倍以上。
- 為所有人提供更完善的保護，包括採用無需安裝修補程式的安全端點 (公司提供的裝置或自攜裝置)，並採取嚴格的帳戶接管防護措施。融入安全考量的設計，預設的安全防護功能。

Google 與眾不同的安全方針之一，在於我們長期投入大量精力，使系統和產品面對這類攻擊時，具備強韌的復原力，而這點已獲得 CSRB 報告認可：「Google 改造了身分系統，盡可能採用有狀態的權杖。也就是說，Google 會在發放每個憑證時指派專屬 ID，並記錄在資料庫中。根據這些專屬 ID，就能判斷收到的憑證來源是否為 Google。Google 也盡可能實施全自動的金鑰輪替機制，並限縮無狀態權杖的驗證期，不讓威脅行為者有充分時間找出及取得有效金鑰。Google 也對基礎架構進行全面安全檢修，包括為保護這些身分系統，導入零信任網路架構，以及硬體支援、符合快速網路身分識別協定 (FIDO) 的雙重驗證 (2FA)。」[19]

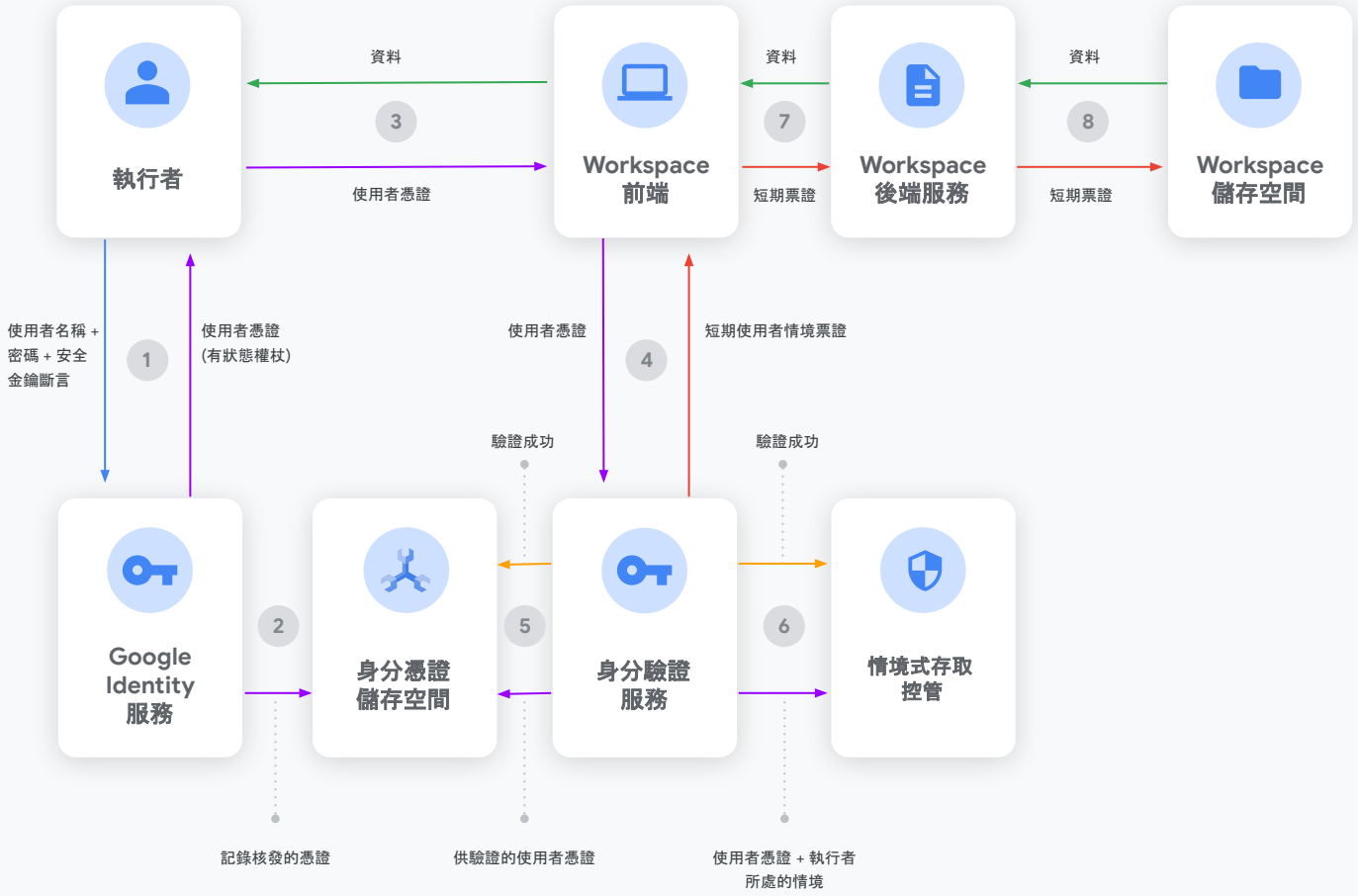
正如 CSRB 指出的，Google 會盡可能利用有狀態的權杖。讓我們進一步解釋這個概念：

- Google Identity 服務會驗證使用者的登入資料，然後將 Cookie 或 OAuth 權杖之類的使用者憑證發送到裝置上。這個憑證會記錄在 Google 的身分憑證儲存空間，並被視為有狀態的憑證。該裝置之後每次向我們的基礎架構提出要求，都必須提供這個使用者憑證。

- 當服務收到使用者憑證，就會將憑證傳遞至身分識別服務，驗證是否為已發布的有效憑證。如果使用者憑證通過驗證，身分識別服務就會傳回短期的使用者情境票證，此票證可用於與使用者要求相關的遠端程序呼叫 (RPC)。之後，對於任何衍生性呼叫，呼叫服務都可以將使用者情境票證做為 RPC 的一部分傳送給受呼叫者。這些票證只能在 Google 內部正式環境中使用。

Google 的有狀態身分識別權杖融入安全考量設計，可透過防止偽造憑證來保護使用者帳戶。即使外部攻擊者竊取加密編譯金鑰，也無法直接使用金鑰存取使用者資料。Google 在授予任何使用者資訊的存取權之前，會透過獨立程序驗證這些權杖是否由其核發。

有狀態權杖的概念架構流程



採用有狀態權杖不是我們保護客戶資料安全的唯一措施。《Google 基礎架構安全性設計白皮書》詳細介紹了我們堆疊中每一層的安全考量，從硬體到用戶端，包括實體安全與人員控管。BeyondProd 也在其中，這是 Google 在基礎架構中實施零信任原則的方法，信任依據是程式碼來源、信任的硬體、服務身分等特徵，而不是 IP 位址或主機名稱等正式環境網路中的位置。採用 BeyondProd，表示服務之間不會預設相互信任；網路邊緣保護措施將隔絕網路攻擊，確保工作負載安全。此外，我們會在所有服務中實施一致政策。如要近一步瞭解這個基礎架構模型的演變過程，請參閱 BeyondProd 白皮書。

深厚的安全文化

Google 是 2009 年極光行動 (Operation Aurora) 的攻擊目標之一，這是中國資助的一連串網路攻擊。我們認為此次行動的幕後黑手，正是 2023 年夏天入侵 Microsoft 的 Storm-0558 組織：「業界認為，Storm-0558 與 2009 年曾攻擊 Google 等二十多家公司的極光行動有關。」[20]

要說最近影響 Microsoft 與客戶的事件與 Google 十多年前遭遇的入侵事件有何不同，那就是我們秉持維護數十億人安全的使命感，徹底改變了看待網路安全的方式。

> 「極光行動是 2010 年由中國向美國民間公司發起的一連串網路攻擊。威脅行為者藉由網路釣魚活動，入侵 Yahoo、Adobe、Dow Chemical、Morgan Stanley、Google 和另外二十多間公司的網路，竊取商業機密。Google 是當時唯一承認受害的公司，並向大眾揭露，某些中國人權社運人士的 Gmail 帳戶遭到入侵。Google 也公開指出這起事件是中國所為，而其他公司為避免影響進入中國市場的機會，一般不會這麼做。極光行動被視為網路戰近代史上的里程碑事件，因為大眾從此意識到網路戰是產業間諜活動的一項手段。此後 Google 便停止在中國的業務，僅保留香港的本地化版本搜尋引擎。Gmail 遭入侵的事件也促使我們採取行動，當使用者帳戶被國家級攻擊者鎖定或入侵時，Google 就會發送通知。後來其他電子郵件服務供應商也紛紛效仿這種做法。」[21]
>
> **極光行動 - 美國外交關係協會**

在「Transparency in the shadowy world of cyber attacks」這篇網誌文章中，我們分享了自身的經驗教訓：「極光行動不僅讓我們瞭解到資訊公開的必要性，我們也學到了更重要的一課：就安全架構而言，哪些措施有效，哪些措施則不起作用。」[22]

在 CSRB 提供建議前，我們的方法已能幫助客戶、機構和政府快速應對，減少威脅行為者的可趁之機。這樣的安全文化落實在我們與客戶互動的方式，同時也決定了工程決策的優先順序及產品投資的策略。

具體來說，我們發起了名為 BeyondCorp 的內部計畫，開創「零信任」與「縱深防禦」的概念，讓每個人員能透過不受信任的網路工作，無須使用 VPN。如今，世界各地的機構都採用相同的做法，將存取控管設定從網路邊界轉移到個別使用者與資料。

深度整合 零信任控管機制，保障客戶安全

Google Workspace 讓客戶得以在 Google 的深層控制基礎上，進一步落實 BeyondCorp 概念，配置額外的資料保護層。這些保護措施十分貼近 CISA 的零信任成熟度模型，其中包括：

密碼金鑰和安全金鑰：

為防止使用者憑證外洩，密碼金鑰是一種不需要密碼的登入方式，能在網站和應用程式中提供安全便利的驗證體驗，讓使用者在手機、筆電或桌機上，使用指紋、臉部辨識或其他螢幕解鎖方式登入。安全金鑰提供防範網路釣魚的硬體式雙重驗證 (2FA)，有助保護高價值使用者。

情境感知存取權 (CAA) 和 BeyondCorp Enterprise (Chrome Enterprise)：

根據使用者身分、位置、裝置安全性狀態、IP 位址等屬性，建立精細的存取權控管安全性政策。透過 CAA，您可以根據使用者所處的情境 (比如他們的裝置是否符合您的 IT 政策) 來控管存取權。

強大的資料控管措施：

客戶可以利用資料遺失防護、資料分類等工具，識別所屬機構的機密資訊。一旦確立資料的風險狀況，客戶就能對員工採取適當的控制措施 (防止共用、下載)。

我們與 CISA 攜手合作 Secure Cloud Business Applications (SCuBA) 計畫，共同制定基準設定規範。如要進一步瞭解 Google Workspace 的零信任控管機制，建議您參閱《美國民營機構零信任最佳實務指南》和 Google Workspace 安全性與信任網頁。

不僅從技術著手，也重視安全方面的**研究**與**投資**

安全已深植於我們的營運架構。我們的資安團隊囊括全世界最多 產的研究人員，在資訊與應用程式安全防護、密碼學、網路安全和威脅模擬領域各有豐碩成果。我們遵循一流標準，與監管機構和科學界合作制定內部流程，規範工作的各個層面。

我們從整個企業的角度出發，採取全方位措施來保護系統，確保客戶資料安全無虞。例如，我們利用 Chrome Enterprise 控制選項，要求所有人員使用安全金鑰存取系統。Google 投入大量資源來提升安全性，包括承諾在 5 年內投資 $100 億美元，用於強化網路安全、擴展零信任計畫、保障軟體供應鏈安全及提升開放原始碼安全性。

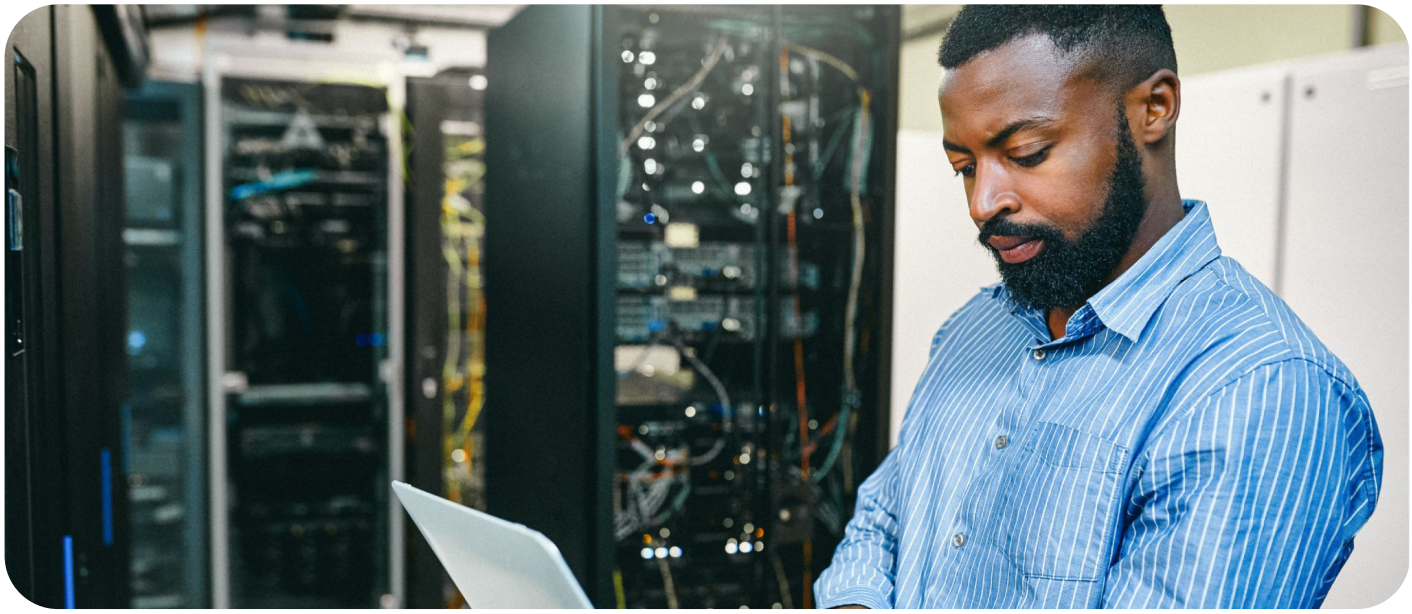
我們的研究：

Google 研究有很多涉及資安、隱私保護及濫用防範的專案。研究成果包括《Building Secure and Reliable Systems》[23]、《Security by Design》[24]、《Develop ecosystems for software safety》[25] 等刊物。Google 的資安研究人員也在實施 Project Zero 計畫，致力研究硬體和軟體系統的零時差安全漏洞。Google 的智慧與資安團隊，包括 Google Cloud 的資安長辦公室、Google 的威脅分析團隊、Mandiant 及各種 Google Cloud 產品團隊，都會定期在 Google 的《Threat Horizons Report》中發布深入分析。

社群參與：

除了發表研究成果來造福社群，Google 資安工程團隊也在經營 Bug Hunters 計畫，邀請外界高手檢測 Google 系統中的安全漏洞。為鼓勵社群人才參與，這項計畫設有獎金。Bug Hunters 計畫下的 Tsunami 是開放原始碼的網路安全通用掃描器，配有可擴充的外掛式系統，能以高精確度偵測高嚴重性的安全漏洞。Tsunami 是 Google 眾多開放原始碼安全專案的其中之一。

正如前述，任何機構都可能遇到精明狡猾的攻擊者，面臨持續不斷的騷擾。自從極光行動後，這 14 多年來，我們已經全面改造平台基本架構、縱深防禦策略，以及以安全原則為核心的企業文化，力求防止內部系統與客戶遭受這類侵擾。



創新引領我們邁向未來

正如前述，CSRB 提出的多項建議已成為 Google 資安策略的核心部分。此外，Google 也積極在解決整個業界面臨的問題，設法提出業界首創的解決方案，應對不斷變化的資安挑戰，相關例證如下：

裝置綁定工作階段控制設定：

為大幅降低 Cookie 遭竊造成的影響，Google 公布了將網路工作階段與裝置硬體加密綁定的全新開放標準。裝置綁定工作階段控制設定能有效打擊 Cookie 盜用行為，因為當驗證工作階段與裝置綁定後，遭竊的 Cookie 就不再有任何價值。

AI 創新：

現在，Gmail 先進的 AI 保護措施已能阻止超過 99.9% 的垃圾郵件、網路釣魚內容和惡意軟體進入您的收件匣。運用大型語言模型，Gmail 中的垃圾郵件減少了 20%，也能更有效率地評估使用者回報的垃圾郵件，單日評估量比先前多出 1,000 倍。最近，我們更將大型語言模型的能力應用於文件分類，推出 AI 分類功能，讓客戶能使用保障隱私的自訂模型，辨識與保護機密資料。未來我們將繼續在產品中建構新的 AI 防禦層，以先進技術更全面保護客戶的安全。

Google Workspace 如何提供協助

我們一向致力於確保客戶安全，提供更安全的工作解決方案。若想瞭解如何為貴機構提供更安全的工作方式，歡迎洽詢您的客戶代表，或留下您的聯絡資訊。

附錄：註腳

註腳號碼	來源
1	CSRB，《Review of the Summer 2023 Microsoft Exchange Online Intrusion》(回顧 2023 年夏季 Microsoft Exchange Online 入侵事件)，第 ii 頁 (CSRB，2024 年)
2	同上，第 iv 頁
3	CISA，ED 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System (ED 24-02：Microsoft 公司電子郵件系統遭國家級駭客入侵，如何化解重大風險) (CISA，2024 年)
4	CSRB，《Review of the Summer 2023 Microsoft Exchange Online Intrusion》(回顧 2023 年夏季 Microsoft Exchange Online 入侵事件)，第 20 頁 (CSRB，2024)
5	同上，第 iii 頁
6	同上，第 iii 頁
7	同上，第 iii 頁
8	同上，第 18 頁
9	同上，第 ii 頁
10	CISA，ED 24-02
11	Microsoft 安全回應中心，Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard (國家級駭客午夜 暴雪攻擊事件後的 Microsoft 行動說明更新) (Microsoft，2024 年)
12	CSRB，《Review of the Summer 2023 Microsoft Exchange Online Intrusion》(回顧 2023 年夏季 Microsoft Exchange Online 入侵事件)，第 iii 頁 (CSRB，2024 年)
13	同上，第 iii 頁
14	同上，第 iii 頁
15	同上，第 iii 頁
17	同上，第 16 頁
18	同上，第 5 頁
19	同上，第 20 頁
20	同上，第 iii 頁
21	美國外交關係協會，Operation Aurora (極光行動) (美國外交關係協會，2010 年)
22	Kent Walker，Transparency in the shadowy world of cyberattacks (分享網路攻擊暗黑世界資訊) (Google，2022 年)
23	Heather Adkins、Betsy Beyer、Paul Blankinship、Ana Oprea、Piotr Lewandowski、Adam Stubblefield，《Building Secure and Reliable Systems》(建構安全可靠的系統) (O'Reilly Media，2020 年)
24	Christoph Kern，《Secure by Design at Google》(Google 融入安全考量的設計) (Google，2024 年)
25	Christoph Kern，《Developer Ecosystems for Software Safety》(開發人員網路安全生態系統) (Google，2024 年 2 月)