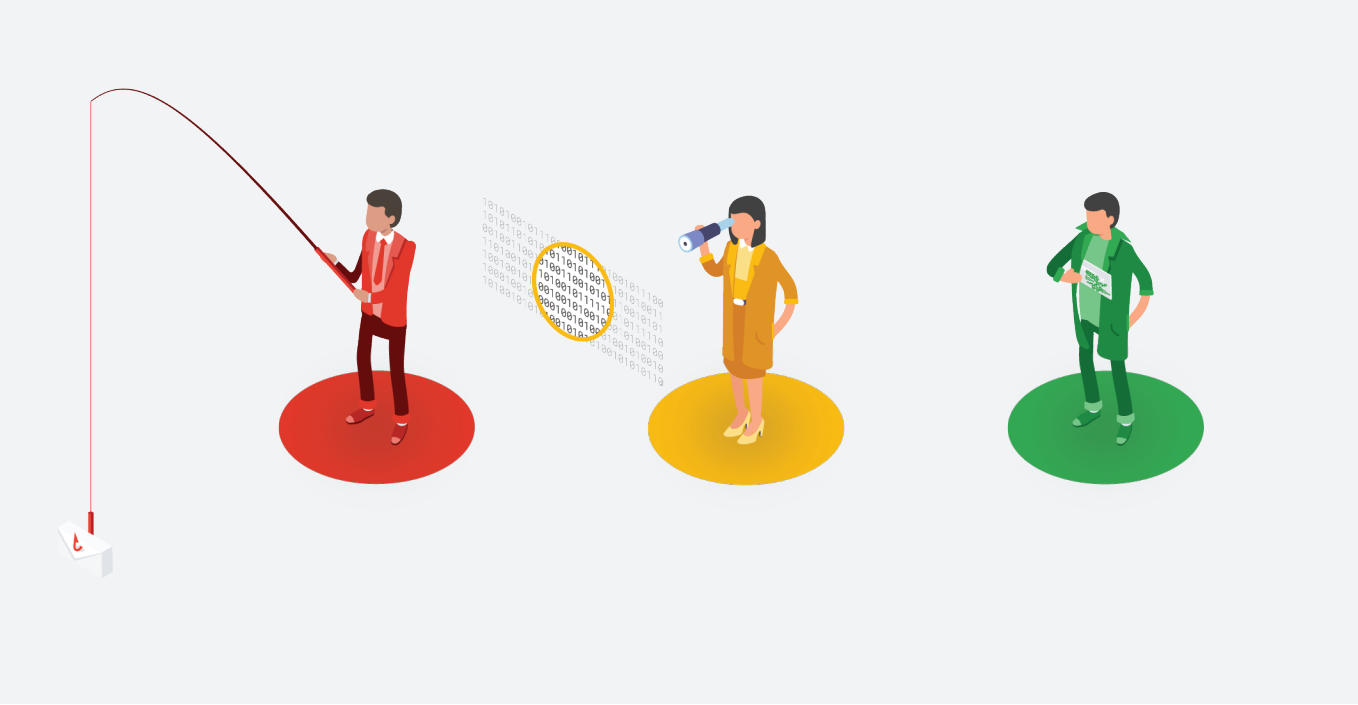
終端專屬的雲端原生安全機制

Chrome Enterprise 採用創新方法來保護資料安全並簡化 IT 管理作業



Chrome Enterprise

Chrome Enterprise

目錄

尋找更好的方法

終端安全性是棘手的難題

保護終端安全是網路安全和 IT 作業專家面臨的最大挑戰之一。他們必須處理各種棘手問題和不斷演進的攻擊行為。

傳統端點十分複雜，通常具有以下特性：

1. 包含數百個軟體，其中有未經修補的舊版本和未經核准的軟體套件，這些都是不肖人士可攻擊的目標
2. 當使用者造訪惡意網站、下載不明的應用程式，或是未執行必要的軟體更新時，將容易遭受攻擊
3. 儲存數 GB 的智慧財產資料、個人識別資訊 (PII) 和使用者憑證
4. 處理程序之間的界線執行不力，只要單一軟體模組遭到入侵，攻擊者即可存取整個系統和企業網路

在這種環境下，網路安全團隊必須耗費極大心力，嘗試監控終端、識別安全漏洞及偵測入侵事件。作業團隊必須在數百個分散各地的裝置間盡可能保持映像檔一致，並修補及更新韌體、作業系統、公用程式、驅動程式、瀏覽器和應用程式，工作量相當龐大。然而更糟的是，有越來越多使用者在家或從遠端工作，導致專為企業網路設計的工具/程序效率越來越低。

重新審視這個模式的時候到了

現在您有機會可以脫離這個困境，並在終端安全和管理作業方面做出顯著改善。

首先，IT 機構可以利用雲端式架構的先天優勢來強化安全性和作業程序。透過雲端 (而非具有安全漏洞的終端) 儲存和分享資訊資產，可簡化監控作業；透過雲端平台 (而非數百個遠端裝置) 集中追蹤及更新軟體執行情形，可大幅簡化相關作業。

其次，技術供應商也從根本上重新思考「雲端原生」的安全性，並導入全新的卓越功能來強化終端安全並簡化端點管理作業。

在這份白皮書中，我們將探討 Google 如何運用雲端運算的先天優勢，以及透過在裝置、韌體、作業系統、瀏覽器和應用程式這五個層面建構創新的多層防禦方式，重新設計端點的安全機制。

此外，我們也將針對以下幾點舉例說明：

1. Google 創新的安全性功能可防禦特定威脅，例如惡意軟體、網路詐騙、偷渡型下載和進階持續性威脅 (APT)
2. Chrome Enterprise 大幅簡化軟體更新等作業、可妥善應對裝置遺失和遭竊的情形，以及管理分散式裝置的安全性政策
3. 可使用 Microsoft Active Directory 和頂尖的第三方企業行動管理服務 (EMM) 工具，將終端管理作業自動化

運用雲端運算的先天優勢

減少終端中的資產數量

雲端式架構的其中一項先天優勢就是將大部分的資訊資產儲存在雲端，而非儲存在端點。假如筆電遺失或遭竊，您不需要擔心客戶名單、業務計畫、收益報表、人力資源資料或軟體程式外洩；如果裝置遭到入侵，不肖人士取得客戶信用卡號碼、員工醫療資訊，或公司財務系統密碼的可能性極低。

縮小受攻擊面

使用雲端式架構可大幅減少安裝在終端的軟體數量。分散式裝置仍需要韌體和作業系統，但不需要將數十個公用程式、驅動程式、瀏覽器、商務應用程式和個人應用程式儲存在傳統終端上。與傳統終端相比，攻擊者可以瞄準的安全漏洞較少，需要安裝、管理和保護的軟體元件數量也大幅降低。

快速頻繁的更新

如果貴機構的裝置分散在國內各處或世界各地，使用傳統方式修補及更新終端上的軟體元件是一項永無止盡又耗費心力的例行公事。而且每當發布新的安全漏洞或出現新的攻擊技術，網路安全和作業人員就必須盡快在數百個終端上進行修補或新增控制項。安全「破口」敞開的時間越長，駭客趁虛而入的機會就越大。

有了雲端式架構，您可以透過單一平台集中更新軟體、部署及管理控制項，大幅減少更新終端狀態所需的工作量。

裝置：內建安全防護和一致性機制

雲端式架構可應用許多創新的安全性和管理功能。讓我們從 Chrome 裝置開始說起，包含搭載 Google Chrome 作業系統和 Chrome 瀏覽器的筆電和平板電腦。有許多領先業界的科技公司都推出 Chromebook，例如 Acer、ASUS、Dell、Google、HP、Lenovo 和 Samsung 等。

硬體安全性模組

所有最新的 Chromebook 都搭載符合 Google 規格的硬體安全性模組。專用晶片上的模組內建快閃記憶體、ROM、RAM 和破壞偵測功能，大幅提高篡改模組資訊的難度。硬體安全性模組中儲存的重要資訊和加密編譯金鑰無法從作業系統存取，可防止特定類型的旁路資訊外洩攻擊和實體故障置入技術。

加密及區隔使用者資料

根據預設，所有 Chromebook 都會將使用者的資料和設定進行加密處理。無論是使用者或其他人都無法停用這項加密功能。

此外，每筆使用者資料和設定都會使用一串獨特的金鑰進行加密。如要使用該金鑰，攻擊者幾乎必須同時取得使用者密碼和安全性模組的存取權。這種做法可大幅提高不肖人士讀取任何使用者資料的困難度，即使不肖人士已取得 Chromebook 和一位使用者的密碼，也無法解密及讀取其他使用者資料。

區隔使用者資料還有另一項優勢，除了可提高與同事/家人共用裝置時的安全性，還能採用如「隨取即用」等尖端做法，提高外借裝置和臨時員工共用裝置的安全性。

情境：防止內部人員盜取資料

澤偉、阿堯和小達共用一部 Chromebook，這三位承包商的上班時間彼此錯開。但澤偉也是一位業餘駭客，他想趁機存取小達使用的伺服器。他知道重要的演算法和專屬軟體都存放在那個伺服器上。澤偉趁工作時登入這部 Chromebook，但他無法存取小達的憑證、網路連線，或她的任何其他資料和設定。存放在那個伺服器上的資料安全無虞。

跨終端的一致性

Chromebook 製造商皆同意符合或超越 Google 針對品質、效能和安全性所設定的規格。裝置的硬體設計必須經過 Google 審核和批准，才能使用 Chrome 的品牌名稱出貨。製造商也同意在每部 Chromebook 上使用相同的韌體、Chrome 作業系統和 Chrome 瀏覽器。(圖 1)

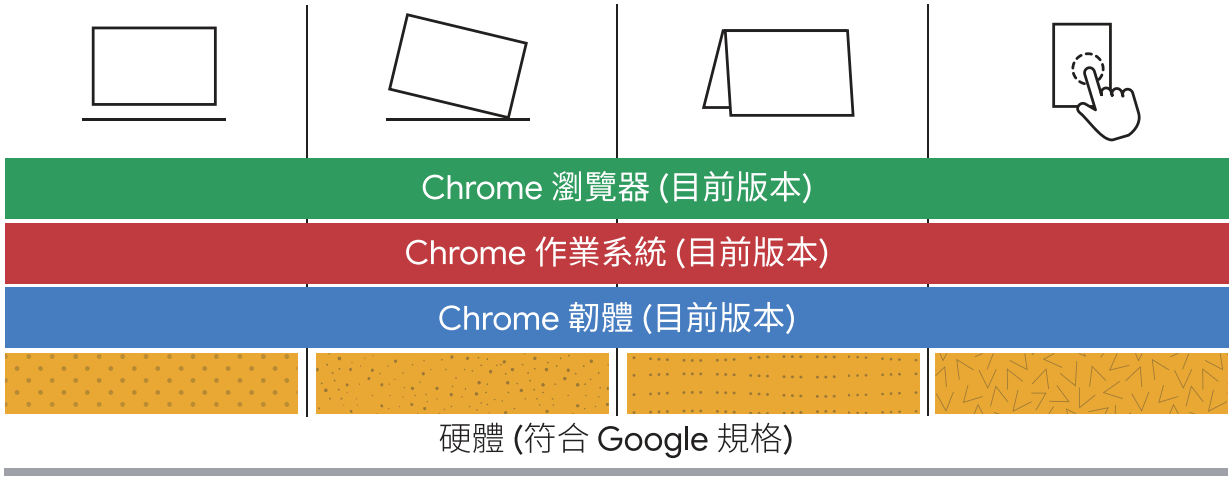


圖 1：為了提供流暢的使用者體驗和簡化管理作業，所有 Chromebook 均搭載同樣的韌體版本、Chrome 作業系統和 Chrome 瀏覽器。

這樣的共通性對使用者和系統管理員來說是一項重要優勢。使用者在所有 Chromebook 上都可享有一致的體驗和更舒適的操作感受。安全性和作業團隊可以提供標準的作業環境，再也不需要管理版本各異的韌體、作業系統、系統公用程式和瀏覽器，或擔心不相容的軟體版本會產生安全漏洞。如果發生問題，也能更輕鬆快速地進行疑難排解。

安全性的最佳選擇

Google 與生態系統合作夥伴合作，針對不精通網路安全或不太瞭解如何使用電腦的使用者，找出可提高網路安全的功能和預設設定。上述有關所有使用者資料都會依據預設進行加密的部分，我們將在後文提供更多範例。

韌體：驗證鏈結

「持續性」是大多數進階的針對性攻擊的關鍵要素。精細複雜的攻擊通常仰賴在終端上植入程式碼或指令碼，攻擊者可以藉此透過重新啟動裝置或系統故障來入侵端點。

雲端式架構阻擋了許多攻擊者在傳統終端上進行持續性攻擊的技術。舉例來說，如果終端上沒有儲存使用者可以安裝的驅動程式或指令碼，就無法利用這些驅動程式或指令碼在重新啟動之後保留惡意程式碼。

然而，不肖人士還是可以嘗試將程式碼置入裝置上儲存的可寫入韌體、作業系統和瀏覽器。

為防止這類情形發生，Google 採用一個名為「驗證開機程序」的技術，以確保重新啟動後所執行的韌體、作業系統和瀏覽器程式碼，皆為 Google 的軟體而且未經改造。

情境：封鎖 Rootkit！

貝拉是一名網路犯罪份子，取得了 Chromebook 存取權和超級使用者的權限。她直接重新掛載可讀寫的根層級分區，然後以核心模組的形式新增一個 rootkit。但是在下一次重新啟動時，根層級分區的該部分簽章並沒有與原先的吻合。開機程序停止，裝置使用韌體和作業系統的備用映像檔重新啟動。重新啟動後，貝拉無法再使用 rootkit 控制這台裝置。

Chromebook 開機後，唯讀韌體使用一個簽章和一個已簽署的雜湊，驗證可供寫入的韌體與經 Google 核准的映像檔完全相符，也就是說，系統會替韌體程式碼運算雜湊並驗證是否與已簽署的雜湊相符。可供寫入的韌體經過驗證之後，就會使用相同的處理程序來驗證系統核心，然後系統核心會繼續驗證在作業系統和 Chrome 瀏覽器中所有的程式碼區塊。如果發現惡意軟體或其他異狀，開機程序就會停止，裝置就會以可供寫入的韌體和作業系統的備用版本重新啟動。(圖 2)

驗證開機程序不僅能阻擋危險的攻擊類別，也能讓作業人員不需再做補救遭入侵的韌體和檔案這類乏味的工作。

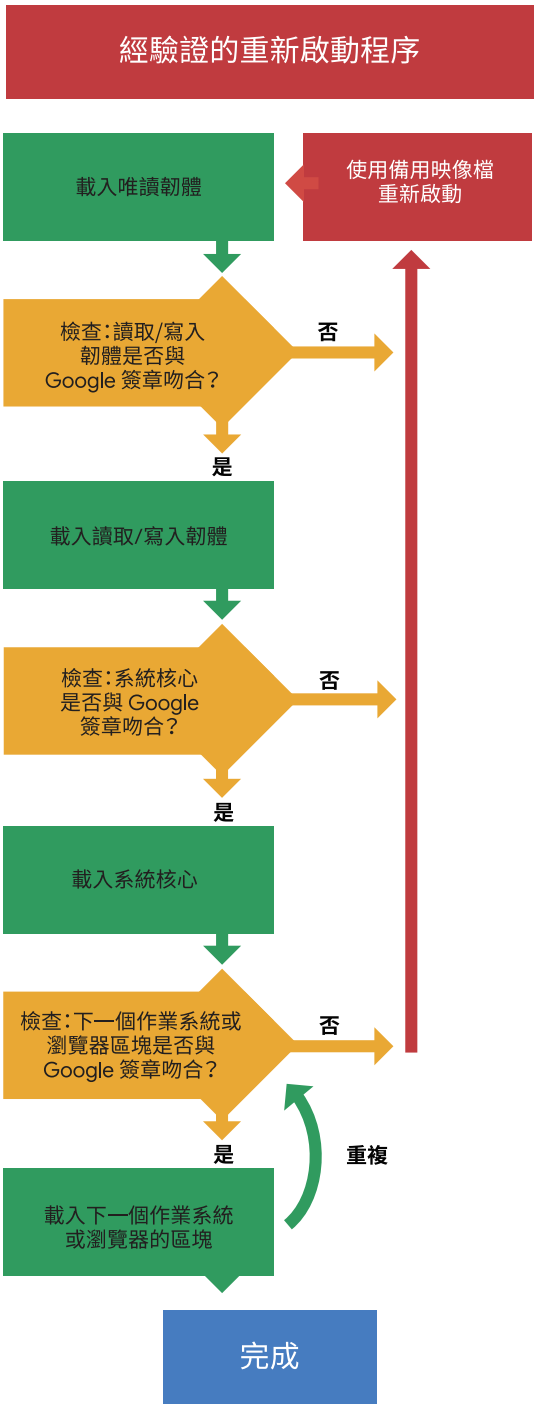


圖 2

作業系統：採用沙箱機制的處理程序和流暢的更新作業

Chrome 作業系統包含了許多安全性功能，能保護應用程式並排除更新和修補作業系統隨之而來的麻煩。

權限區隔和沙箱機制處理程序

許多網路攻擊類別使用遭入侵的網站或雲端應用程式來控制終端上的軟體元件。

在雲端原生環境，可入侵的作業系統元件、公用程式、驅動程式和其他軟體將大幅減少。但 Chrome 作業系統架構的功用不僅如此，它還能防止受攻擊者控制的應用程式影響其他軟體。

譬如 Chrome 作業系統採用沙箱機制處理程序，可以強制執行處理程序間的嚴格邊界。除非符合嚴格的限制條件，否則應用程式之間無法互相通訊。每個執行程序只能使用實際所需的權限。許多安全導向的機構會將機密資訊限於「需要知道」的人員存取，Chrome 作業系統則僅限有實際「使用需求」的處理程序進行互動。

情境：向勒索軟體說不

阿均花了幾分鐘為他的 Chromebook 螢幕尋找新的數位桌布。倒霉的是，他找到的《要塞英雄》粉絲網站是一個由網路犯罪份子所控制的「水坑」。當他點擊連結要下載檔案時，卻出現惡意程式碼，試圖加密 Chromebook 所有的資料和檔案。不過幸運的是，這些攻擊程式碼的行為在單一沙箱機制處理程序中就受到控制。阿均看到一個寫著「無法執行檔案」的提示，而勒索軟體的攻擊在取得使用者資料前即停止。

流暢更新作業系統

對於多數的安全性和作業團隊來說，要使作業系統維持在最新狀態是十分頭痛的問題。傳統終端的作業系統更新為終端使用者帶來許多困擾。這些更新往往會將端點鎖定數分鐘或超過一小時。不僅因為降低生產力而增加成本，還可能讓使用者感到困擾，對 IT 機構產生不滿。

更糟的是，使用者時常拒絕更新，使裝置容易遭受攻擊。

面對這樣的挑戰，Google 提供了一個創新解決方案。每個裝置都儲存作業系統的兩個版本，也就是目前版本和前一個版本。當系統使用目前的作業系統運作時，更新的版本可以在背景程式下載和儲存，不會對使用者造成影響。當使用者重新啟動，更新的作業系統在幾秒內即可載入。(圖 3)

這樣的處理方式也簡化了驗證開機程序，詳情將我們將進一步說明。如果系統啟動時，發現執行中作業系統的程式碼遭人篡改，前一個未經竄改的版本已儲存在裝置，將可以立即使用。

Chromebook 排除了作業系統元件在例行性更新時的頭痛問題。實際上，Google 大約每六週就可以更新 Chrome 作業系統，比其他主要的作業系統更新來得頻繁許多。系統也會在極短時間內部署安全修補程式，抵禦新發現的作業系統安全漏洞，縮短受攻擊威脅的時間。

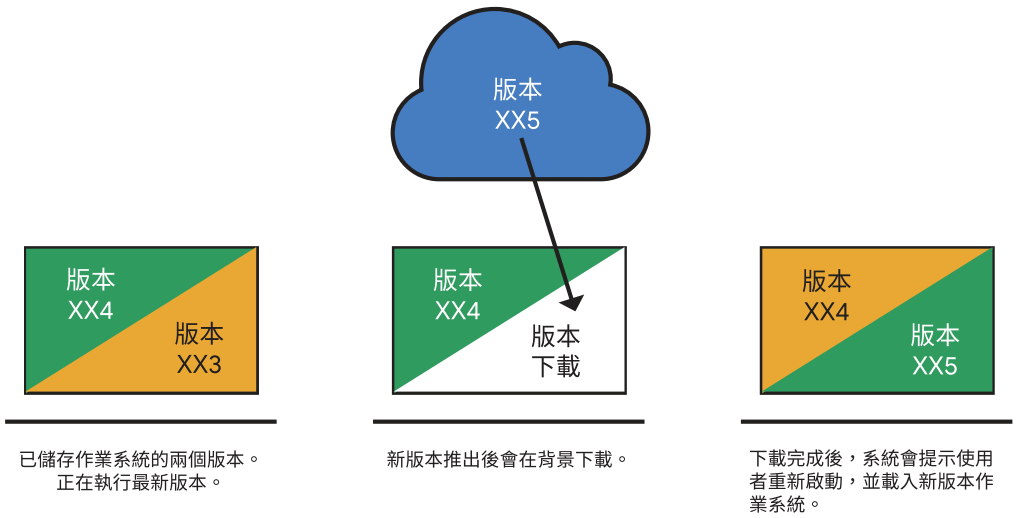


圖 3：作業系統新版本已於背景下載，不會打擾使用者工作。

瀏覽器：網站隔離、安全瀏覽和雙重驗證功能

在 Chromebook 上，使用者和網路的所有互動都是透過 Chrome 瀏覽器。Google 領先業界的瀏覽器內建創新安全功能，為使用者帶來莫大益處。

分頁沙箱機制和網站隔離

我們在 Chrome 作業系統討論的沙箱機制概念也適用於 Chrome 瀏覽器。在瀏覽器中每個開啟的分頁都有專屬沙箱，可以大幅降低單一分頁攻擊擴及至其他分頁的機會。

同樣的原理也可進一步應用在網站隔離。在許多情況下，會有許多網站在單一分頁內存取。例如，在單一網站瀏覽 HTML 網頁的動作，可能需要從第二個網站下載圖像，並從第三個網站下載影片，接著從第四個網站下載指令碼。有了網站隔離機制，這些網站的每個處理程序都會分開進行。(圖 4) 有了 Chrome 瀏覽器，系統管理員可以選擇要隔離所有網站或是特定網站。

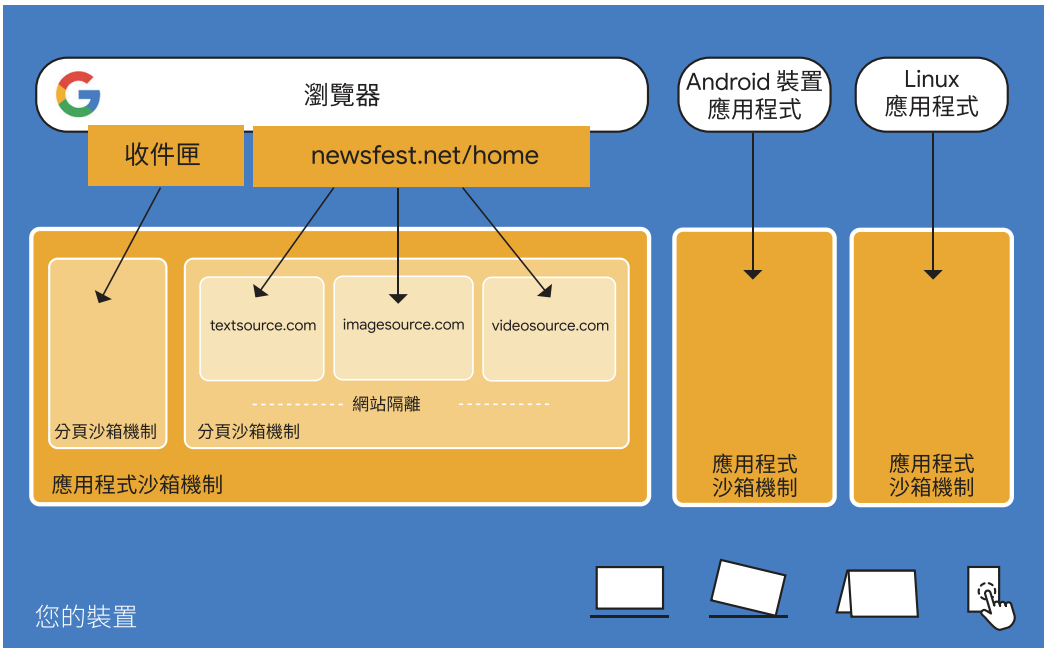


圖 4：Chrome 作業系統和 Chrome 瀏覽器提供多個層面的隔離機制，包含網站、分頁和應用程式的隔離。

這些機制有助於保護系統免於威脅，避免受到如跨網站指令碼以及 Spectre 和 Meltdown 等臆測執行的旁路攻擊，在這些攻擊當中，惡意網站會試圖存取屬於不同網站記憶體中的處理程序或資料。

安全瀏覽機制

當今企業面臨的許多重大威脅，都與遭入侵網站發起的惡意軟體和網路詐騙攻擊有關。

當使用者造訪的網站含有惡意軟體或網路詐騙內容，或是下載可疑檔案，Google 的安全瀏覽功能就會警告使用者。這項機制的技術奠基於 Google 服務，該服務每天查獲數千個有安全疑慮的網站，保護三十億部裝置。

安全瀏覽訊息不僅在 Chrome 瀏覽器畫面顯示，也在 Google 搜尋和 Android 應用程式中顯示，提醒使用者避免前往危險網站，同時也在 Gmail 訊息中顯示，提醒使用者勿點擊惡意網站的電子郵件連結。

情境：避開網路詐騙攻擊

艾莉是一家小型製造公司的財務長。她收到一封來自執行長的電子郵件，請她立刻電匯兩萬美金給新的中國供應商，以便能在極短缺元件的供應上取得優勢。艾莉知道執行長正在中國出差安排供應商的事宜，因此這封電子郵件看起來是合理的。但是當她要點擊電子郵件連結前往新供應商的網站時，收到一則警告，表示該網站是詐騙網站，請她在警告畫面上點擊「返回安全網頁」的連結。安全瀏覽功能幫助了艾莉避開透過商務電子郵件入侵的網路詐騙攻擊。

安全金鑰和雙重驗證

即便使用者憑證已遭駭，雙重驗證機制還是能為系統和資料提供防護。驗證憑證時，使用者必須提供某項已知資訊 (通常是密碼)，並搭配另一項措施 (經常是驗證金鑰或發送至智慧型手機的代碼)。

Google 提供的有效雙重驗證功能，可說是世界最快也最簡單的方式。使用者只需前往 Google 帳戶，選取「兩步驟驗證」並選擇第二重身分驗證的方式。驗證的選項包含傳送文字代碼、在手機上輕觸提示，或將 Titan 安全金鑰透過 USB 連接埠連結至 Chromebook。為了方便起見，使用者可以將數部裝置設定為信任的裝置，日後登入這些裝置時不須進行第二重身分驗證。

應用程式：惡意軟體偵測、建立白名單和黑名單

Chromebook 可以執行各式各樣的應用程式，包括 Android 應用程式，Gmail、Google 文件、Google 試算表、Google 簡報、Google 繪圖等 Office 生產力應用程式，以及 Chrome 擴充功能、以 Linux 為基礎的應用程式和漸進式網頁應用程式 (PWA)。註：PWA 是一種可以快速載入的應用程式，能提供與安裝在本機應用程式不相上下的功能和回應速度。

當企業授予使用者存取權，使其能透過 Chrome 線上應用程式商店存取 Google 提供的應用程式，以及透過 Google Play 商店存取 Android 應用程式時，企業將受益於多項可強化安全性並簡化管理作業的功能。

伺服器端惡意軟體偵測和遠端解除安裝

Google Play 安全防護是全球部署最廣泛的行動威脅保護服務，每天為二十億名使用者提供防護。所有的 Android 應用程式上架到 Google Play 商店前，Andriod 安全團隊的專家都會進行嚴格的安全測試。Google Play 商店不會接受違反政策的應用程式和開發人員。

此外，Google Play 安全防護會持續掃描和驗證 Google Play 商店的應用程式。當應用程式出現惡意軟體，系統除了會將應用程式立即從 Google Play 商店停權，也會將其從所有下載的系統解除安裝。

透過 Google Play 商店進行應用程式管理和建立許可清單

使用者時常會因為下載含有安全漏洞或實際由不肖人士開發的應用程式，而助長了資料侵害事件。

情境：抑制影子 IT

卡洛管理一個橫跨四大洲的國際行銷團隊。他希望能推行協作工具來改善溝通和規劃的成效。當他在網路上找到一篇名為「前二十大協作工具」的文章時，並沒有想到這些工具有許多都缺乏企業級安全性和管理功能。還好在花上好幾個小時嘗試所有工具之前，他瀏覽了公司的 Google Play 管理版商店。他發現了兩個經核准的團隊協作應用程式：Slack 和 Google Hangouts。這兩個應用程式都具備絕佳的功能和安全性。此外，公司的 IT 機構皆能支援應用程式，使用任一個應用程式可以讓他的團隊與使用同樣應用程式的所有其他群組一同協作。

數十年以來，許多 IT 系統管理員嘗試藉由告誡使用者只安裝核准的應用程式，或鎖定終端只讓核准的應用程式在終端上執行，來抑制混亂叢生的下載情形。前項方式的效果不彰，因為核准的應用程式清單囊括的項目難免太少，無法滿足每個人對商用應用程式和個人應用程式及娛樂的需求。後者的方法也行不通，因為要鎖定傳統終端在技術上十分困難，通常會受到使用者大力反對。

以網路為基礎的技術讓安全性和作業團隊有新的機會，可以遏止未經授權的應用程式，而不會讓使用者感到失望或厭煩。

Google Play 商店提供使用者數千個企業生產力、溝通和協作、管理企業流程、新聞、娛樂和遊戲的應用程式，所有應用程式都經過 Android 安全性團隊測試，確保未含有安全漏洞或嚴重的安全缺陷。

系統管理員可以為機構建立一個 Google Play 管理版商店，收錄廣泛但種類豐富的應用程式集。舉例來說，他們可能會提供公司員工各式各樣的生產力和協作應用程式，但限制員工使用遊戲和社交媒體應用程式。(圖 5)

Google Play 管理版商店可以視情況進一步輕鬆建立許可清單，如此一來，機構的所有人員都必須使用相同的生產力和協作工具，同時只允許從其他少量精選應用程式中挑選使用。

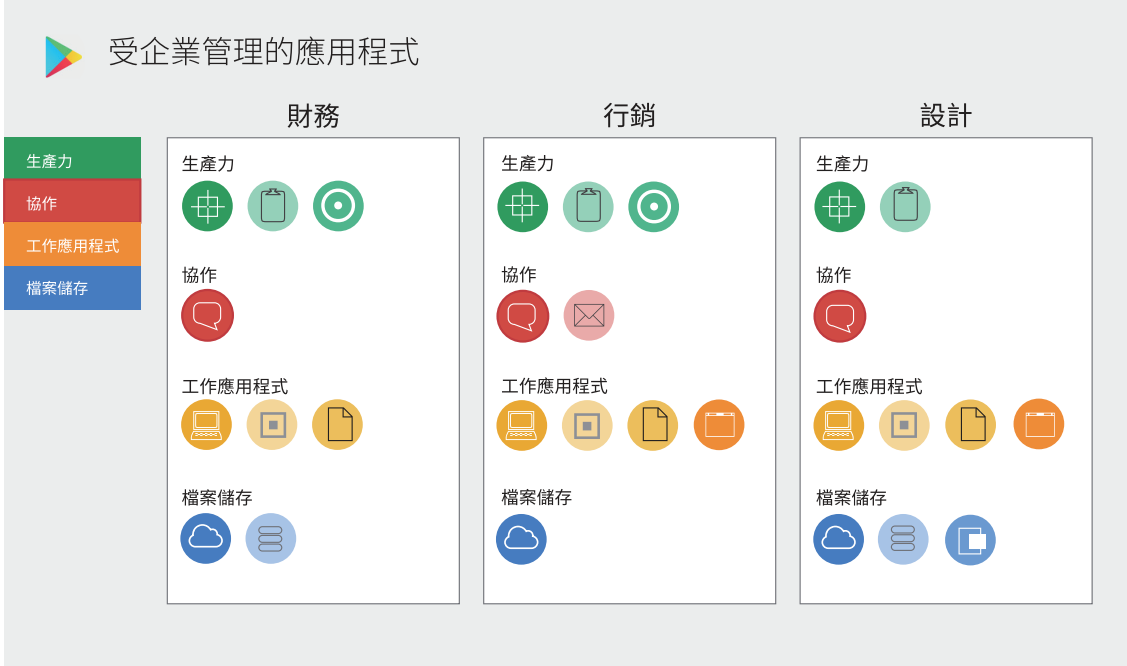


圖 5：有了 Google Play 管理版商店，企業的每個群組都能存取授權應用程式的收錄清單。

搭配 Chrome Enterprise 進行集中化管理

Chrome Enterprise 讓安全性和營運團隊能夠在 Chromebook 和其他搭載 Chrome 作業系統的端點上集中管理政策，並可在 Windows、Mac 和 Linux 系統上管理 Chrome 瀏覽器政策。Chrome Enterprise 授權具備裝置管理功能，並享有 24 小時全年無休的 Google 支援服務，有助於協助企業拓展環境，管理數萬位使用者和其裝置。

精選 Chrome Enterprise 政策一覽

系統管理員可利用 Chrome Enterprise 在終端設定並執行超過 300 項安全性和設定政策。受管理的 Chrome 裝置安全性相關重要功能如下：

佈建和取消佈建裝置。系統管理員可以註冊裝置或允許使用者註冊裝置，如此一來，就能透過使用者機構訂定的 Chrome Enterprise 政策來管理和保護這些裝置。系統管理員可以取消佈建裝置，以停用政策並防止裝置存取企業資源。

遠端停用裝置。如果裝置遺失或遭竊，可以從遠端停用。

限制登入。系統管理員可允許使用者以匿名方式登入裝置 (訪客瀏覽功能)、必須使用 Google 或 G Suite 帳戶登入，或僅限一或多位特定人員存取。

設定暫時模式 (使用者登出後清除資料)。系統管理員可以將裝置設為暫時模式，當使用者登出後，系統會清除這些使用者的資料和設定 (包含瀏覽記錄、擴充功能和相關資料，以及 Cookie 等網站資料)。暫時模式讓共用裝置、資訊站裝置和短期使用者裝置在使用上更加安全。

限制或要求網頁應用程式和瀏覽器擴充功能。系統管理員可以禁止使用者安裝任何 Chrome 網頁應用程式和瀏覽器擴充功能 (自訂瀏覽體驗的小型軟體程式)、禁止安裝特定應用程式和擴充功能，或只允許使用者安裝來自特定網址的應用程式和擴充功能。也可以強迫使用者安裝特定應用程式和擴充功能。

依據權限封鎖應用程式。許多 Chrome 應用程式和瀏覽器擴充功能需要權限，才能使用位於安裝裝置的資源。系統管理員可以禁止使用特定權限的應用程式和擴充功能進行安裝。舉例來說，系統管理員可以禁止安裝需要特定權限的應用程式和擴充功能，例如擷取畫面/視窗或分頁內容、讀取剪貼簿內容、從裝置麥克風或攝影機擷取音訊或視訊、取得使用者地理位置、查詢裝置網路的中繼資料，或覆寫裝置的電源管理功能。這個功能降低了 IT 機構的風險，同時讓使用者能自由安裝沒有安全疑慮的「無害」應用程式。

停用藍牙和地理位置。裝置上的藍牙和位置追蹤功能可以設為停用。

限制使用外部儲存裝置。可以完全禁止使用外部儲存裝置 (如 USB 隨身碟、外接硬碟、光學儲存裝置及記憶卡)，或只在唯讀模式下允許使用。

管理遠端存取和單一登入。系統管理員可以為遠端存取和 SAML 式單一登入 (SSO) 設定參數，讓使用者存取網路和網頁應用程式時能兼顧安全與便利性。

追蹤裝置和使用者。每部裝置的報表都會顯示作業系統和韌體等級、CPU 和 RAM 的使用統計資料、外接式儲存裝置、使用情形指標、診斷資料、最近登入的使用者，以及使用者的活躍時間。

委派管理和彈性管理

有了 Chrome Enterprise，管理工作可以透過委派來分擔，將群組和部門的管理責任賦予適當人選。此外，角色建立功能可針對受管理的裝置、使用者和應用程式，授予系統管理員不同的讀寫設定權限。

Chrome Enterprise 提供政策建立和施行上的彈性。系統管理員可以為使用者和使用者群組建立政策，在此情況下每位使用者在其所有裝置上都會看到相同的政策。此外，系統管理員也可以為裝置建立政策，無論使用的是哪一位使用者，這些政策都會在每一台裝置上施行。

情境：不行，這場會議不准偷聽

公司的執行長和財務長即將出國，針對一筆重要交易進行協商。如果策略協商遭到另一方或所在國的情報服務機構竊聽，公司將遭逢鉅額損失。所幸您可以暫時停用藍牙，封鎖具備 Chromebook 麥克風和攝影機權限的 Chrome 網頁應用程式和瀏覽器擴充功能 (必須重新啟動裝置，變更才會生效)。

運用您的管理基礎架構

Chrome Enterprise 具備專屬的主控台供系統管理員使用，其設計符合您現有的管理基礎架構。

與 Active Directory 和 Google Cloud Identity 整合

Chrome Enterprise 管理控制台已經和 Microsoft Active Directory 和 Google Cloud Identity 整合。譬如您現在可以在 Active Directory 註冊 Chrome 裝置，也可以根據 Active Directory 中所定義的使用者群組，將 Chrome 政策推行至使用者和裝置。

搭配頂尖企業行動管理服務解決方案使用

企業行動管理服務產品能協助企業註冊與管理筆電、平板電腦、智慧型手機和其他行動裝置，並對這些裝置提供支援。如果您的企業已投資企業行動管理服務解決方案 (例如 Cisco Meraki、Citrix XenMobile、IBM MaaS360、ManageEngine Mobile Device Manager Plus 以及 VMWare Airwatch)，您可以繼續使用這些產品來管理 Chromebook 和其他端點。

總結：前所未有的安全性和操作管理流程

雲端運算讓企業有機會重新思考傳統端點的模式。雲端原生方法能有效強化端點安全性，並大幅簡化終端管理。

Chrome 裝置運用雲端運算的先天優勢，包含減少終端中的資產數量、縮小受攻擊面和快速簡單的更新。此外，雲端原生思維為創新安全和管理能力鋪展了一條道路，包含內建於硬體和韌體的安全性功能，有效採用沙箱機制、使用者層級加密、快速流暢的作業系統更新、安全瀏覽、簡單的雙重驗證、建立應用程式許可清單，以及範圍擴及數萬名使用者和裝置的安全性及操作政策簡單管理流程。

由此得來的運算環境具備以下特點：

1. 將安全性納入設計考量
2. 相較於傳統端點更容易管理
3. 能融入既有的基礎架構

如要進一步瞭解 Chrome Enterprise 安全性機制，請造訪

https://cloud.google.com/chrome-enterprise/security/