白皮書

企業在安全終端的當務之急

贊助商：蘋果

Tom Mainelli　　Michael Suby

2023 年 9 月

IDC 觀點

是什麼讓 IT 決策者夜不能寐？答案是安全問題。聰明的 IT 決策者深知，無論一家企業經營得多好，或者它的產品、服務可能多受歡迎，一旦出現安全問題，整個企業都可能在一夜之間陷入困境。

不幸的是，這個世界並沒有變得更加安全。企業間諜、無賴政權、組織犯罪，甚至是普通的竊賊都已提高了技術水準。為了比壞人搶先一步，IT 部門必須保持警覺，隨時準備採納新的供應商和技術，以確保員工、客戶和資料的安全。

IT 所面臨的安全挑戰不勝枚舉，涉及從終端（電腦）到資料中心、連接萬物的網路以及運行所有設備的軟體等方方面面。在本文中，我們將重點討論確保終端安全的重要性，因為究其根本，如果終端不安全，其他領域的安全就都沒有意義。

終端安全所面臨的主要挑戰之一是，傳統上要確保終端的安全往往意味著最終使用者必須犧牲使用體驗，操作著難以使用的鎖定的裝置；當這種情況發生時，任何安全方案中的另一個主要薄弱環節就會浮現，就是使用者，因為使用者通常會本著完成工作的精神找到規避安全措施的方法。當安全成為使用者的障礙時，就難以達到安全的目的。

技術的進步使我們越來越有可能在保障安全的同時，仍維持高品質的使用者體驗。惡意軟體檢測、資料保護、身份驗證、晶片和軟體融合等方面的進步意味著現今的終端不需要為了強化安全性而犧牲生產力。

方法

IDC 於 2023 年 7 月對美國和加拿大的 IT 決策者進行了一項線上調查（n=513），詢問他們對廣義安全的看法，特別是保護電腦終端安全的重要性。受訪者來自不同行業、擁有 500 名(包含)以上員工的公司。這些 IT 決策者支援多種電腦作業系統，包括微軟 Windows、蘋果 macOS 和 Google ChromeOS，他們需要為自己的公司選擇、購買或部署安全軟體，或是管理從事這些工作的員工。

概況

安全問題仍然是 C 級高階主管的當務之急，具有前瞻性思維的公司已意識到良好的安全性不僅只是「錦上添花」，而是在不斷變化的威脅環境中，企業要健康、蓬勃發展所必需，而這種威脅環境持續由高度協調一致且資金充足的惡意行為者所驅動。

根據 IDC 於 2023 年 3 月針對擁有 500 名(含)以上員工的企業 IT 決策者進行的未來企業復原力和支出調查，全球超過 50%的受訪公司在過去 12 個月中遭受過導致業務中斷的勒索軟體攻擊；超過三分之一的受訪者表示，勒索軟體攻擊導致業務中斷了一週或更長時間。儘管大型公司可以說擁有更強大的安全協

議，但它們也難以倖免於此類攻擊，事實上，受勒索軟體造成中斷影響最大的企業規模是員工人數在 1000 到 2499 人（71%）、2500 到 4999 人（72%）和 5000 到 9999 人（70%）的公司。換句話說，無論公司規模大小，都無法倖免於難。

該調查還指出，終端是勒索軟體攻擊的主要入口，最初的入侵點包括網頁瀏覽（21%）、可攜式儲存裝置（18%）、電子郵件附件（17%）、供應鏈（17%）、電子郵件中的網址（14%）和內部人員存取（8%）。

越來越多的員工在混合環境和遠端環境中工作，這種持續轉變只會使 IT 部門更難以對付勒索軟體和其他安全風險。IDC 於 2022 年 12 月進行的終端安全調查顯示，超過 97%的企業有一部分員工進行遠端辦公，儘管此數字預期在未來 12 個月內會有所下降，但在可預見的未來仍將居高不下。

在各公司努力應對大量遠端員工帶來的持續挑戰之際，越來越多的公司開始實施零信任策略。最佳實踐的重點領域包括建立安全控制基準、進階終端安全防禦、裝置驗證（確保連接到網路的裝置是合法的）以及強使用者身份驗證。

當考慮到上述所有因素時，我們調查中的受訪者絕大多數都選擇提高整體資料安全性和確保電腦安全，將之作為最重要的 IT 優先事項就不足為奇了，如圖 1 所示。

值得注意的是，在下圖中，IT 的第三重要主題是透過更好的裝置提高員工的生產力。當我們要求受訪者選出他們認為最重要的三個主題時，選擇「更好的裝置」選項的人數最多。這讓 IT 記住了一個關鍵資訊：安全固然重要，但不能以犧牲員工的生產力為代價，最佳的裝置能同時具備出色的安全性和最終使用者滿意度，且不會讓使用體驗不會受到安全問題的影響。

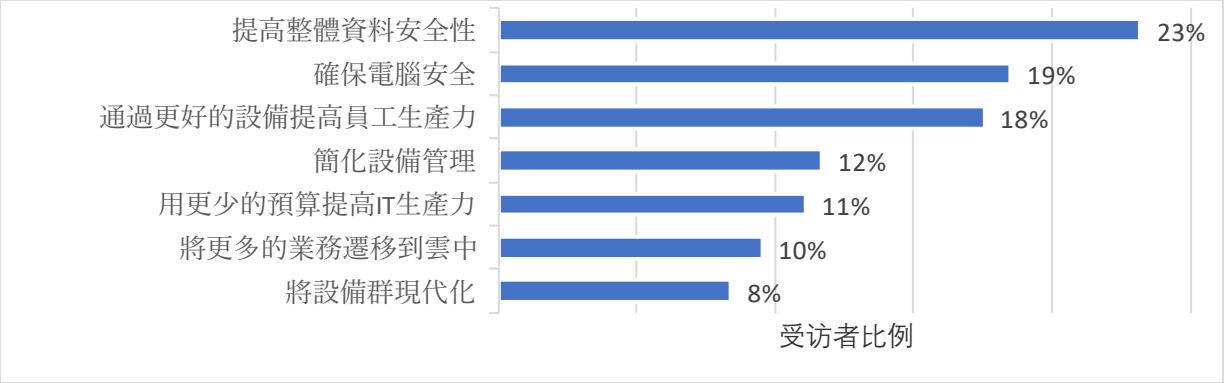
當我們問 IT 決策者在選擇下一個電腦供應商的首要決定因素是什麼時，安全性排在第一位，超過了效能、對現有應用程式的支援以及與現有 IT 基礎架構的整合。也許最值得注意的是，規格選項幾乎名列榜尾。

如需瞭解最重要的 IT 優先事項，請參見圖 1。如需瞭解選擇電腦供應商時的首要考慮因素，請參見圖 2。

圖 1

IT 的重中之重：資料和終端安全

問：以下哪些 IT 主題是貴公司目前的重中之重？



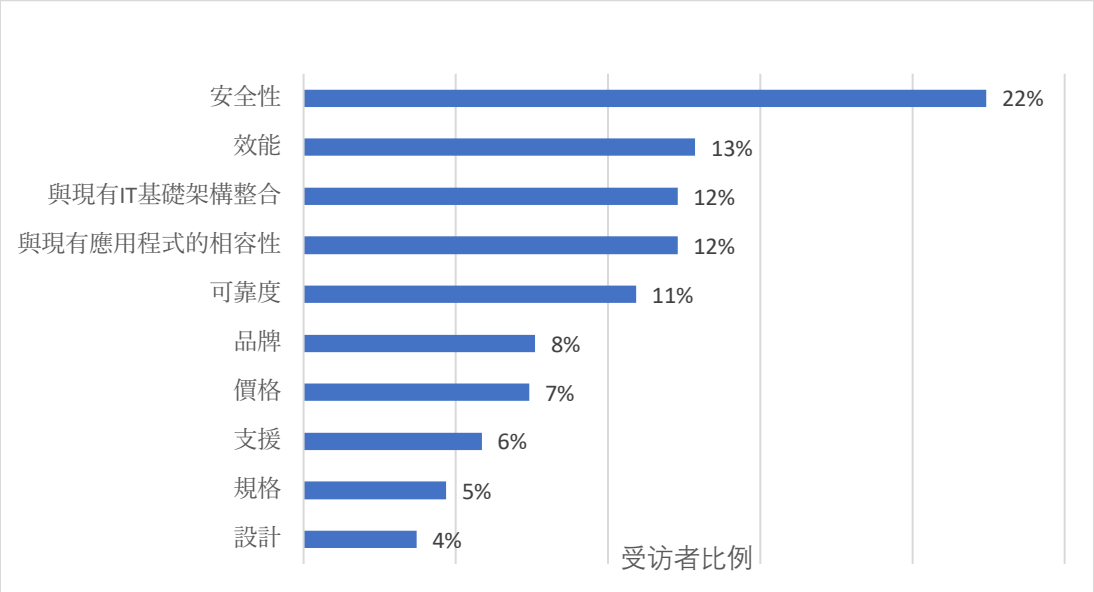
來源：IDC 安全終端調查，n=513

注：資料包括被評為最重要的主題（排名第 1）

圖 2

選擇電腦供應商時的首要因素

問：在為自己的公司選擇電腦時，最重要的決定因素是什麼？



來源：IDC 安全終端調查，n=513

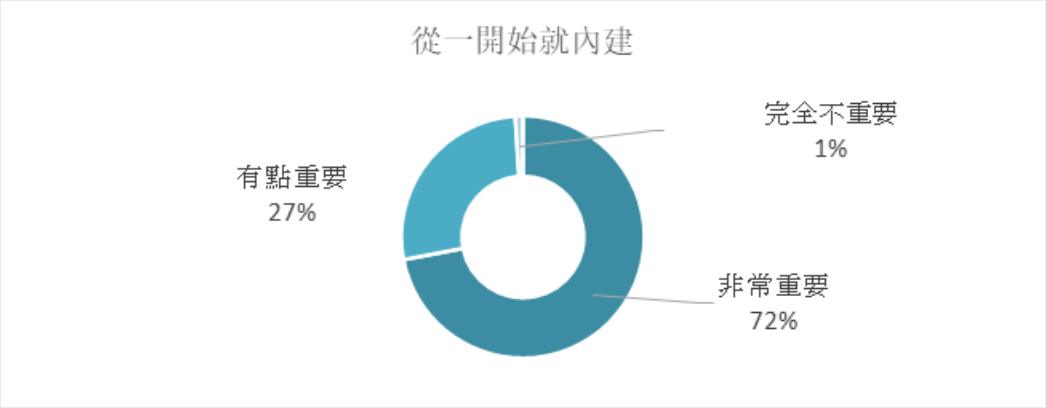
注：資料包括被評為最重要的因素（排名第 1）

受訪者對於內建安全功能和整合資料保護這兩個概念有強烈的共鳴。當被問及「從一開始就在電腦（包括晶片、韌體和作業系統）中內建安全功能，以保護電腦免受目前和未來威脅的影響，您認為有多重要？」絕大多數人的回答是積極的，72%的人認為非常重要，27%的人認為有點重要，只有 1%的人認為這根本不重要。值得注意的是，再進一步探究可發現在醫療保健和金融組織的 IT 決策者中，認為它非常重要的比例甚至更高（分別為 84%和 75%）。整合資料保護這一概念的得分同樣很高。我們的問題是「您認為將資料加密功能整合到電腦硬體中有多重要？」71%的人認為非常重要，29%的人認為有點重要，0%的人認為不重要。如需瞭解內建安全功能和整合資料加密的詳細資訊，請參見圖 3。

圖 3

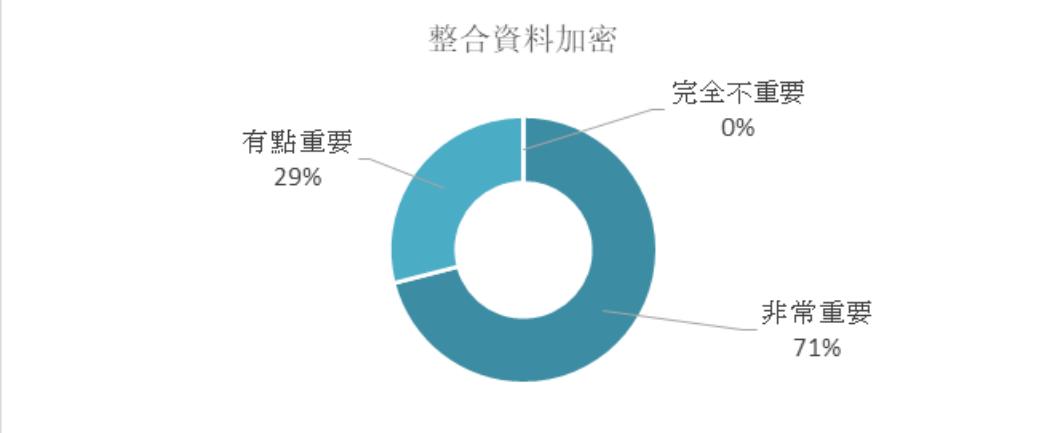
內建安全功能和整合資料加密的重要性

問：從一開始就在電腦（包括晶片、韌體和作業系統）中內建安全功能，以保護電腦免受目前和未來威脅的影響，您認為這有多重要？



來源：IDC 安全終端調查，n=513

問：您認為將資料加密功能整合到電腦硬體中有多重要？



來源：IDC 安全終端調查，n=513

雖然內建安全功能的硬體非常重要，但整合資料加密也是一項關鍵要求，因為安全專家都知道，任何安全鏈中最薄弱的環節通常是最終使用者。這就是使用者身份驗證如此重要的原因，也是技術供應商努力發展身份驗證技術的原因；遺憾的是，我們的調查顯示，許多企業在此領域的工作落後。

從積極的方面來看，我們的調查顯示，68%的受訪者表示他們的公司要求使用複雜的密碼，63%的受訪者表示他們使用雙因素身份驗證。在較不積極的方面，只有 23%的受訪者使用單點登入技術（SSO），20%的受訪者使用生物識別安全技術（如指紋或臉部識別）。值得注意的是，在我們的受訪者中，有 56%的人認為生物識別身份驗證比密碼安全得多，35%的人認為生物識別身份驗證比密碼更安全一點，9%的人認為生物識別身份驗證與密碼同樣安全，沒有人（0%）認為生物識別身份驗證比密碼不安全。

最近新推出的一種重要的身份驗證技術是密碼金鑰(Passkey)，密碼金鑰是一種數位憑證，利用金鑰對來提供比密碼更安全的解決方案。由於這項技術還很新，只有 14%的受訪者表示自己的公司已使用這項技術，但明智的 IT 決策者如今應該密切關注這項技術。如需瞭解使用者身份驗證使用情況的詳細資訊，請參見圖 4。

圖 4

使用者身份驗證方法

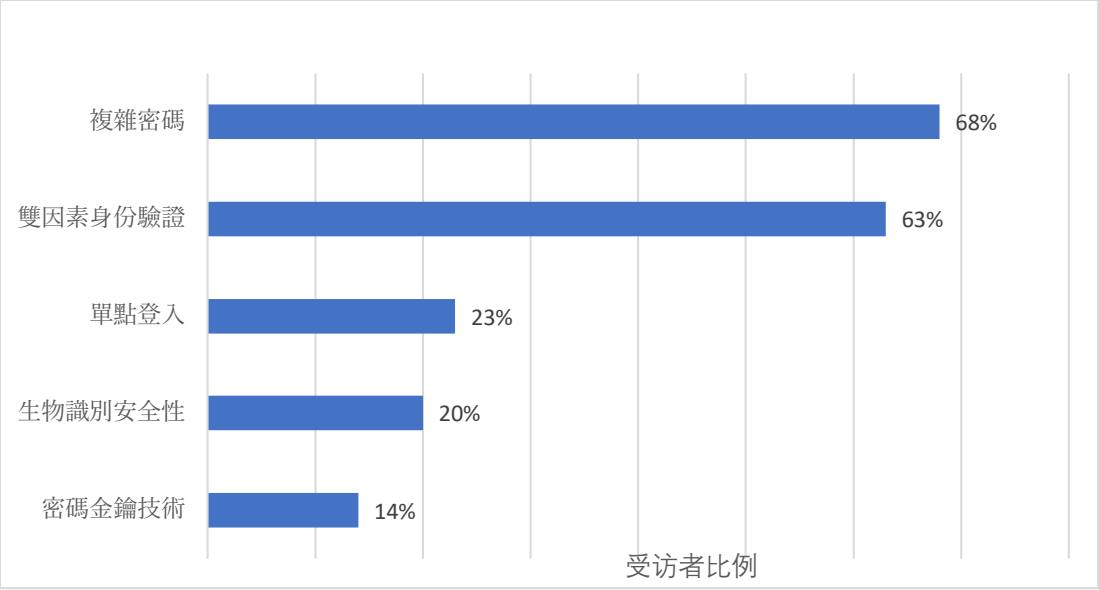
問題 1：貴公司是否要求員工使用複雜密碼登入電腦？

問題 2：貴公司是否部署了支援指紋掃描等生物識別安全措施的電腦？

問題 3：貴公司是否已開始研究使用密碼金鑰技術的好處？

問題 4：貴公司是否要求使用雙因素身份驗證？

問題 5：貴公司是否利用了單點登入（SSO）功能？（是/否）



來源：IDC 安全終端調查，n=513

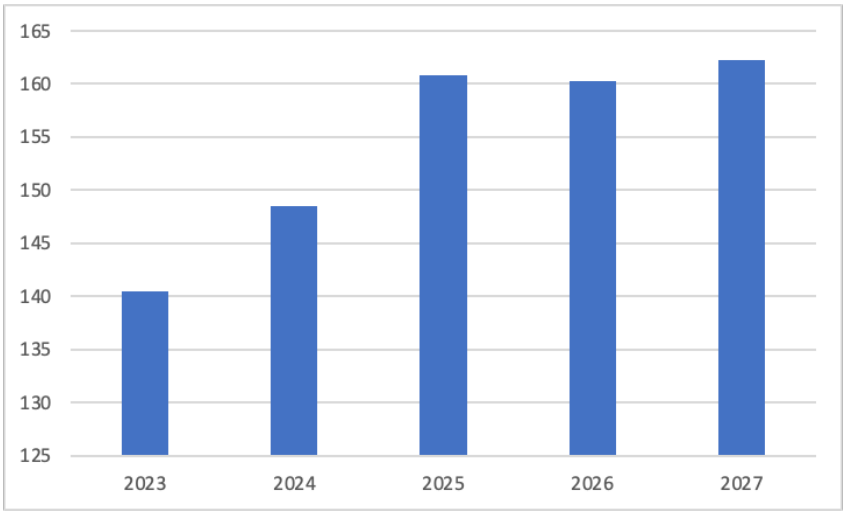
資料顯示的是回答「是」的百分比。

令人震驚的是，有相當高比例的受訪者甚至沒有實施複雜密碼（32%）或雙因素身份驗證（37%）等基本驗證協議。**值得借鑒的最佳實踐**是確保貴公司在整個公司範圍內實施統一的身份驗證形式，在確定了這個基準線之後，再開始考慮將 SSO 功能與強大的主身份驗證協議結合；最後，在完成下一次硬體更新換代時，深入瞭解能夠支援最高級別身份驗證的電腦：生物識別安全和密碼金鑰技術。啟用生物識別技術和密碼金鑰代表著未來員工可以快速、安全地登入電腦，並立即登入應用程式和網站。

我們將在本節討論最後一點，即您的下一次硬體更新換代。許多公司安裝的電腦老舊且需要更換，即使貴公司在 2020 年之前就購買了相當大比例的新終端，但這些電腦也將快接近四年大關。在此期間，硬體安全不斷發展，以應對現實中的威脅；或許同樣重要的是，這些產品大多是在企業廣泛轉變為遠端和混合工作方式之前出廠的，這意味著許多產品缺乏現今網路會議和協作應用所必需要的高品質的攝影機、麥克風和揚聲器。在經歷了數年出貨量減緩之後，IDC 個人運算裝置追蹤報告（IDC Personal Computing Device Tracker）預測該類別產品在未來幾年將呈現成長。注：商用單位指非消費者實體購買的單位。如需瞭解 IDC 的消費/商用電腦預測，請參見圖 5。

圖 5

全球商用電腦預測



來源：IDC PCD Tracker，2023 年 8 月

企業應不斷重新評估員工的電腦需求，才能保持市場競爭力，吸引並留住頂尖人才。過去，IT 部門必須在安全性和員工滿意度之間做出權衡取捨，而如今，合適的供應商可以幫助企業找到無需妥協的解決方案。最後，**另一個值得考慮的最佳實踐**是在下一次硬體部署中採用零信任存取原則，這種策略假設每當有裝置嘗試存取公司資源時，在透過驗證之前都不應該加以信任；零信任採用各種技術和流程來證明裝置（最佳作法是從晶片到關鍵 IT 和應用程式安全）、所連接的網路（例如，公共 Wi-Fi 與私人網路）的安全狀態和使用者身份。

考慮在企業中使用 Mac

如今，越來越多的 IT 部門開始支援 Mac，我們的調查指出了其中的關鍵原因。在我們的受訪者中，有 76%的人認為 Mac 比其他電腦更安全；而在未來 12 個月內，採用更多 Mac 的首要原因是受訪者認為 Mac 更安全（47%），緊隨其後的是易於部署和管理（36%）。

蘋果客戶聚焦

「蘋果產品的一個真正重要的特點是，隱私和安全實際上已經嵌入了產品本身，而不是事後才想到的，這也是我們非常欣賞的一點。」— Linda Jojo，美國聯合航空公司執行副總裁兼首席顧客長

蘋果公司致力於提供出色的使用者體驗，同時透過軟體將安全性嵌入蘋果晶片，從而強化安全性。蘋果公司的觸控 ID 就是一個範例，這是一種內建的生物識別安全功能，蘋果晶片具有 Secure Enclave 功能，可對用於保護觸控 ID 資料的密碼進行加密和保護。

為了解決作業系統和啟動順序被損毀的風險，Mac 配備了安全啟動和簽名系統磁碟區。安全啟動確保在啟動時只啟動經過加密認證的 macOS 版本，而簽名系統磁碟區可在運行時保護作業系統的完整性。過時的軟體也會帶來網路風險，蘋果公司可自動執行軟體更新，並對端到端派發和安裝加以保護，從而最大限度地降低此類網路風險。

優秀的第三方軟體有助於提高員工生產力，但這些軟體絕不能包含惡意軟體。蘋果公司採用多層次的方法來防止惡意軟體，蘋果的 Mac 應用程式商店會掃描每個應用程式以檢測是否存在惡意軟體。由於 MAC 上的軟體也可以從網路下載，因此蘋果要求開發者將其應用程式提交給蘋果公司的公證服務，該服務可以掃描檢測是否存在惡意軟體；MacOS 中包含的蘋果 Gatekeeper 會檢查是否經過公證，並阻止未經簽署的應用程式運行。此外，蘋果公司的反惡意軟體工具 XProtect 可以阻止和刪除任何已知的惡意軟體。

資料是企業價值最高的資產之一，必須得到相應的保護。在 Apple 服務（如 iMessage 和 iCloud）中，晶片強制 FileVault 加密、蘋果公司支援的 VPN 協議和端到端加密相結合，確保資料在靜態、傳輸和使用過程中都受到保護。

隨著社交工程成為威脅分子的熟練技能之一，最終使用者必須提高警覺，這是一項艱鉅的責任，但蘋果公司透過 Safari 詐欺網站告警來協助履行此一責任。此外，由於身份驗證憑證經常被威脅分子竊取，蘋果公司的密碼金鑰支援簡化了企業實現身份驗證方法現代化的途徑，同時也不會犧牲正向的最終使用者體驗。

良好的安全性與可靠的裝置管理密切相關，為此，蘋果公司提供了一系列裝置管理功能，包括內建的行動裝置管理（MDM）框架。Apple Business Manager 實現了零接觸部署並連結到 MDM 解決方案，而適用於 Mac 的端點安全 API 可讓開發人員建構解決方案來監控、分析和回應安全威脅。蘋果公司還提供了與內建 SSO 框架的身份整合，該框架可與現代身份供應商（IdP）協同合作。

最後，蘋果公司在 macOS 中提供的這些安全功能，包括主要和次要軟體更新，企業或消費者皆無需支付額外費用。

挑戰/機遇

儘管威脅環境不斷演進，但 IT 部門仍面臨著用更少的資金、更少的 IT 人員和更少的資源應對更複雜威脅環境的挑戰。除了應對每家企業都面臨的日常安全風險，許多 IT 組織還肩負著透過部署硬體、軟體和服務來提高員工生產力和滿意度的任務。要成功完成這兩項任務——提高安全性以及提升員工生產力及滿意度——看似很難，但這也為 IT 部門帶來了重要的機遇，即有機會重新評估所購買的硬體、軟體和服務、供應商，並且為日益增加的混合型員工部署這些硬體、軟體和服務。此外，現在顯然應該重新計算總體擁有成本（TCO）模型，以更好地反映企業購買和使用技術的現狀。

結論

安全性在現在和將來都是 IT 部門最關切的議題。在 IT 預算緊縮、重大硬體更新換代迫在眉睫之際，有必要重新評估未來的供應商。考慮實施有關身份驗證和零接觸部署的最佳實踐，並採購可實現這些轉變的硬體。如果有供應商提供具有內建安全功能和資料加密功能的電腦，您可以借此既實現安全性又提供正向的使用者體驗，而不必再為安全性而犧牲生產力和員工滿意度。

關於 IDC

國際資料公司（IDC）是全球著名的資訊技術、電信和消費科技諮詢、顧問和會展服務專業供應商。IDC 旨在幫助 IT 專業人士、業務主管和投資機構制訂以事實為基礎的技術外包決策和業務發展策略。IDC 在全球擁有超過 1100 名分析師，他們具有全球化、區域性和當地語系化的專業視角，對 110 多個國家的技術發展趨勢和業務行銷機會進行深入分析。在 IDC 超過 50 年的發展歷史中，眾多企業客戶借助 IDC 的策略分析而達致關鍵業務目標。IDC 是 IDG 旗下子公司，IDG 是全球領先的媒體出版、研究及會展服務公司。

全球總部

140 Kendrick Street
Building B
Needham, MA 02494
美國
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com