DELL Technologies

如何對抗現代網路威脅

運用整合式端點安全性與可管理性

CROWDSTRIKE intel ABSOLUTE®

DELL Technologies

執行摘要

新興攻擊手法造成新的風險。透過協同合作的多層防禦，搶先一步抵禦現代端點威脅。瞭解硬體遙測如何與軟體整合，以改善整個機隊的安全性和可管理性。運用易於管理的裝置和解決方案，加快中斷攻擊、支援零信任原則並安全地進行創新。

目錄

威脅情境

挑戰

解決方案

使用案例與對策

關鍵要點與行動呼籲

威脅情境

個案研究

2023 年，Eclypsium 發現臺灣製造商銷售的主機板韌體存在缺陷。研究人員原本的目的只是要讓韌體保持在最新狀態，卻發現程式碼的實作方式不安全，可能會讓該機制遭到劫持並用於安裝惡意軟體。

這項發現特別令人擔憂的幾個原因

- 韌體漏洞導致客戶暴露。
- 該漏洞存在於裝置的某個區域中，傳統上很難偵測到威脅。
- 它可用於發起略過認證檢查的遠端攻擊。

摘自頭條新聞...

威脅情境

意義

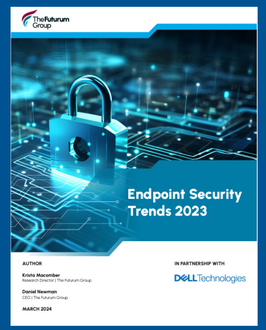
這是讓 IT 與資安團隊挑燈夜戰的主要因素：

以裝置為基礎的攻擊。

這些複雜的惡意攻擊可讓攻擊者取得具特殊權限的存取權。更重要的是，其中許多攻擊者可以關閉僅限傳統軟體的保護 (例如防毒軟體)，而且完全不會被發現。

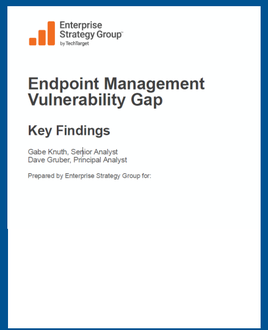
根據最近針對 IT 和資安專業人員進行的全球問卷調查[1]，組織採購新硬體時，其首要評估準則包括：

自動化偵測 BIOS 韌體事件



69% 的組織回報在過去 12 個月內，至少發生「一次」裝置層級攻擊。這比 2020 年的研究結果多達 1.5 倍[2]！

高風險組態



超過 75% 的組織回報，他們至少經歷過一次由未知、未受管理或管理不善的端點裝置所導致的網路攻擊[3]。

挑戰

那麼，是什麼讓裝置成為易受攻擊的目標呢？

可見度

這些攻擊在傳統上缺乏可見度和可觀測性的裝置部分執行，因此很難發現。

可據以行動性

組織通常備有數十種工具，而且個別運作。因此，如果偵測到攻擊，快速回應和補救將是一項重大挑戰，也需要大量的手動作業。

解決方案

可見度

可據以行動性

身為全球最大的技術供應商之一，Dell 非常重視安全性。這正是**我們打造商用電腦的原因，從一開始就優先考慮可見度和可據以行動性**。這讓 IT 和資安部門作業具備能力。

我們的商用電腦隨附**獨家內建安全性功能**，例如 BIOS 驗證[4] 和攻擊指標[4]，可協助偵測威脅，避免造成損害。我們透過 **Dell 專屬裝置遙測**功能顯示這些偵測[4]。Intel vPro® 上的-Dell 商用電腦在裝置層級偵測到潛在威脅時，便可將其傳送至作業系統，以進行更快、更有效的調查與回應

業界領導地位

Dell 提供全世界最安全的商用電腦[4]

瞭解在面對現代化威脅的情況下要如何維持裝置信任。

閱讀 Principled Technologies 關於裝置安全性的研究報告 →


Principled Technologies®

A Principled Technologies report: In-depth research. Real-world value.

A comparison of security features in Dell, HP, and Lenovo PC systems

Approach

Dell™ commissioned Principled Technologies to investigate 10 security features in the PC security and system management space:

- Support for monitoring solutions
- BIOS security and protection features
  - Platform integrity validation
  - Device integrity validation via off-site measurements
  - Component integrity validation for Intel® Management Engine (ME) via off-site measurements
  - BIOS image capture for analysis
  - Built-in hardware cache for monitoring BIOS changes with security information and event management (SIEM) integration
- Microsoft Intune management
  - BIOS setting management integrations for Intune
  - BIOS access management security enhancements for Intune
- Remote management
  - Intel vPro® remote management
  - PC management using cellular data

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original equipment manufacturers (OEMs): Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device application.

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

解決方案

透過共同運作的安全性與可管理性對抗威脅

Dell 和我們連結的合作夥伴生態系統，正努力為工作空間帶來可見度和可據以行動性。其中包括：

- Dell 供應鏈安全性和內建硬體與韌體防禦功能
- Intel 的核心矽晶和「作業系統底層」保護
- 透過 Dell 和統一端點管理主控台提供可管理性
- 範圍涵蓋端點、網路及 CrowdStrike 和 Absolute 等合作夥伴之雲端的進階威脅防護

生態系統使用電腦遙測作為連接器，有助於彌補 IT 與安全性解決方案之間，威脅可能趁虛而入的差距。此方法不僅有助於防止攻擊，還可以偵測和回應攻擊，並在攻擊後復原和補救。

使用案例與對策

為了示範整合的安全性和可管理性如何提高網路韌性，我們將介紹兩個使用案例，包括攻擊情境和對策。

首先是對 BIOS 韌體的攻擊。在這裡，我們會看到 BIOS 降級攻擊的網路攻擊鏈[5] 如何發揮作用。

BIOS 降級保護

初步存取：透過可移除媒體複製 + 網路釣魚

步驟 1a

惡意內部人員利用現有的 BIOS 漏洞，從遠端竊取作業系統認證。駭入裝置並降級 BIOS。

步驟 1b

攻擊者發動魚叉式網路釣魚攻擊，在管理員誤在惡意網站上驗證時，竊取工作階段權杖。

步驟 2

認證存取

攻擊者透過建立其他管理員帳戶來實現持續性，並繼續在網路中移動。

步驟 3

橫向移動

攻擊者對應網路並找到系統管理伺服器。

步驟 4

外流

攻擊者透過 Web 服務流出資料。

使用案例與對策

BIOS 降級對策

敵人以前所未有的速度闖入網路。事實上，CrowdStrike 的全球威脅報告指出，在 2023 年，電子犯罪突破平均時間 (闖入系統並橫向移動所需的時間) 從 2022 年的 84 分鐘減少到 62 分鐘。觀察到的最快突破時間僅為 2 分 7 秒[6]！

以下說明 Dell 和我們的合作夥伴 Intel® 及 CrowdStrike 如何運用硬體輔助安全性來協助攔截並抵抗攻擊鏈上的 BIOS 降級攻擊。

使用案例與對策

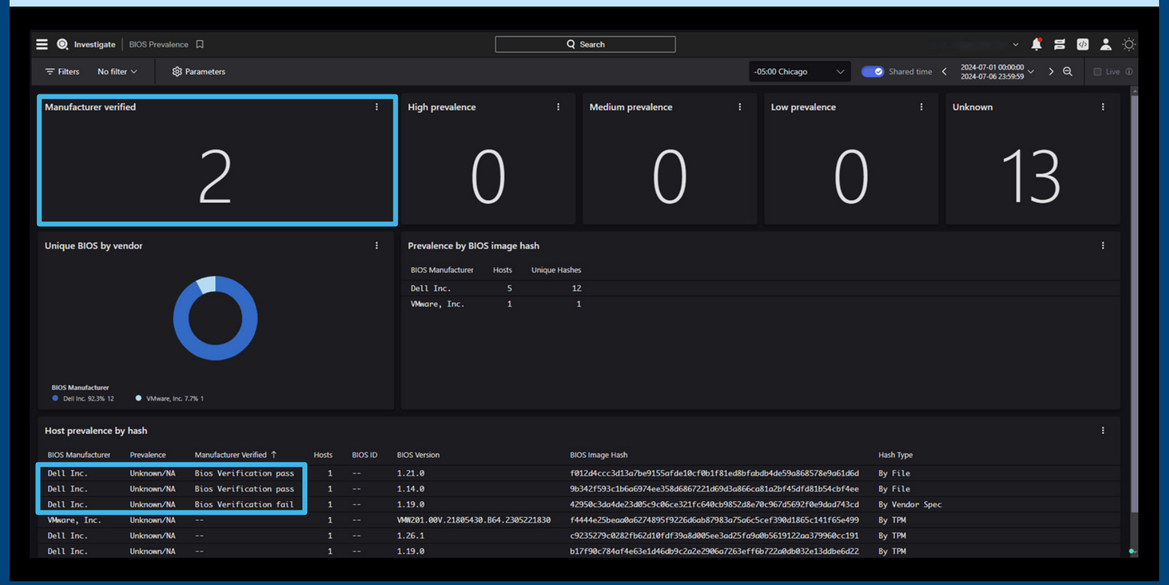
BIOS 降級對策

敵人以前所未有的速度闖入網路。事實上，CrowdStrike 的全球威脅報告指出，在 2023 年，電子犯罪突破平均時間 (闖入系統並橫向移動所需的時間) 從 2022 年的 84 分鐘減少到 62 分鐘。觀察到的最快突破時間僅為 2 分 7 秒[6]！

以下說明 Dell 和我們的合作夥伴 Intel® 及 CrowdStrike 如何運用硬體輔助安全性來協助攔截並抵抗攻擊鏈上的 BIOS 降級攻擊。

防止 | **偵測和回應** | 還原和補救

在 CrowdStrike Falcon 平台中偵測 BIOS 證明：啟用 Dell 裝置遙測後，管理員能以遠端方式在 CrowdStrike Falcon 中檢視內建安全性功能 (例如 BIOS 驗證) 的通知，協助在造成任何永久性損壞之前，加快偵測可疑活動的速度。



使用案例與對策

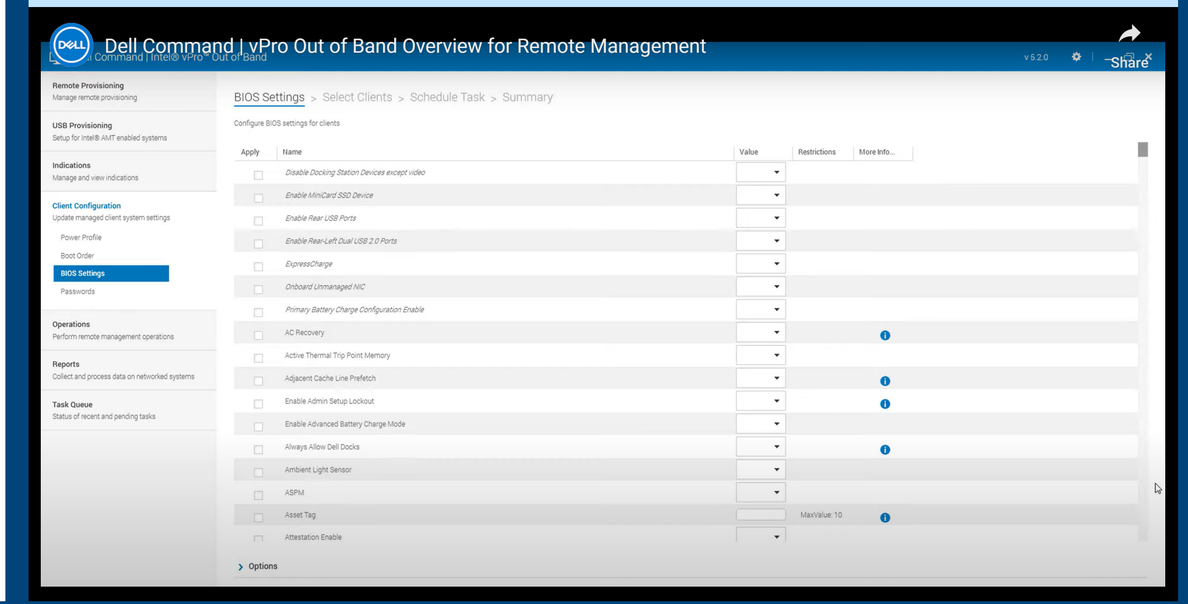
BIOS 降級對策

敵人以前所未有的速度闖入網路。事實上，CrowdStrike 的全球威脅報告指出，在 2023 年，電子犯罪突破平均時間 (闖入系統並橫向移動所需的時間) 從 2022 年的 84 分鐘減少到 62 分鐘。觀察到的最快突破時間僅為 2 分 7 秒[6]！

以下說明 Dell 和我們的合作夥伴 Intel® 及 CrowdStrike 如何運用硬體輔助安全性來協助攔截並抵抗攻擊鏈上的 BIOS 降級攻擊。

防止 | 偵測和回應 | **還原和補救**

補救 BIOS 降級：協助防止未來對頻外系統的威脅。搭載 Intel vPro 的 Dell Client Command Suite 可實現遠端補救。



使用案例與對策

在第二個使用案例中，以下說明軟體供應鏈攻擊之攻擊鏈中的步驟如何發揮作用。

軟體供應鏈攻擊

步驟 1

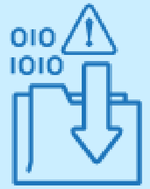
初步存取：供應鏈遭入侵

攻擊者將惡意程式碼注入軟體公用程式 (BIOS/韌體)。

步驟 2

持續性

客戶在更新裝置時會下載惡意程式碼。
攻擊者安裝惡意軟體。



步驟 3

橫向移動

攻擊者欺騙他們剛剛攻擊的使用者，並向其他使用者傳送惡意連結。該使用者按一下連結，而攻擊者竊取其登入資料。

步驟 4

外流

攻擊者流出資料。

使用案例與對策

供應鏈已成為攻擊者的主要目標。雖然這些攻擊不太常見，但成功攻擊的結果可能破壞性極大，因為組織仍在學習如何加強防禦。

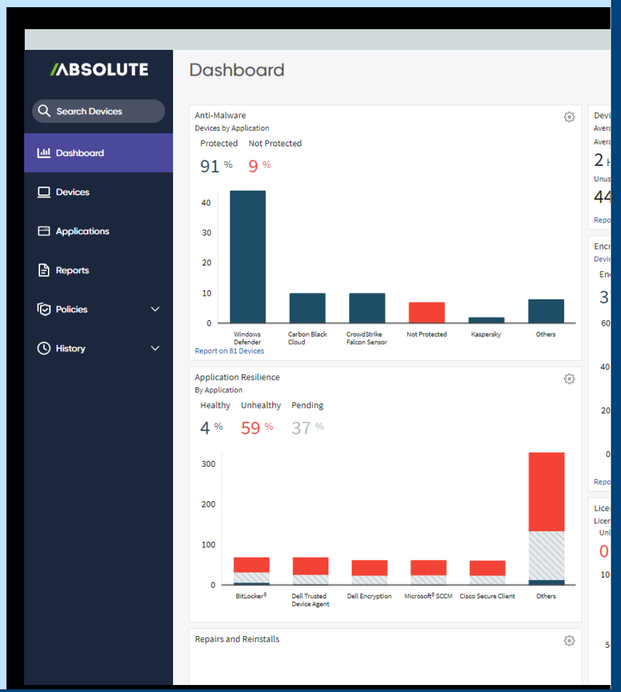
所有技術供應商的核心責任，是確保他們銷售的產品不會無意中透過漏洞為使用者帶來風險。

為了協助防止攻擊並提供對安全性堆疊的韌性，Dell 與 Intel® 均遵守安全開發週期[7] 的嚴格程序和通訊協定。額外的供應鏈保證，例如 Dell 安全元件驗證[8]，加上 Absolute 的韌體層級安全性 (如右圖所示)，在電腦的整個生命週期中都能讓客戶放心。

防止 | **偵測和回應** | **還原和補救**

出廠時的端點可見度：可透過在 Dell 代管工廠中內嵌的 Absolute，查看所有線上和離線裝置。Absolute 客製工廠安裝 (CFI) 可移除部署中的一個步驟，並保護可能運送至倉儲和多個最終使用者位置的裝置。從雲端型儀表板中完整檢視機隊，從而降低風險。

- 輕鬆找出並維護 IT 資產和應用程式的完整清單
- 尋找並繪製您的整個機群
- 最佳化資產使用率並監控安全狀態
- 跨平台支援 (Windows、Mac 和 Chrome)
- 內嵌於 27 種主流電腦 OEM 的 BIOS 中



使用案例與對策

供應鏈已成為攻擊者的主要目標。雖然這些攻擊不太常見，但成功攻擊的結果可能破壞性極大，因為組織仍在學習如何加強防禦。

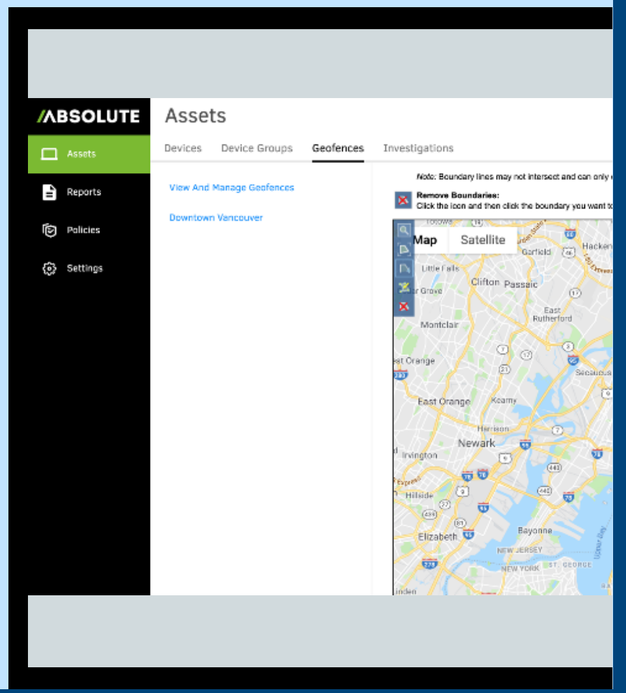
所有技術供應商的核心責任，是確保他們銷售的產品不會無意中透過漏洞為使用者帶來風險。

為了協助防止攻擊並提供對安全性堆疊的韌性，Dell 與 Intel® 均遵守安全開發週期[7] 的嚴格程序和通訊協定。額外的供應鏈保證，例如 Dell 安全元件驗證[8]，加上 Absolute 的韌體層級安全性 (如右圖所示)，在電腦的整個生命週期中都能讓客戶放心。

防止 | **偵測和回應** | 還原和補救

控制端點：使用 Absolute，偵測端點何時遭到入侵 (例如，關鍵應用程式被惡意軟體損壞，或電腦在運送過程中遺失)。採取遠端行動，透過使裝置無法使用及/或刪除裝置中所包含的資料，立即補救威脅。

- 在裝置超出界定範圍時提供防護
- 遠端防護和清除關鍵資料
- 執行符合法規遵循認證的壽命結束資料抹除作業
- 鎖定裝置以隨需保護關鍵資產
- 啟用遠端韌體保護



使用案例與對策

供應鏈已成為攻擊者的主要目標。雖然這些攻擊不太常見，但成功攻擊的結果可能破壞性極大，因為組織仍在學習如何加強防禦。

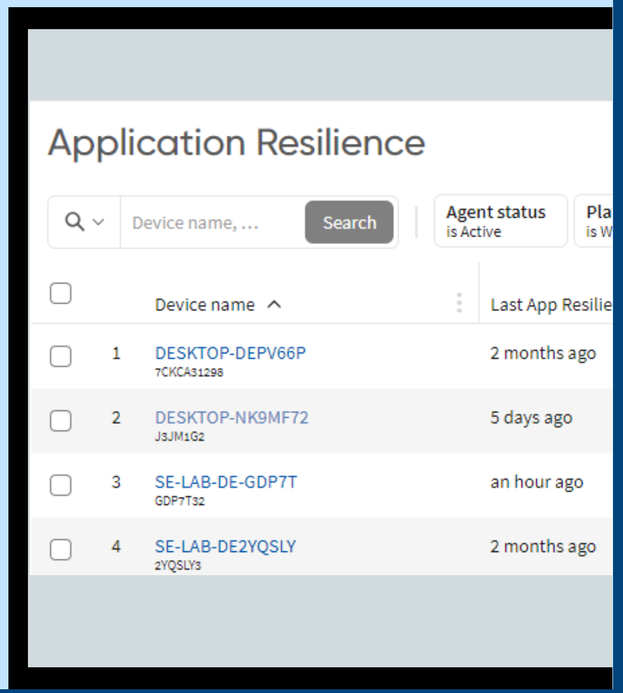
所有技術供應商的核心責任，是確保他們銷售的產品不會無意中透過漏洞為使用者帶來風險。

為了協助防止攻擊並提供對安全性堆疊的韌性，Dell 與 Intel® 均遵守安全開發週期[7] 的嚴格程序和通訊協定。額外的供應鏈保證，例如 Dell 安全元件驗證[8]，加上 Absolute 的韌體層級安全性 (如右圖所示)，在電腦的整個生命週期中都能讓客戶放心。

防止 | 偵測和回應 | **還原和補救**

自我修復：透過在 Dell BIOS 韌體內嵌的 Absolute Persistence，在偵測到竄改時，回到原始狀態。Absolute 可自行修復或持續處理應用程式復原目錄 (超過 80 個應用程式) 中，任何遭入侵的端點或支援的應用程式，包括現有的其他對策程式庫，例如 Dell Trusted Device 應用程式、Zscaler。

- 尋找並輕鬆刪除端點上的敏感性資料
- 透過自訂的指令檔程式庫採取補救措施
- 監控和自我修復應用程式
- 龐大且不斷成長的第三方端點控制應用程式復原目錄
- 與 Absolute 調查團隊一同調查和尋找遺失或遭竊的裝置



關鍵重點

機隊的安全性取決於其中的個別電腦。

為了對抗現代化威脅，裝置必須以安全的方式組建且必須具有內建安全性。

確保端點安全性和可管理性共同運作，以攔截、抵抗攻擊並從中復原。

安全性是一項團隊作業。善用硬體和軟體，獲得最佳防禦。

深入瞭解：

聯絡我們：Global.Security.Sales@Dell.com

請造訪：Dell.com/Endpoint-Security

追蹤我們：LinkedIn @DellTechnologies | X @DellTech

跨出下一步

不論組織規模大小，安全性都是令人頭疼的議題。**僱用經驗豐富的安全與技術合作夥伴，實現端點安全現代化。**

Dell Trusted Workspace 可協助確保端點安全，讓您打造支援零信任的現代化 IT 環境。Dell 獨家提供全方位的軟硬體保護產品組合，有助於減少攻擊面。我們高度整合的防禦型措施結合了內建防禦和持續警戒，可有效消除威脅。透過為現今雲端型世界打造的安全性解決方案，使用者可保持生產力，IT 團隊也能夠高枕無憂。

1. 資料來源：TechTarget 旗下企業策略集團，由 Dell Technologies 委託進行的自訂研究問卷，《*Assessing Organizations' Security Journeys*》(評估組織的安全性歷程)，2023 年 11 月。
2. 資料來源：Futurum 集團，《Endpoint Security Trends》(端點安全性趨勢)，2023 年。
3. 資料來源：TechTarget 旗下的企業策略集團，研究報告，《*Managing the Endpoint Vulnerability Gap: The Convergence of IT and Security to Reduce Exposure*》(管理端點漏洞差距：IT 和安全性整合以減少暴露)，2023 年 5 月。
4. 根據 2024 年 10 月的 Dell 內部分析。適用於搭載 Intel 處理器的電腦。並非所有電腦均可使用所有功能。部分功能需另外選購。經 Principled Technologies 驗證。《A comparison of security features》(安全性功能比較)，2024 年 4 月。
5. 資料來源：《What is the Cyber Kill Chain?》(什麼是網路攻擊鏈？)簡介指南 – CrowdStrike。
6. 資料來源：《CrowdStrike 2024 Global Threat Report》(CrowdStrike 2024 年全球威脅報告)。
7. 資料來源：建立裝置信任的三個注意事項 | Dell USA。
8. 資料來源：如何保密裝置信任 | Dell USA。