DELL Technologies

端點安全性是您零信任歷程的基本要素

備妥零信任的三項建議

執行摘要

零信任是一段長遠的歷程，這不是組織實作的產品或解決方案：它是用來管理安全性的策略架構，需要隨著時間的推移而建立。此電子書可為尋求零信任轉型的 IT 決策者提供實務指南，特別著重說明：端點裝置安全性扮演了什麼樣的角色，協助我們在隨處皆可工作的世界中建立真正安全的現代化基礎。

目錄

網路國情咨文

隨著世界日益趨向遠端/混和及雲端工作模式，安全性威脅與日俱增。

過去幾年來，保護組織資料資產的複雜度已大幅攀升。隨著採用遠端/混和式工作方式的增加，雲端技術對企業生產力已經產生顛覆性的影響，不過這也不是沒有代價的。從只管理內部部署基礎結構轉變為採用雲端，這項轉變為有心人士創造了更大的攻擊面，造成的影響也隨之擴大。舉例來說，如果攻擊得手，攻擊者所影響的，不僅只是單一客戶，而是雲端服務的所有客戶，還有他們在整個供應鏈中的客戶都可能受到影響，威脅行為者(民族國家和一般罪犯皆然)可獲得相當可觀的回報，因此他們會鍥而不捨地尋找新漏洞入侵。

網路犯罪造成的全球損失預計**將在 2025 年攀升至 10.5 兆美元**[i]

Verizon 的研究指出，據報 2022 年有 **5,200** 起經證實的資料外洩事件發生 –**數量是前一年的 1.3 倍**[ii]

當今隨處工作的環境所產生的影響

組織必須設法不斷演變的威脅態勢中保持領先。

所以說，隨著世界日益趨向遠端工作模式，可能產生哪些影響？有兩件事會發生：

所有組織都會遭受攻擊，...

「如果有一個目標明確的實體非常想進入您的系統，那麼他們得手的機率相當高。」

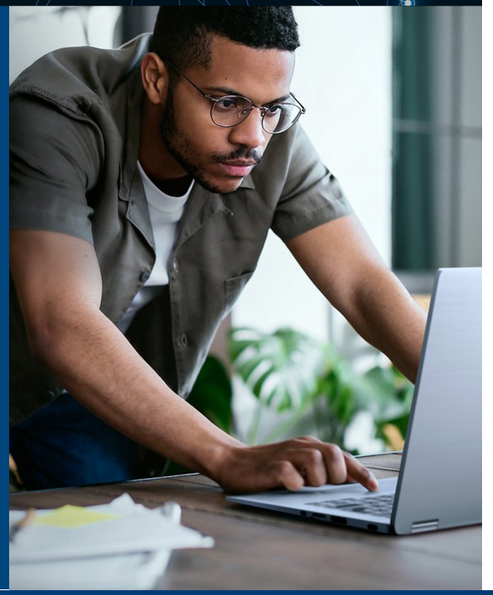
— 海軍上將 Michael Rogers，國家安全局前局長兼美國網戰司令部前指揮官[iii]

...而且稍有不慎，後果可能不堪設想。

「資料外洩的損失創下歷史新高，2022 年平均為 435 萬美元，[相較於 2020 年成長了 12.7%]。」[iv]

攻擊媒介正在增加，攻擊面也在擴大，沒有任何公司可以確保百分之百安全。組織必須假設最嚴重的情況，並改善防禦措施來面對無可避免的攻擊。

69% 的組織經歷過某些類型的網路攻擊，原因歸咎於某些疏於管理的網際網路資產[v]



安全策略必須與時俱進

我們必須接受雲端型環境。這正是零信任能夠派上用場的地方。

傳統安全模型不再有效。原因如下：

任何組織若要具備有效的安全狀態，必須對五大控制點負責：端點、工作負載、身分識別、網路和雲端。目標是為了保護應用程式和資料。

傳統方法經常分散孤立，讓使用這些方法的組織更容易遭受攻擊。

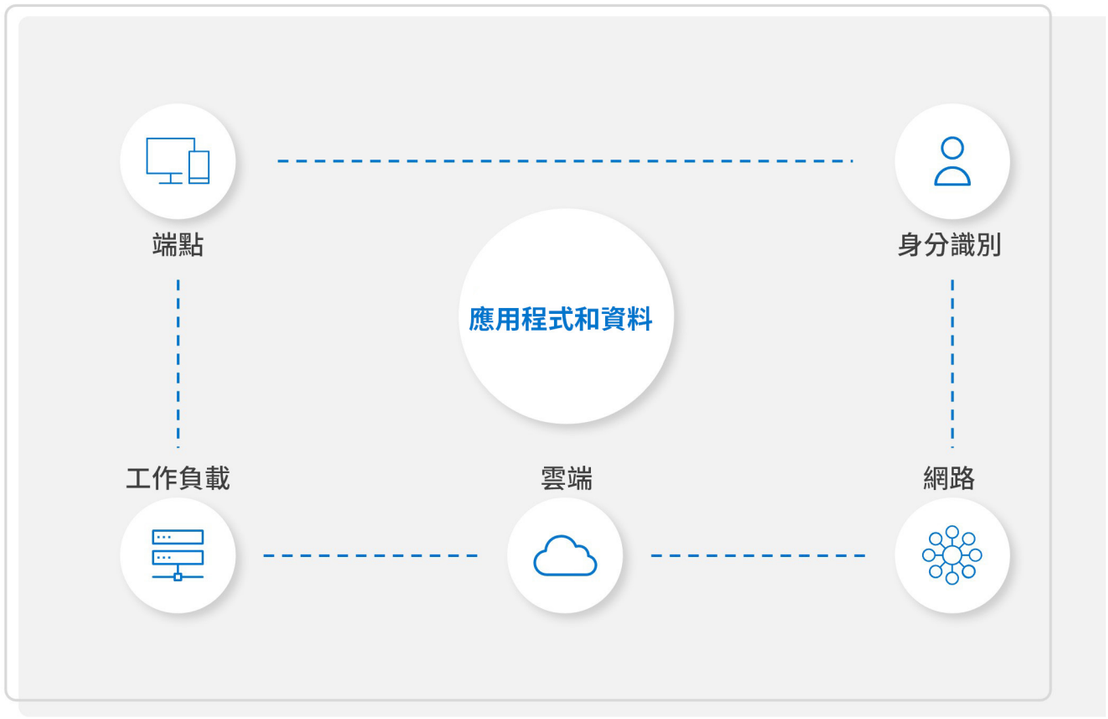
待續...

安全策略必須與時俱進

我們必須接受雲端型環境。這正是零信任能夠派上用場的地方。

現代化方法的發展可提供更多控制力，各控制點之間也能享有更良好的通訊。但隨著我們採用日益趨向遠端/混和式的工作環境，我們需要進一步強化周邊安全。

待續...

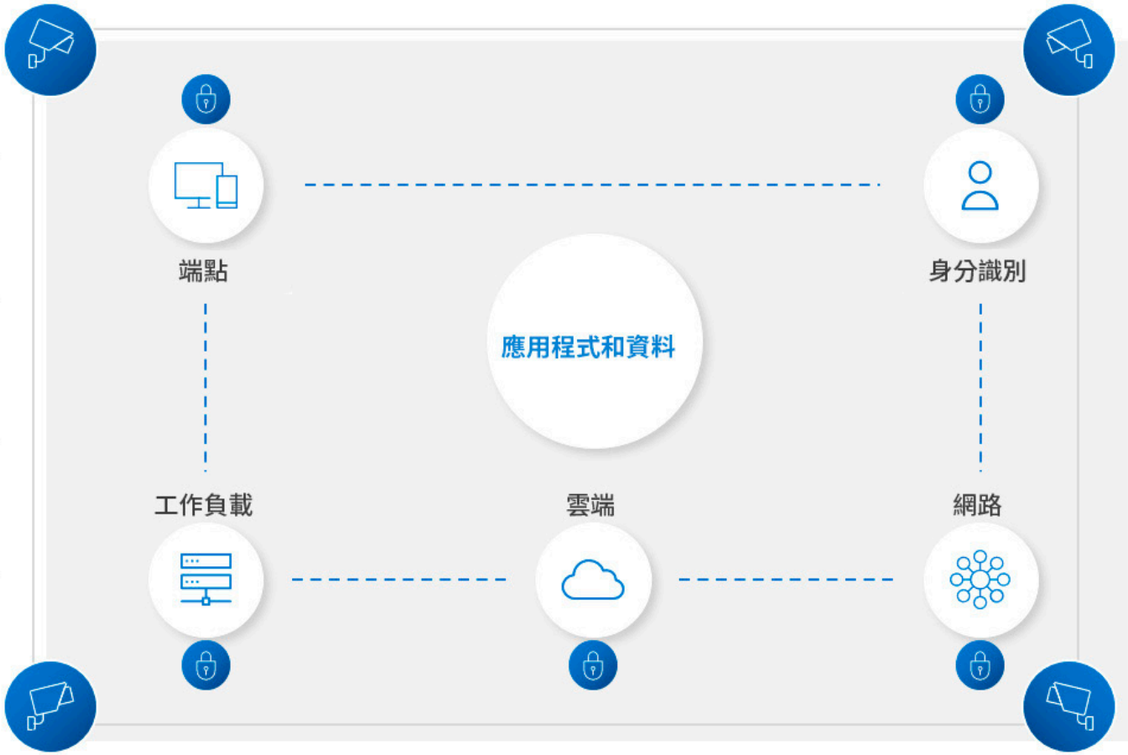


安全策略必須與時俱進

我們必須接受雲端型環境。這正是零信任能夠派上用場的地方。

如今員工隨處皆可工作，舉凡住家、咖啡廳和旅館等，他們經常使用不安全的 Wi-Fi，也幾乎無法連回受防火牆保護的辦公室與資料中心。既定情況可能是：員工從自己的裝置直接連線到網際網路，再連到雲端檔案伺服器和軟體即服務 (SaaS) 應用程式來處理企業資料。

隨著攻擊守法日益複雜，攻擊媒介數量不斷增加，以絕對信任為基礎的傳統安全策略不再奏效。這正是零信任能夠派上用場的地方。

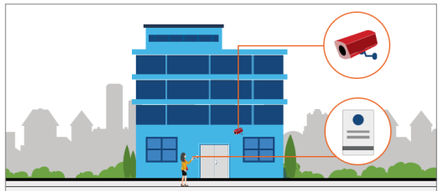


瞭解零信任的基礎知識

零信任為安全性注入全新思維，並取代了*絕對*信任 (也就是只要使用者通過驗證，就能不受限制的漫遊網路)。零信任翻轉了此典範，讓組織能夠明確掌控 IT 環境。

讓我們用一個為人熟知的概念比喻零信任：大樓安全協議。

您在公司辦公室工作，入職時獲得一張識別證，並瞭解了安全協議。您每天進入辦公大樓，大樓各處都設有監視器。您會在多個位置出示通行證。當您坐在辦公桌前，輸入密碼就能解鎖電腦。



一名員工抵達辦公大樓，取出證件以進入大樓。

待續...

瞭解零信任的基礎知識

零信任為安全性注入全新思維，並取代了*絕對*信任 (也就是只要使用者通過驗證，就能不受限制的漫遊網路)。零信任翻轉了此典範，讓組織能夠明確掌控 IT 環境。

讓我們用一個為人熟知的概念比喻零信任：大樓安全協議。

您在公司辦公室工作，入職時獲得一張識別證，並瞭解了安全協議。您每天進入辦公大樓，大樓各處都設有監視器。您會在多個位置出示通行證。當您坐在辦公桌前，輸入密碼就能解鎖電腦。

一名員工抵達辦公大樓，取出證件以進入大樓。

他們使用證件來進入前往指派之樓層的電梯。

待續...

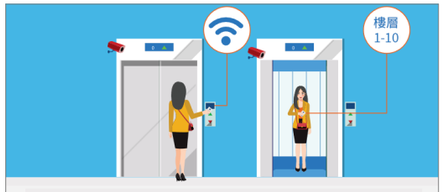
瞭解零信任的基礎知識

零信任為安全性注入全新思維，並取代了*絕對*信任 (也就是只要使用者通過驗證，就能不受限制的漫遊網路)。零信任翻轉了此典範，讓組織能夠明確掌控 IT 環境。

讓我們用一個為人熟知的概念比喻零信任：大樓安全協議。

您在公司辦公室工作，入職時獲得一張識別證，並瞭解了安全協議。您每天進入辦公大樓，大樓各處都設有監視器。您會在多個位置出示通行證。當您坐在辦公桌前，輸入密碼就能解鎖電腦。

一名員工抵達辦公大樓，取出證件以進入大樓。



他們使用證件來進入前往指派之樓層的電梯。

員工再次使用證件以啟動電梯內的樓層選擇。

待續...

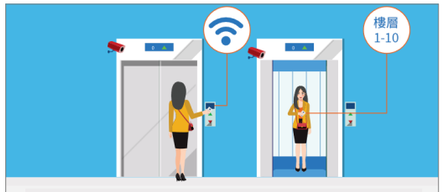
瞭解零信任的基礎知識

零信任為安全性注入全新思維，並取代了*絕對*信任 (也就是只要使用者通過驗證，就能不受限制的漫遊網路)。零信任翻轉了此典範，讓組織能夠明確掌控 IT 環境。

讓我們用一個為人熟知的概念比喻零信任：大樓安全協議。

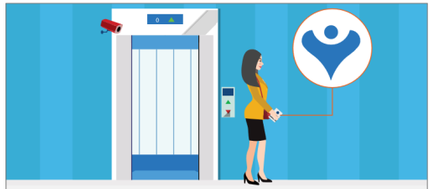
您在公司辦公室工作，入職時獲得一張識別證，並瞭解了安全協議。您每天進入辦公大樓，大樓各處都設有監視器。您會在多個位置出示通行證。當您坐在辦公桌前，輸入密碼就能解鎖電腦。

一名員工抵達辦公大樓，取出證件以進入大樓。



他們使用證件來進入前往指派之樓層的電梯。

員工再次使用證件以啟動電梯內的樓層選擇。



抵達該樓層後，員工走進辦公室套房。

待續...

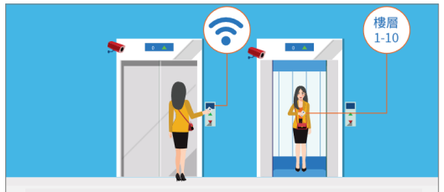
瞭解零信任的基礎知識

零信任為安全性注入全新思維，並取代了*絕對*信任 (也就是只要使用者通過驗證，就能不受限制的漫遊網路)。零信任翻轉了此典範，讓組織能夠明確掌控 IT 環境。

讓我們用一個為人熟知的概念比喻零信任：大樓安全協議。

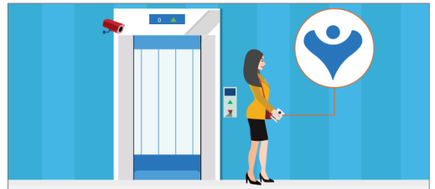
您在公司辦公室工作，入職時獲得一張識別證，並瞭解了安全協議。您每天進入辦公大樓，大樓各處都設有監視器。您會在多個位置出示通行證。當您坐在辦公桌前，輸入密碼就能解鎖電腦。

一名員工抵達辦公大樓，取出證件以進入大樓。



他們使用證件來進入前往指派之樓層的電梯。

員工再次使用證件以啟動電梯內的樓層選擇。



抵達該樓層後，員工走進辦公室套房。

他們刷 ID 卡以進入套房。

待續...

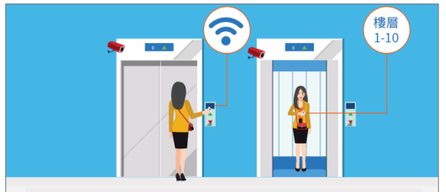
瞭解零信任的基礎知識

零信任為安全性注入全新思維，並取代了*絕對*信任 (也就是只要使用者通過驗證，就能不受限制的漫遊網路)。零信任翻轉了此典範，讓組織能夠明確掌控 IT 環境。

讓我們用一個為人熟知的概念比喻零信任：大樓安全協議。

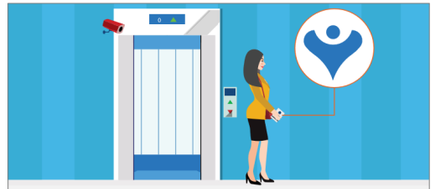
您在公司辦公室工作，入職時獲得一張識別證，並瞭解了安全協議。您每天進入辦公大樓，大樓各處都設有監視器。您會在多個位置出示通行證。當您坐在辦公桌前，輸入密碼就能解鎖電腦。

一名員工抵達辦公大樓，取出證件以進入大樓。



他們使用證件來進入前往指派之樓層的電梯。

員工再次使用證件以啟動電梯內的樓層選擇。



抵達該樓層後，員工走進辦公室套房。

他們刷 ID 卡以進入套房。

員工至辦公桌就座並使用密碼解鎖電腦。

待續...

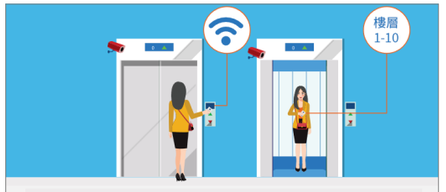
瞭解零信任的基礎知識

零信任運作方式如下。

雇主從您入職起便識別了您的身分。自此，您每次要求存取都需經過驗證以保護組織資產 (使用者、資料等)。為增添額外安全性，保全會透過監視器關注您的一舉一動。只要有任何異常行為皆需接受調查，例如試圖進入您不應進入的辦公空間。

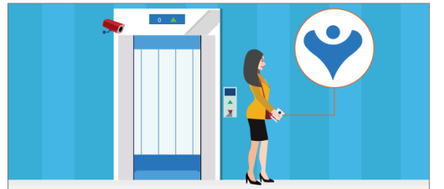
如今，我們發現使用者、裝置、應用程式和資料頻繁出現在公司網路以外的位置，這種情況前所未見。因此，使用者身分已成為安全盲點，身分洩漏是大多數入侵事件的關鍵因素。零信任程序可修正此問題。

一名員工抵達辦公大樓，取出證件以進入大樓。



他們使用證件來進入前往指派之樓層的電梯。

員工再次使用證件以啟動電梯內的樓層選擇。



抵達該樓層後，員工走進辦公室套房。

他們刷 ID 卡以進入套房。

員工至辦公桌就座並使用密碼解鎖電腦。

啟動零信任原則

端點安全是零信任轉型的關鍵要素。

若要有效啟用零信任策略，您必須保護端點安全。

根據 MITRE ATT&CK® 框架，現今有心人士會使用九種「初始存取技術」以侵入網路 *(請參閱圖例)*。[vi] 研究顯示，傳統防禦措施無法在雲端型環境中保護端點安全。攻擊者只需要找到單一進入點即可。透過端點，威脅執行者便能夠惡意探索裝置在整個生命週期中的眾多漏洞。

隨著裝置數量增加，端點成為越來越顯著的攻擊媒介。

零信任模型中的安全原則以明確的細節定義何謂「已知良好」，並封鎖其餘一切。威脅管理接著會監控任何偏離已知良好的情況，標幟不尋常的行為並觸發適當行動來補救潛在威脅。

圖例 1/3

啟動零信任原則

端點安全是零信任轉型的關鍵要素。

若要有效啟用零信任策略，您必須保護端點安全。

根據 MITRE ATT&CK® 框架，現今有心人士會使用九種「初始存取技術」以侵入網路 *(請參閱圖例)*。[vi] 研究顯示，傳統防禦措施無法在雲端型環境中保護端點安全。攻擊者只需要找到單一進入點即可。透過端點，威脅執行者便能夠惡意探索裝置在整個生命週期中的眾多漏洞。

隨著裝置數量增加，端點成為越來越顯著的攻擊媒介。

零信任模型中的安全原則以明確的細節定義何謂「已知良好」，並封鎖其餘一切。威脅管理接著會監控任何偏離已知良好的情況，標幟不尋常的行為並觸發適當行動來補救潛在威脅。

圖例 2/3

啟動零信任原則

端點安全是零信任轉型的關鍵要素。

若要有效啟用零信任策略，您必須保護端點安全。

根據 MITRE ATT&CK® 框架，現今有心人士會使用九種「初始存取技術」以侵入網路 *(請參閱圖例)*。[vi] 研究顯示，傳統防禦措施無法在雲端型環境中保護端點安全。攻擊者只需要找到單一進入點即可。透過端點，威脅執行者便能夠惡意探索裝置在整個生命週期中的眾多漏洞。

隨著裝置數量增加，端點成為越來越顯著的攻擊媒介。

零信任模型中的安全原則以明確的細節定義何謂「已知良好」，並封鎖其餘一切。威脅管理接著會監控任何偏離已知良好的情況，標幟不尋常的行為並觸發適當行動來補救潛在威脅。

圖例 3/3

備妥
零信任的
三項建議

讓貴組織
準備好邁向
成功的零信任轉型。

1

建立正確的原則和控制來支援您的業務優先事項。

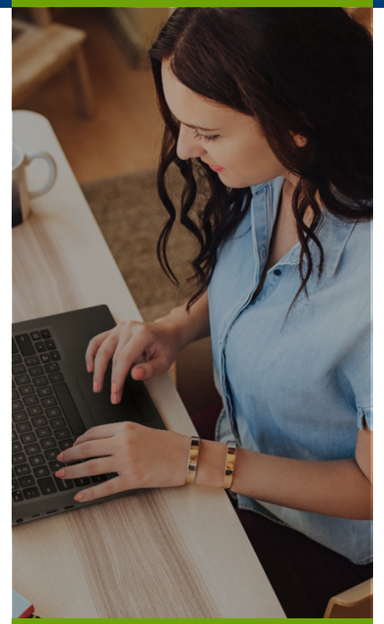
若要有效實作零信任，原則引擎和原則管理扮演著關鍵角色。但組織的安全預算有限，因此必須先確定您的業務優先事項。您試圖保護哪些最關鍵的資產和 IP？將該攻擊面與組織允許的風險相互權衡。

接著檢閱目前設置的原則和控制。現今風險源自於我們生活的雲端型世界，您的原則引擎有將此情況納入考量嗎？

在原則設置妥當以控管使用者存取您最重要的資產後，接著就可以擴大保護範圍。

深入瞭解

如需詳細資訊，請*觀看此影片*，Dell 網路專家會探討現今組織面臨的主要安全風險。



隨著越來越多使用者、應用程式、資料及裝置出現在公司網路以外位置，**82%** 的 IT 安全決策者表示必須重新評估安全原則。[x]

備妥
零信任的
三項建議

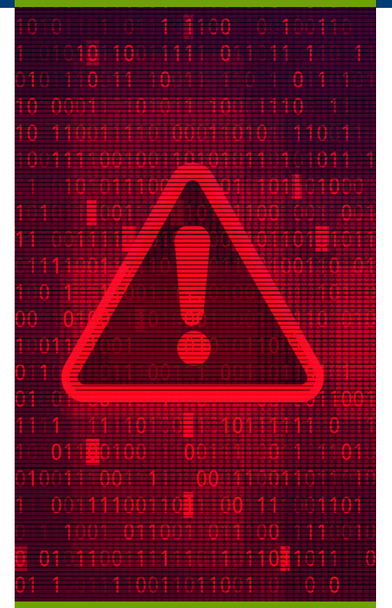
讓貴組織
準備好邁向
成功的零信任轉型。

2 第一步是安全的裝置。

為零信任計畫建立穩固的基礎。使用以安全性為設計與開發理念的裝置來增強您的防禦措施。其中包括：

A. **以硬體及韌體為基礎的防護**，保護端點堆疊並提供可見度 (例如：偵測 BIOS 是否遭入侵並對 IT 部門發出警示)。為貴組織配備相關技術，在每次出現新的存取要求時驗證身分，並將對員工生產力的影響盡可能降至最低。

B. **供應鏈防護與完整性控制**，保護電腦生命週期的各個階段。如近年所見，供應鏈攻擊的殺傷力不容小覷。若要建置真正的零信任架構，認證、驗證和監控工作必須從供應鏈開始。您的合作廠商必須 1) 採用安全實務，並且 2) 允許您驗證裝置的完整性 (從採購、製造到交付過程)。



在 **2021** 年，某家 IT 管理公司向至少 **1,500** 位客戶散播勒索軟體攻擊。[xi]

深入瞭解

如需深入瞭解裝置安全性的最佳實務，請參閱 Dell 和 Intel 的白皮書：
在作業系統外部和底層實現全面的安全性。

備妥
零信任的
三項建議

讓貴組織
準備好邁向
成功的零信任轉型。

3 致力在生態系統中實現順暢的整合及互通性。

若要取得有效的安全狀態，需具備的三大條件如下：

A. 整合 IT 生態系統中所有防禦措施、

B. 即時的可見度，以及

C. 視需要採取行動的能力。

在雲端型世界中，就算是放任最微小的漏洞也可能造成可怕夢魘，因此所有系統必須能識別潛在威脅*並且* 隨時準備好採取必要行動。

您的系統是否已整合，還是各自孤立運作？當 IT 管理員收到網路上有 BIOS 遭入侵的警示，您的原則引擎能否觸發特定工作流程？在整合環境中，自動化作業應立即隔離有問題的 BIOS、限制任何額外存取並執行修補。

您能夠全面掌握所有端點的狀態嗎？理想上，您的每一層都會有豐富的遙測資料流入，包含供應鏈 (例如卸貨區) 和韌體 (例如 BIOS 層級的防篡改警示)。

但此遙測的成效完全取決於您的整合。您能夠對資料採取行動嗎？具備正確的資源 (例如技術純熟的網路安全人才) 相當重要，如此您才能瞭解有助於解決問題的資料和程式工作流程。

41% 的組織
正在部署零信任[xii]

DELL Technologies

重點回顧

零信任是安全性的未來趨勢。

- 在我們迎接工作的未來發展時，攻擊媒介卻大幅增加了。
- 入侵事件防不勝防，早晚會發生。必須設置為最壞情況做好準備的防禦措施，將攻擊面縮減至最小。
- 零信任為安全性注入全新思維，讓組織能夠明確掌控 IT 環境。
- 維護安全的現代化基礎的關鍵，在於啟用零信任原則的端點防護。
- 精確定位您最重要的資產，排定建置零信任架構的優先順序。
- 向提供內建防護並深入投資供應鏈控制的廠商取得裝置。
- 評估安全性和 IT 互通性。持續嵌入各式工作流程，以增強您的安全狀態。

採取後續行動

不論組織規模大小，安全性都是令人頭疼的議題。不妨尋求經驗老到的安全性與技術合作夥伴，協助精簡您的零信任轉型歷程。

Dell Trusted Workspace 可協助保護端點，讓您打造支援零信任的現代化 IT 環境。Dell 獨家提供全面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護和持續警戒，可有效消除威脅。透過為現今雲端型世界設計的安全性解決方案，使用者可保持生產力，IT 團隊也能夠高枕無憂。

連絡我們：EndpointSecurity@Dell.com

造訪我們的網站：Dell.com/Endpoint-Security

關注我們：LinkedIn @DellTechnologies | Twitter @DellTech

DELL Technologies

[i] Cybersecurity Almanac 第 2 版。Cybersecurity Ventures，2022年 https://cybersecurityventures.com/cybersecurity-almanac-2022/

[ii] Ponemon Institute 和 IBM，「Cost of a Data Breach Report」(資料外洩的成本報告)，2022 年 https://www.ibm.com/security/data-breach

[iii] 美國心臟學院，「You Will Be Hacked. Plan Now: Cybersecurity in Health Care」(您將遭受駭客攻擊。立即研擬對策：醫療照護業網路安全)，2021 年 https://www.acc.org/Latest-in-Cardiology/Articles/2021/11/01/01/42/Feature-You-Will-Be-Hacked-Plan-Now-Cybersecurity-in-Health-Care

[iv] Ponemon Institute 和 IBM，「Cost of a Data Breach Report」(資料外洩的成本報告)，2022 年 https://www.ibm.com/security/data-breach

[v] 「ESG Complete Survey Results, Security Hygiene and Posture Management」(ESG 完整調查結果、安全檢疫和狀態管理)，2022 年 https://www.esg-global.com/research/esg-complete-survey-results-security-hygiene-and-posture-management

[vi] MITRE ATT&CK https://attack.mitre.org/tactics/TA0001/

[vii] Futurum，「Four Keys to Navigating the Hardware Security Journey」(硬體安全性歷程的四大關鍵)，2020 年 https://futurumresearch.com/research-reports/four-keys-to-navigating-the-hardware-security-journey/

[viii] Verizon 資料外洩調查報告，2022 年 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[ix] Verizon 資料外洩調查報告，2022 年 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[x] Absolute 端點風險報告，2021 年 https://www.absolute.com/go/reports/endpoint-risk-report/

[xi] TechTarget，2021 年 https://www.techtarget.com/searchsecurity/news/252503605/Kaseya-1500-organizations-affected-by-REvil-attacks

[xii] Ponemon Institute 和 IBM，「Cost of a Data Breach Report」(資料外洩的成本報告)，2022 年 https://www.ibm.com/security/data-breach