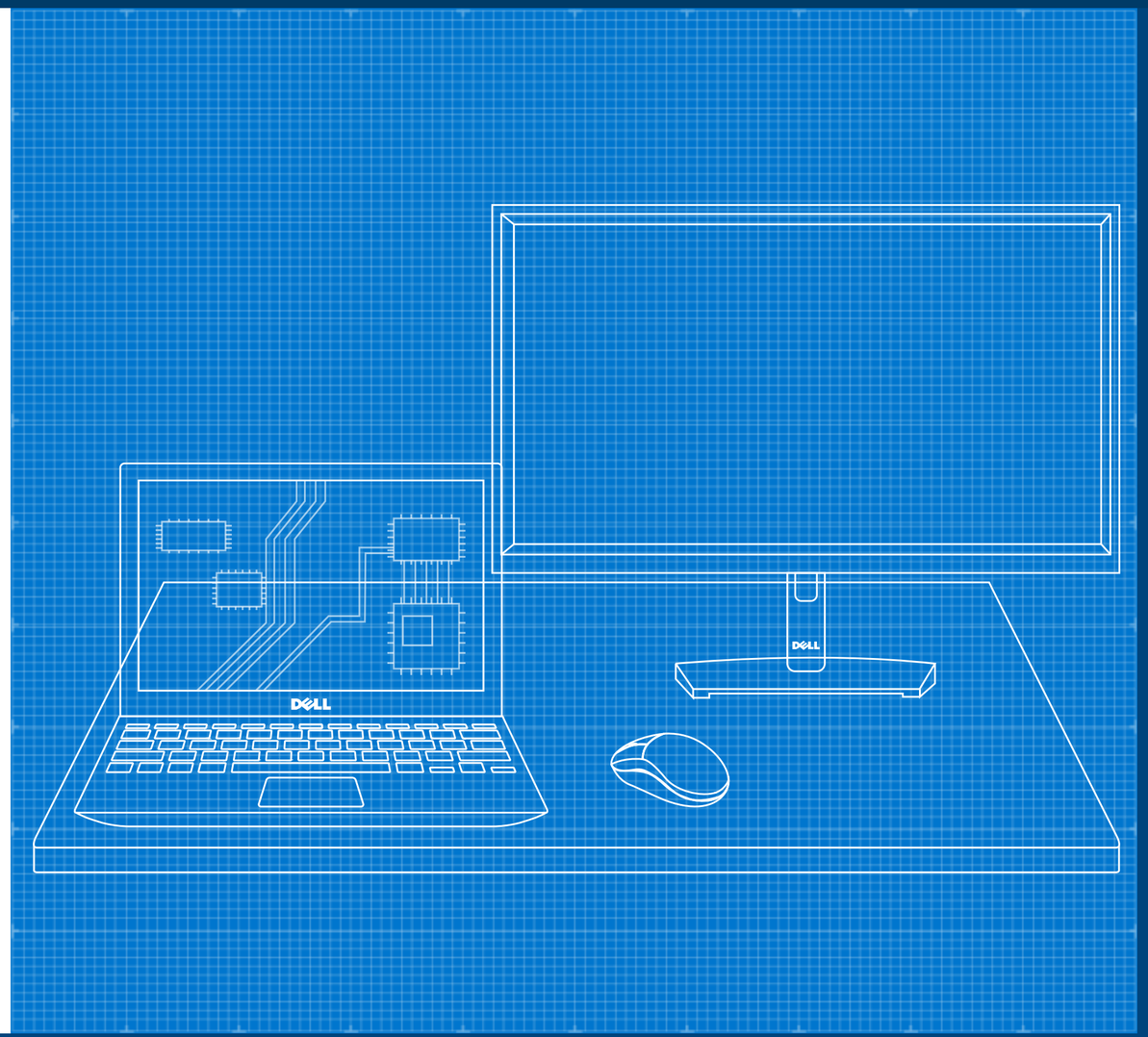
可信賴工作空間剖析

透過多層防禦提升機群安全性



執行摘要

網路攻擊無可避免，且規模及複雜度也正在與日俱增。端點裝置、網路和雲端環境已成為主要目標。

本電子書針對在不斷演進的威脅情境之中實現最有效端點防禦的所需要素，為 IT 和安全決策者提供指導。

目錄

威脅情境

轉換為混合工作模式帶來了新的複雜度和攻擊媒介，且**端點、網路和雲端正在擴展攻擊面**。

此外，攻擊者現在利用鎖定運算堆疊不同層級的先進技術，與有效系統流程融合。部分方法甚至允許攻擊者在*完全無法被偵測的情況下*獲得特權存取權限，並可停用軟體保護。

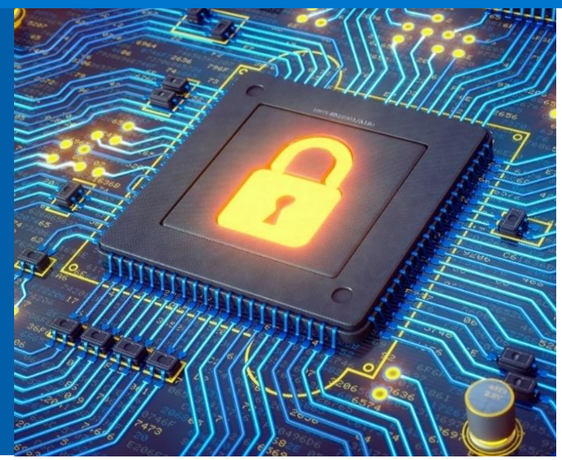
許多組織已著手建立「零信任」架構，以應對這些威脅。然而，若要啟用零信任原則，您必須能夠保持裝置信任度。

隨著攻擊日益頻繁，且先進技術創造新的攻擊媒介，**您該如何保持裝置信任度**？

[1]CrowdStrike 全球威脅報告，2023 年。
[2]Dell 創新指數調查，2023 年。

您知道嗎...

2022 年內，71% 的攻擊並非基於惡意軟體，同比增長 9%[1]



接受調查的組織中，僅 41% 可以非常有自信地宣告自己的技術和應用程式嵌入了安全性設計[2]

探索零信任，提升您的網路安全成熟度？請參閱電子書：*《Endpoint security is an essential element of your Zero Trust journey》(端點安全性是您零信任歷程的基本要素)*。

挑戰

為了實現有效的端點安全性，瞭解您的對手與其作業方式至關重要。

考慮到駭侵的潛在回報，**攻擊者通常會多次嘗試侵入同一組織，利用不同方法和進入點來提高勝算。**舉例來說，單一裝置的生命週期內，攻擊者可以透過數十種媒介試圖利用漏洞。

傳統防禦措施並不足以確保端點的安全。因為組織強化某個攻擊面時，威脅發動者可以轉向其他容易攻擊的目標。隨著世界朝向混合式邁進，威脅發動者已識別新的端點攻擊媒介，並導致毀滅性的後果。

請參閱右側的攻擊範例

供應鏈攻擊：針對供應商進行攻擊，以取得其系統、資料和/或網路的存取權，進而存取其客戶的系統、資料和/或網路。**範例：硬體供應鏈攻擊，由元件竄改所引發：**

攻擊者攔截個人電腦運輸，並更換硬碟。

IT 在整個公司內部署遭到入侵的裝置。

攻擊者安裝惡意軟體，以在使用者登入時擷取登入資料。

社交工程攻擊：誘騙最終使用者，使其提供可取得裝置和網路存取權限的敏感資訊。**範例：欺騙攻擊，由釣魚電子郵件所引發：**

最終使用者誤信釣魚電子郵件，並在偽造網頁上提供登入資料。

攻擊者使用有效的登入資料由遠端存取該網路。

攻擊者透過網路服務竊取資料、將被盜取的資料進行加密，並以此勒索贖金。

確保現代工作空間的安全

端點保護方面，您需要在裝置整個生命週期內的各種狀態下實施預防、偵測與回應，以及復原與補救措施，範圍涵蓋個人電腦的採購和製造、商品運送和部署、使用過程，直到汰換。想像一下這個綜合攻擊面的大小！

最有效的網路安全策略是針對最糟情境制定計劃。該策略假設可能發生入侵，並嵌入多層防禦，盡可能快速且頻繁地中斷攻擊。同時包含補救功能，以將重複發生的風險降至最低。

[3]Dell 創新指數調查，2023 年。

預防

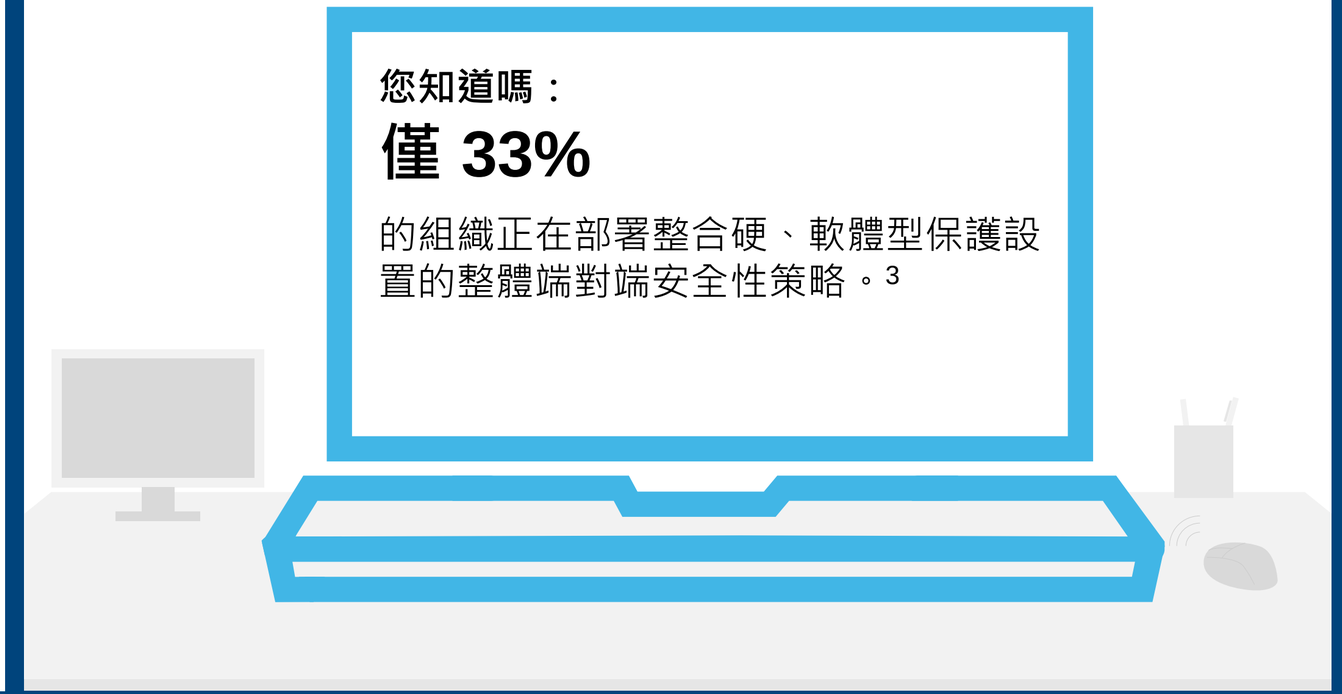
透過專為阻擋攻擊所設計的防禦措施，讓自己成為更小的目標。

偵測與回應

始終假設入侵，並保持警覺。

復原與補救

減輕攻擊影響，並恢復正常運作。



可信賴工作空間剖析

現代端點安全需要具備三點：

1. **軟體安全性：**如今，我們發現企業網路之外的使用者、裝置和資料比起以往更為廣泛。軟體安全性不僅保護裝置，還將保護擴展至經常發生惡意活動的網路和雲端環境。

2. **硬體安全性：**裝置必須包含內建安全性功能。這涉及硬體和韌體安全性，可保護使用中的裝置。若要防衛工作空間，您必須內建提供裝置可見度與控制的功能。

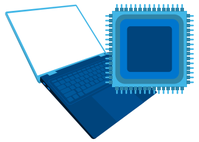
3. **供應鏈安全性：**裝置必須以安全的方式組建。這表示應與 a) 了解威脅情境，並且 b) 可在情境演變時利用該知識的供應商合作。安全的個人電腦設計、開發和測試可將產品漏洞的風險降至最低，供應鏈控制則可減輕產品竄改的風險。

解析多層級安全防護

(列舉安全措施的代表性範例)

軟體安全性

- 次世代防毒 (NGAV)
- 端點偵測和回應 (EDR)
- 延伸偵測和回應 (XDR)
- 雲端資料保護
- 網路保護
- 自動化自我修復



硬體和韌體安全性

- 啟動期間驗證
- 執行階段驗證
- 使用者認證
- 安全通知與警示/遙測

供應鏈安全性

- 安全的開發實務
- 安全的供應鏈實務
- 元件驗證
- 篡改證據封裝

我們的方法：Dell Trusted Workspace

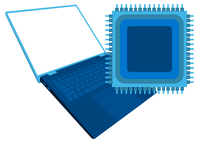
Dell 是全球組織的安全性和 IT 合作夥伴。與點解決方案不同，Dell 著重於整體安全成果，正在組建一套中斷攻擊鏈的解決方案，讓您更經得起網路攻擊的考驗。**Dell Trusted Workspace 包含：**

- 獨特的**硬體和韌體保護**，使 Dell 成為業界最安全的商用個人電腦。[4] *(搭配式及內建式安全性)*
- **業界領先軟體**合作夥伴生態系統，可為裝置、網路和雲端提供進階威脅保護。*(層疊式安全性)*

[4]根據 2023 年 9 月的 Dell 內部分析結果。適用於搭載 Intel 處理器的個人電腦。並非所有個人電腦均可使用所有功能。部分功能必須另外選購。

合作夥伴生態系統提供層疊*式*軟體安全性

- **Dell SafeGuard and Response**：**CrowdStrike**、**VMware Carbon Black** 和 **Secureworks** 提供威脅偵測、回應與補救措施。
- **Dell SafeData**：**Netskope** 提供雲端行應用程式的可見度、監控和資料遺失預防措施。**Absolute** 實現應用程式和網路的自我修復。



透過業界最安全的商用個人電腦提供內*建*硬體和韌體安全性[4]

保護使用中裝置的範例功能：

- **Dell SafeBIOS** 離線主機 BIOS Verification*和 Indicators of Attack*可協助在惡意活動入侵個人電腦前將其攔截。
- **Dell SafeID** 透過專屬的安全晶片保護使用者認證。*
- **離線主機韌體驗證**保持高特權韌體的完整性。*
- 透過 **Dell Trusted Device 軟體**，Dell 整合裝置遙測與業界領先的軟體，全方位提升機群安全性。*

搭配*式*供應鏈安全性協助確保個人電腦從首次開機即安全無虞

- **Dell SafeSupply Chain** 插件 (例如 Dell 安全元件驗證) 為產品完整性提供額外保障。

** Dell 獨家*

與 Dell 一起歸納統整

在硬體和軟體應對措施準備就緒的情況下，利用協助預防常見攻擊的防禦措施來縮小攻擊面。

偵測與回應功能會處理可能漏掉的隱匿式攻擊。

第 4 頁討論的供應鏈攻擊案例中，當您與 Dell 合作時，**安全的供應鏈實務**等預防性措施可在攻擊鏈初期中斷攻擊。如果漏掉某個攻擊，也可採取額外應對措施 (例如 **SCV**)。

社交工程攻擊案例中，即使攻擊者成功誘騙使用者交出有效認證，**SafeID 等硬體型使用者驗證**可立即阻止攻擊者，並拒絕進一步的存取。**新一代 Secure Web Gateway** 等安全軟體可提供另一層的監控保護。

對抗由元件竄改**引發的硬體供應鏈攻擊**。

攻擊者攔截個人電腦運輸，並更換硬碟。

- **安全的供應鏈實務**
- 篡改證據封裝
- 門鎖

IT 在整個公司內部署遭到入侵的裝置。

- 安全元件驗證 (SCV)
- 執行階段驗證

攻擊者安裝惡意軟體，以在使用者登入時擷取登入資料。

- 雲端存取安全性代理程式
- 新一代 Secure Web Gateway

對抗由釣魚電子郵件**引發的社交工程攻擊**。

最終使用者誤信釣魚電子郵件，並在偽造網頁上提供登入資料。

- NGAV
- EDR
- XDR

攻擊者使用有效的登入資料由遠端存取該網路。

- SafeID 提供多因素驗證
- 零信任網路存取

攻擊者透過網路服務竊取資料、將被盜取的資料進行加密，並以此勒索贖金。

- 新一代 Secure Web Gateway + 使用者實體行為分析

重點回顧

入侵無可避免。有效的端點安全性會始終假設最糟情境，並專注於從發生的任何位置 (裝置、網路到雲端) 中斷攻擊鏈。

任何解決方案都無法 100% 阻擋攻擊。結合硬體與軟體應對措施，獲得最佳防禦。

您的安全度取決於您的供應商。要求您的供應商概述其安全性措施。

Latitude 筆記型電腦與二合一個人電腦

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

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。**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。