DELL Technologies

零信任
提升網路安全性的途徑

與經驗豐富的技術和安全性合作夥伴一起踏上零信任歷程。

提高網路安全成熟度的組織正在建立可行藍圖，以找出可減少攻擊面、偵測及因應網路威脅的方法，並實作可從網路攻擊中復原的方法，而這些動作均可透過零信任功能完成。

為了解決日益複雜的網路威脅，Dell 運用我們的解決方案與合作夥伴提供的內建安全性功能，協助客戶實現符合客戶業務目標的零信任方法。

什麼是零信任？

將您的網路想像成一座城堡。當放下橋梁讓他人進入時，這些人便可隨意漫遊。是時候將週邊防禦安全模式更新為更現代化、更安全的零信任框架了。

相較於您購買的產品，零信任是一種架構式安全性方法。此方法絕對不相信任何人，且在授予任何人或任何對象資源存取權之前，一律會驗證業務用途是否正當。

這表示此方法預設為不信任使用者和裝置，即使使用者和裝置已連線至授權網路或已預先通過驗證亦然。

絕不信任，一律驗證。

安全 IT 生態系統的基礎

國家標準暨技術研究院 (NIST) 定義的零信任框架已由美國國防部 (DoD) 採用並內建於架構中。

此框架包含相互關聯的七大支柱，可在所有安全領域中引導 Dell Technologies。結合在一起後，這些支柱可提供多層面的整合式架構，實現全方位的資安措施，從而保護貴組織的資料和基礎架構。

由於難以整合各種安全性功能以及掌握多個資安服務供應商之間分散的選項，因此零信任機制的採用一直具有挑戰性。

NIST

U.S. Department of Defense

DELL Technologies

提高零信任成熟度。

無論您處於歷程的哪個階段，Dell 都有解決方案可提供協助。

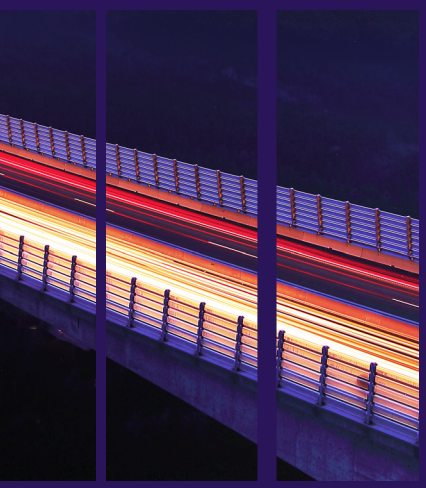
Dell Technologies 可為貴組織帶來選擇和彈性。如果您想要提高網路安全成熟度，我們可以提供安全性解決方案與零信任功能，協助您增強自己的強化能力，以便偵測和防範惡意網路活動並從中復原。

啟用零信任原則。

提供提高網路安全成熟度的選擇與彈性。

Dell Technologies 提供安全性解決方案和零信任功能，可協助您增強自己的強化能力，以便偵測和防範惡意網路活動並從中復原。運作方式如下：

- 內建保護措施，可增強自動化功能、威脅情報、驗證、可見度等
- 提供各種服務，可開發藍圖、整合關鍵技術及主動管理，以支援零信任機制
- 專業的管理型安全性諮詢服務
- 廣泛的合作夥伴生態系統



大幅簡化零信任機制採用過程。

運用完全整合的架構全力推動。

零信任是一種架構式安全性方法，因此並非單一產品，並且需要精心規劃且協調一致的解決方案。Dell 正在減輕零信任整合的負擔。下面介紹我們的做法：

- Dell 正在建立第一個且唯一由美國國防部進行設計、測試及驗證的完全整合零信任架構

DELL Technologies

啟用零信任原則。

透過以特定安全性生態系統為基礎的方式實現零信任。

Dell 可協助提高網路安全成熟度，以支援零信任策略，進而減少攻擊面、強化偵測功能，並加快從網路威脅中復原的速度。

在圖示的每個零信任支柱中，都有與關鍵領域相應的技術、程序及人員，而且這些領域需要安全性和業務原則以保護您的組織。Dell 資訊安全服務可提供以下協助：

- 安全性成熟度、零信任及風險評估
- 策略和藍圖開發
- 關鍵零信任功能管理型服務

DELL Technologies

零信任基礎。

我們提供進階內嵌安全性解決方案，可讓您在邁向零信任之路時取得優勢。

Dell Data Protection

Cyber Recovery 存放庫 | PowerProtect Data Manager | CyberSense Transparent Snapshot | CloudIQ | 系統鎖定 | 偏差偵測 | 安全的企業金鑰管理 | TLS 1.3 | IPv6 | 多因素驗證 | 單一登入 | 角色型存取 | CloudIQ

Dell PowerEdge 伺服器

軟體材料清單 | 安全元件驗證 | Silicon Root of Trust | 系統鎖定 | 偏差偵測 | 安全企業金鑰管理 | TLS 1.3 | IPv6 | 多因素驗證 | 單一登入 | 角色型存取 | CloudIQ

Dell 儲存平台

資料隔離 | 資料不變性 | 威脅偵測 | 存取控制驗證 | 資料加密 | STIG 強化 | Hardware Root of Trust | 安全開機 | 數位簽署韌體 | 角色型存取 | 安全快照

Dell HCI/CI

Hardware Root of Trust | 安全開機信任鏈 | 數位簽署更新 | 金鑰管理 | 安全記錄 | 分散式虛擬交換器 | VM 隔離 | 驗證與授權 | 生態系統連接器 | 持續驗證狀態 | 軟體程式碼完整性 | 電子相容性對照表

Dell 商用電腦

BIOS/韌體安全性 | 硬體安全性 | 供應鏈保證 | 威脅管理軟體 (EDR、XDR、VDR) | 網路和雲端資料保護軟體

Dell 邊緣解決方案

硬體/軟體/VM 證明 | 安全登錄 | 信任鏈 | 安全的作業系統/應用程式交付 | 資料權限管理

Dell 網路交換器

SmartFabric | CloudIQ | SD-WAN | VLAN 分段 | Enterprise SONiC | 存取控制清單 | RADIUS | TACACS+ | 加密技術 | 交換器強化 | 微分段 | 虛擬路由和轉送

DELL Technologies

我們的加速方法。

Project Fort Zero 提供快速且徹底的方法，可將零信任機制全面整合至您的整個組織中。

Project Fort Zero 提供經驗證的方法，可立即提高零信任成熟度、縮短採用時間、減少中斷情形及管理成本。

根據我們的專業知識和業界影響力，美國國防部要求 Dell Technologies 協助加快採用零信任機制的速度。為了協助公家機關和私有部門組織簡化採用過程並在全球擴充零信任架構，Dell 正在建立生態系統，並主導超過 30 家領先業界之技術與安全公司的整合。我們正在為世界各地的私人和公共組織主導零信任架構的開發與全球擴充。這證明了 Dell 對美國國防部實現零信任之目標的承諾。

內部部署

在資料安全性和法規遵循至關重要的各組織資料中心內。

遠端或區域

在零售商店等位置，安全且即時的客戶資料分析可提供競爭優勢。

可拆式邊緣

在飛機或車輛等具有間歇性連線情況的位置，需要暫時性實作以確保作業持續性。

DELL Technologies

我們將協助您部署美國國防部為進階零信任機制提出的全部 152 項活動，從而加快零信任機制採用速度。

執行啟用程式

準則 | 組織 | 訓練 | 材料 | 領導階層與教育業者 | 人員 | 設施 | 政策

零信任目標層級

使用者信任

- 使用者詳細目錄
- 應用程式型權限
- 規則型動態存取 (第 1 部分)
- 組織MFA/IDP
- 實作系統並減少具有特殊權限的使用者 (第 1 部分)
- 組織身分識別生命週期管理
- 依預設原則拒絕使用者
- 單一驗證
- 實作系統並減少具有特殊權限的使用者 (第 2 部分)
- 組織身分識別生命週期管理 (第 1 部分)
- 實作UEBA 工具
- 定期驗證
- 企業PKI/IDP (第 1 部分)

裝置信任

- 裝置說明工具差距分析
- 將 NextGen AV 工具與 C2C 整合
- 受管理的 NPE/PKI 裝置
- 依預設原則拒絕裝置
- 實作 UEDM 或同等工具
- 企業裝置管理 (第 1 部分)
- 實作 EDR 工具並與 C2C 整合
- 實作資產、漏洞及修補程式管理工具
- 企業 IDP (第 1 部分)
- 實作以 C2C/法規遵循為基礎的網路授權 (第 1 部分)
- 實作應用程式控制和 FIM 工具
- 有限的管理型 BYOD 和 IOT 支援
- 企業裝置管理 (第 2 部分)
- 實作 XDR 工具並與 C2C 整合 (第 1 部分)

應用程式和工作負載

- 應用程式/程式碼識別
- 資源授權 (第 1 部分)
- 建立 DevSecOps 軟體工廠 (第 1 部分)
- 已核准二進位檔/程式碼
- 漏洞管理方案 (第 1 部分)
- SDC 資源授權 (第 1 部分)
- 資源授權 (第 2 部分)
- 建立 DevSecOps 軟體工廠 (第 2 部分)
- 自動化應用程式安全性與程式碼補救 (第 1 部分)
- 漏洞管理方案 (第 2 部分)
- 持續驗證
- SDC 資源授權 (第 2 部分)

資料信任

- 資料分析
- DLP 執行點記錄和分析
- DRM 執行點記錄和分析
- 定義資料標記標準
- 實作資料標記和分類工具
- 檔案活動監控 (第 1 部分)
- 實作 DRM 和保護工具 (第 1 部分)
- 實作執行點
- 互通性標準
- 制定 SDS 原則
- 手動資料標記 (第 1 部分)
- 檔案活動監控 (第 2 部分)
- 實作 DRM 和保護工具 (第 2 部分)
- 透過資料標籤和分析執行 DLP (第 1 部分)
- 將 DAAS 存取與 SDS 原則整合 (第 1 部分)
- 透過資料標籤和分析執行 DRM (第 1 部分)
- 將 SDS 解決方案和原則與企業 IDP 整合 (第 1 部分)

網路和環境

- 定義精細控制存取規則和原則 (第 1 部分)
- 定義 SDN API
- 定義精細控制存取規則和原則 (第 2 部分)
- 實作 SDN 可程式化基礎架構
- 資料中心巨集分段
- 實作微分段
- 將流量分段至控制管理和資料平面
- B/C/P/S 巨集分段
- 應用程式和裝置微分段
- 保護傳輸中資料

自動化和協調流程

- 原則詳細目錄和開發
- 工作自動化分析
- 回應自動化分析
- 工具法規遵循分析
- 組織存取設定檔
- 實作 SOAR 工具
- 標準化 API 呼叫和結構描述 (第 1 部分)
- 工作流程擴充 (第 1 部分)
- 企業安全性設定檔 (第 1 部分)
- 企業整合與工作流程佈建 (第 1 部分)
- 實作資料標記和分類 ML 工具
- 標準化 API 呼叫和結構描述 (第 2 部分)
- 工作流程擴充 (第 2 部分)

可見度和分析能力

- 擴充考量
- 記錄剖析
- 資產 ID 和警示相互關聯
- 威脅警示 (第 1 部分)
- 實作分析工具
- 網路威脅情報方案 (第 1 部分)
- 記錄分析
- 威脅警示 (第 2 部分)
- 使用者/裝置基準
- 建立使用者基準行為
- 基準和剖析 (第 1 部分)
- 網路威脅情報方案 (第 2 部分)

目標活動總數：91

資料來源：《DoD Zero Trust Strategy》(美國國防部零信任策略) 出版物，2022 年 11 月 7 日

DELL Technologies

進階零信任機制

使用者信任

- 規則型動態存取 (第 2 部分)
- 企業角色和權限 (第 1 部分)
- 替代彈性 MFA (第 1 部分)
- 即時核准與 JIT/JEA 分析 (第 1 部分)
- 企業身分識別生命週期管理 (第 2 部分)
- 使用者活動監控 (第 1 部分)
- 持續驗證 (第 1 部分)
- 持續驗證 (第 2 部分)
- 企業 PKI/IDP (第 3 部分)
- 企業角色和權限 (第 2 部分)
- 替代彈性 MFA (第 2 部分)
- 即時核准與 JIT/JEA 分析 (第 2 部分)
- 企業身分識別生命週期管理 (第 3 部分)
- 使用者活動監控 (第 2 部分)
- 企業 PKI/IDP (第 2 部分)

裝置信任

- 企業 IDP (第 2 部分)
- 實作以 C2C/法規遵循為基礎的網路授權 (第 2 部分)
- 實體活動監控 (第 1 部分)
- 將裝置安全性 Slack 與 C2C 完全整合
- 企業 PKI (第 1 部分)
- 完整的管理型 BYOD 和 IoT 支援 (第 1 部分)
- 實作 XDR 工具並與 C2C 整合 (第 2 部分)
- 實體活動監控 (第 2 部分)
- 企業 PKI (第 2 部分)
- 完整的管理型 BYOD 和 IoT 支援 (第 2 部分)

應用程式和工作負載

- 豐富資源授權屬性 (第 1 部分)
- 豐富資源授權屬性 (第 2 部分)
- 持續的運作授權 (ATO) (第 1 部分)
- 自動化應用程式安全性與程式碼補救 (第 2 部分)
- REST API 微分段
- 持續的運作授權 (ATO) (第 2 部分)

資料信任

- 手動資料標記 (第 2 部分)
- 資料庫活動監控
- 自動化資料標記和支援 (第 1 部分)
- 透過資料標籤和分析執行 DRM (第 2 部分)
- 透過資料標籤和分析執行 DLP (第 2 部分)
- 將 DAAS 存取與 SDS 原則整合 (第 2 部分)
- 將 SDS 解決方案和原則與企業 IDP 整合 (第 2 部分)
- 整合 SOS 工具和/或與 DRM 工具整合 (第 1 部分)
- 自動化資料標記和支援 (第 2 部分)
- 全方位的資料活動監控
- 透過資料標籤和分析執行 DRM (第 3 部分)
- 透過資料標籤和分析執行 DLP (第 3 部分)
- 將 DAAS 存取與 SDS 原則整合 (第 3 部分)
- 整合 SDS 工具和/或與 DRM 工具整合 (第 2 部分)

網路和環境

- 網路資產探索與最佳化
- 即時存取決策
- 處理微分段

自動化和協調流程

- 企業安全性設定檔 (第 2 部分)
- 企業整合與工作流程佈建 (第 2 部分)
- 實作 AI 自動化工具
- 工作流程擴充 (第 3 部分)
- 由分析驅動的 AI 決定 A&O 修改項目
- 實作教戰手冊
- 自動化工作流程

可見度和分析能力

- 威脅警示 (第 3 部分)
- 基準和剖析 (第 2 部分)
- UEBA 基準支援 (第 1 部分)
- UEBA 基準支援 (第 2 部分)
- 支援 AI 的網路存取
- 支援 AI 動態存取控制

進階活動總數：61

Dell Technologies 可以簡化快速實現零信任成熟度所帶來的複雜性。

資料來源：《DoD Zero Trust Strategy》(美國國防部零信任策略) 出版物，2022 年 11 月 7 日

DELL Technologies

滿足所有組織的需求。

提高零信任成熟度。

零信任是一個明確定義的框架和一套原則，能針對如何確保安全性提供相關指引，並可使用各種功能加以實作。無論您是要全力採用零信任機制，還是著重於目標改善項目，並與零信任原則保持一致，Dell 都是經驗豐富的安全性合作夥伴，可協助您推動安全性歷程。

化學

資訊科技

通訊

緊急服務

食品與農業

防禦

醫療照護與公共衛生

製造業

金融

核能反應器

商業

政府機關

能源

運輸

用水和廢水

水壩

DELL Technologies

DELL Technologies

經驗豐富的技術與安全性合作夥伴，可協助您推動組織的零信任歷程。

實作零信任機制，藉此長期提升網路安全性。

Dell 資訊安全服務提供：

安全性成熟度和
整體風險的專家評估。

零信任藍圖開發。

安全性活動的持續管理。

DELL Technologies

Dell.com/SecuritySolutions

要求回電

與安全性顧問交談

請致電 1-800-433-2393