DLP資料外洩防護

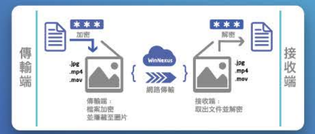
USB儲存裝置管控 | 三方認證 | 檔案異動 | 即時監控 | 詳細記錄

USB儲存裝置、使用者與電腦均符合規範方能存取該USB，並且即時詳細記錄USB操作與檔案異動。

螢幕浮水印 | 防止資訊拍攝洩漏

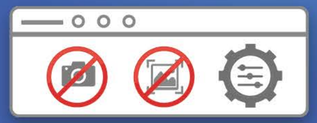
使用者可自定義浮水印格式，並於電腦開機時顯示於桌面，以防止機密資訊被拍攝外洩。

檔案加/解密 | 無感加密 | 支援多種檔案格式 | 資訊隱藏技術



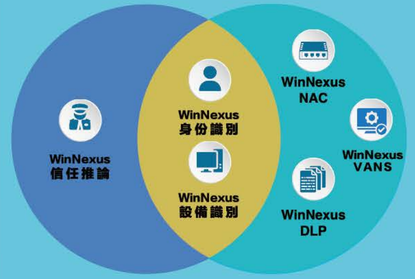
使用者操作檔案完畢後關閉檔案立即加密。確保檔案安全性並且可利用資訊隱藏技術，確保竊聽者無法得知機密檔案存在的事實。

文件閱覽、截圖防護 | 即時防護 | 自定義防護模式



當機密文件開啟時，限制使用者的剪貼簿與截圖功能，並且可自訂義受限制程度。

WinNexus 零信任 Zero Trust



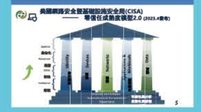
核心架構 基於*NIST SP 800-207*標準設計，採用零信任架構 (ZTA)三階段策略，提供動態的身分驗證與授權機制，確保每次存取都經過驗證。

動態信任 系統會根據使用者情境與設備的即時狀態，動態調整存取權限，確保最小權限原則的落實，並能更靈活地應對各種潛在威脅。

地端閘道 獨創的地端存取閘道管理機制，以分散式部署的方式在內部網路的關鍵節點，精準控制設備存取，實現區域內部的零信任訪問管理。

無縫整合 *ZTA*安全方案不僅是單一產品，更可與現有安全模組*(NAC/VANS/DLP)*無縫整合，高度符合*CISA*零信任成熟度模型原則，展現出卓越的適配性，形成全面且穩固的防禦體系。

金融業零信任規範 五大支柱



政府零信任規範 三階段

contact infos

教育訓練

產品採購
(共同供應契約)

社群平台

官方網站

235 新北市中和區建一路186號11樓
407台中市西屯區台灣大道四段 925號16樓之3
700台南市中西區樹林街二段33號思源樓二樓M211

WinNexus 全領域資安防護網

National-Certificated WinNexus Overall Information

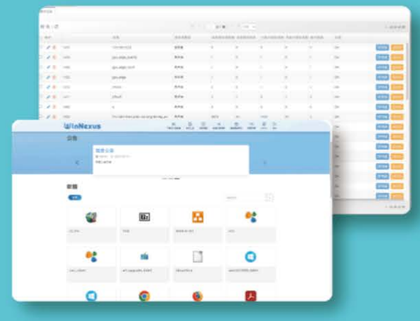
EDR | IOT | DLP | NAC 網路控管 | 零信任 | 一鍵 GCB FCB CIS | VANS 資產自動更新

靜默安裝 | 資產辨識 | 資產管理 | 軟體精準派送 | 資訊安全

誠雲科技股份有限公司
CT-CLOUD TECHNOLOGY CO.,LTD.

軟體派送

支援VANS　軟體管控　資訊安全　用量統計　靜默安裝



掃描　掃描並回報終端電腦完整的軟體使用狀況，包含已安裝軟體、軟體版本、軟體使用時間、軟體使用頻率等資訊。

回報　系統即時回報派送數據，精準掌握每一台電腦的派送結果，並分析派送失敗原因。

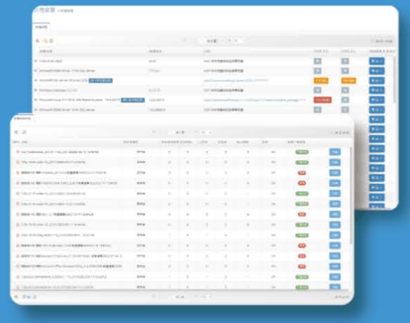
管制　整合AD Server帳號伺服器作為帳號登入管制機制，無需使用AD Server即可獨立運作。

靜默　在不干擾使用者工作的狀態下，悄無聲息地執行軟體更新與Hotfix安裝等動作。

效益　有效版權管理，按照使用需求採購足夠數量的軟體，不浪費亦不會不足。

VANS 自動修補

智能比對　自動更新　視覺圖表　整合管理　軟體修補



回報　系統即時回報派送數據，精準掌握每一台電腦的派送結果，並分析派送失敗原因。

更新　改善耗時的版本更新與Hotfix派送作業，並且記錄歷次修正過程。自動化部署管理讓管理者省時省心，全面防護無死角。

比對　具備「智慧比對功能」，依據技服中心最新標準，找出需要修正的軟體弱點，讓您無需等待技服中心的比對結果，弱點補強自己先來。

紀錄　完整記錄軟體及其變更資訊，包含軟體安裝/卸載/版本變更紀錄。

一鍵 GCB /FCB/CIS

智慧套用　作業系統　應用程式　網通設備　瀏覽器

一鍵完成 一鍵還原　一鍵完成GCB組態掃描、套用、確認。如遇突發狀況，提供「一鍵還原」原始組態，工作不停頓，最大程度減少損失。

視覺圖表　系統自動整合GCB條例資料，智慧轉換圖表呈現，使管理者對GCB應用狀況能夠全面掌控。

回報修正　派送結果詳細確實，除統計正確率，亦提供派送失敗的原因，加速修正。

一網打盡　作業系統、瀏覽器、應用程式與網通設備中的防火牆GCB一次搞定。

EDR 端點偵測

即時監控　智慧反應　檔案紀錄　一鍵安裝　郵件告警

即時偵測　第一時間監控所有異常的行為活動，不讓惡意人士有任何漏洞可鑽。

智慧反應　彙整全球專業資安經驗結晶，輔助人員做出正確判斷。

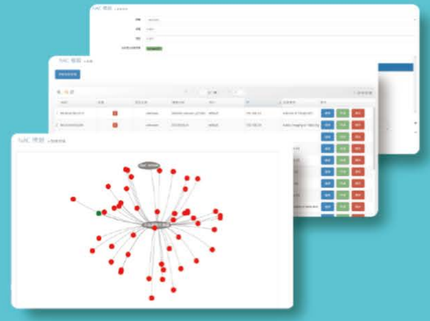
檔案紀錄　記錄所有檔案的hash變更歷程，杜絕遭惡意程式竄改的可能性。

一鍵安裝　一鍵輕鬆完成安裝和卸載，節省下花費時間人力個別操作的大量成本。

郵件告警　資安事件發生的第一時間自動寄送告警郵件至指定信箱，資安防護零時差。

NAC 網路控管

802.1x　設備連線、阻斷　網路隔離　網路拓樸



802.1x　藉由802.1x規範，無需額外硬體設備，即可對網路進行管控。

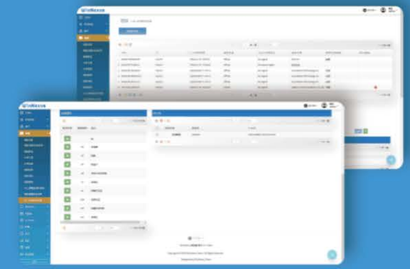
設備連線阻斷　管理者可於管理介面對區域網路中的各設備進行手動連線、阻斷網路，讓特殊需求的機器可入網，或手動阻斷異常的設備。

網路隔離　通過認證的用戶，將根據身分被分配到不同的VLAN，不同VLAN間彼此隔離無法相連，可確保訪客不會直接接觸到重要設備。

網路拓樸　網路拓樸圖記錄網路內每台設備的狀態，將所有設備用視覺化的方式呈現。

IOT 線上設備辨識

硬體異動　國籍偵測　人性管理　門禁管制　郵件警示



蒐集檢測　自動蒐集網段內所有上線裝置之網卡資訊，並檢測 Agent 安裝狀態。

廠牌比對　迅速比對連線裝置廠牌名稱與該廠牌註冊國籍，無痛排查大陸製資通訊產品。

偵測示警　自由設定偵測國籍、警示接收人員，並即時偵測、發送e-mail示警，大幅提升防護等級。

門禁把關　定時檢查IOT產品存活率，排查出失效的門禁系統與網路攝影機，並即時警示，避免因門禁或攝影設備損壞而造成資安破口。