

WinNexus

全領域資安防護網

零信任&VANS資安弱點通報專家

誠雲科技_教育訓練課程



即刻報名



報名資格

- 初階課程：WinNexus軟體用戶
- 中階課程：已完成初階課程的用戶

上課地點

- 北 新北市中和區建一路186號11樓之4
- 中 台中市西屯區台灣大道四段925號17F-1
- 南 台南大學創新育成中心M217室

初階課程

- 課程時間：週五開課 10:00-16:00
- 課程日期：2024/06/07(中) 2024/10/18(南)
2024/07/19(北) 2024/11/22(北)
2024/08/23(中) 2025/01/17(中)

中階課程

- 課程時間：週五開課 10:00-16:00
- 課程日期：2024/11/15(南)
2024/12/27(北)

WinNexus × 零信任

身分鑑別

- 以無密碼雙因子方式達成身分鑑別
 - 運用如FIDO2相關技術鑑別使用者之身分
- 提供具備簽章與加密之鑑別聲明
 - 提供API函式庫，使機關之資源系統(RP)可解密並驗證鑑別聲明以確保其機密性與完整性



設備鑑別

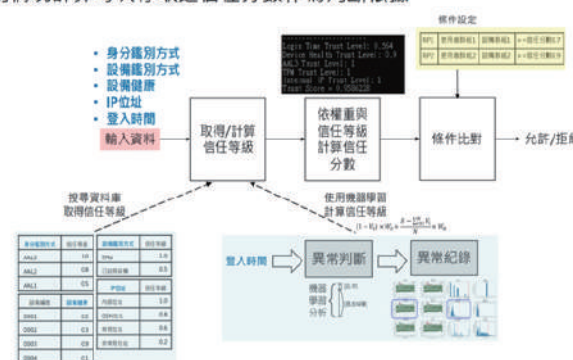
- 基於公開金鑰技術之設備鑑別方法
 - 透過TPM或Agent產生金鑰與憑證，完成設備註冊與鑑別
- 設備健康管理
 - 持續性設備健康狀態監控
 - 依設備健康狀態計算設備健康信任等級



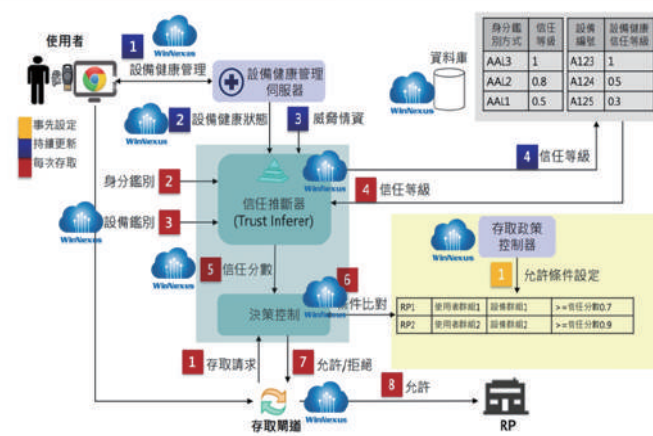
A. 作業系統更新	VANS
B. 防毒更新	VANS
C. 應用軟體更新	VANS
D. 組態合規	GCB

信任推斷

- 基於信任推斷機制決定存取權限
 - 依使用情境計算每次存取之信任分數作為判斷依據



完整零信任登入流程



教育訓練



產品採購



社群平台



官方網站

WinNexus

全領域資安防護網

National-Certificated WinNexus Overall Information

一鍵

- GCB
- FCB
- CIS

作業系統 • 瀏覽器
網通 • 應用程式



資產VANS

資通安全弱點通報機制



VANS自動更新

資安弱點 • 一鍵修補



EDR

端點偵測及應變機制



IOT

設備廠牌辨識



零信任

身分識別 • 設備識別 • 信任推斷



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

- ☑ 資產管理
- ☑ 軟體派送
- ☑ 資訊安全

如有包班需求，請洽詢合作經銷商或業務

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

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

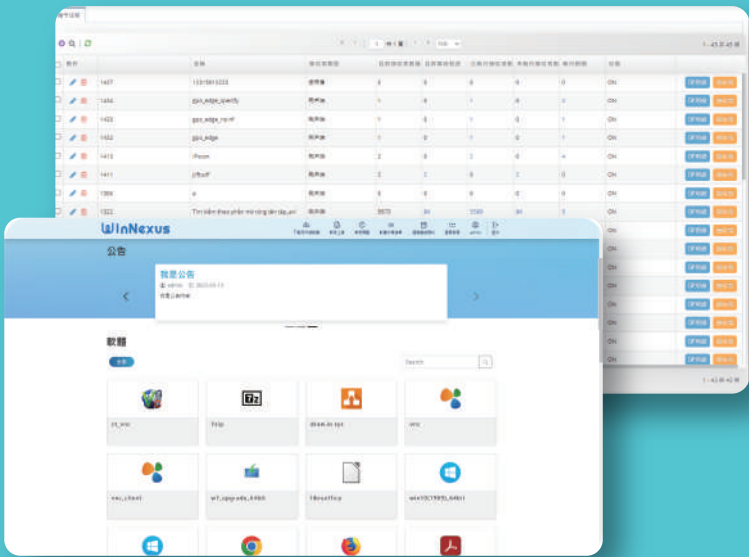
整合AD Server帳號伺服器作為帳號登入管制機制，無需使用AD Server即可獨立運作。

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。



資產VANS



智能比對

軟體資產

弱點項目

整合管理

資料同步

整合

強強聯手，VANS整合資產管理模組，軟體資產一手管理，最有效率。

即時

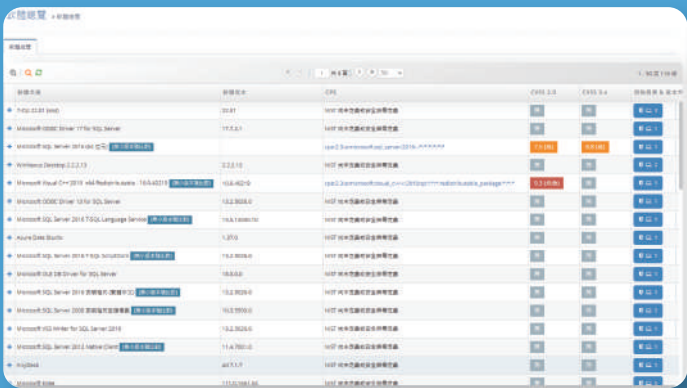
每天與NVD資料同步，取得最新軟體弱點資訊。

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。



軟體ID	軟體名稱	廠商名稱	軟體版本	CPE 2.3	CVE 弱點名稱
Test01	Test01	Microsoft Windows 10	Microsoft Corporation	10.0.17134.1	CVE-2017-14482 Microsoft Windows 10 17134.1
Test01	Test01	Microsoft Windows 10	Microsoft Corporation	10.0.17134.1	CVE-2017-14482 Microsoft Windows 10 17134.1
Test01	Test01	Microsoft Windows 10	Microsoft Corporation	10.0.17134.1	CVE-2017-14482 Microsoft Windows 10 17134.1
Test01	Test01	Microsoft Windows 10	Microsoft Corporation	10.0.17134.1	CVE-2017-14482 Microsoft Windows 10 17134.1
Test01	Test01	Microsoft Windows 10	Microsoft Corporation	10.0.17134.1	CVE-2017-14482 Microsoft Windows 10 17134.1
Test01	Test01	Microsoft Windows 10	Microsoft Corporation	10.0.17134.1	CVE-2017-14482 Microsoft Windows 10 17134.1
Test01	Test01	Microsoft Windows 10	Microsoft Corporation	10.0.17134.1	CVE-2017-14482 Microsoft Windows 10 17134.1
Test01	Test01	Microsoft Windows 10	Microsoft Corporation	10.0.17134.1	CVE-2017-14482 Microsoft Windows 10 17134.1
Test01	Test01	Microsoft Windows 10	Microsoft Corporation	10.0.17134.1	CVE-2017-14482 Microsoft Windows 10 17134.1
Test01	Test01	Microsoft Windows 10	Microsoft Corporation	10.0.17134.1	CVE-2017-14482 Microsoft Windows 10 17134.1

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

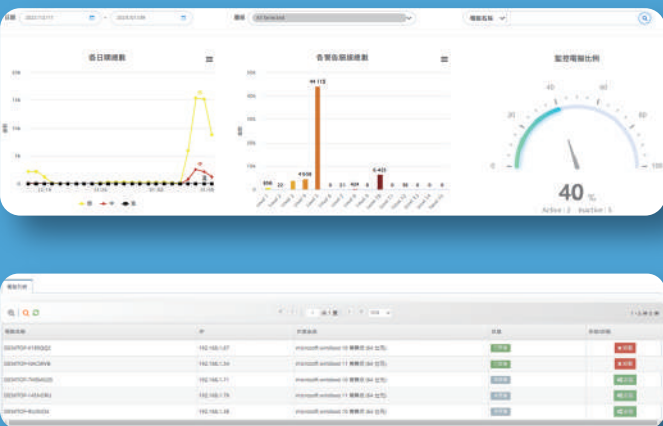
記錄所有檔案的hash變更歷程，杜絕遭惡意程式竄改的可能性

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。



VANS自動更新



自動更新

即時回報

視覺圖表

靜默安裝

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

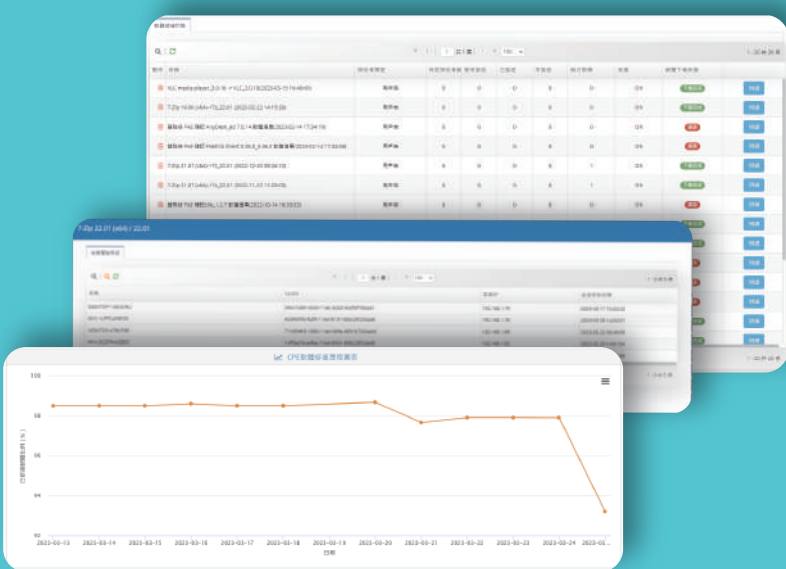
改善耗時的版本更新與Hotfix派送作業，並且記錄歷次修正過程。自動化部署管理讓管理者省時省心，全面防護無死角。

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。

圖表

系統自動整合含有CPE資料的弱點軟體，智慧轉換圖表呈現，使管理者能夠全面掌握CPE軟體的數量及漏洞評分狀況。



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

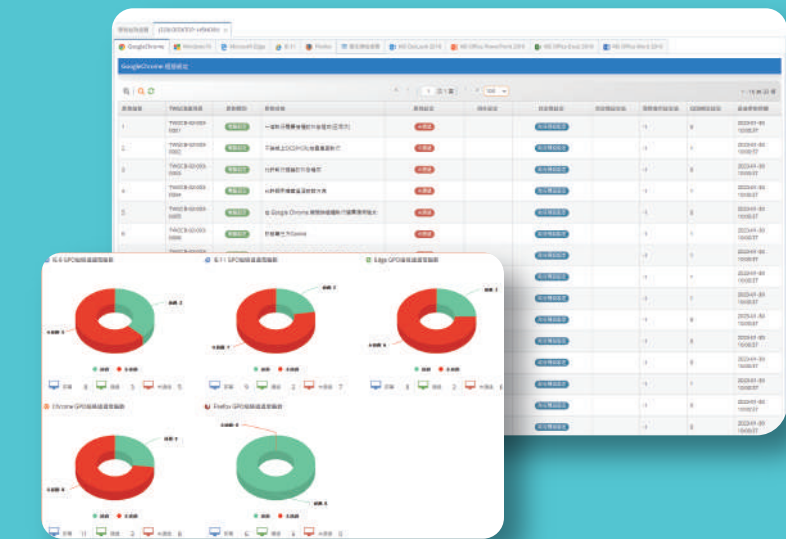
系統自動整合GCB條例資料，智慧轉換圖表呈現，使管理者對GCB應用狀況能夠全面掌控。

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。



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。

