鈺眾資安

Endpoint Security Problem Solved

鈺眾資安 威脅資產管理
(VANS-軟體資產、弱點風險與Patch自動修補管理)

- **提高安全性**
- **提高穩定性**
- **增強的性能**
- **更好的合規性**
- **提高生產力**

先進的惡意程式攻擊防護與系統安全管理

先進且自動化的威脅資產管理，由於網路活動的日趨複雜，大部份駭客都利用已知的系統弱點來撰寫攻擊程式碼(ExploitCode)以行企業資訊系統的入侵行為。企業主機環境則常由於忘記更新軟體修正檔，使得本身資訊系統遭到非經授權的存取或導致其它安全性問題風險。藉由自動化工具進行系統風險管理，提早發現系統維運及網站安全弱點、及時完成弱點修補作業免藉由弱遭受入侵攻擊。Comodo威脅資產管理是一套自動化的系統弱點管理工具，提供客戶系統弱點結果。隨時掌握系統的弱點與風險狀況，可提早發現系統維運安全弱點與及時完成弱點修補作業，避免藉由弱點受入侵攻擊。Comodo威脅資產管理提供集中的IT與端點安全管理儀表板，資安管理人員可隨時掌握納管設備資訊及其系統安全狀態。

鈺眾資安提供了最不耗用系統資源的次世代端點安全用戶端 Agent，僅僅45MB資源需求，即可完成縱深安全的防護架構。

方案特色

ADDT派送系統快速部屬上線

自動化資產盤點方式，提升軟體清冊彙整效率

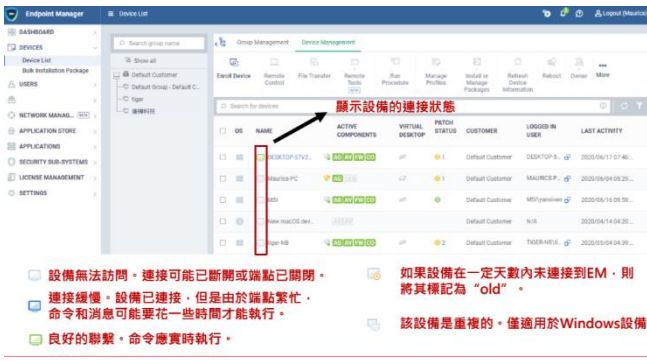
自動且持續性之漏洞修補排程，提升修補成功率

定期且有效率的軟體版次更新，縮短漏洞被利用的空窗期

系統查詢追蹤，掌握電腦修補情形，並找出漏網之魚，避免造成資安破口

單一系統因應行政院VANS政策，簡化資產盤點及漏洞修補流程，大幅降低人力

VANS 模組功能特色



非嵌入於資產管理系統，有助於提升系統防護安全

自動比對軟體資產的 CPE 格式並正規化轉換

可自定作業系統或廠商名稱，補強正規化資訊

提供匯出 CPE 正規化清冊後手動上傳或自動上傳 VANS 系統

1. **漏洞評估**：使用漏洞掃描器和滲透測試等工具識別系統和軟件中的漏洞。
2. **漏洞分析**：分析漏洞以確定威脅的潛在影響和嚴重性。
3. **風險緩解**：實施措施來緩解已識別的風險，例如補丁管理、安全控製或軟件更新。
4. **持續監控**：持續監控您的系統和軟件，

銓眾資安股份有限公司 | 新北市三重區重新接102號10樓

| TEl 02-7753-8590- | FAX 02-2938-6711 |

網址:https://www.crowd.com.tw