近年來重大資安事件、資料外洩、ATM 盜領、勒索軟體...等日益精進的攻擊手法，駭客目標遍及民間企業、金融單位、及政府單位皆受到強烈的威脅。

企業網路環境的內憂外患，唯有確實掌握所有設備資訊及所在位置，全面清查同仁是否確實安裝防毒軟體、資產管理軟體等 Agent 式產品的部署狀況，及安裝版本是否最新。進一步結合 AD(Active Directory) 檢查是否所有用戶端皆加入網域，以確保所有用戶端可接收 GPO 派送資安政策，及一併清查用戶端是否有留存的 Local Admin 權限，唯有將內部網路安全性提升，協助企業全力防堵駭客入侵的管道，才是有效管理內網資訊安全根本的解決之道。

協助解決以下內網資訊安全管理問題：

- 用戶端是否都有納入網域管理
- 用戶端或主機端的 GPO 是否都派送成功
- 用戶端遺有多少 Local Admin 帳號存在
- 防毒軟體、資產管理軟體、DLP 都只監控已安裝 Agent 的設備
- 發生資安事件時，無法提供有效稽核資料依據
- 非法設備連線管理
- 無法即時掌握設備移動

資安管理自動化，有效性落實：

- Security Intelligence Portal 協助政府、金融客戶落實 ISO27001 ／ ISMS ／金檢稽核（內稽／外稽）資安二次覆核
- Security Intelligence Portal 協助製造業客戶落實 ISO27001 ／沙賓／客戶資安要求規範之特規，有效性

- 端點設備 Agent 部署管理 100% 落實
- Local Admin 全面清查覆核，AD 帳缺異常登出入監控、GPO 落實

■ 端點設備自動化管理

1. 採無縫 (seamless) 式接入，使用者無需變更現有網路架構，導入最方便
2. 使用 Web 介面與嚴謹的偵測阻擋技術，讓 IT 人員可即時掌握內網資安事件，輕鬆控管內網運作狀態
3. 依 IP 網段設定政策，管理方便有彈性
4. 所需佔用頻寬少，資訊收集快速，可第一時間掌握資安訊息
5. 操作簡易，快速部署，擴充性強，全方位的報表與內網稽核軌跡，讓資訊安全與網路穩定度面面俱到
6. 協助申請 IP 流程自動化，簡化管理降低維護成本輕鬆做好管理
7. 管理者可掌握有漏洞的作業系統設備有多少，並預先訂定防範措施
8. 可避免不團機造成駭客入侵軟體更新不完整，內網資安更完善，也是協助落實即能減輕的好幫手

■ AD 進階管理系統

1. 整合 AD 使用者訊息及網域資訊，管理更方便，防堵更完善
2. 限制 AD 帳號由被授權電腦登入，避免有心人士入侵
3. 若違反政策可執行封鎖
4. 快速精準掌握 GPO 套用情形
5. 彈性的報表呈現方式，讓管理人員輕鬆準備主管機關檢查所需的報表，省時又方便
6. 落實行政院國家資通安全會報技術服務中心推動各機關導入 GCB 的目的
7. 掌握用戶端本機最高權限帳號資訊做更完善的資安防護

■ 內網資安智慧管理系統
(Agentless NAC++)

1. 不須植入代理程式 (Agent)，快速製作出稽核所需之資安軟體 (防毒、資產管理及 DLP) 部署率報表
2. 整合客戶所使用的資安軟體系統做管理，防護更完善
3. 大量節省管理人員製作部署率報表的時間
4. 管理者可以在同一管理平臺上清楚資安軟體部署情形

主機名稱	WhatsUp Monitor	TMCM ofScanner	TMCM ofScanPolicy	DLP	SCCM
PM2DELL	Ping /	11.0	12.495.00	12.5	5.00.8239.1000
PDC	Ping /	11.0	12.495.00	12.5	5.00.8239.1000
VMNFSSPA	Ping /	11.0	12.495.00		
TRAINING(NF5	Ping /	11.0	12.495.00		5.00.8239.1000
Unknown	Ping / FTP / Time /				
ERPMAC	Ping /			12.5	5.00.8239.1000
RDC	Ping /			12.5	
Unknown	Ping /		12.495.00		
Unknown	Ping /				
Unknown	Ping /				
Unknown	Ping /				
Unknown	Ping /				
Unknown	Ping /				
Unknown	Ping /				
Unknown	Ping /				
IMS459	Ping /				
YIMCM				12.5	5.00.8239.1000