

內部網路端點安全防護解決方案

企業內部網路經常發生下列的安全問題

- 公司內部網路遭受古董級蠕蟲的攻擊，已經採購了防毒軟體卻沒有效果。原因可能是使用者並未安裝，被使用者私自移除或是被私自關閉，但 IT 人員缺乏有效的方法管理。
- 公司的網路流量被 P2P 軟體佔用。網路型 P2P 攔截設備價格太高而且效果又不滿意。較刁鑽的 P2P 軟體用了公司不能阻擋的埠號，又無法攔截。
- NAC (Network Access Control) 的解決方案可以檢驗每個端點安全狀況，但導入不易，不是要大幅變更現有網路架構，就是要更換所有網路，許多方案僅支援特定廠牌型號。
- 安裝 NAC 的 agent 軟體常與其他現有軟體相衝突，來賓或訪客的電腦也難以安裝 agent 軟體。

Sentriant™ AG 解決的問題

- 保護內部網路免於受到保護不週的網路端點的威脅：
AG 可檢查每部上網的端點，已發布的作業系統漏洞是否補齊？防毒軟體是否已安裝及更新？是否使用者偷偷安裝易產生漏洞的軟體？以降低因端點電腦防護不週全造成的網路問題。
- 落實網路安全性政策，確實得知並強制每部電腦端點依公司要求配置：
檢查各項軟體安裝狀況，如公司要求網路瀏覽器的安全等級設定要至高安全性或是巨集指令不允許執行，AG 可確認使用者是否私自修改，阻止不合安全政策的端點電腦連上網路。
- 隔離安全防護不夠周延或不合於公司政策的端點：
AG 可隔離漏洞沒補齊的電腦端點於內網之外，避免內部網路被保護不週全的端點電腦被惡意程式做為跳板間接危及企業整體內部網路。或是隔離私自安裝公司不允許的軟體的電腦，例如可能導致公司吃上智慧財產權官司的 P2P 軟體。

Sentriant™ AG 的優勢

- **快速的端點掃描速度**：僅需 4 秒鐘¹的掃描速度，對使用者日常作業的影響最小。
- **豐富的掃描項目**：包括端點電腦的作業系統的安全更新是至最新版，防毒軟體、個人防火牆或是防間諜是否安裝，安裝了是否啟動，啟動了是否更新，
- **可完全無需在端點電腦安裝掃描軟體(Agentless)**：AG 可支援掃描端點電腦而完全無需在該部電腦內安裝任何掃描軟體(Agent)，大幅減輕建置 NAC 的 MIS 人員

¹ 在 Agent 模式下

負擔，並且掃描項目與安裝 Agent 時一樣豐富。

- **適用各種暨有之網路架構：**可應用於 802.1X、DHCP、Gateway 模式網路架構，客戶導入時無需對現有網路架構做大幅度變動，NAC 可以輕易導入暨有的網路環境。
- **無需搭配特定廠牌網路設備：**採用業界網路標準協定，無需擔心客戶現有網路設備廠牌為何，或是已混合有多家廠牌設備。
- **Agent、Active-X 及 Agentless 等各種端點模式可同時並存於同一網路：**僅需一部 AG server 即可，
- **可以允許 current user license：**無上線的端點或離開網路的端點可重覆使用同一套使用者授權數目 (License Pool)。

