SecureAge

SecureAPlus

多層的端點安全

必要的安全層次

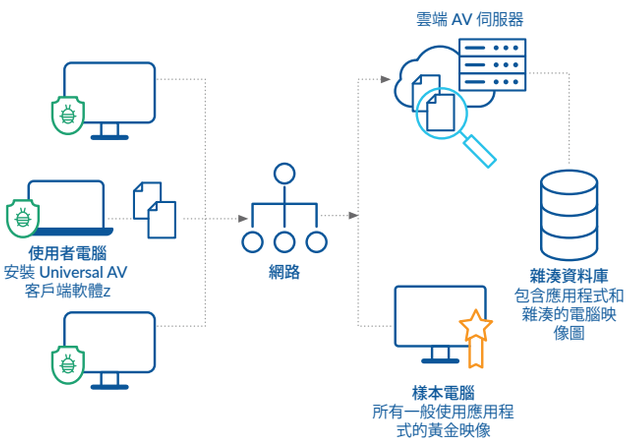
SecureAPlus 是必要安全功能的獨特結合體, 能夠保護企業端點免於已知或未知、檔案型態或是無檔案型態、企業內部或是外部的各種媒介攻擊.

Universal Anti-Virus
雲端先進的檢測技術

沒有任何單一防病毒引擎能夠 100% 檢測到各種的威脅, 當然相對地也就無法對某些特定型態的威脅創造好的檢測結果.

Universal AV 結合多個防病毒引擎, 可以在任何指定的時間掃描檔案並享有高的病毒檢測率, 這是一般傳統防病毒軟體所無法實現的. 所有的掃瞄作業都在雲端, 並不會消耗本地資源進行病毒掃描, 讓端點也可以使用既有的本地防毒軟體選項.

組合診斷服務能提供即時保護的關鍵情報, 做為應用程式控制的決策選擇.



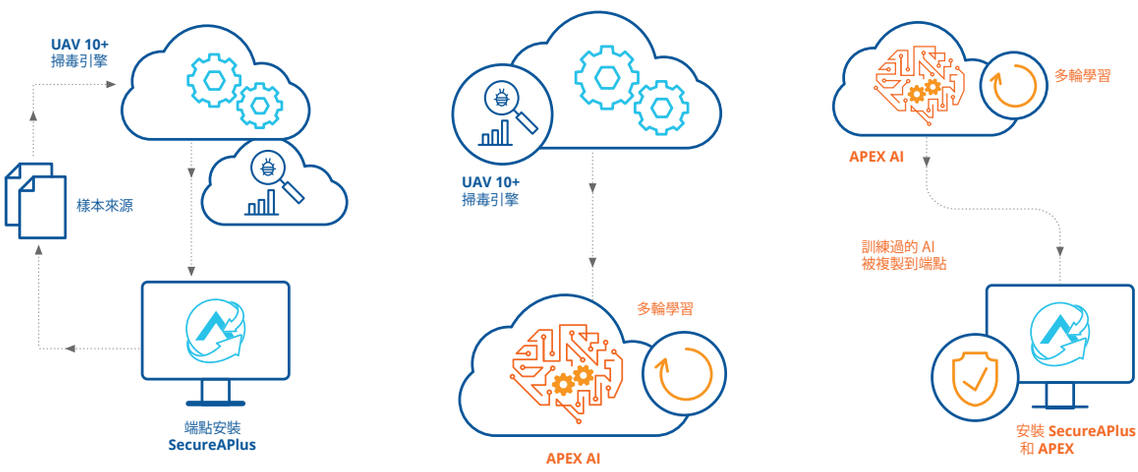
結合多個防病毒軟體引擎診斷	威脅偵測是透過多個防病毒軟體進行, 以便為每次掃描提供至少第二個掃描意見.
雲端的病毒掃描技術	透過雲端指定的掃描程序確保端點硬體的效能.
快速的完整系統掃描	定期自動執行, 只需幾個簡單點擊就可以快速完成掃描週期.
掃描各種情況	當啟動時並定期進行快速完整系統掃描, 隨選掃描允許使用者在任何時間隨時檢查任何檔案, 而及時掃描可以防禦對抗進入您系統內的潛在威脅.
可設定的掃描配置	開啟或關閉某些特定掃描選項, 將機密敏感資料夾排除於雲端掃描, 設定檔案上傳大小限制以及更多設定.
與離線解決方案相容	透過雲端掃描程序, 端點可以選擇使用現有的或是將來選用的第三方離線解決方案而沒有相容的問題.

SecureAge APEX 人工智能引擎
由人工智能提供的威脅檢測

隨著愈來愈多的威脅以驚人的速度變異為更進階的形式, 若是僅僅倚賴識別現有威脅的傳統檢測技術, 將會造成端點很容易遭受到零日攻擊和變種惡意軟體攻擊.

SecureAge APEX 引擎利用人工智能 (AI) 和深度學習的力量來應對當今和未知的威脅.

結合大數據的強大功能, APEX 引擎能夠透過有效和可靠地發現病毒惡意模式, 遠遠超越傳統的掃描模式, 並且能夠依據以往的經驗快速有效率地做出決策. 同時可以針對病毒在爆發期間試圖感染端點的所有新的以及未曾見過的惡意軟體變種, 進行自我更新調整知識庫, 對抗這些惡意軟體.



雙管齊下的檢測方法	APEX 整合了 Universal AV 以及包含第三方離線防病毒引擎選項的最新和傳統病毒掃描技術, 可以有效涵蓋已知和未知的變體惡意軟體.
深度學習技術	能夠識別威脅而無需使用基於病毒碼簽名的技術, 而是依據先前累積學習的資料, 來識別威脅.
透過學習培訓精進	結合雲端技術進行大量資料的學習培訓, 確保引擎保持經過學習培訓後的更新版本, 和傳統以病毒簽名方式的防毒軟體比較, 擁有更小的軟體足跡.
離線作業	在本地進行培訓學習和儲存, 無需透過互聯網的連接就可以偵測到最新的威脅.
與其他病毒掃描技術相容	Universal AV 和/或 其他第三方離線防病毒引擎一起作業.

應用程式控管 & 白名單
端點安全策略的核心

每天幾乎都會產生近百萬個變種惡意軟體, 傳統的防病毒解決方案在這些惡意軟體初次出現時雖然很努力去偵測, 但還是很難檢測到這些威脅. 更糟糕的是, 一些進階的惡意軟體會適應迴避既有的安全措施, 從而領先一步, 市場上任何可用的防病毒軟體幾乎都無法檢測到這些威脅.

應用程式控制 & 白名單透過依照規劃的安全程序來實現安全. 優先封鎖處理能夠確保任何檔案在未獲信任前無法造成任何傷害, 直到該檔案被確認為乾淨安全無疑後才可被啟動. 這可以阻止進階的和零日惡意軟體的威脅軌跡, 同時讓您每次都能處在安全的控管狀態.

輕鬆建立白名單	使用功能強大的雜湊功能在端點上建立初始白名單.
匯入 & 匯出 白名單	從基準電腦匯出白名單, 方便在組織的其他電腦端點上佈署安全白名單.
特權 & 非特權使用者的模式	互動模式允許您動態更新白名單, 而鎖定模式可以限制非特權使用者啟動不信任的檔案.
不同情境使用者的進階模式	信任所有、觀察模式和寧靜模式, 用來滿足受控制環境的使用.
防禦更廣泛的攻擊媒介	使用命令列規則可以對抗可被移植的可執行檔案、惡意腳本(scripts)和無檔案攻擊.
可靠的智慧情資	藉由多個支援的智慧情資檢測來源, 突顯出被封鎖阻止的威脅, 方便將不受信任的檔案加入白名單時的智慧決策依據.
一目了然的通知資訊	在互動模式下獲得通知時, 透過適當顏色的標記加諸於任何被封鎖的檔案或是應用程式, 能夠輕鬆識別相關資訊.
實際操作	當檢測到威脅時, 可以使用刪除或隔離的選項阻止或信任不受信任的檔案.
線上 & 離線作業	無論互聯網或是網路的連接如何, 應用程式控制 & 白名單都可以在每個端點的本地運行.

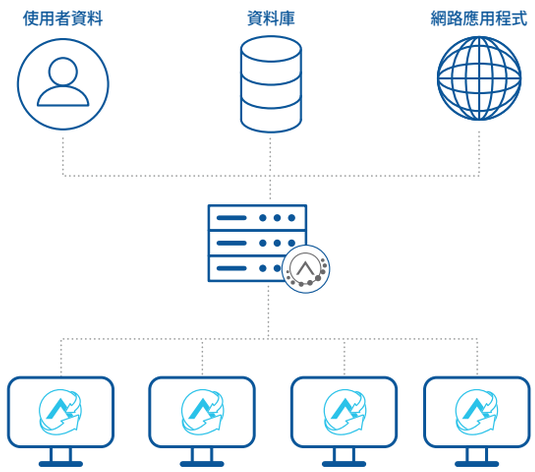
大規模集中式安全管理

對於企業或是更大型的佈署, 通常端點的數目是以數百甚至於是數千來計算的. 擴展應用程式控制和白名單的優勢, 同時又能夠隨時進行管理, 是成功佈署 SecureAPlus 所必須滿足的關鍵要求.

安全管理伺服器 Security Management Server (SMS) 允許 IT 管理員在大量端點上能夠輕鬆監視、更新和推送已被核准的白名單, 確保最少的停機時間和最高的工作效率.

SMS 利用雲端商業等級硬體的優勢以及虛擬電腦實現進階安全控制, 以幫助管理員達成應用程式控制、白名單以及其他資料安全的功能*.

*與 SecureAge 套裝組合解決方案配合作業, 整合其他功能, 例如加密, 的資料安全



大規模佈署 & 激活	透過將以批准的白名單推送到新佈署的設備, 輕鬆將 SecureAPlus 批量安裝到企業端點.
Web 控制台使用者介面	管理員可以透過專門的 web 入口網站來管理連接到網路上任何電腦之 SecureAPlus 的安全.
白名單管理	透過管理和強制白名單, 僅允許受信任的和授權的應用程式運行於端點上, 確保標準化的客戶端系統配置.
黑名單管理	透過建構和過濾未知以及未經授權的應用程式黑名單, 增強惡意軟體的管理
請求白名單核准系統	IT 管理員可以在鎖定模式下遠端回應非特權使用者的請求, 將未經授權的應用程式新增到白名單中.
軟體更新推送控制	將 SecureAPlus 軟體更新推送到特定群組的端點設備

SecureAPlus 其他主要功能

SecureAPlus 補足應用程式控制 & 白名單、Universal AV 和 APEX 人工智能引擎的核心保護功能, 更進一步具備能夠增強企業端點安全性的其他功能.

命令列規則	透過包含一組易於自我客製化以及可擴充的初始規則, 擴展白名單的安全覆蓋範圍, 對抗無檔案的攻擊.
電子郵件警示 & 病毒感染報告	當檢測到端點被病毒感染時, 能夠透過電子郵件立即獲得詳細的病毒感染報告以及電子郵件的警報. 就算受病毒感染的端點已經關閉了, 透過 24/7 全天候在雲端不斷進行掃描工作的 Universal AV, IT 管理員仍舊能夠獲得警報通知.
USB 儲存設備存取控管	控管外部 USB 儲存設備插入端點時以預先設定的安全方式處理. 具備允許或關閉讀取和/或寫入存取以及儲存裝置白名單的控制項功能.
密碼保護設置	防止透過密碼未經授權來竄改 SecureAPlus 的設置.

技術規格

硬體需求:

- 2 GHz Pentium 4 或更高
- 1GB RAM 或安裝的 Windows 作業系統所建議的 (以較高者為準)
- 300 MB 硬碟可用空間或更多
- 本地硬碟格式化為 NTFS
- 最小螢幕解析度: 1024×768 (在 100% 比例下)

可用語言:

中文(繁體和簡體)、英語、法語、德語、匈牙利文、印尼文、義大利文、日語、波蘭文、俄語、土耳其文、越南語

支援的作業系統:

- Windows 10 (32-bit & 64-bit)
- Windows 8.1 (32-bit & 64-bit)
- Windows 8 (32-bit & 64-bit)
- Windows 7 Home Basic (32-bit & 64-bit) 和以上
- Windows XP SP3 (32-bit & 64-bit)^
- Windows Vista SP2 和以上 (32-bit & 64-bit)
- Windows Server 2016 (64-bit)
- Windows Server R2 2012 (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2008 R2 & 以上 (64-bit)
- Windows Server 2008 SP1 & 以上 (32-bit & 64-bit)
- Windows Server 2003 R2 SP1 & 以上 (32-bit & 64-bit)^

^命令列規則和 APEX AI 人工智能引擎與這些版本的 Windows 不相容

需要更多的資訊嗎?
www.secureaplus.com • secureaplus@secureage.com

Copyright © 2020 SecureAge Technology. 版權所有.