# PGP® Endpoint Application Control

Protecting systems from unauthorized and malicious software

Part of the PGP® Encryption Platform

未經授權及惡意的程式讓使用者暴露在高度風險中, 也影響工作運行. 每次有新的惡意軟體威脅出現或是不支援的軟體造成系統衝突時, IT人員就疲於奔命的到處救火. 企業需要一套好的方法來降低因不斷更新病毒碼及惡意程式特徵或是軟體相容性引發的系統重灌等等的沒有效益的事情。

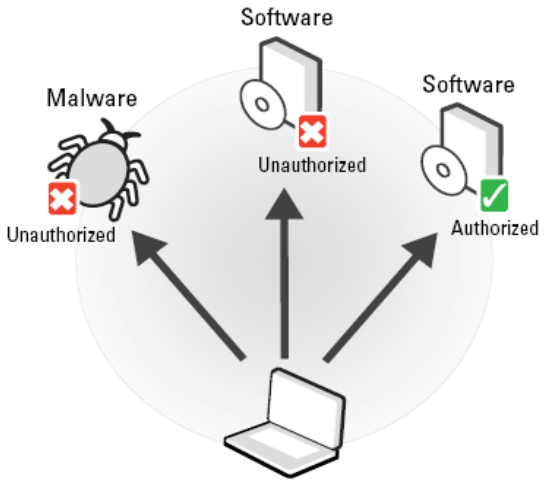
PGP Endpoint Application Control 使用強制安全政策, 主動防衛系統免於來自未經授權或惡意軟體的威脅, 它使用白名單定義信任的與授權的程式, 只允許白名單內的程式才能執行。

## 主動與自動的防衛

- 自動的安全政策強制實行: 不需使用者介入, 自動防衛系統免於不明程式的威脅
- 不需更新特徵碼(Signature): 白名單技術提供自我防衛, 拒絕不明程式的執行
- 自動發掘應用程式: 快速建立白名單
- 腳本(Script)與巨集(Macro)防衛: 拒絕對象包括腳本與巨集
- 無所不在的防衛: 白名單內容使用Hash技術, Hash與允許權存放在本機內, 即使離線也能提供無所不在的防衛

## 符合法規要求

- 詳細記錄應用程式執行意圖與行為, 提供軟體安全稽核證據




## 日常作業不中斷

- 降低IT管理成本與Helpdesk負擔, 預防惡意程式經由網路散播造成停機威脅
- 免擔心修補(Patch)更新: 安全政策彈性可允許自動授權更新

## 透通的使用者經驗

- 背景執行保護: 使用者不需介入與變更操作習慣, 系統自動在背景提供防護
- 單一登入(Single Sign On): 結合 Microsoft AD 或 Novel eDirectory, 使用者只需登入一次即可受到防衛保護

使用效益

- 防止來路不明的程式: 主動式與自動化的強制性安全設定, 只允許被信任的與授權的軟體才能執行, 避免執行到惡意程式及來路不明軟體的風險
- 減低管理負擔: 使用白名單(Whitelist)方式, 降低因為不明程式威脅而須經常更新系統與使用者叫修問題
- 確保商務持續運作: 拒絕未經授權程式的執行, 防止已知及未知程式的威脅
- 符合法規: 應用程式的執行企圖與安全政策內容都有稽核記錄, 可滿足相關法規要求
- 透通性的使用者經驗: 自動化與背景執行模式, 不影響使用者, 不降低生產力

玉山科技股份有限公司
http://www.asiapeak.com
(02)77128295