opentext™

資料表

ZENworks Endpoint Security Management

利用可偵測位置的規則型解決方案保護您最易受攻擊的 IT 資產。它能有效防範惡意程式威脅、保護每台電腦的資料、控制端點傳遞與存取資訊的方式，並可從單一主控台監控端點裝置以維持良好狀態。

產品焦點

OpenText ZENworks Endpoint Security Management 為您所有的 Windows 桌上型電腦和行動電腦提供詳盡的規則型控管功能，包含依據使用者角色及位置自動變更安全性組態的能力。ZENworks 從單一集中主控台建立及管理規則，因此能強制執行嚴密控管且調適性高的安全性規則，讓最終使用者不必再承擔任何組態或強制執行的負擔。ZENworks Endpoint Security Management 也具備強大的用戶端自我防禦功能，可保障安全性規則不會遭到規避；此外，它還擁有一套完整的監控、警告、報告和稽核工具。

主要優點

ZENworks Endpoint Security Management 可協助您的組織：

- 為您最易受攻擊的 IT 資產 (亦即組織邊緣的行動電腦) 提供全方位的集中式安全防護。
- 減輕最終使用者的負擔，讓使用者不必再設定及維持其裝置的安全設定與解決方案，進而提高生產力。
- 從單一主控台有效率地管理貴組織內各電腦的所有端點安全性層面。
- 依據使用者角色、位置及其使用的裝置，自動調整端點安全性規則與限制。
- 由您的安全性專家 (而非缺乏經驗的使用者) 再度取得定義、強制執行及維持端點安全性的掌控權，以確保安全。
- 搭配 ZENworks Suite 使用時，可透過將組態、修補程式、資產和端點安全管理全部整合在單一主控台上 (並可部署為虛擬裝置) 的單一管理平台，來管理端點生命週期及安全問題。

主要功能

惡意軟體威脅防護

ZENworks Endpoint Security Antimalware 可保護 Windows 桌上型電腦、伺服器和行動電腦，防範已知與未知的 (零時差) 惡意軟體威脅。其中包括：

- 透過各種偵測方法，提供多層安全性的反惡意軟體引擎技術。傳統的特徵碼偵測功能可防範已知威脅；一般偵測功能可防範已知的威脅變體；而進階試誤型分析則可防範未知的零時差威脅。

系統要求

如需詳細的產品規格與系統要求，請造訪：
www.microfocus.com/zh-tw/products/zenworks/specs

- 在檔案複製、移動、開啟或執行時，即時偵測惡意軟體。
- 在排定的時間或手動啟始時，掃描本機和網路磁碟機位置。
- 插入卸除式磁碟機時，進行掃描。
- 解毒、隔離或刪除受感染及可疑的檔案。
- 透過集中式管理主控台設定所有端點惡意軟體防護行為。
- 透過集中式管理主控台的儀表板，監控裝置的惡意軟體狀態和偵測到的威脅。

USB 與儲存裝置安全性

ZENworks Endpoint Security Management 提供專為確保合理使用抽取式儲存裝置而設計的強大功能。其中包括：

- 資料防竊保護可讓您啟用、停用或將任何抽取式檔案儲存裝置設定為唯讀，此類儲存裝置包括 USB、WPD (Windows 可攜式裝置)、磁片、CD/DVD 以及 Zip 磁碟機、.mp3 播放器、快閃式記憶體、SCSI 和 PCMCIA 卡等。
- 嚴密的白名單控制可讓管理員管控 USB 和 WPD 裝置的使用情況。
- 防止無法稽核之交易的功能，可將能夠複製資料而不會留下稽核線索的本機儲存裝置阻隔在外。
- 光學讀寫裝置 (DVD/CD) 與軟碟機控制可根據使用者的所在位置與安全環境，允許、拒絕磁碟機的存取，或將磁碟機存取設定為唯讀。
- 自動播放/自動執行功能控制可為您整個組織提供集中式自動播放/自動執行的控制功能。

資料加密

ZENworks Endpoint Security Management 可讓您加密所有端點上的抽取式儲存裝置和固定磁碟資料夾。其中包括：

- 使用原生 Microsoft 技術加密，而非額外的加密驅動程式；BitLocker 可用於抽取式磁碟機加密和固定磁碟資料夾的加密檔案系統 (EFS)。
- 集中式金鑰管理功能，讓管理員可復原加密的檔案。
- 抽取式磁碟機驗證，可在所有裝置或僅在 ZENworks 管理的裝置上解除鎖定加密的抽取式磁碟機。
- 選用的固定磁碟資料夾驗證，需要在 Windows 登入後輸入第二個密碼，才能存取加密的資料夾。

無線安全性

ZENworks Endpoint Security Management 可集中控制使用者於何地、何時及如何連線至無線網路。其中包括：

- Wi-Fi 管理可讓您為無線存取點建立白名單及黑名單，並可執行規則以限制、停用或封鎖特定狀況下的 Wi-Fi 通訊。
- Wi-Fi 安全控管可限制符合加密標準之無線存取點的 Wi-Fi 通訊。
- Wi-Fi 介面卡封鎖僅允許端點使用企業核准的 Wi-Fi 介面卡連接無線存取點。

連接埠控制

除了 Wi-Fi 安全之外，ZENworks Endpoint Security Management 亦為所有其他類型的有線及無線連接埠，以及通訊裝置提供完整的保護。其中包含 LAN、USB、1394 (火線)、序列埠與平行埠，以及數據機、藍牙與紅外線 (IrDA) 連線。

VPN 強制措施

為了提升裝置連線至開放網路，或需要從外部位置存取內部網路時的安全性，ZENworks Endpoint Security Management 提供的 VPN 強制執行可確保使用者僅能使用經授權的VPN連線，以防範「雙面惡魔」(Evil Twin) 攻擊，並避免使用者執行「分割通道」等危險動作。

應用程式控制

ZENworks Endpoint Security Management 的應用程式控制元件可為您所有端點上執行的應用程式提供精準的規則型控管功能。其中包括：

- 應用程式黑名單可封鎖已知惡意或不適當的應用程式。
- 位置型應用程式控制可允許特定應用程式執行、拒絕存取網路，或避免多個應用程式同時執行，這一切皆依據使用者所在位置的安全程度而定。
- 防毒軟體與間諜軟體的完整性檢查可確認所有必要的安全性應用程式皆正常執行，接著隔離並矯正不相容的裝置。

和我們交流
OpenText 執行長
Mark Barrenechea 的部落格

先進的防火牆防護

ZENworks Endpoint Security Management 與傳統應用程式層或鉤驅動程式防火牆截然不同，是位於每一個網路介面卡 (NIC) 的網路驅動程式介面規格 (NDIS) 層中。這可確保流量進入電腦時即擁有完整的安全性防護。ZENworks Endpoint Security Management 包含以下特定防火牆功能：

- 可設定狀態的防火牆防護僅允許裝置發起的通訊流量回傳給裝置
- TCP/UDP 連接埠規則與存取控制清單 (ACL) 嚴密管控特定裝置的防火牆運作行為
- 位置型防火牆運作行為控制將依據裝置位置的相對安全性情況，自動套用不同的連接埠規則及 ACL
- 集中化規則型控制可控管最終使用者或未經授權的管理員無法停用或規避的防火牆設定
- 真正的隔離功能可在電腦的安全完整性失效時，保護網路安全