Ivanti Endpoint Security for Endpoint Manager

Ivanti®Endpoint Security for Endpoint Manager 由 Landesk 提供，旨在預防、偵測和修復最複雜的威脅，包括勒索軟體。強大、多層的保護自動化探索、清點和修補管理，並且防止惡意軟體執行或散播。結合 Ivanti Unified Endpoint Manager 時，該解決方案可讓您隔離裝置、隔離時遠端控制，以及修復或重新建立受感染系統的映像。與 Ivanti Unified Endpoint Manager 的這個整合增加了效率和對您的 IT 環境的控制。

防止您的環境受到勒索軟體和其他現代化的威脅)

藉由 Ivanti Endpoint Security for Endpoint Manager，您可以瞭解尋找和修復惡意軟體、診斷問題和識別錯誤或未核准程序所需的一切。如果勒索軟體侵入您的網路，Endpoint Security 將截住勒索軟體、消滅它、通知其他連線的機器，並防止惡意軟體在連線的機器上執行。強大的遠端功能允許您隔離、調查和修復或重新建立跨網路的端點的映像。此外，裝置封鎖和連線控制可讓您監控和限制 I/O 裝置的存取。應用程式控制防止零日攻擊、匿蹤攻擊和其他複雜的威脅。資料保護功能防止惡意軟體加密您的檔案。

探索和清點您所有的網路裝置和軟體

主動和被動探索技術即時識別和清點所有啟用 IP 的裝置，即使是所謂的「惡棍」裝置，例如無線集線器和

防火牆後的裝置。自動探索也協助您找出那些裝置上的所有軟體，包括使用情況詳細資料。而且在搭配 Ivanti Cloud Services Appliance 使用時，Ivanti Endpoint Security for Endpoint Manager 可以清點、掃描、隔離和修補遠端裝置，不需要與虛擬私人網路 (VPN) 連線。

自動修補確保穩定和安全的環境

Ivanti Endpoint Security for Endpoint Manager 透過最佳做法、自動化流程和快速部署簡化了修補程式管理，對使用者不會有任何影響。除了可以可靠的修補跨您的網路的多種作業系統和第三方軟體外，甚至還可以修補移動中、在遠端位置或睡眠中的裝置。

以裝置和連線封鎖強化端點

裝置控制和應用程式防火牆功能限制端點可以存取的外部裝置或連線的類型。您也可以封鎖可能用於引進惡意軟體或偷竊資料的裝置。應用程式防火牆協助阻止惡意軟體「與主機通訊」，導致主機的大部份變成沒有用處。解決方案記錄複製到外部裝置的檔案，以此保證您可以通過您的安全稽核。

產品內容	功能	產品內容	功能	產品內容	功能
裝置探索	主動、被動與無代理程式探索和清點 - 瞭解要修補和保護哪一個裝置。此外，還可以偵測和尋找無線存取點。	勒索軟體偵測	偵測惡意加密、將其消滅和通知 IT 與其他機器。	網路隔離	隔離網路上的裝置，防止傳輸惡意軟體，但允許遠端控制裝置。
修補	自動化多個作業系統和第三方應用程式的修補。	勒索軟體預防	防止加密檔案和在其他地方執行。	惡意軟體圍堵	偵測到時將惡意軟體隔離。
	有系統的透過前導群組和逐漸加大的部署環排程和推出修補程式。	惡意軟體偵測	根據簽章、網路和行為的偵測。	遠端修復	遠端控制；遠端砍掉程序；遠端檔案管理；遠端重新建立映像；遠端部署其他鑑識工具和指令集
	防止修補程式透過重新開機管理和維護視窗干預使用者的生產力。	惡意網站偵測	防止使用者瀏覽可疑的網站。	儀表板和報告	Ivanti Xtraction 儀表板 - 強大的洞察力，不需要試算表專家。漏洞、修補和安全活動儀表板，結合提示與詳盡的安全報告。
修補情報	收集終端用者與修補效能有關的反饋意見，更好的關聯有影響的修補程式建立的事件 使用者。	無檔案防護	封鎖 Microsoft 巨集發起的無檔案攻擊。	SIEM 整合	傳送事件記錄給 SIEM 工具，便獲得進一步的情報和鑑識結果。
				高度統一的 IT 解決方案	功能
安全配置管理	適用於 PCI 的新式符合性內容。	應用程式控制	動態白名單學習您環境中的內容，並且防止未獲得授權的程式碼執行。	Windows 10 Migration 和 Windows as a Service (更新)	自動化您交付已個人化和準備好提供給使用者的 Windows 10 機器的方式，然後保持 Microsoft 提供給您的所有更新的通道。
	編寫其他符合性內容的能力。	裝置控制	防止使用卸除式儲存裝置和連接埠引入惡意軟體或複製敏感資料，並記錄所有複製資料的 活動。	編寫其他符合性內容的能力。	在使用者開始或移動位置時，提供正確的存取權、應用程式和資源 - 然後在使用者離開時，移除他們的權限和授權。
防火牆	封鎖惡意應用程式，防止與主機通訊和傳輸資料。			自助 IT	建立在背景結合 一切的服務目錄 - 服務、部署、資產管理 - 使用者只需要按下按鈕。

以進階的應用程式控制防止零日攻擊威脅

應用程式控制功能透過阻止惡意軟體和指令集執行及運用記憶體保護技術，防止受到檔案式和無檔案攻擊。學習功能將誤判降到最少，並允許合法應用程不中斷的執行。雲端式知名資料庫提供有關應該允許哪一種應用程式在您的環境中執行的進一步洞察力。

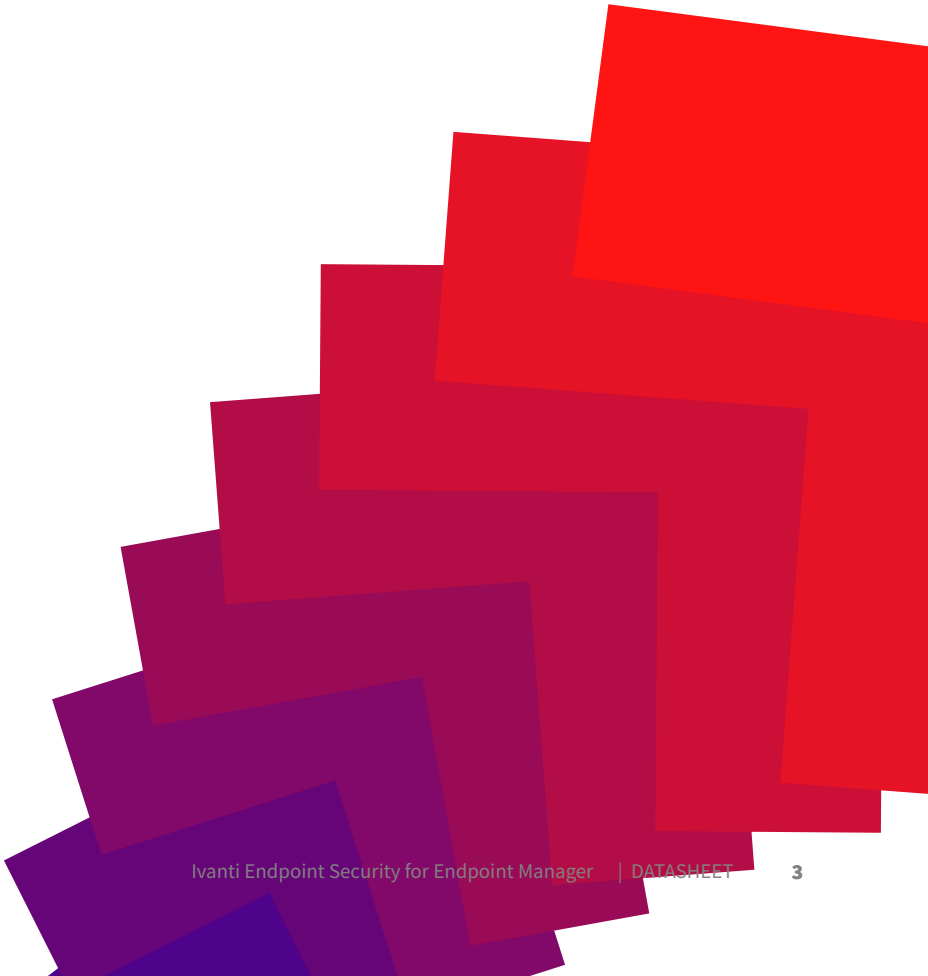
查看、行動和顯示結果

Ivanti Endpoint Security for Endpoint Manager 也提供一系列的報告和儀表板，協助您監控您在安全方面所花費心力的有效性。儀表板讓您可以在目視資料內採取行動。此可見度包括與實施原則、符合性等級、使用者行為、修補狀態、即時安全爆發警示等有關的詳細報告。

透過統一的 IT 強化安全

如其名稱所暗示，此解決方案與 Ivanti Endpoint Manager 整合，統一了端點安全性和管理。這樣可以快速自動化安全和 IT 管理原則、最佳化 IT資源。取得無可比擬的跨 IT 安全性與管理活動的可見度，降低風險並改善決策。

Ivanti Antivirus 可作為附加元件，除了防止已知的惡意軟體外，還可以透過行為分析偵測到惡意軟體。但如果您有其他防毒解決方案，Ivanti Endpoint Security for Endpoint Manager 可以讓您管理您選擇的第三方防毒解決方案。



關於 Ivanti

Ivanti 讓 Everywhere Workplace 成為可能 在 Everywhere Workplace，員工使用五花八門的裝置存取 IT 網路、應用程式和資料，以在任何地方工作時保持工作效率。Ivanti 自動化平台將公司領先業界的統一端點管理、零信任安全和企業服務管理解決方案連接起來，為企業提供單一管理平台，使裝置能夠自我修復和自我保護，終端使用者能夠自助服務。超過 40,000 個客戶 (包括財星雜誌百大企業中的 78 間企業) 選擇 Ivanti 來搜尋、管理、保護和服務從雲端到邊緣的 IT 資產，並為員工提供卓越的終端使用者體驗，無論他們在哪裏工作，以何種方式工作。如需更多資訊，請瀏覽 Ivanti.com.cn

ivanti.com
1 800 982 2130
sales@ivanti.com