SOPHOS

Cybersecurity made simple.

Sophos Endpoint for Windows 說明

目錄

關於 Sophos Endpoint for Windows....1
Sophos Endpoint....2
狀態....3
事件....5
設定....7
如何....9
掃描一個檔案....9
掃描電腦或伺服器....9
清除威脅....9
變更安全設定....9
立即更新....10
疑難排解....10
加密您的電腦....10
當您忘記密碼時，請存取您的電腦....11
我的檔案傳輸為何受到攔截？....12
支援....13
法律聲明....14

1 關於 Sophos Endpoint for Windows

此說明檔案提供關於 Endpoint for Windows 的資訊，並逐步解釋程序。

2 Sophos Endpoint

Sophos Endpoint 在電腦和伺服器上運行以為它們提供防護。

限制
您可能沒有此處描述的所有功能。這取決於您的許可權。

Sophos Endpoint 是從 Sophos Central Admin 集中設定和管理的。

但是，您可以在電腦或伺服器上完成一些任務：

- 檢查電腦的狀態。
- 掃描檔案、電腦或伺服器是否出現威脅。
- 請參閱電腦或伺服器上事件的詳情，例如，偵測到的威脅。
- 清除威脅。
- 變更安全設定。例如，您可以關閉一些功能以便您進行故障排除。
- 更新。
- 疑難排解。

注意事項
您需要使用管理員登入並輸入竄改防護密碼一清除威脅或變更設定。

相關概念

狀態 （第 3 页）
您可檢查安全狀態並掃描您的電腦或伺服器。

事件 （第 5 页）
事件頁面顯示電腦或伺服器上的事件，例如偵測到的威脅。

相關工作

掃描一個檔案 （第 9 页）
您可掃描單個檔案。

掃描電腦或伺服器 （第 9 页）
按照以下指示掃描您的電腦或伺服器。

清除威脅 （第 9 页）
請按照以下指示清除已偵測到的威脅。

變更安全設定 （第 9 页）
按照以下指示變更安全設定。

立即更新 （第 10 页）
請按照以下指示更新您的病毒定義。

疑難排解 （第 10 页）
按照以下指示進行疑難排解。

3 狀態

您可檢查安全狀態並掃描您的電腦或伺服器。

限制
您可能沒有此處描述的所有功能。這取決於您的許可權。

狀態頁面能讓您：

- 查看電腦或伺服器的安全狀態。
- 掃描電腦或伺服器是否出現威脅。
- 查看已安裝的功能及其安全狀態。

注意事項
頁面右下方的關於連結使您能夠更新病毒定義並對產品進行故障排除。

安全狀態

頁面上部的一個圖示顯示此狀態。

設定	描述
 綠色。	沒有警示，或者僅有優先權低的警示。
 紅色。	優先權高的警示。
 黃色。	優先權為中級的警示。
 灰色。	狀態未知。

下方顯示了已安裝的所有功能及其安全狀態。

掃描計算機

按一下掃描，掃描電腦或伺服器上的所有檔案以確定是否有威脅。

完成掃描之後，您將看到一份掃描結果摘要。如果偵測到威脅，您可以前往事件頁面以檢視詳情。

4 事件

事件頁面顯示電腦或伺服器上的事件，例如偵測到的威脅。

限制
您可能沒有此處描述的所有功能。這取決於您的許可權。

您可以篩選事件，例如，僅顯示需要您採取行動的事件，或者搜尋特定類型的事件。

事件清單

該清單顯示：

- 嚴重性：清單最左側的圖示顯示事件是具有高優先順序還是具有中優先順序，或是通知。
- 來源。清單左側的圖示表示報告該事件的 Sophos 功能。
- 事件發生時的日期和時間。
- 事件的描述。
- 允許您採取行動的連結（如果需要任何行動）。僅有在您作為管理員登入的情況下才會顯示。

如需查看每個事件的詳細信息，請按一下右側箭頭以將其展開。

您所能採取的行動和 Sophos Central Admin 中所提供的一樣。在 Sophos Central Admin 幫助 中的警示頁面上檢視清單。

您可以按照以下類型篩選事件：

事件類型	描述
惡意軟體與可能不需要的應用程式	惡意軟體是惡意軟體的通用術語。它包括病毒、蠕蟲、木馬以及間諜程式。 可能不需要的應用程式 (PUA) 是指撥號程式、遠端管理工具以及黑客工具等不具有惡意但通常被認為不適合大多數商業網路的程式。
網頁威脅	網頁威脅包括惡意網站、未分類的網站和有風險的下載。 一些網站通常也被視為不適合於商業網路，例如成人網站或社交媒體。這些都會被攔截。
惡意行為	惡意行為是軟體中偵測到的已在電腦或伺服器上運行的可疑行為。 勒索軟體是一種惡意軟體，它會拒絕您存取您的檔案，除非您支付贖金。

事件類型	描述
受控項目	此類別包括： • 並不具有安全威脅但您判定不適合在您的辦公環境內使用的應用程式。 • 外圍和卸除式媒體。 • 有風險的下載或不適合於辦公環境的網站。 • 包含您不想洩露的敏感資訊（例如，個人或財務詳細資訊）的檔案。
惡意資料流	惡意資料流是指電腦之間的資料流，會表現出一種可能控制電腦或伺服器的企圖（一種「命令和控制」攻擊）。
入侵程式	Sophos 可以防範的漏洞包括：利用瀏覽器漏洞和瀏覽器外掛程式的劫持性和入侵性應用程式、Java 應用程式、媒體應用程式和 Microsoft Office 應用程式。

5 設定

您可以臨時變更電腦或伺服器上的安全設定。

在您進行故障排除時您可能需要完成這一步。例如，您可能想要關閉一項功能以確定它是否會在計算機上引發問題。

限制
您可能沒有此處描述的所有功能。這取決於您的許可權。

限制
僅有在您已輸入竄改防護密碼（可由 Sophos Central 管理員提供）的情況下才可使用設定頁面。

如何變更設定

勾選標記有覆寫 Sophos 中央策略達 4 小時以進行故障排除的方塊。

現在您可以在此頁面上進行變更。變更將臨時覆寫您（或另一管理員）從 Sophos Central Admin 套用的策略。

四個小時後，設定會自動恢復至集中執行的策略設定。

如果需要的話，您可提前將設定恢復。你無法使用滑動控制項對單個功能進行此操作。相反，關閉覆寫 Sophos 中央策略達 4 小時以進行故障排除。

Deep Learning（深度學習）

Deep Learning 會使用進階機器學習偵測威脅。它可以識別惡意軟體和可能不需要的應用程式，而無需使用簽章。

即時掃描

即時掃描在使用者嘗試存取項目時對其進行掃描，但在確認其安全之前會拒絕存取。您可以選擇：

- 檔案：此操作掃描本地檔案和（如果在策略中選取這一項）網路共用。
- 網際網路：此操作掃描網際網路資源。它可以掃描正在進行的下載、攔截對惡意網站的存取並偵測信譽度低的網站。

對使用者的控制

- 外圍控管功能使您能夠存取外圍和卸除式媒體。
- 應用程式控管功能能讓您偵測並且攔截不具有安全威脅但您判定不適合在您辦公環境使用的應用程式。
- 網頁控管功能讓您能夠防止出現具有風險的下載，控制使用者能夠存取的站點並且防止資料丟失。
- 資料遺失防止功能讓您能夠監控和限制包含敏感資料的檔案的傳輸。

- 篡改防護功能可讓您限制變更。如果啓用該功能，本機系統管理員需要使用必要的密碼來變更安全設定或解除安裝 Sophos Endpoint。

執行階段保護

執行階段保護透過偵測端點計算機上的可疑或惡意行為或資料流來防止受到威脅。您可以選擇：

- 勒索軟體偵測：此功能可以防止受到惡意軟體的威脅，惡意軟體會限制對檔案的存取，然後要求付費來釋放它們。
- 安全瀏覽：此功能可以保護您的網頁瀏覽器以防其受到惡意軟體的利用。
- 入侵程式削弱：此功能可以保護最容易受到惡意軟體利用的應用程式，比如 Java 應用程式。
- 網路威脅防護：此功能可以偵測端點計算機和伺服器之間的資料流，表現出一種可能控制端點計算機的企圖。它包括封包檢查，該檢查可以掃描網路通訊，在威脅可能損害作業系統或應用程式之前將其識別並攔截。

  注意事項
  如果您關閉了網路威脅防護，則 EDR 功能、「隔離」和「阻擋」也會關閉。

- 惡意行為偵測：它偵測並攔截已知具有惡意或可疑的行為。

電腦控制

您可以在電腦和伺服器上監控 Windows 防火牆（和其他已註冊的防火牆）。

6 如何...

6.1 掃描一個檔案

您可掃描單個檔案。

若要掃描檔案，請執行以下操作。

- 在 Explorer 中，在檔案上按滑鼠右鍵並選擇掃描。

6.2 掃描電腦或伺服器

按照以下指示掃描您的電腦或伺服器。

要掃描電腦或伺服器上的所有檔案：

1. 前往狀態頁面或偵測頁面。
2. 按一下掃描。
   完成掃描之後，您將看到一份掃描結果摘要。
3. 如果偵測到威脅，您可以前往事件頁面以檢視詳情。

6.3 清除威脅

請按照以下指示清除已偵測到的威脅。

要清除威脅，請執行以下操作：

1. 按一下管理員登入並輸入竄改防護密碼（可由您的 Sophos Central 管理員提供）。
2. 前往事件頁面以查看已檢測到的威脅詳情。
3. 在威脅詳情旁邊尋找動作連結。

您所能採取的行動和 Sophos Central Admin 中所提供的一樣。在 Sophos Central Admin 幫助中的警示頁面上檢視清單。

6.4 變更安全設定

按照以下指示變更安全設定。

若要變更安全設定：

1. 在介面右上方按一下管理員登入。
2. 輸入竄改防護密碼（可由您的 Sophos Central 管理員提供）。
   現在，在功能表列，出現設定連結。
3. 前往設定頁面。
4. 勾選標記有覆寫 Sophos 中央策略達 4 小時以進行故障排除的方塊。
5. 使用頁面上的滑動控制項關閉安全功能。

四個小時後，設定將自動恢復至集中執行的策略設定。

注意事項
如果需要的話，您可提前將設定恢復。你無法使用滑動控制項對單個功能進行此操作。相反，取消選中覆寫 Sophos 中央策略達 4 小時以進行故障排除。

6.5 立即更新

請按照以下指示更新您的病毒定義。

若要更新，請執行以下操作：

1. 按一下 關於。
2. 點選立即更新。

6.6 疑難排解

按照以下指示進行疑難排解。

如需進行疑難排解，請執行以下操作：

1. 按一下 關於。
2. 點選開啟 Endpoint Self Help 工具以收集問題資料，或者跟隨連結前往社群論壇。

6.7 加密您的電腦

按照以下說明加密您的電腦。

限制
裝置加密僅在端點電腦上可用。

裝置加密功能加密使用 Windows BitLocker 技術的電腦的硬碟。您的管理員定義您在每次存取電腦時是否需要驗證。

如果不需要驗證，則收到 Sophos Central 策略，重新啟動電腦後，您的硬碟加密會自動開始。在本情況下，您無需執行任何動作。

如需驗證，您需要進行以下操作：

1. 顯示 Sophos Device Encryption 對話方塊時，請按照對話方塊中的指示操作。具體的指示取決於您的系統及管理員定義的策略設定。
    - 如果裝置加密策略要求 PIN 碼或密碼以進行驗證，請按照螢幕上的指示操作以建立 PIN 碼或密碼。

        注意事項
        建立 PIN 碼或密碼時請謹慎。預先開機環境僅支援美式英語鍵盤配置。如果您現在使用特殊字元建立 PIN 碼或密碼，當您稍後輸入該 PIN 碼或密碼登入時，可能需要使用不同的金鑰。

    - 如果裝置加密策略要求 USB 金鑰進行驗證，則您需要將 USB 快閃磁碟連接至您的電腦。USB 快閃磁碟機必須是 NTFS、FAT 或 FAT32 格式。

2. 當您點選重新啟動並加密時，電腦將重新啟動並加密硬碟。您可以照常工作。

注意事項
您可以選擇稍後再做以關閉對話方塊。但是，下次您登入時它將還會出現。

Sophos Central 為系統磁碟區加密之後，資料卷的加密已啟動。卸除式資料卷，例如 USB 磁碟機，將不會進行加密。

當您登入電腦時，您可能需要 PIN 碼、密碼或 USB 金鑰來解鎖您的系統磁碟區。資料卷會自動解鎖。

6.8 當您忘記密碼時，請存取您的電腦

按照以下步驟存取您的電腦。

如果您由於忘記了 PIN 碼、密碼或 USB 金鑰而無法登入電腦，則您需要一個修復金鑰。

如果您使用的是 Sophos Device Encryption，則該修復金鑰儲存於 Sophos Central 中。如需獲取您的修復金鑰，請執行以下動作之一：

- 登入到 Sophos 自助入口網站，並按照 幫助 中的指示操作。
- 要求您的管理員為您擷取修復金鑰。如果您無法使用自助入口網站，執行此操作。

相關工作
使用 BitLocker 修復 （第 11 页）
按照以下指示修復您的電腦。

6.8.1 使用 BitLocker 修復

按照以下指示修復您的電腦。

如需修復您的電腦，請執行以下操作：

1. 重新啟動電腦，並在 BitLocker 登入螢幕中按下 Esc 鍵。
2. 在 BitLocker 修復螢幕中，找到修復金鑰識別碼。
   修復金鑰識別碼 顯示的時間很短。要使其再次顯示，您必須重新啟動電腦。
3. 聯絡管理員，並將修復金鑰識別碼告訴他們。
   管理員需在 Sophos Central 中找到您電腦的修復金鑰，並將該金鑰給您。
4. 在 BitLocker 修復螢幕中，輸入該修復金鑰。
   你現在可以啟動電腦。
5. 按照屏幕上的說明在提示時創建新的 BitLocker PIN 或密碼。

   在執行 Windows 7 的電腦上，您看不到任何說明。您需要手動重設 PIN 碼/密碼。

您可再次存取電腦。

注意事項
一個恢復金鑰僅能使用一次。如果稍後需要再次恢復電腦，您將需要擷取新的修復金鑰。

7 我的檔案傳輸為何受到攔截？

您可能會看到訊息，告訴您檔案傳輸（例如，複製、移動或透過電子郵件傳送檔案）受到攔截。這是因為您的公司已設定了策略，以確保您不會無意中將資訊傳送給不應擁有該資訊的使用者。訊息有兩種類型。

訊息	描述
傳輸受到攔截	如果您收到了「已攔截檔案傳輸」訊息，您無法傳輸該檔案。您的管理員可能會在該訊息中新增一些建議。
可以允許傳輸	如果您收到了「已攔截檔案傳輸請求」訊息，您可以決定是否傳輸該檔案。您的管理員可能會在該訊息中新增一些建議。如果您確定這樣做為安全，請點選允許。

8 支援

您可使用以下其中一項方法，取得 Sophos 產品技術支援服務：

- 造訪 community.sophos.com/ 內的 Sophos 社群，尋找其他遭遇到相同問題的使用者。
- 造訪 www.sophos.com/zh-tw/support.aspx 內的 Sophos 技術支援知識庫。
- 於 www.sophos.com/zh-tw/support/documentation.aspx 下載產品說明文件。
- 請於此處向我們的支持團隊發送權證 https://secure2.sophos.com/zh-tw/support/contact-support/support-query.aspx。

9 法律聲明