# Microsoft Defender for Endpoint

企業端點安全平台

旨在協助企業網路預防、偵測、調查和回應進階威脅。

* **端點行為感測器**。 Windows 10 和 11 嵌入了感測器。首先收集和處理來自作業系統的行為訊號。然後，將感測器資料傳送到組織的 Microsoft Defender for Endpoint 的私有、隔離的雲端實例。
* **雲端安全分析**。企業雲端產品（例如 Microsoft 365）和線上資產在整個 Windows 生態系統中應用大數據、裝置學習和獨特的 Microsoft 光學。然後，Microsoft Defender for Endpoint 將行為訊號轉化為針對進階威脅的洞察、偵測和建議回應。
* **威脅情報**。 Microsoft 威脅追蹤人員和安全團隊產生威脅情報。然後，合作夥伴用自己的威脅情報來增強這些資訊。威脅情報讓 Microsoft Defender for Endpoint 能夠：
  + 識別攻擊者工具、技術和流程。
  + 當它在收集的傳感器數據中觀察到它們時產生警報。

# Microsoft Defender for Endpoint 架構

Microsoft Defender XDR 套件包含各種安全服務，例如 Microsoft Defender for Endpoint、Microsoft Defender for Office 365 和 Microsoft Defender for Cloud Apps。下圖顯示了 Microsoft Defender for Endpoint 體系結構中所包含的服務。

Microsoft Defender for Endpoint 體系結構的服務包括：

* [威脅和漏洞管理](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/next-gen-threat-and-vuln-mgt)。這種內建功能使用改變遊戲規則的基於風險的方法來發現、確定優先順序並修復端點漏洞和錯誤配置。
* [攻擊面減少](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack-surface-reduction)。減少攻擊面的功能集提供了堆疊中的前線防禦。為了支援此功能，組織應確保正確設定配置設定並套用緩解技術。透過這樣做，減少攻擊面的能力可以抵抗攻擊和利用。這些功能還包括網路保護和 Web 保護。這些功能可控制對惡意 IP 位址、網域和 URL 的存取。
* [下一代保護](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/next-generation-protection)。為了進一步加強網路的安全邊界，Microsoft Defender for Endpoint 使用旨在捕獲所有類型的新興威脅的下一代保護。
* [端點檢測和響應](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-endpoint-detection-response)。此功能可偵測、調查和回應進階威脅，從而突破前兩個安全支柱。進階搜尋提供基於查詢的威脅搜尋工具，可讓您主動尋找違規行為並建立自訂偵測。
* [自動調查和修復](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/automated-investigations)。 Microsoft Defender for Endpoint 可以快速回應進階攻擊。它還提供自動調查和修復功能，有助於在幾分鐘內大規模減少警報。
* [裝置的 Microsoft 安全性分數](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/tvm-microsoft-secure-score-devices)。 Microsoft Defender for Endpoint 包含 Microsoft 裝置安全性分數。此功能可以幫助組織：
  + 動態評估企業網路的安全狀態。
  + 識別未受保護的系統。
  + 採取建議的措施來提高組織的整體安全性。
* [微軟威脅專家](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-threat-experts)。 Microsoft Defender for Endpoint 的新託管威脅搜尋服務提供主動搜尋、優先順序以及其他上下文和洞察。這些功能進一步使安全營運中心 (SOC) 能夠快速且準確地識別威脅並做出回應。

Microsoft Defender for Endpoint 客戶必須申請 Microsoft 威脅專家託管的威脅搜尋服務，才能獲得主動的定向攻擊通知並按需與專家協作。該服務是一項附加功能。 Microsoft 威脅專家功能接受您加入其託管威脅搜尋服務後，它始終包含目標攻擊通知。對於尚未註冊 Microsoft 威脅專家但希望體驗其優勢的用戶，請依序前往**「設定」**、「**常規」**、**「進階功能」**、**「Microsoft 威脅專家」**進行申請。一旦接受，您將獲得定向攻擊通知的好處。您也可以開始為期 90 天的專家點播試用。請聯絡您的 Microsoft 代表以獲得專家點播的完整訂閱。

* [集中配置與管理、API](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/management-apis)。將 Microsoft Defender for Endpoint 整合到現有工作流程中。
* [與 Microsoft 解決方案整合](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/threat-protection-integration)。 Microsoft Defender for Endpoint 直接與各種 Microsoft 解決方案集成，包括：
  + - Microsoft Defender for Cloud
    - Microsoft Sentinel
    - Microsoft Intune
    - Microsoft Defender for Cloud Apps
    - Microsoft Defender for Identity
    - Microsoft Defender for Office 365
    - Skype for Business

[**https://www.microsoft.com/videoplayer/embed/RE4vnC4?rel=0&postJsllMsg=true%3Fazure-portal%3Dtrue**](https://www.microsoft.com/videoplayer/embed/RE4vnC4?rel=0&postJsllMsg=true%3Fazure-portal%3Dtrue)

# 在 Microsoft Intune 中設定 Microsoft Defender for Endpoint

完成以下步驟以透過 Microsoft Intune 啟用 Microsoft Defender for Endpoint：

1. 先導覽至**Microsoft Intune 管理中心**。為此，請在**Microsoft 365 管理中心 的**導覽窗格中選擇「**顯示全部」** 。在**「管理中心」**群組下，選擇**「端點管理員」**。
2. 在**Microsoft Intune 管理中心 的**導覽窗格中選擇**終結點安全性。**
3. 論**端點安全 |在「概述」**頁面的中間窗格的**「設定」部分下，選擇Microsoft Defender for Endpoint**。
4. 論**端點安全 | Microsoft Defender for Endpoint**頁面，向下捲動至**共用設定**部分，然後選擇**開啟 Microsoft Defender 安全性中心**。此步驟將開啟**Microsoft Defender**入口網站。
5. 在**Microsoft Defender**入口網站的左側導覽窗格中，依序選擇**「設定」**、**「終結點」**、**「進階功能」**。
6. **將Microsoft Intune 連線**設定的切換開關設定為**開啟**。
7. 選擇**儲存首選項**。
8. **將Android 裝置連接**到 Microsoft Defender for Endpoint設定為**開啟。**將**iOS/iPadOS 裝置連接**到 Microsoft Defender for Endpoint 設定為**開啟。將Windows 裝置連接**到 Microsoft Defender for Endpoint設定為**開啟。**
9. 選擇**保存**。

# 使用 Microsoft Defender 漏洞管理管理端點漏洞

Microsoft Defender 漏洞管理會根據下列因素來決定漏洞的優先順序：

* 威脅情勢
* 您組織中的檢測
* 有關易受攻擊設備的敏感訊息
* 業務背景

內建的無代理掃描程式可持續監視和偵測組織中的風險。

Asset discovery and inventory

**內建的無代理掃描程式可持續監視和偵測組織中的風險。**

Vulnerability and configuration assessment

**安全基線評估**

**軟體和漏洞的可見性**

**網路份額評估**

**威脅分析和事件時間表**

**瀏覽器擴充功能**

**數位證書**

Risk-based intelligent prioritization

**重點關注新出現的威脅**

**查明主動違規行為**

**保護高價值資產**

Remediation and tracking

**向 IT 發送補救請求**

**阻止易受攻擊的應用程式**

**替代緩解措施**

**即時修復狀態**

### 探索網路中的設備

使用下列進階搜尋 (Kusto) 查詢來取得有關網路清單中所述的每個網路名稱的更多上下文。查詢列出過去 7 天內連接到某個網路的所有已上線設備。

DeviceNetworkInfo

| where Timestamp > ago(7d)

| where ConnectedNetworks != ""

| extend ConnectedNetworksExp = parse\_json(ConnectedNetworks)

| mv-expand bagexpansion = array ConnectedNetworks=ConnectedNetworksExp

| extend NetworkName = tostring(ConnectedNetworks ["Name"]), Description = tostring(ConnectedNetworks ["Description"]), NetworkCategory = tostring(ConnectedNetworks ["Category"])

| where NetworkName == "<your network name here>"

| summarize arg\_max(Timestamp, \*) by DeviceId

使用 parse\_json 函數將 ConnectedNetworks 欄位解析為 JSON 物件，能夠提取其中的屬性。然後，使用 mv-expand 函數展開 ConnectedNetworks 陣列，以便進行進一步的分析。

### 取得設備資訊

使用以下進階搜尋 (Kusto) 查詢來取得特定裝置的最新完整資訊。

DeviceInfo

| where DeviceName == "<device name here>" and isnotempty(OSPlatform)

| summarize arg\_max(Timestamp, \*) by DeviceId

### 對發現的設備使用高級搜索

DeviceInfo

| summarize arg\_max(Timestamp, \*) by DeviceId // Get latest known good per device ID

| where isempty(MergedToDeviceId) // Remove invalidated/merged devices

| where OnboardingStatus != "Onboarded"where isempty(MergedToDeviceId) 過濾掉已被合併或無效的裝置，只保留有效的裝置。

 where OnboardingStatus != "Onboarded" 排除已進行上線設置 (Onboarded) 的裝置。

呼叫 SeenBy 函數，您可以獲得有關哪個已登入裝置看到已發現裝置的詳細資訊。這些資訊可以幫助確定每個已發現設備的網路位置。然後它可以幫助在網路中識別它。

DeviceInfo

| where OnboardingStatus != "Onboarded"

| summarize arg\_max(Timestamp, \*) by DeviceId

| where isempty(MergedToDeviceId)

| limit 100

| invoke SeenBy()

| project DeviceId, DeviceName, DeviceType, SeenBy

### 查詢網路相關資訊

DeviceNetworkEvents

| where ActionType == "ConnectionAcknowledged" or ActionType == "ConnectionAttempt"

| take 10

獲得與連線確認和連線嘗試相關的最近 10 個裝置網路事件

# 減少威脅和漏洞暴露

Microsoft Defender 漏洞管理儀表板將暴露分數分為以下等級：

* **0-29**。曝光分數低。
* **30-69**。中等曝光分數。
* **70-100**。高曝光分數

透過兩種方式存取組織的安全建議。它們都顯示在**Microsoft Defender**入口網站中導覽窗格中的**漏洞管理**群組下：

* **建議**。選擇此選項會將帶到**「安全建議」**頁面。此頁包含組織中發現的威脅和漏洞的安全建議清單。
* **儀表板**。選擇此選項可查看**頂級安全建議**和公司的**暴露分數**。

儀表板的**頂級安全建議**部分列出了組織的改進機會。使用前面提到的因素（威脅、違規可能性和價值）對機會進行優先排序。選擇建議後，將進入包含更多詳細資訊的**安全建議頁面。**

安全**建議**頁面顯示以下資訊：

* 發現的弱點數量
* 相關組件
* 威脅洞察
* 暴露設備數量
* 地位
* 修復類型
* 補救活動
* 對曝光分數和 Microsoft 裝置安全分數的影響
* 相關標籤
* **開啟軟體頁面**。選擇**“開啟軟體頁面**”選項以獲取有關軟體的更多背景信息。此資訊可包括：
  + 威脅背景
  + 相關推薦
  + 發現的弱點
  + 暴露設備數量
  + 發現的漏洞
  + 安裝了軟體的設備的名稱和詳細信息
  + 版本分佈
* **修復選項**。
* **例外選項**。