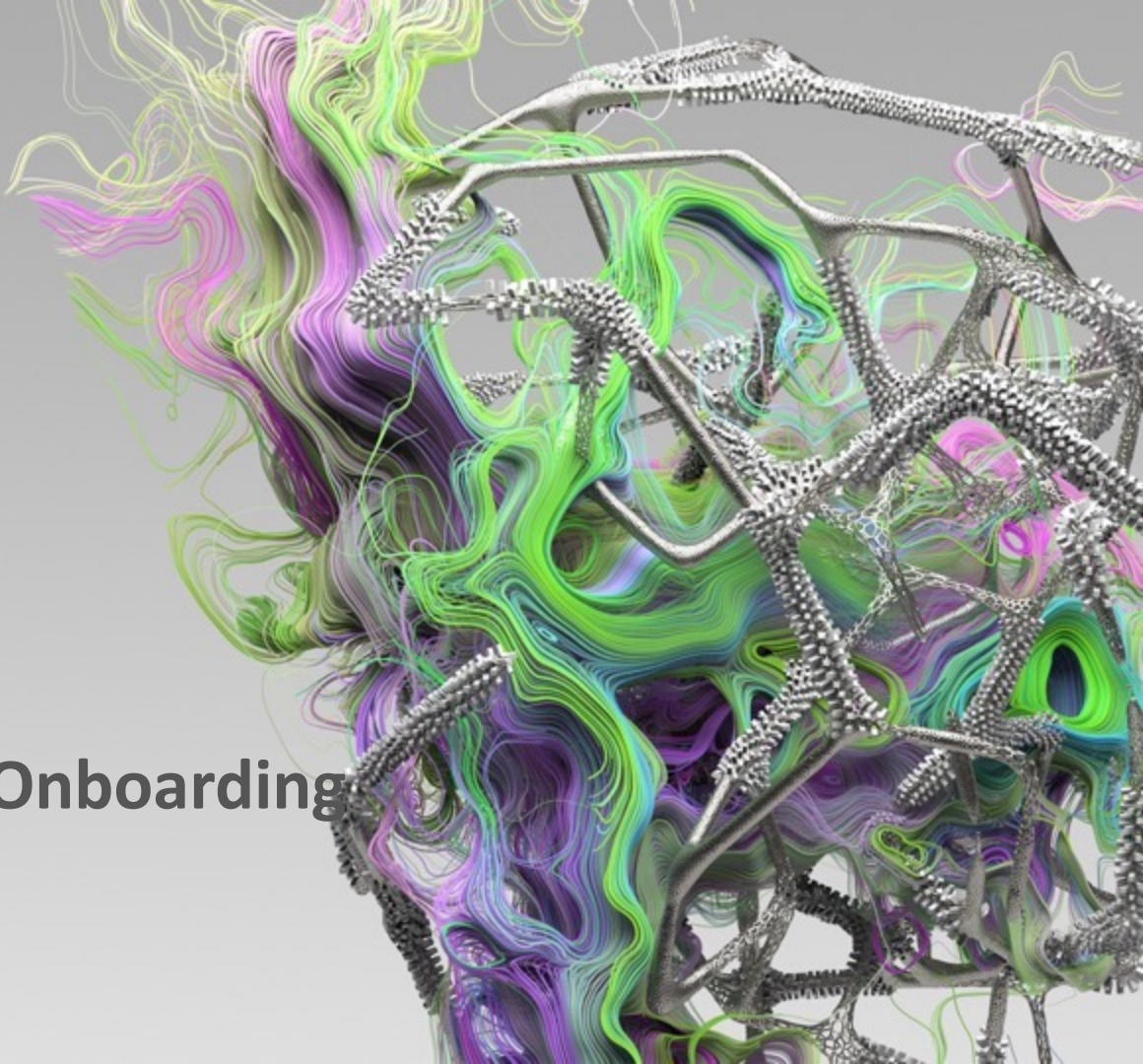




Vision One™

Apex One (on-prem) Onboarding

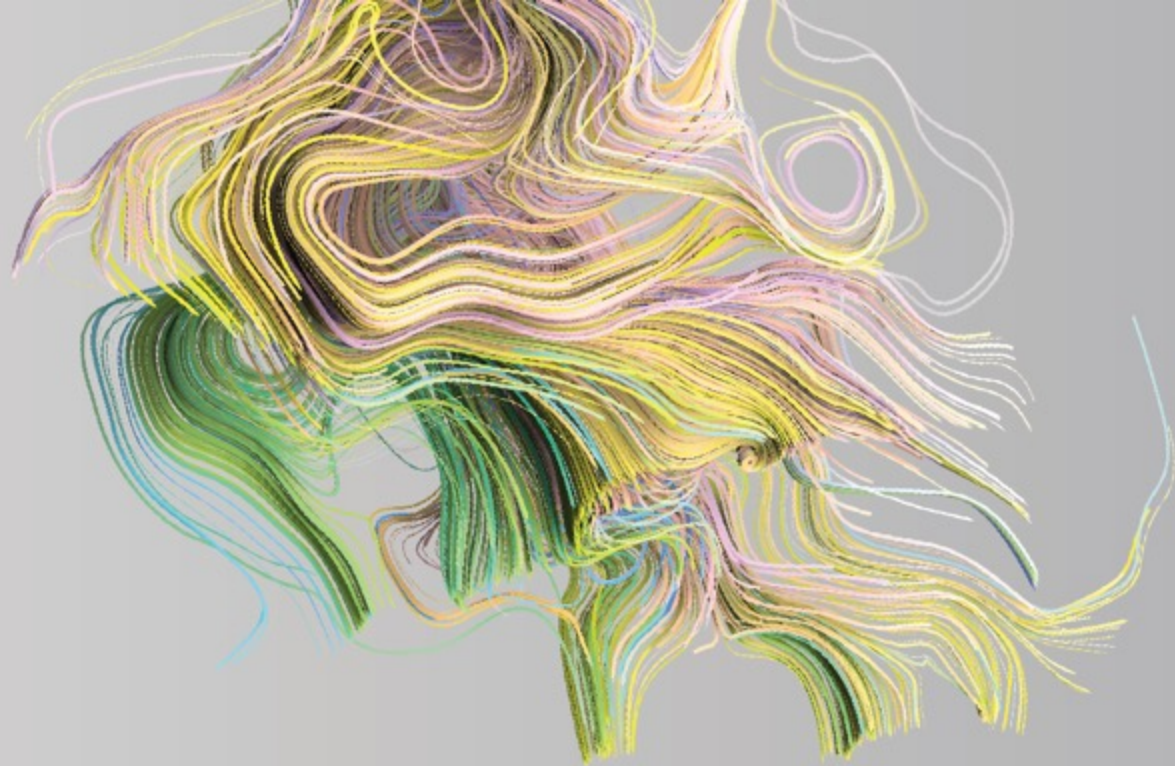
趨勢科技



為什麼要做Onboarding？

Onboarding程序主要將Apex One server所管理的所有用戶端，向Vision One報到。將可省下在大量主機逐一安裝報到程式(EndpointBasecamp)的時間。在Onboarding完成後，將可在Vision One console上，對目標主機啟動XDR sensor。

注意：切勿將尚未完成onboarding程序的Apex One server所管理的用戶端，移轉到已經onboarding的Apex One server。這將會造成用戶端無法正常向Vision One報到。



Onboarding前置準備

Onboarding前置準備(一)

每次登入Apex One web console即可觸發onboarding程序，但需要以下條件：

1. Apex One Patch 3 (build 8378) 以上
2. Apex One server及agent可透過不需要驗證帳密的proxy或是直接連到網際網路，且中間沒有SSL加解密的機制
3. 防火牆需要開放的位址(請參閱以下頁面)：
<https://docs.trendmicro.com/en-us/enterprise/trend-micro-vision-one-online-help/intro-and-gs-part/getting-started/firewall-permissions/firewall-fqdn-singap.aspx>
4. Apex One agent主機的時間同步設定正確

Onboarding前置準備(二)

5. 如果網路環境有嚴格限制內對外通訊位址，請確認以下位址沒有被阻擋：

<http://crl.entrust.net/>

<http://ocsp.entrust.net/>

<http://aia.entrust.net/>

<http://crl.affirmtrust.com/>

<http://ocsp.affirmtrust.com/>

<http://aia.affirmtrust.com/>

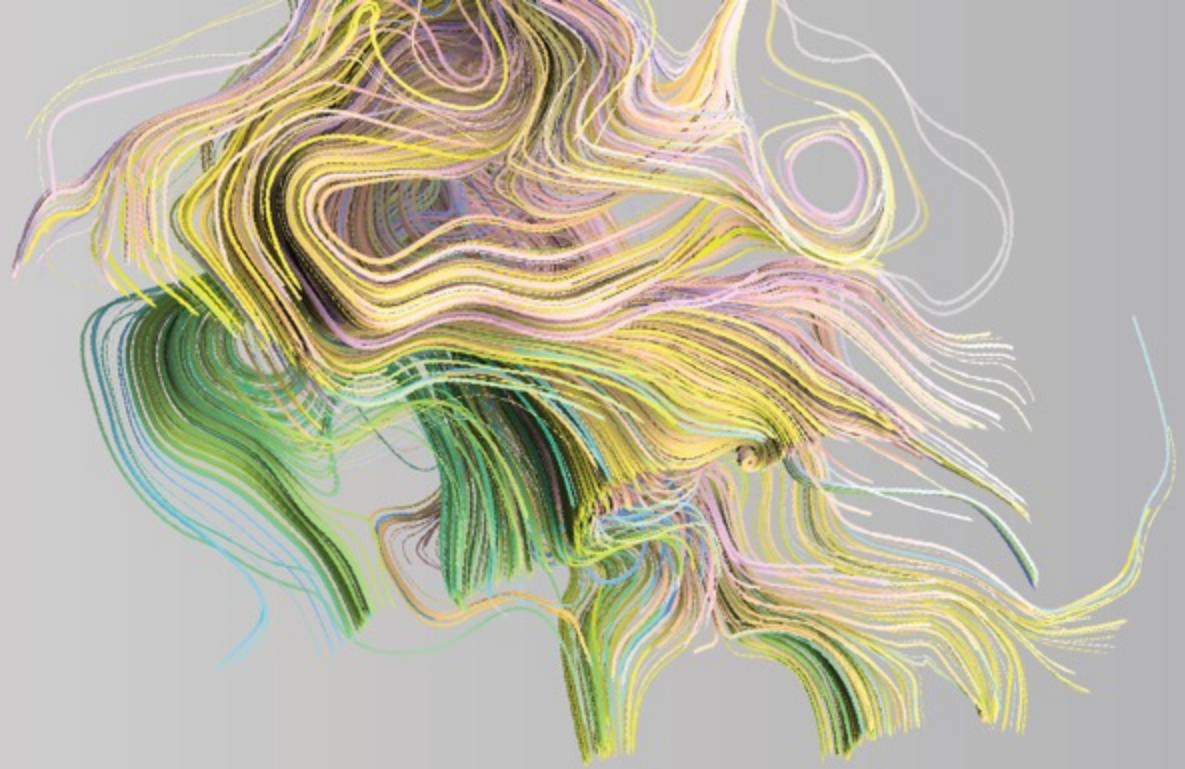
<http://ctldl.windowsupdate.com/>

6. 在Apex One server上，以系統管理員身份執行cmd，並執行以下指令：

```
cd C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV
```

```
Svrsvcsetup.exe -checkOnboardingAPI
```

```
Svrsvcsetup.exe -PrepareXBCpatch -AcceptXBCPII yes
```

Registering Vision One

Apex One Onboarding 程序

登入Apex One web console後，看到藍色橫幅標題

Check the Trend Micro Early Warning Service to see if you are affected by the latest LockBit 2.0 attack. [More Details](#)

或是看到promotion畫面點選其中按鈕，即可進行onboarding程序

×

Examine Systems for Signs of a LockBit 2.0 Ransomware Attack

LockBit resurfaces with version 2.0, brandishing updated techniques against critical industries.

LockBit, which was first observed in 2019, recently resurfaced with version 2.0. Its updated features include automatic encryption, which operators claim to be one of the fastest in today's ransomware threat landscape. The attackers also rely on various tools, such as StealBit for automatically exfiltrating data, and Process Hacker, PC Hunter, and batch files for disabling processes and services in the affected system. LockBit 2.0 employs the double extortion scheme where operators threaten to publicize unpaying victims' data.

How can you discover indicators of infection?

Trend Micro Vision One delivers powerful XDR capabilities to help you detect and respond to threats. Trial Trend Micro Vision One for 60 days for free to receive real-time updates on potential indicators of compromise on endpoints, mailboxes, servers, and networks.

Check if I'm affected, using Trend Micro Vision One

Apex One Onboarding 程序

請輸入CLP(Customer Licensing Portal)帳號，
如果還沒有CLP帳號，請繼續參考以下操作步驟。

Check for Nefilim Ransomware in Systems

Organizations outside of the Commonwealth of Independent States (CIS) are potentially at risk for ransomware infection.

First seen in March 2020, Nefilim employed a wide arsenal of tools and malware. It has also been analyzed as one of the first few ransomware routines that employ the double extortion technique. Nefilim has been observed as sharing code similarities with Navity, and primarily targets non-CIS countries and organizations. It spreads via exposed RDPs, stolen credentials, and unpatched vulnerabilities. In addition to encrypting files, Nefilim threatens to publish stolen information via a data leak site when the ransom demanded remains unpaid.

Execution

● **Starter batch files**, which are custom batch files that contain a list of processes and services to terminate, are used to execute other components, as well as the ransomware itself.

Credential Access

● **Password recovery tools**, such as LaZagne and HiefPass, are third-party tools that can be used to gather or retrieve account credentials that are stored in the system.

Discovery

● **AdFind** is a third-party program that can be used for Active Directory query. SMB Tool is a program that can be used to perform reconnaissance on machines in a local network via SMB.

OS Credential Dumping

● **Mimikatz** is a third-party program that can be used to obtain both account and credentials that are used and stored from the operating system and software.

Impair Defenses

● **PowerTools**, such as GMER, PC Hunter, and Process Hacker, are third-party tools that can be used to terminate antivirus-related processes and services in systems.

Experience XDR in just a few steps. Get high-fidelity alerts with cloud-native, cross-layer correlation.

Use this account to access your Trend Micro Vision One console anywhere.



[Need help signing in?](#)

☐ I agree to the [Terms of Service \(Global | Japan\)](#), [Privacy Notice](#), and [Data Collection Notice](#).

☐ I allow Trend Micro to scan my Smart Protection Network data for early attack indicators.

[Get Started](#)

① 註冊CLP帳號

請登入CLP，請在以下欄位以RK序號註冊新帳號

 Customer Licensing Portal

建立帳號或登入

您需要有趨勢科技帳號才能使用和管理您的產品使用授權。您是否已經有帳號？

注意： 如果您早已使用其他的趨勢科技服務，可使用同一個帳號來登入。

☐ 是，我已經有趨勢科技帳號。
登入您的帳號來啟動使用授權、升級試用版使用授權或新增使用授權的授權數目。

☒ 否，我是首次使用的使用者。
建立新的趨勢科技帳號。

僅限輸入一個產品或服務授權碼。您可以在建立帳號後，註冊其他產品或服務授權碼。

繼續

 Customer Licensing Portal

檢閱產品資訊

Apex One and Apex Central Full Feature for Windows and Mac

啟動碼：	OS-
使用授權：	251
到期日：	2021/12/31
使用授權：	完整版

☒ 我已閱讀並接受適當的趨勢科技合約 [全球隱私權聲明](#) 和 [資料蒐集聲明](#)。

- 對於雲端服務 (包括 SaaS)，請參閱 [雲端服務的服務條款](#)。
- 對於所有其他企業產品，請參閱 [全球商業軟體和裝置合約](#)。

繼續 取消

① 註冊CLP帳號 – 填寫基本資料

注意：一個CLP帳號視為一個公司行號，不建議多個管理者各自建立CLP帳號，也不要將公司購買的產品授權分別註冊到不同CLP帳號下。

填寫公司資訊與建立登入雲端服務帳號資訊



Customer Licensing Portal

填寫表單以註冊產品或服務

您是代表客戶的經銷商嗎？
☐ 是 ☒ 否

客戶公司資訊

公司名稱：*

國家/地區：*

選取國家/地區

地址：*

城市：*

州/省：

郵遞區號：*

帳號資訊

建立管理員帳號，以管理貴公司購買的使用授權。

帳號名稱：*

使用 4 到 25 個英數字元、底線或連字號。

密碼：*

請至少輸入 8 個字元，並混合使用大寫字母、小寫字母和數字。

確認密碼：*

電子郵件信箱：*

聯絡人：*

名字

姓氏

聯絡電話：*

區碼

電話號碼

分機

☐ 在產品維護到期前傳送電子郵件通知

繼續

取消

② 透過 CLP 開啟 Vision One 主控台



Customer Licensing Portal

TM_TS_SMB ▾

產品/服務

公司 ▾

說明 ▾

產品/服務

+ 提供金鑰

◆	產品/服務 ◆	作用中使用授權 ◆	使用授權 ◆	到期日 ▾	處理行動
✓	Trend Micro Vision One™ Note: Formerly named Trend Micro XDR		Free	2023/12/31	🔗 開啟主控台

② 透過 Apex One 開啟 Vision One 主控台

Trend Micro Apex One™ 192.168.222.30 root

資訊中心 評估 用戶端 記錄檔 更新 管理 嵌入程式 說明

Trend Micro XDR — 利用 10% 免費的 XDR 使用授權，體驗趨勢科技高準確偵測和警訊的強大功能與無限智慧。請立即使用您的趨勢科技帳號存取 Trend Micro XDR 主控台。

開啟主控台

摘要 +



0

已知安全威脅



0

未知安全威脅



0

策略違規



1

受管理的用戶端



0

已過期的用戶端



0

未受管理的端點

勒索軟體摘要

最近 7 天

0 次勒索軟體嘗試已偵測到

	Web	0
	網路流量	0
	雲端同步	0
	電子郵件	0
	自動執行檔案	0
	本機或網路磁碟機	0

勒索軟體防範的最佳做法

偵測到的前幾名勒索軟體

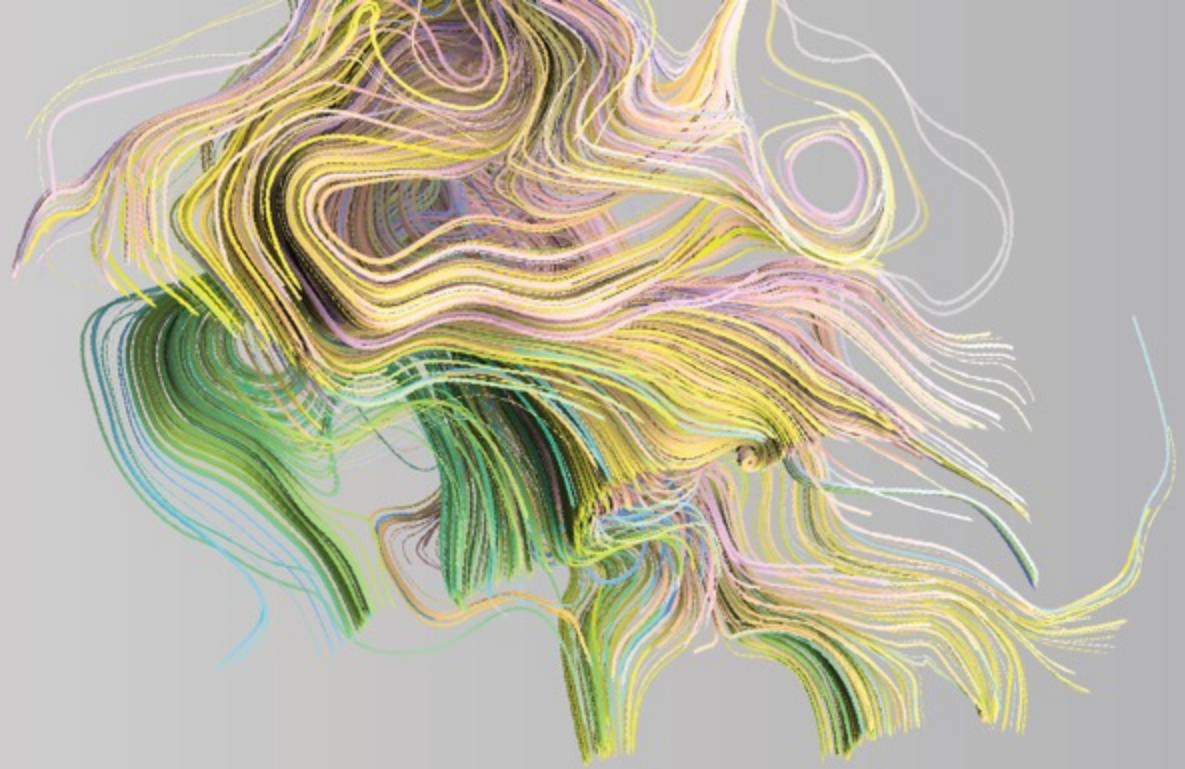
勒索軟體類型 最近 7 天

安全威脅名稱	偵測數
沒有可顯示的資料	



產品授權啟用

請參照「建立CLP帳號及啟用 Product or Credit 授權」的P.4~P.7設定。



Install XDR Sensor

Windows 支援平台

- **Desktop**

- Windows 11 (64-bit)
- Windows 10 (32/64-bit)
- Windows 8.1 (32/64-bit)
- Windows 7 (32/64-bit)

- **Server**

- Windows Server 2022 (64-bit)
- Windows Server 2019 (64-bit)
- Windows Server 2016 (64-bit)
- Windows Server 2012 / 2012 R2 (64-bit)
- Windows Server 2008 R2 (64-bit)

最小需求: CPU:2 cores/ 記憶體:512 MB/ 硬碟可用空間:3 GB

Linux/Mac 支援平台

- **Linux**

- Red Hat Enterprise Linux 6/7/8 (64-bit)
- Amazon Linux (64-bit)
- Amazon Linux 2 (64-bit)
- CentOS Linux 6/7/8 (64-bit)
- Ubuntu 16/18/20

— **建議規格: 記憶體: 5 GB / 硬碟可用空間: 1 GB**

- **Mac**

- macOS High Sierra (10.13) 以上

— **硬碟可用空間: 3 GB**

安裝 XDR sensor (方法一)

注意：已經完成onboarding的Apex One，其所管理的agent都已經出現在Endpoint Inventory，不需要再次執行XDR sensor安裝步驟，可直接進行啟用程序。

此步驟適合沒有安裝Apex One agent目標主機，下載安裝程式：
登入Vision One > Endpoint Inventory > Agent Installer

The screenshot shows the 'Agent Installer' page in the Trend Micro Vision One console. The page is titled 'Trend Micro Vision One™ Endpoint Inventory'. Below the title, there are two tabs: 'Endpoint List' and 'Agent Installer', with 'Agent Installer' being the active tab. The main content area contains instructions: 'Install the agents on as many endpoints as possible to have more comprehensive visibility of your environment. You can directly download the installer or paste the link in your web browser to automatically download the agent.' Below this, there are three cards for different operating systems: Windows (32-bit, 64-bit), macOS (64-bit), and Linux (64-bit). Each card lists supported versions and provides a link to 'View deployment instructions' along with download icons.

Trend Micro Vision One™ Endpoint Inventory

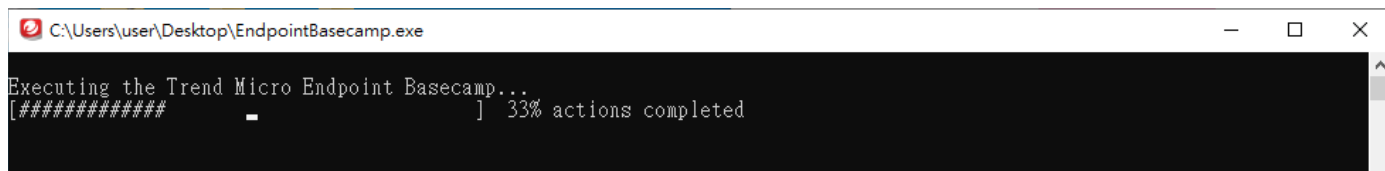
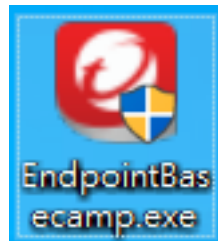
Endpoint List Agent Installer

Install the agents on as many endpoints as possible to have more comprehensive visibility of your environment.
You can directly download the installer or paste the link in your web browser to automatically download the agent.

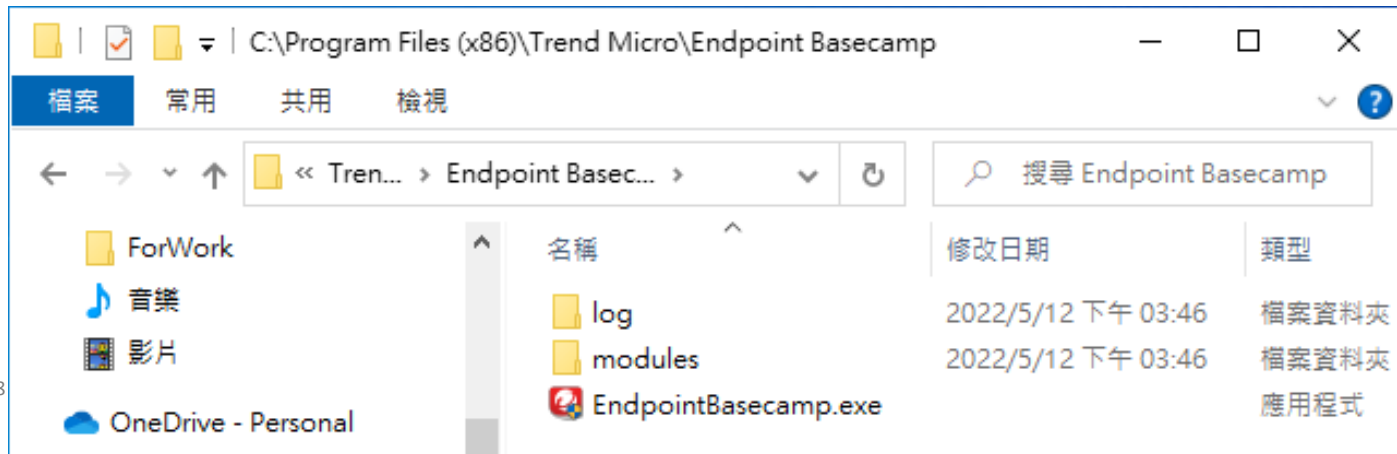
Windows (32-bit, 64-bit)	macOS (64-bit)	Linux (64-bit)
Supported on: Windows 7/8.1/10/11, Windows Server 2008 R2/2012/2016/2019/2022	Supported on: macOS High Sierra (10.13) and later	Supported on: Red Hat Enterprise Linux, CentOS, Amazon Linux, Ubuntu OS (View versions)
View deployment instructions   	View deployment instructions   	View deployment instructions   

安裝 XDR sensor (方法一)

在目標主機下載後，以系統管理員身份執行。
待執行完成，該視窗會自動關閉。



後續可在以下路徑看到下列資料夾：



安裝 XDR sensor(方法二)

此方法適合agent不能連接網際網路，可以透過Service Gateway回傳資料

前置準備：

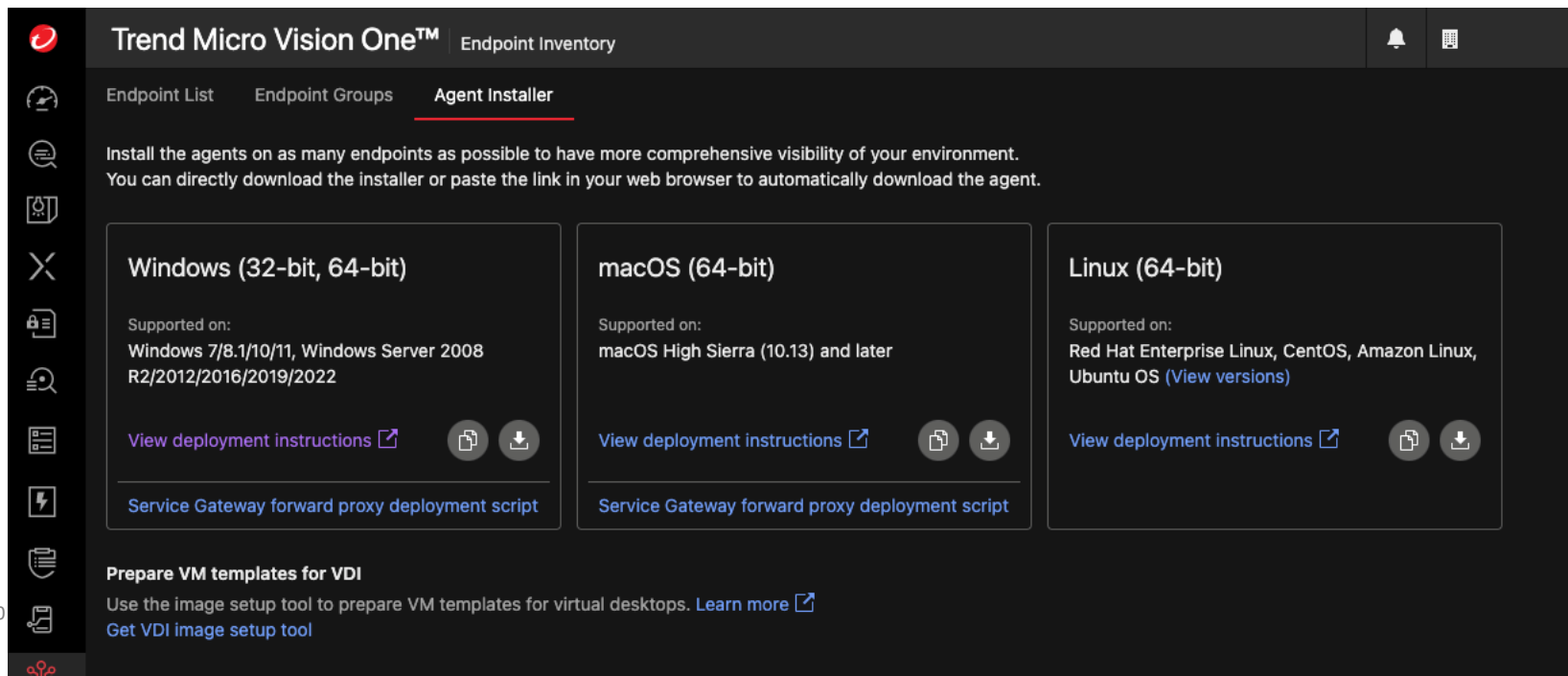
1. 需要先建立Service Gateway，請參考

[安裝Service Gateway\(for ESXi\)](#)或[安裝Service Gateway\(for Hyper-V\)](#)。

2. 需要透過技術支援專線申請開通Endpoint Groups

安裝 XDR sensor(方法二)

開通Endpoint Groups, 且建立並連接Service Gateway後,
在Agent Installer中, 可以看到Service Gateway forward proxy deployment script



Trend Micro Vision One™ Endpoint Inventory

Endpoint List | Endpoint Groups | **Agent Installer**

Install the agents on as many endpoints as possible to have more comprehensive visibility of your environment.
You can directly download the installer or paste the link in your web browser to automatically download the agent.

Windows (32-bit, 64-bit)

Supported on:
Windows 7/8.1/10/11, Windows Server 2008 R2/2012/2016/2019/2022

[View deployment instructions](#)

[Service Gateway forward proxy deployment script](#)

macOS (64-bit)

Supported on:
macOS High Sierra (10.13) and later

[View deployment instructions](#)

[Service Gateway forward proxy deployment script](#)

Linux (64-bit)

Supported on:
Red Hat Enterprise Linux, CentOS, Amazon Linux, Ubuntu OS ([View versions](#))

[View deployment instructions](#)

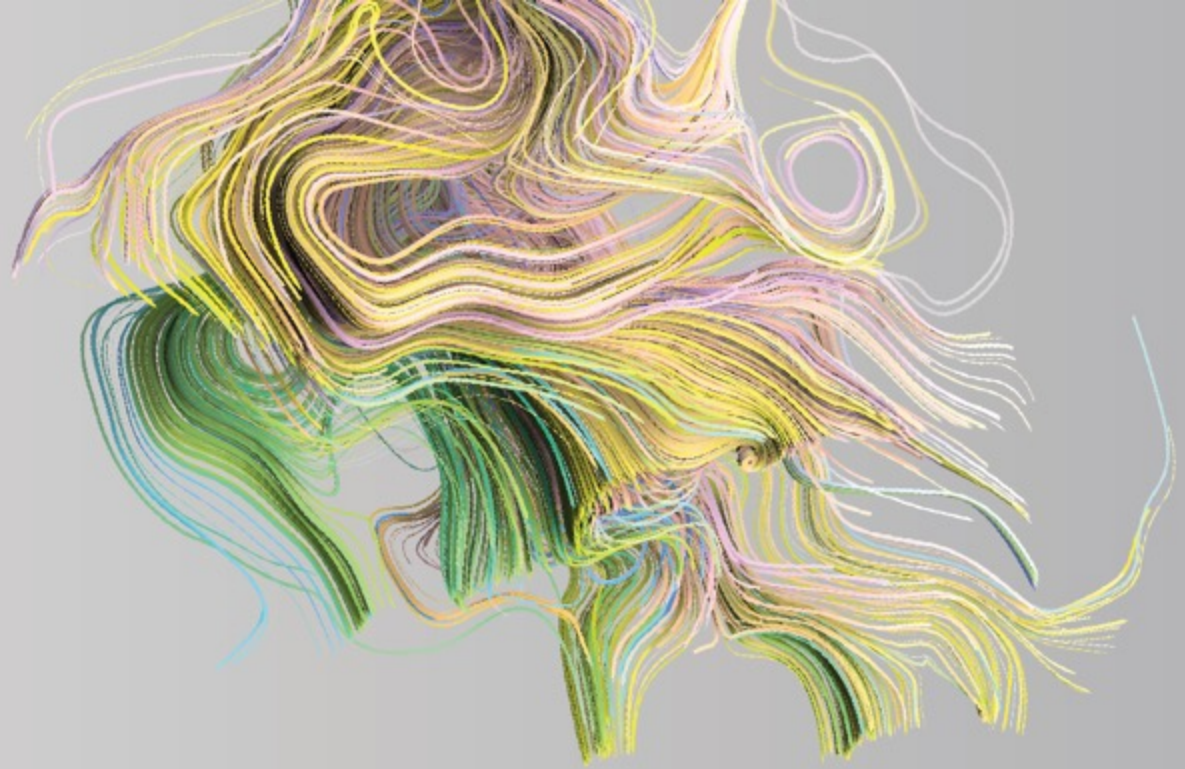
[Service Gateway forward proxy deployment script](#)

Prepare VM templates for VDI
Use the image setup tool to prepare VM templates for virtual desktops. [Learn more](#)
[Get VDI image setup tool](#)



安裝 XDR sensor(方法二)

請參照「[如何開啟Service Gateway forward proxy](#)」中5a~5h的步驟。

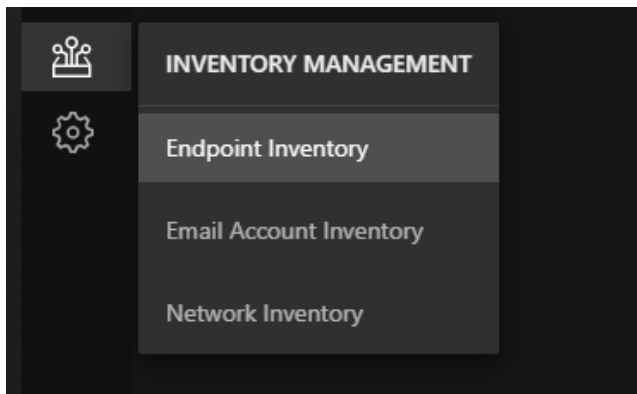


Enable XDR Sensor

對目標主機啟動XDR sensor

注意：如果已經啟用Endpoint Group，僅能透過Security Policies對特定群組啟動XDR sensor(如：方法二)，無法單獨指定單一目標啟動。

登入Vision One > 切換到Endpoint Inventory



對目標主機啟動XDR sensor

方法一：在EI app(Endpoint Inventory)清單中勾選，並啟用。

The screenshot displays the Trend Micro Vision One™ Endpoint Inventory interface. On the left, the 'Endpoint List' tab is active, showing a table of endpoints. Two endpoints are selected, indicated by blue checkmarks in the selection column. A red box highlights the 'Enable' button above the table. A red arrow points from this button to the 'Enable XDR Sensor' dialog box on the right. The dialog box shows the details of the two selected endpoints, including their names and operating systems (Windows 10). At the bottom of the dialog, a red box highlights the 'Enable Now (2)' button, with another red arrow pointing to it from the 'Enable' button in the main interface.

Trend Micro Vision One™ Endpoint Inventory

Endpoint List Agent Installer

All 154 No filter

Enable Remove × 2 selected

Endpoint name	IP address
[icon]	192.
[x] [icon]	192.
[x] [icon]	192.
[icon] yWu	192.
[icon]	192.

Enable XDR Sensor

After enabling XDR capabilities on the following supported endpoints, the endpoints automatically start sending activity data to Trend Micro for state-of-the-art threat detection and alerting.

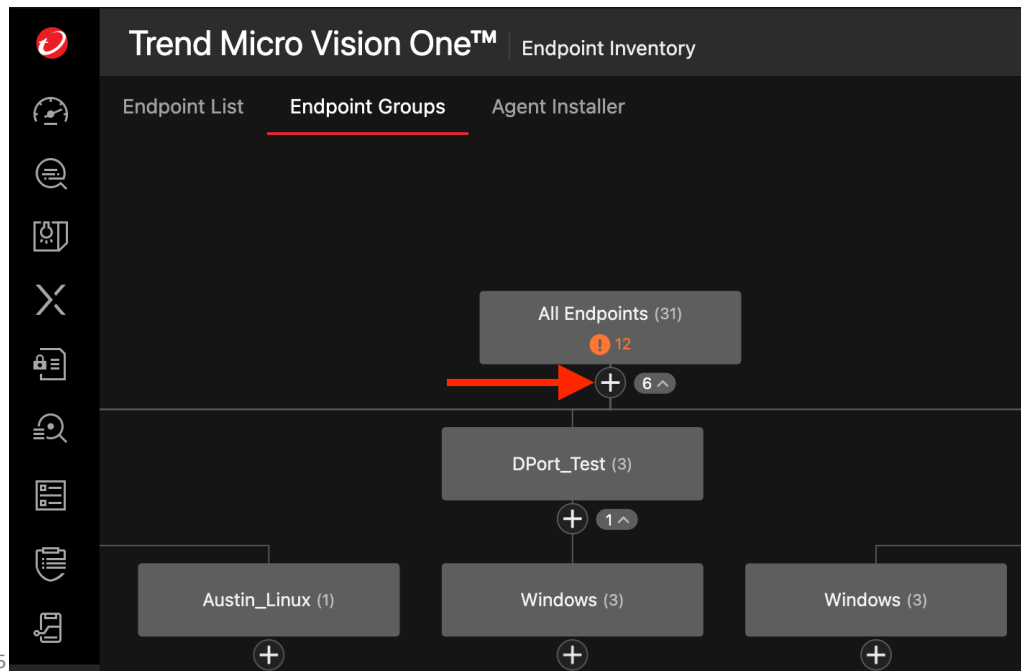
Endpoint name	Operating system
L	Windows 10
I	Windows 10

Enable Now (2) Cancel

對目標主機啟動XDR sensor

方法二：運用分組概念，對特定群組自動啟用XDR Sensor。

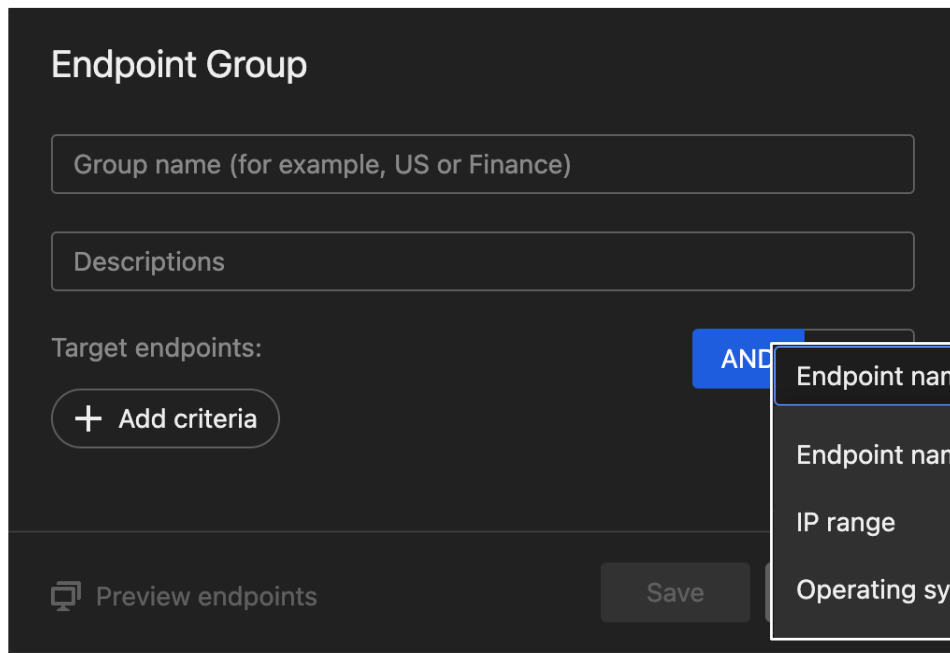
在Endpoint Groups中，點選「加號」。



對目標主機啟動XDR sensor

方法二：運用分組概念，對特定群組自動啟用XDR Sensor。

設定群組資訊，並選擇過濾端點的條件：



Endpoint Group

Group name (for example, US or Finance)

Descriptions

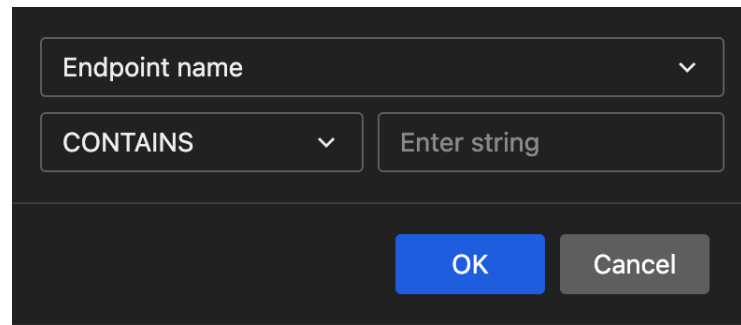
Target endpoints:

+ Add criteria

AND

Preview endpoints

Save



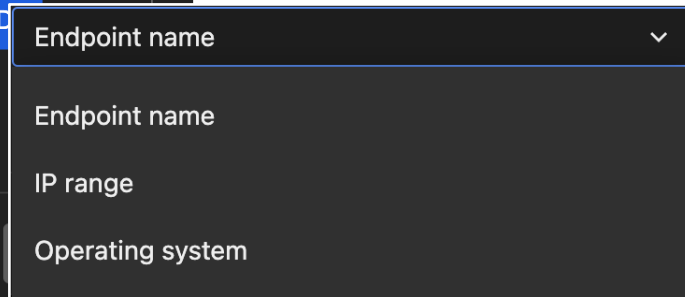
Endpoint name

CONTAINS

Enter string

OK

Cancel

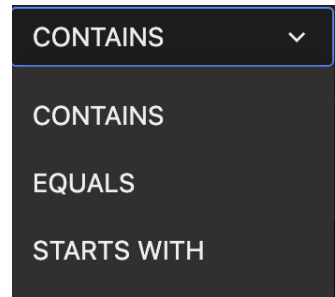


Endpoint name

Endpoint name

IP range

Operating system



CONTAINS

CONTAINS

EQUALS

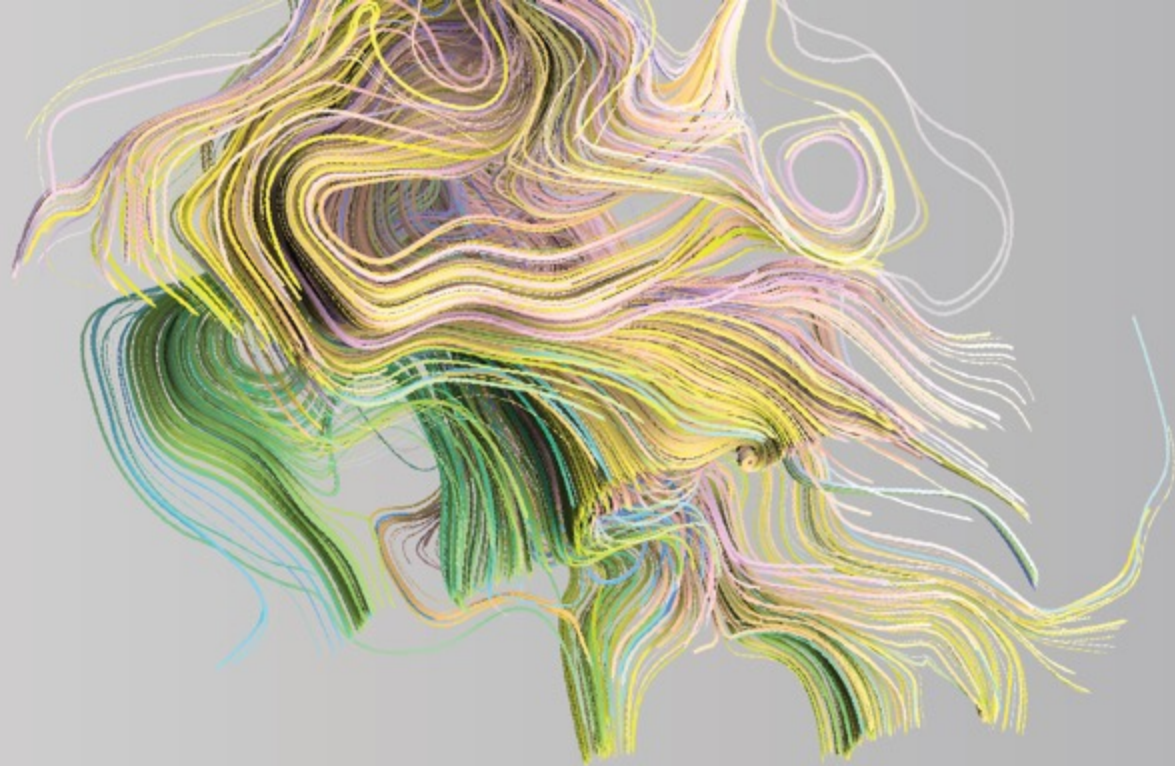
STARTS WITH

對目標主機啟動XDR sensor

方法二：運用分組概念，對特定群組自動啟用XDR Sensor。

切換到Security Policies > Endpoint，選擇特定群組，即可設定是否啟用功能。

The screenshot displays the Trend Micro console interface. On the left, a sidebar menu shows 'SECURITY POLICIES' and 'Endpoint'. The main area is titled 'Endpoint Security Policies' and shows a hierarchy: 'Nathan (3)' is the parent group, and 'Windows (0)' is a child group highlighted with a red box. A red arrow points from this 'Windows (0)' group to the 'XDR Endpoint Sensor' toggle in the 'Security Agent Settings' panel on the right. In this panel, the 'XDR Endpoint Sensor' toggle is turned on (blue), and the 'Vulnerability Detection' toggle is also turned on. The 'XDR Endpoint Sensor' section includes the text: 'Once enabled, the endpoints automatically start sending activity data to Trend Micro for state-of-the-art threat detection and alerting.'



補充資訊



補充資訊

關於更多Vision One參考資訊, 請查看[V1 KB main page](#)