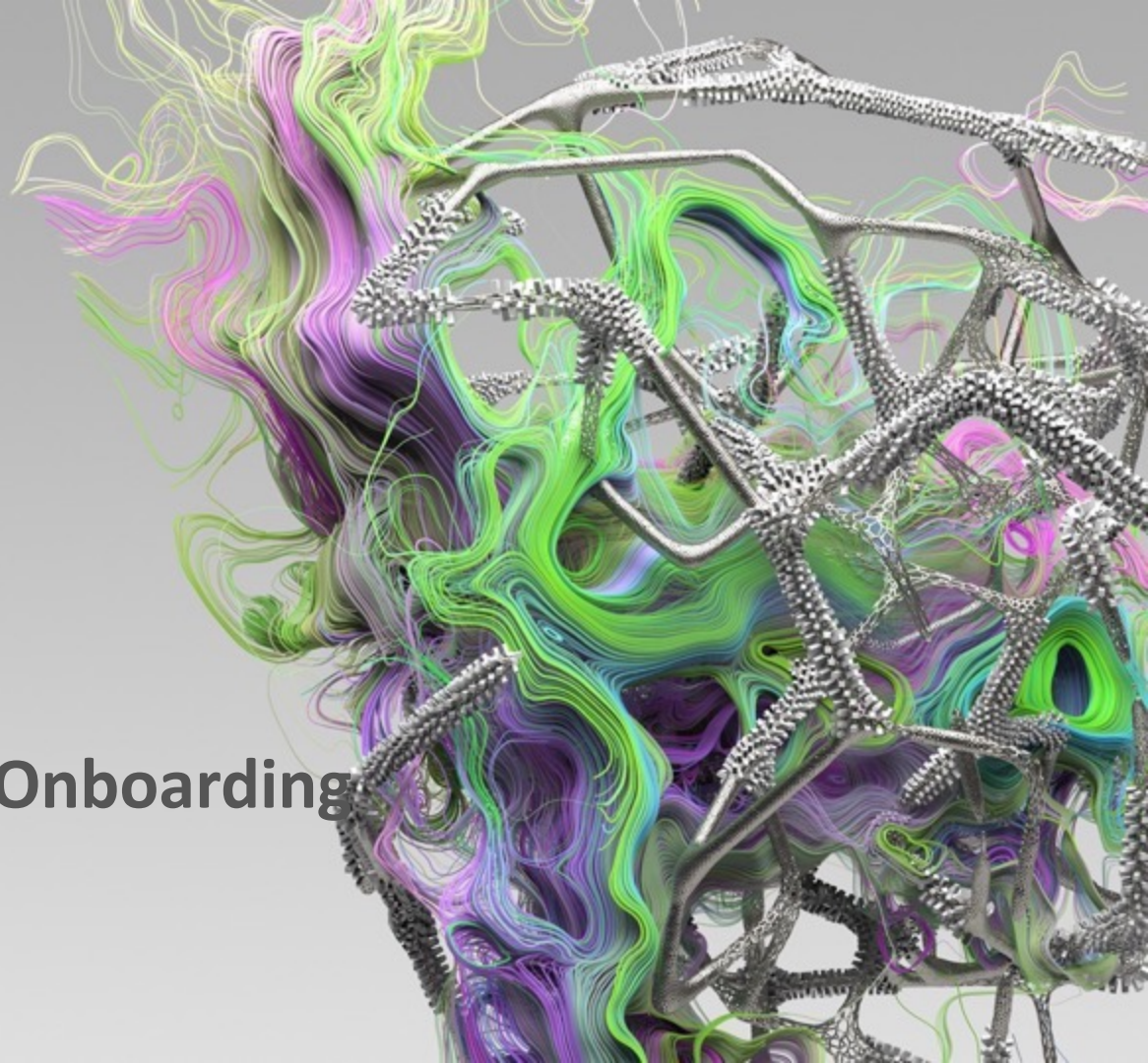


Vision One™

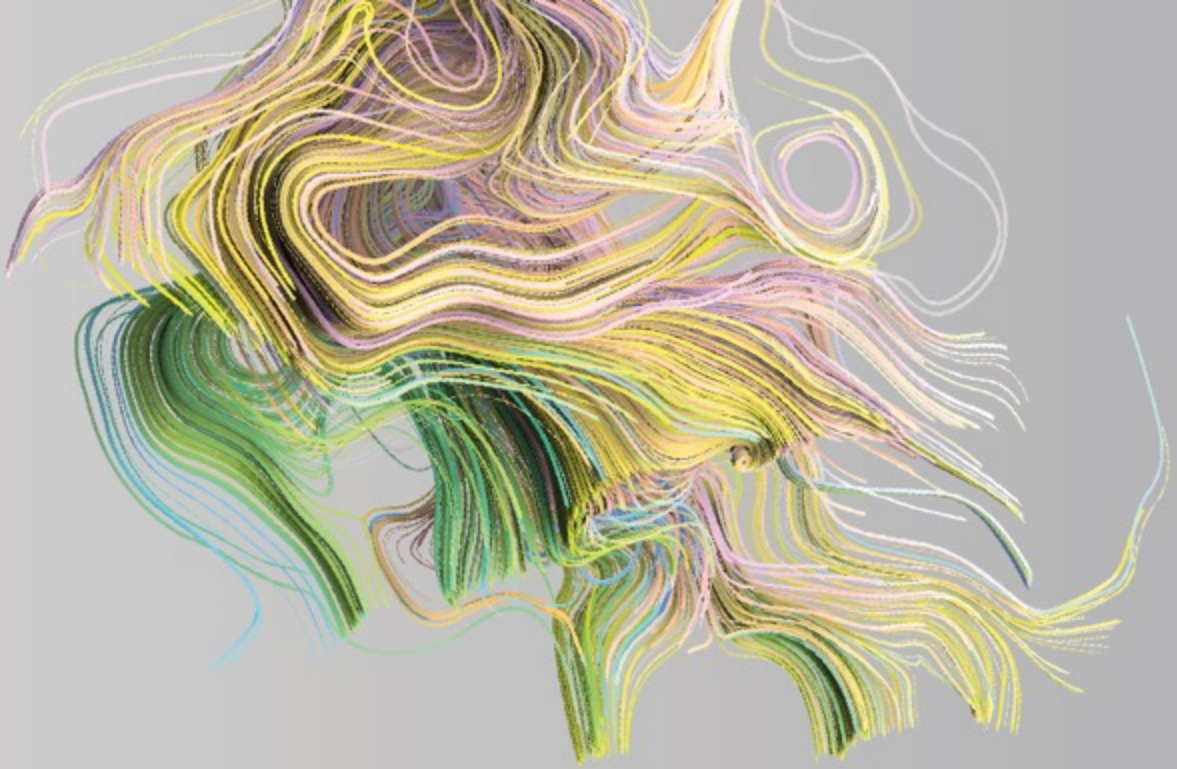
Apex One (on-prem) Onboarding

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

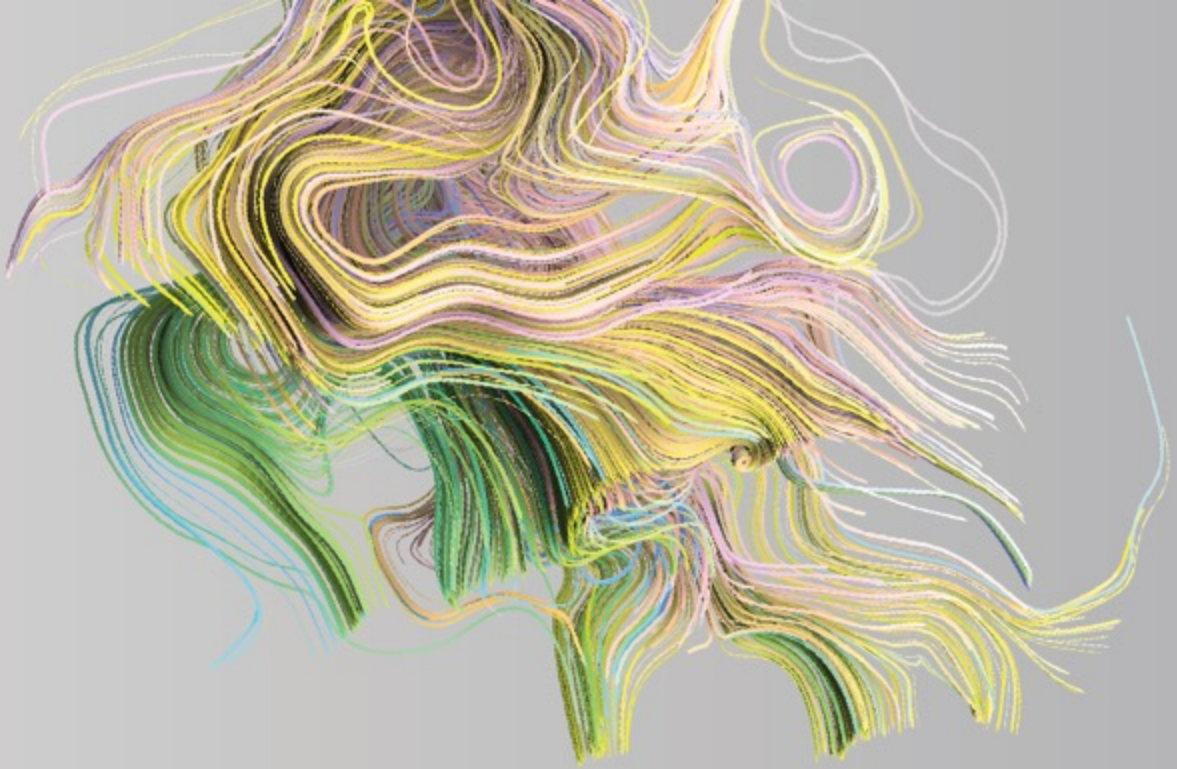
Onboarding前置準備(一)

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)

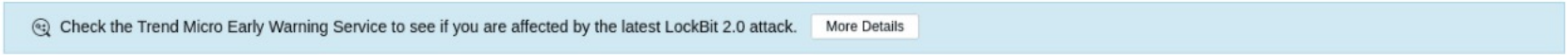
5. 如果網路環境有嚴格限制內對外通訊位址，請確認以下位址沒有被阻擋:
   http://crl.entrust.net/
   http://ocsp.entrust.net/
   http://aia.entrust.net/
   http://crl.affirmtrust.com/
   http://ocsp.affirmtrust.com/
   http://aia.affirmtrust.com/
   http://ctldl.windowsupdate.com/
6. 在Apex One server上，以系統管理員身份執行cmd，並執行以下指令:
   cd C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV
   Svrsvcsetup.exe -checkOnboardingAPI
   Svrsvcsetup.exe -PrepareXBCpatch -AcceptXBCPII yes



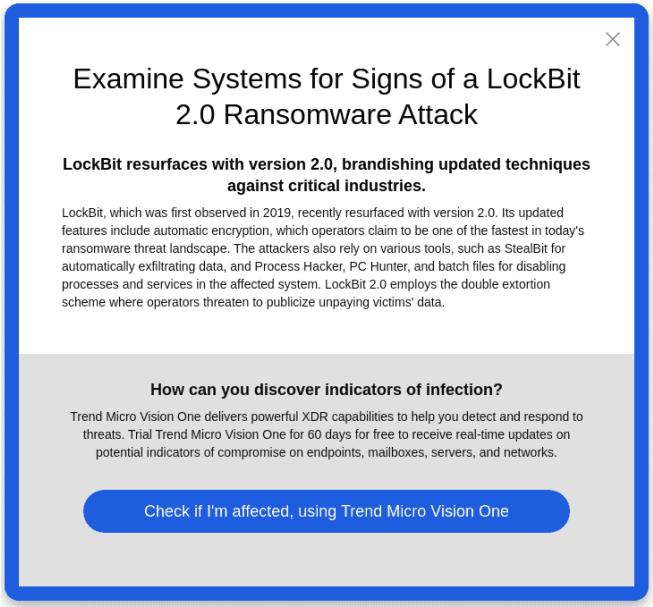
Registering Vision One

Apex One Onboarding 程序

登入Apex One web console後，看到藍色橫幅標題

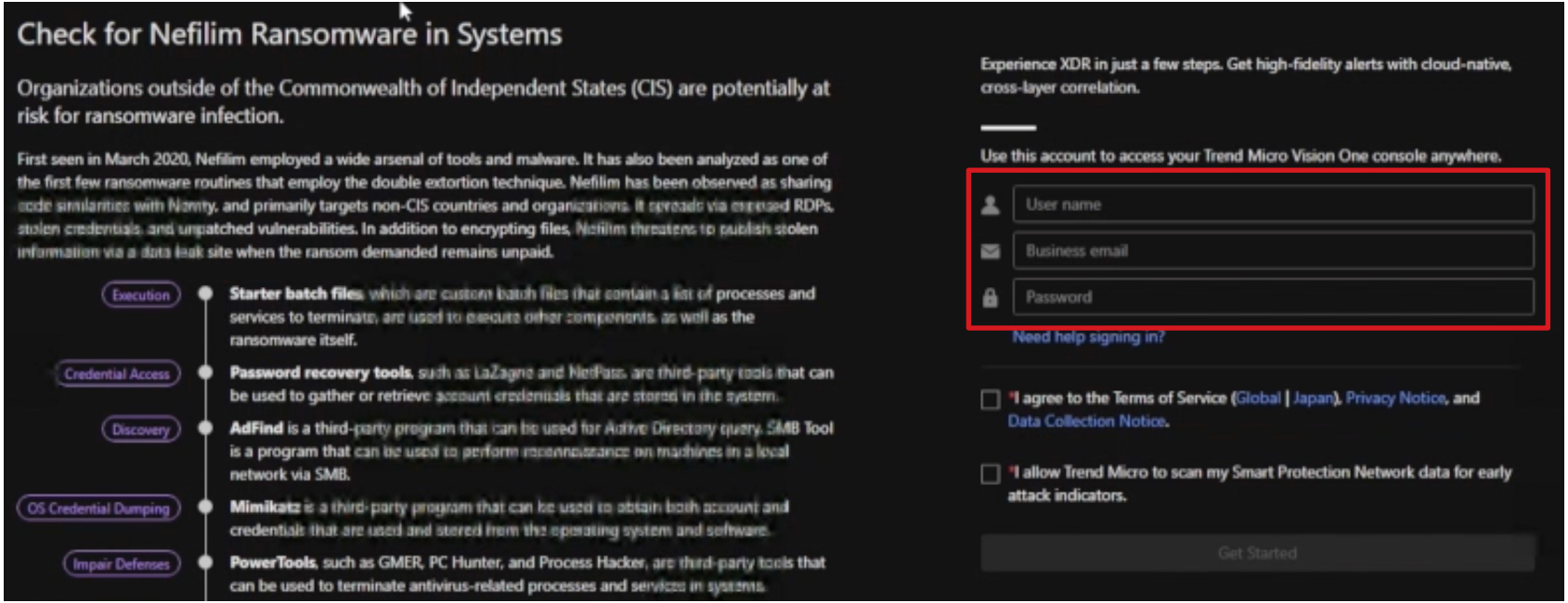


或是看到promotion畫面點選其中按鈕，即可進行onboarding程序



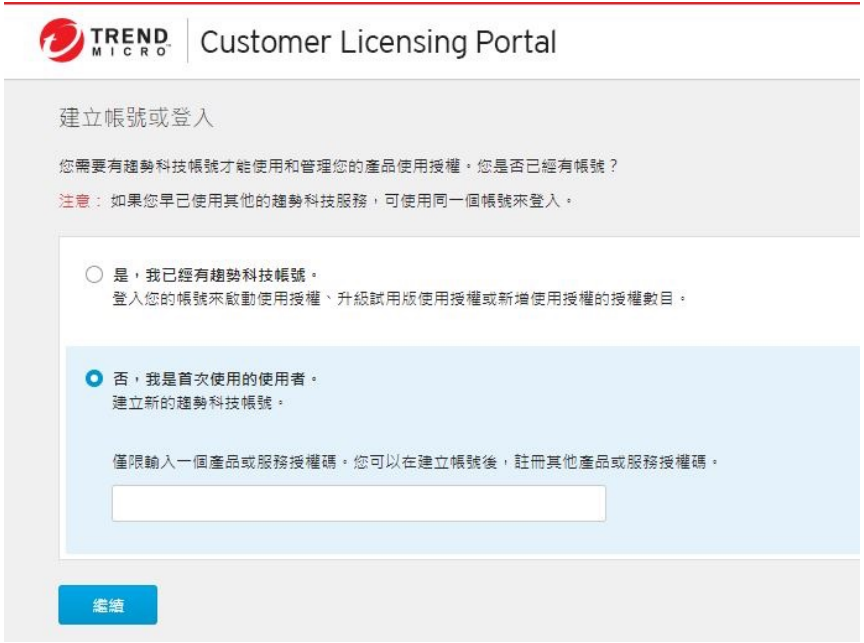
Apex One Onboarding 程序

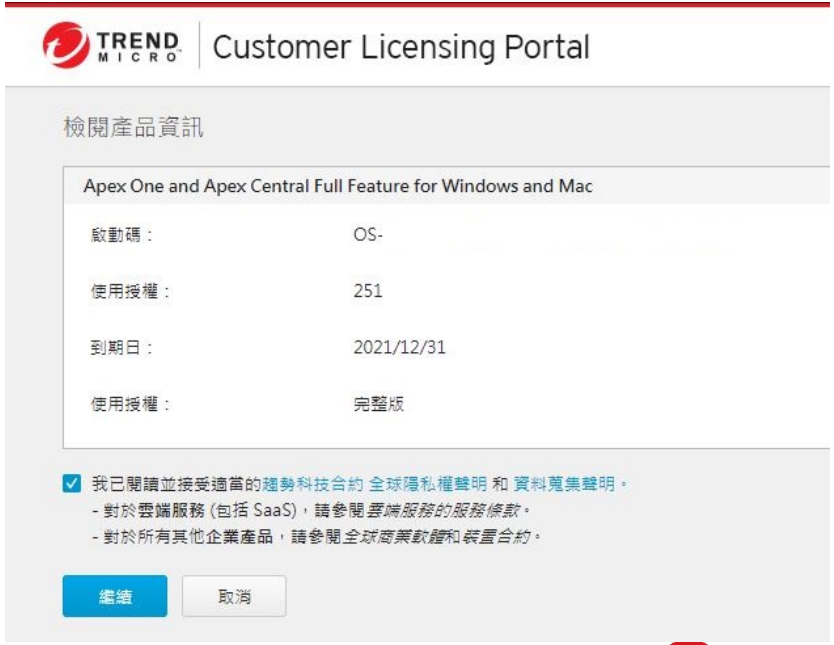
請輸入CLP(Customer Licensing Portal)帳號,
如果還沒有CLP帳號，請繼續參考以下操作步驟。



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

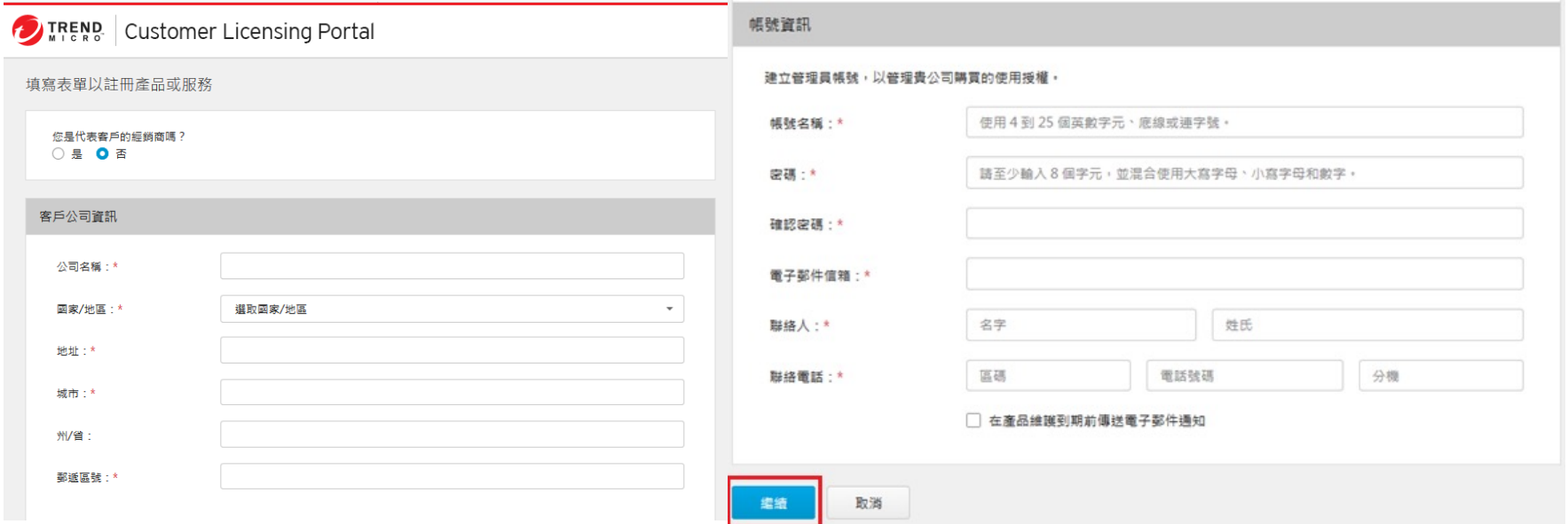




① 註冊CLP帳號 – 填寫基本資料

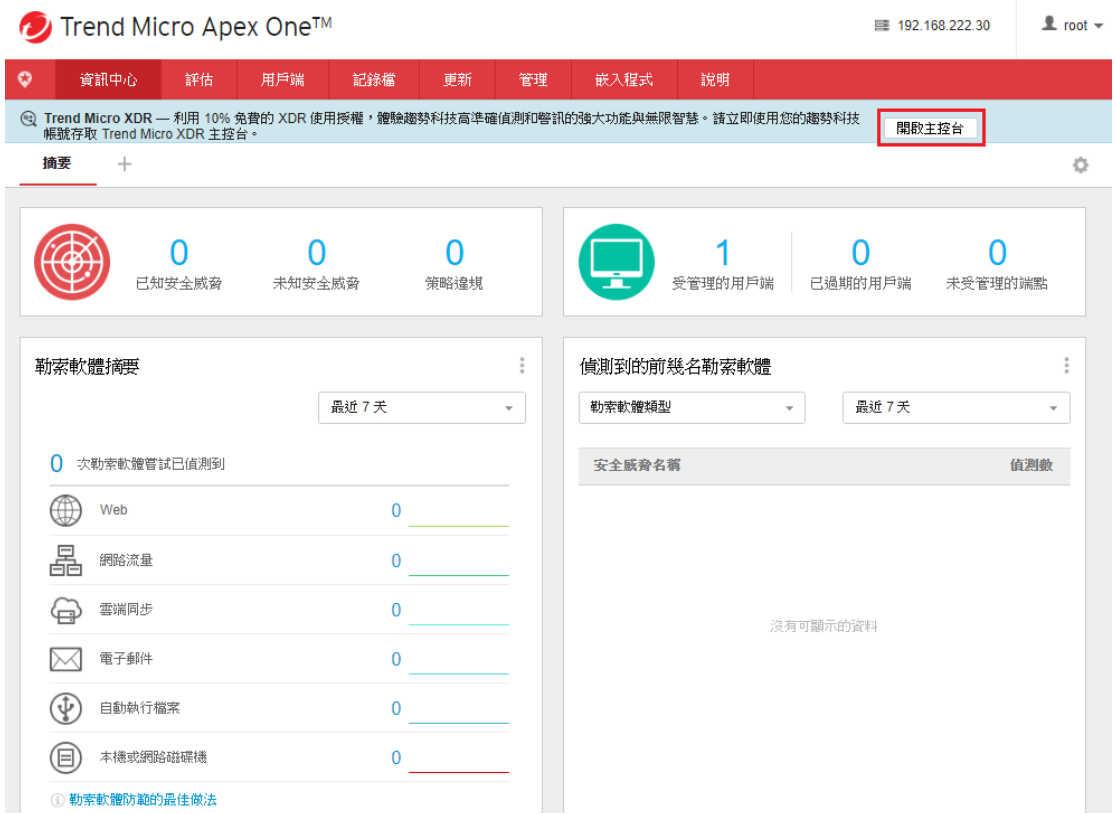
注意：一個CLP帳號視為一個公司行號，不建議多個管理者各自建立CLP帳號，也不要將公司購買的產品授權分別註冊到不同CLP帳號下。

填寫公司資訊與建立登入雲端服務帳號資訊



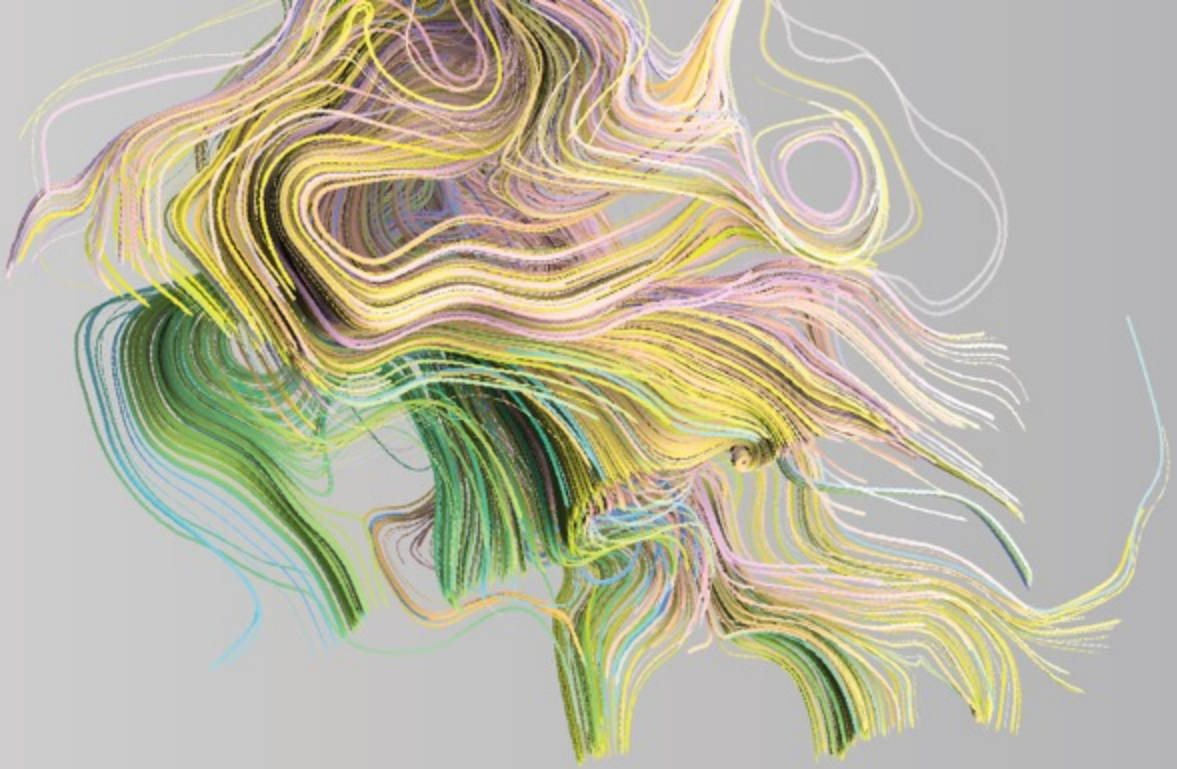
② 透過 CLP 開啟Vision One主控台

② 透過 Apex One 開啟Vision One主控台



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

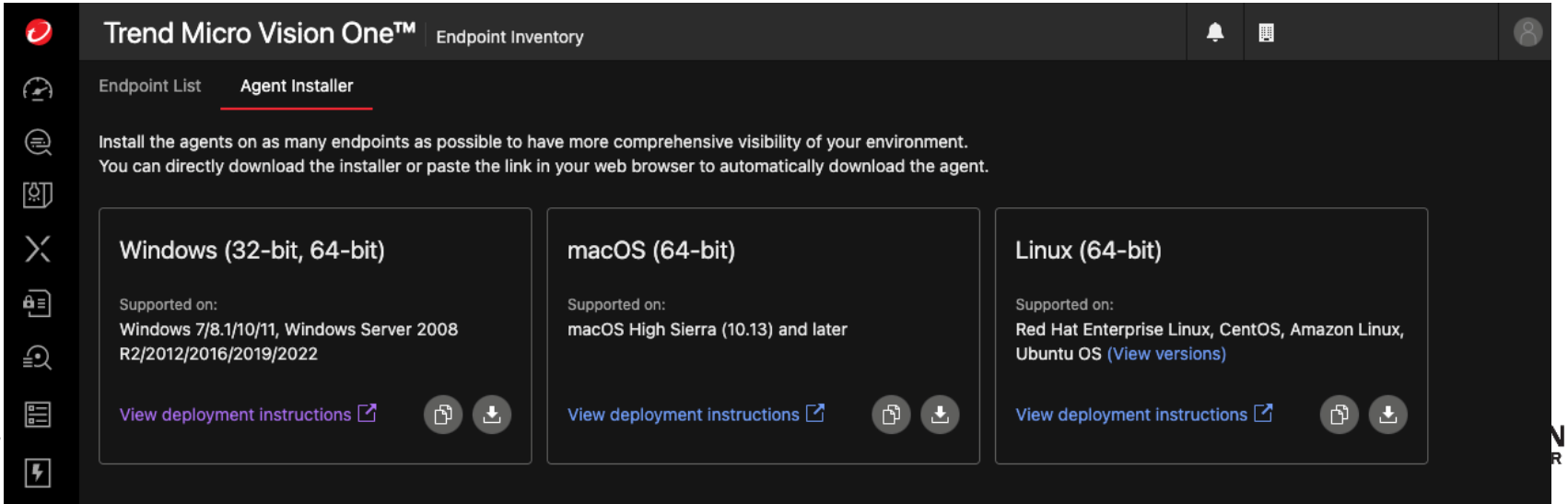
- **Linux**
  - Red Hat Enterprise Linux 6/7/8 (64-bit)
  - Amazon Linux (64-bit)
  - Amazon Linux 2 (64-bit)
  - CentOS Linux 6/7/8 (64-bit)
  - Ubuntu 16/18/20
  - ***建議規格: 記憶體 : 5 GB / 硬碟可用空間: 1 GB***

- **Mac**
  - macOS High Sierra (10.13) 以上
  - ***硬碟可用空間: 3 GB***

安裝 XDR sensor（方法一）

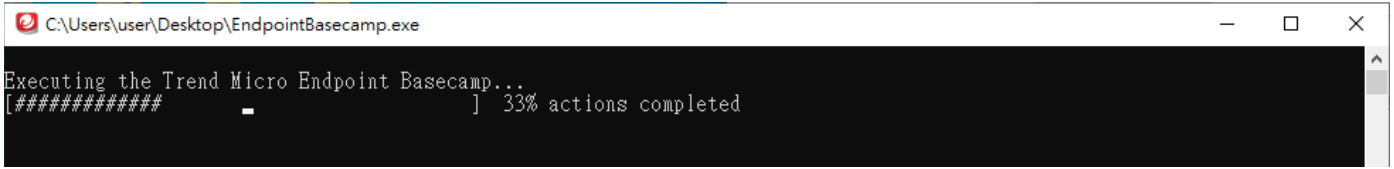
注意：已經完成onboarding的Apex One，其所管理的agent都已經出現在Endpoint Inventory，不需要再次執行XDR sensor安裝步驟，可直接進行啟用程序。

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

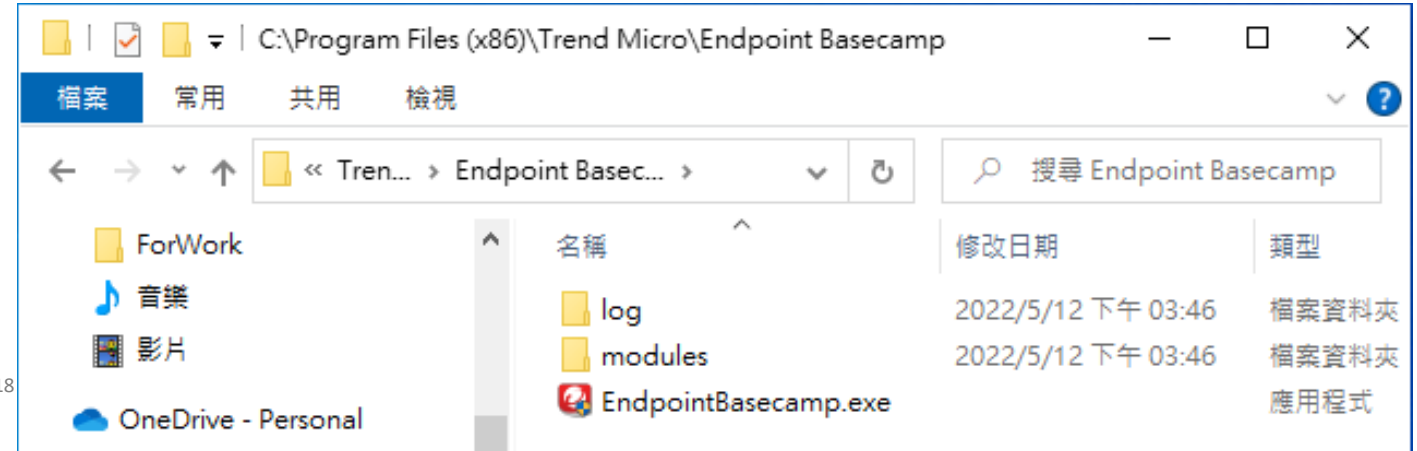


安裝 XDR sensor（方法一）

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：

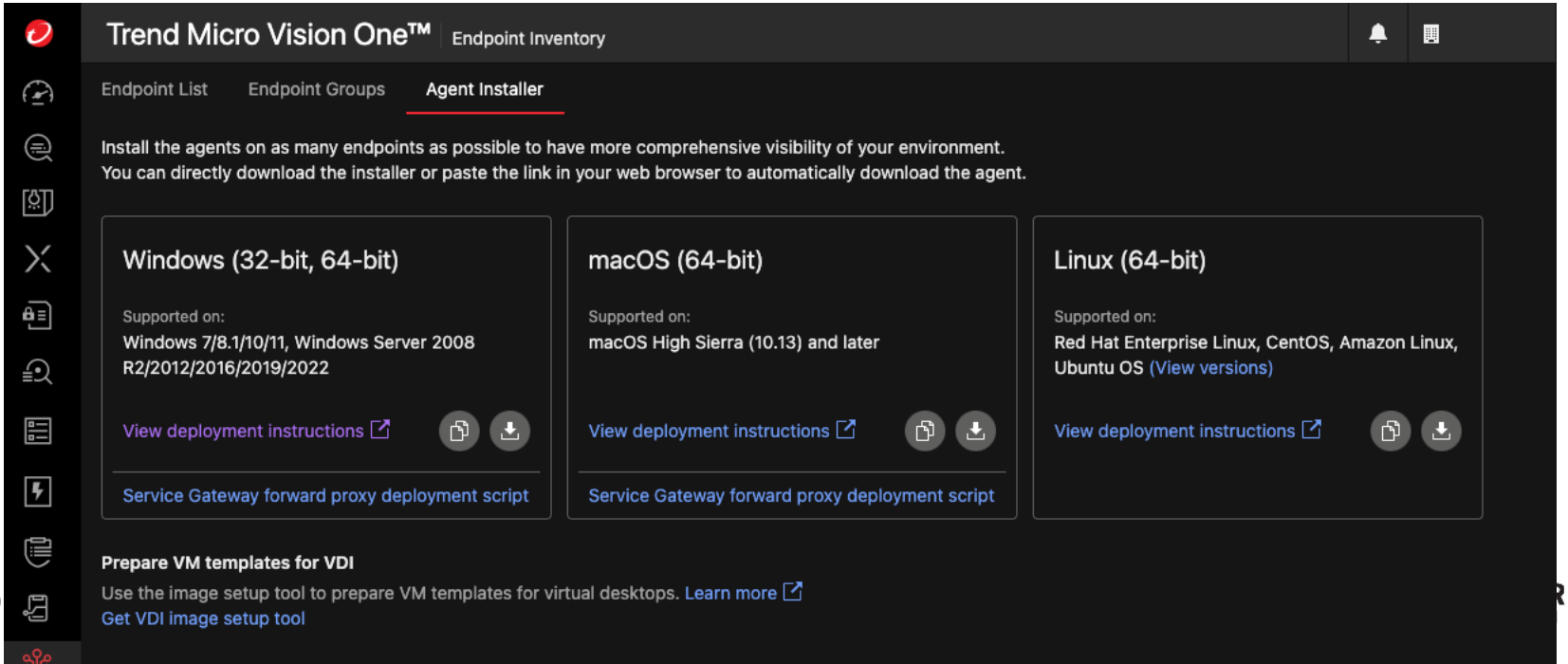
1. 需要先建立Service Gateway，請參考

   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

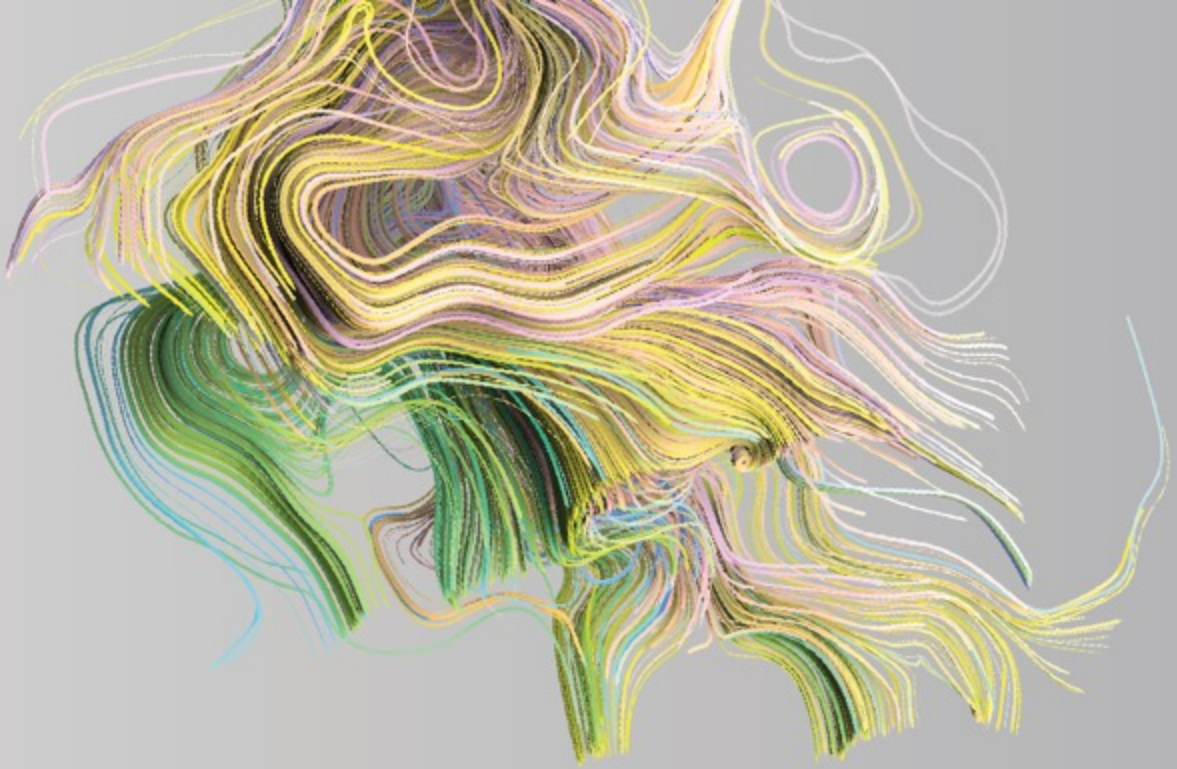
安裝 XDR sensor（方法二）

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 depolyment script



安裝 XDR sensor（方法二）

請參照「如何開啟Service Gateway forward proxy」中5a~5h的步驟。

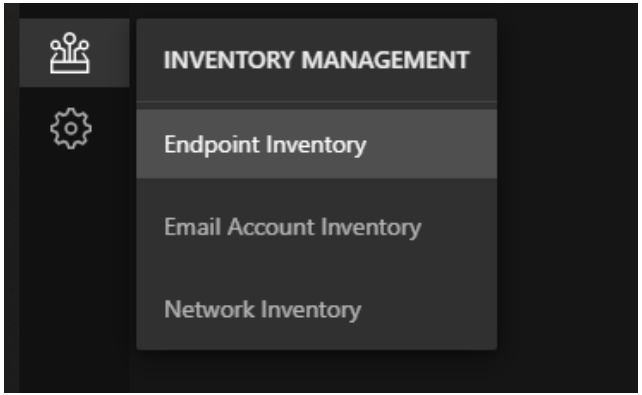


Enable XDR Sensor

對目標主機啟動XDR sensor

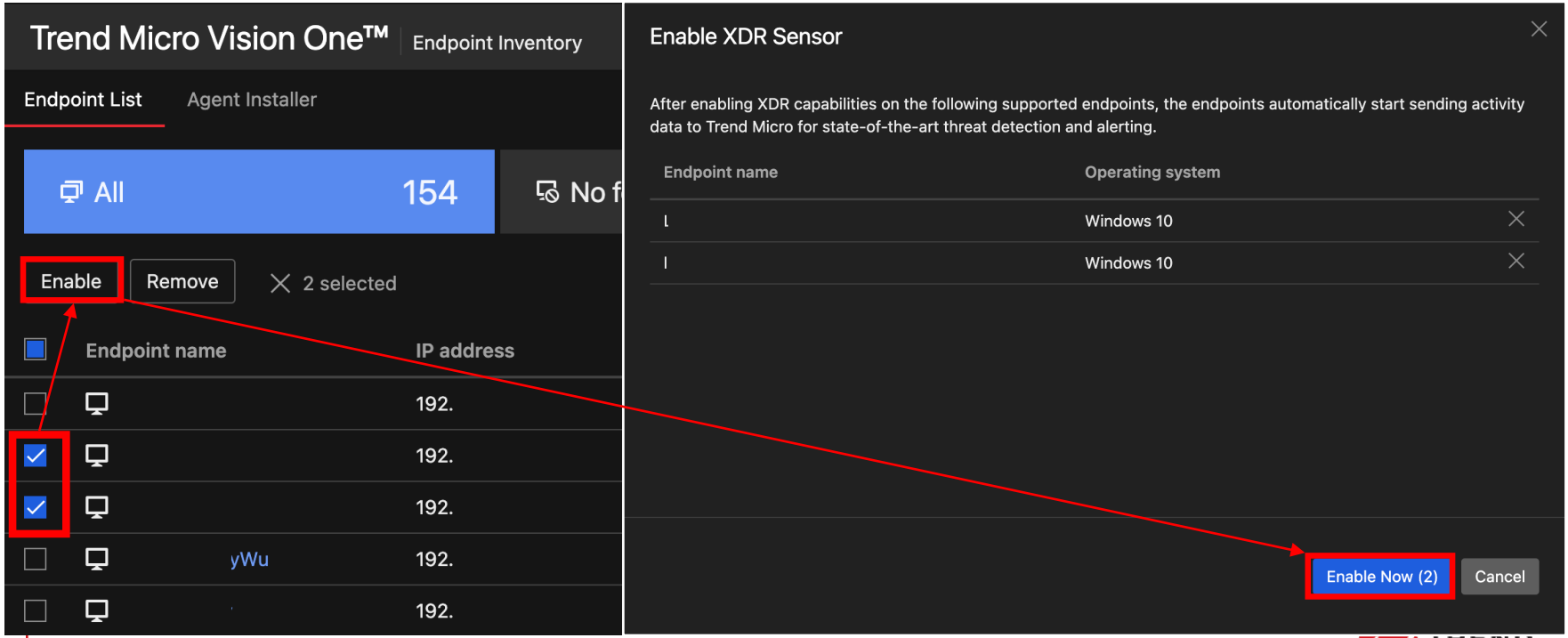
注意：如果已經啟用Endpoint Group，僅能透過Security Policies對特定群組啟動XDR sensor（如：方法二），無法單獨指定單一目標啟動。

登入Vision One > 切換到Endpoint Inventory



對目標主機啟動XDR sensor

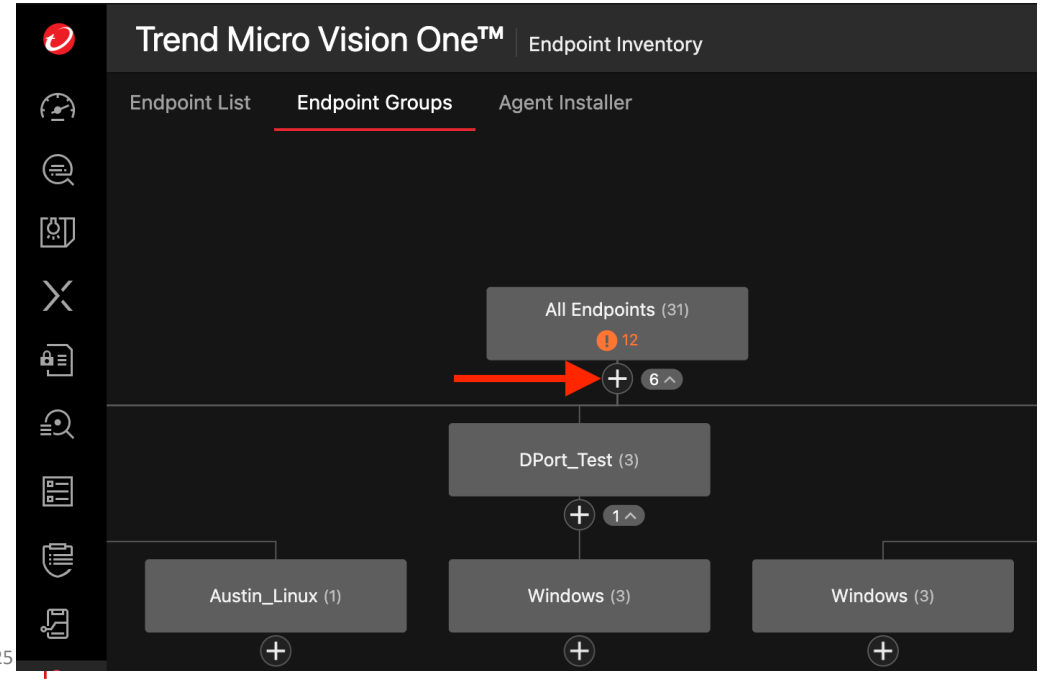
方法一：在EI app(Endpoint Inventory)清單中勾選，並啟用。



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。

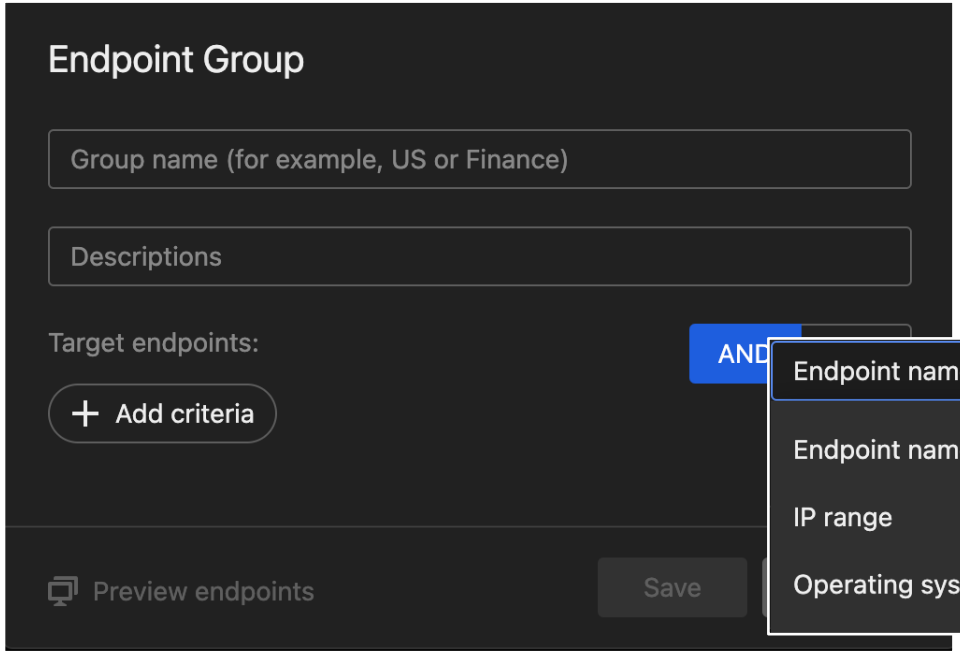
在Endpoint Groups中，點選「加號」。

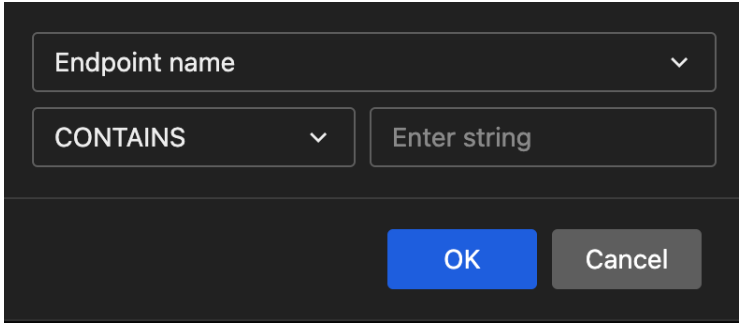


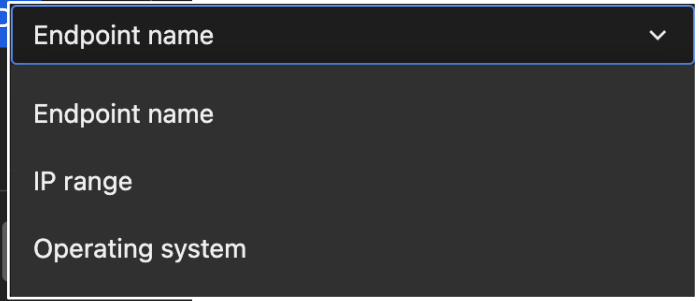
對目標主機啟動XDR sensor

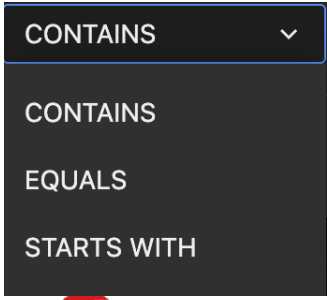
方法二：運用分組概念，對特定群組自動啟用XDR Sensor。

設定群組資訊，並選擇過濾端點的條件：





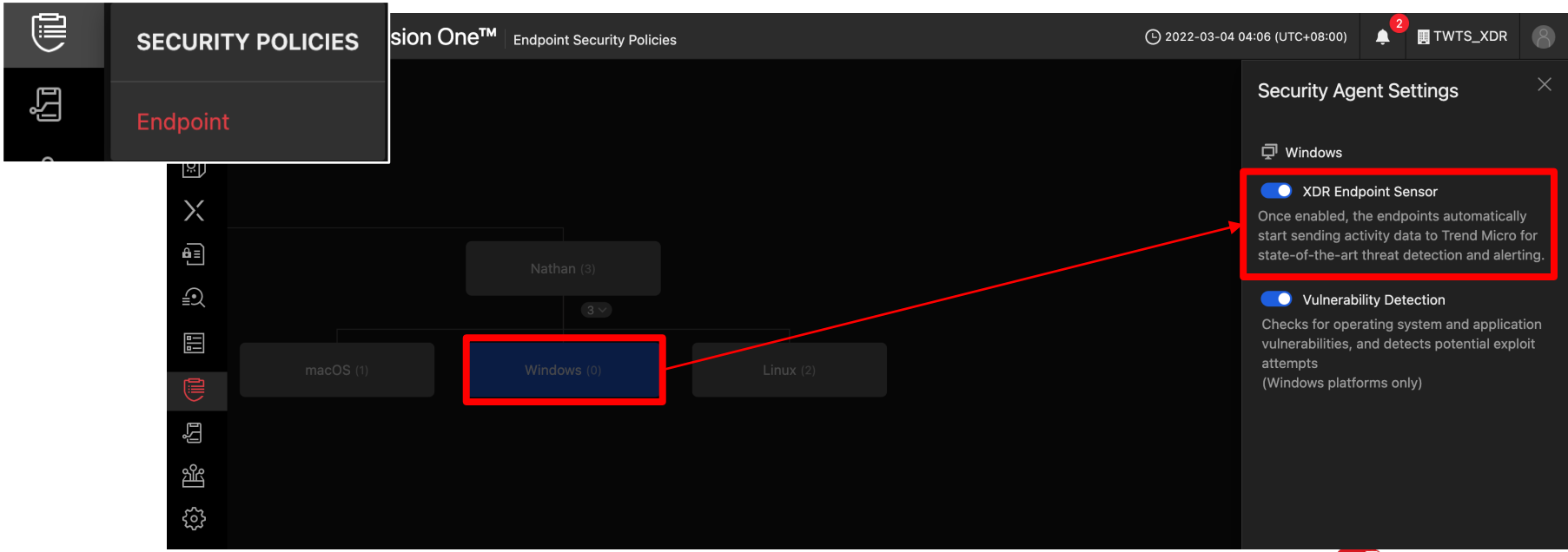


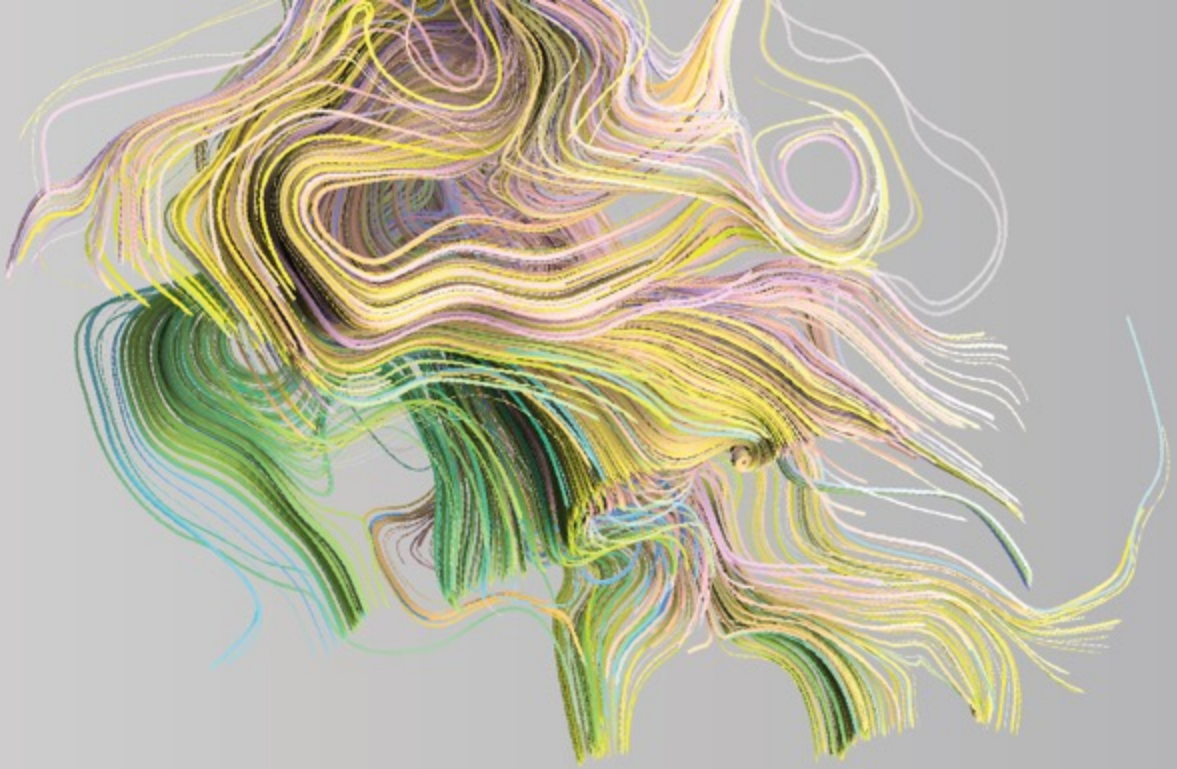


對目標主機啟動XDR sensor

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。





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