

Trend Micro Security Assessment Service 試用申請

申請 URL

<https://resources.trendmicro.com/security-assessment-service-us.html>

填入相關申請資訊

Register to select your preferred assessment from within the Trend Micro Vision One console.

* First Name:

* Last Name:

* Email Address:

* Phone Number:

* Company:

* Number of Employees:

* Country:

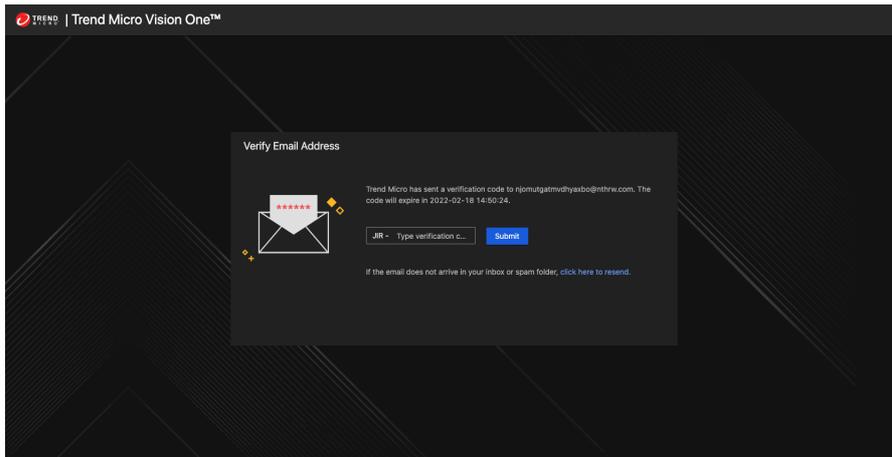
* Data center location:

* I agree to the Terms of Service (Global | Japan), Privacy Notice, and Data Collection Notice.

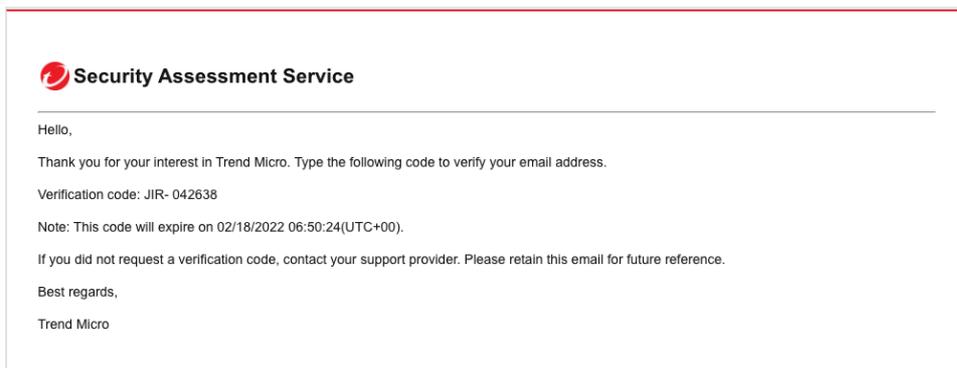
START

Data Center Location 台灣客戶建議使用 Singapore

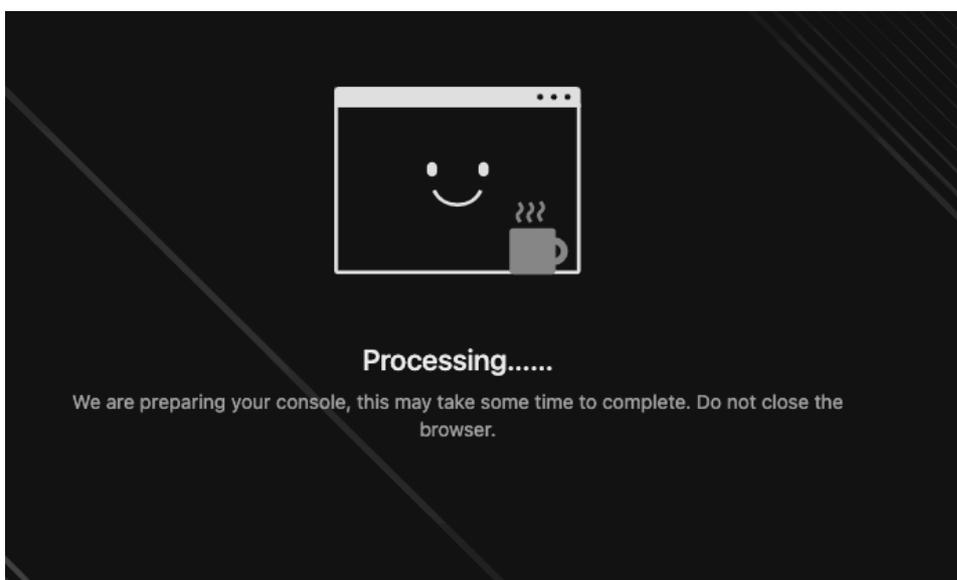
完成資料填入後點擊“Start”，系統會出現要求輸入驗證碼



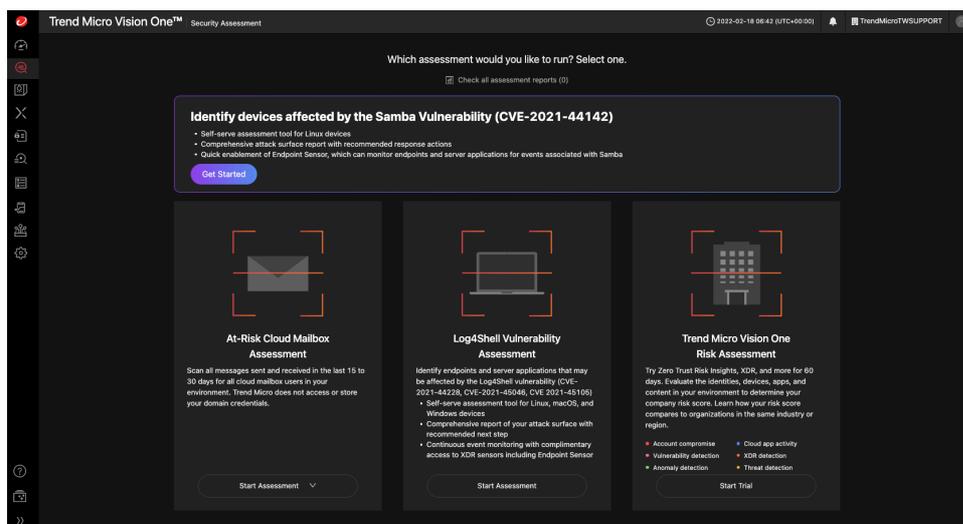
請確認您的信箱有收到來自趨勢科技發出的驗證碼信件，並且輸入信件中提供的驗證碼。請注意，驗證碼有時效性，若超過時效，請點擊上述步驟畫面中“Click to resend”重新寄送驗證碼。



驗證碼輸入完畢且正確，系統將會開始建立全新趨勢科技 VisionOne 平台。



等待建立完成後，您將會自動登入到 VisionOne 平台



同時，您也會收到一封註冊成功的信件

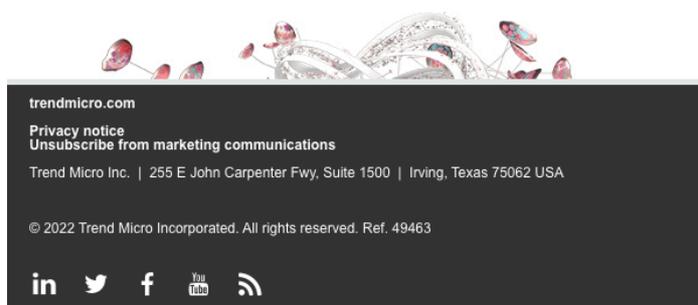


Thank you for registering for the Trend Micro Security Assessment Service. Using the Trend Micro Vision One™ platform, this complimentary service offers insight into your attack surface, identifies potential threats in your environment and provides a detailed, downloadable report with recommended response actions.

[Start assessment](#)

You have the option to extend your assessment to trial XDR sensors for endpoint, server, email, and network to continuously monitor, detect and respond to attacks for free for 60-days after sign-up.

Thank you,
The Trend Micro Team



請點擊信件中“Start assessment”的按鈕進行密碼重新設定步驟
點擊後會出現 Reset password 的畫面，請點擊“Send verification code”

Reset password

Email address: njomutgatmvdhyaxbo@nthrw.com

Verification code:

New password ⓘ

Confirm password

Submit

Reset password

Email address: njomutgatmvdhyaxbo@nthrw.com

Verification code:

If the email does not arrive in your inbox or spam folder, [click here](#) to resend (173s).

New password ⓘ

Confirm password

Submit



Hello,

Thank you for your interest in Trend Micro. Type the following code to verify your email address.

Verification code: 8LJ-542381

Note: This code will expire on 2022/02/18 06:58:53 UTC+0.

If you did not request a verification code, contact your support provider. Please retain this email for future reference.

Best regards,
Trend Micro

Reset password

Email address: njomutgatmvdhyaxbo@nthrw.com

Verification code: 8LJ - 542381
If the email does not arrive in your inbox or spam folder, [click here to resend \(119s\)](#).

New password ⓘ

Confirm password

[Submit](#)

Submit 後返回登入頁面，登入帳號請填入申請的 Email Address

Extended detection and response

Beyond the single vector
Connecting email, endpoints, servers, cloud workloads, and networks provides a broader perspective and a better context to hunt, detect, and contain threats.

Correlated detection
Powerful security analytics correlate data across the customer environment and Trend Micro's global threat intelligence to deliver fewer, higher-confidence alerts, leading to better, earlier detection.

Integrated investigation and response
One place for investigation simplifies the steps to achieving an attack-centric view of an entire chain of events across security layers with the ability to take response actions from a single place.

Sign In

Remember me

[Continue](#)

[Need help signing in?](#)
[Don't have an account? Create one](#)

輸入 Reset 後的密碼登入，登入後系統會提醒是否啟用兩階段驗證功能。若不需要，可以點擊畫面中右下角“Skip for now, I accept the risks”

⚠ Security Alert

Due to the advanced capabilities of modern cybercriminals, password protection alone can no longer be trusted to protect internet accounts from unauthorized access. To adequately safeguard your Trend Micro Account, turn on two-factor authentication (2FA) immediately.



What is Two-factor Authentication (2FA)?
2FA lets you use your mobile device to confirm your identity when signing into your Trend Micro Account. This added layer of security prevents unauthorized access to your Trend Micro SaaS product consoles, even if your password is stolen.
[Learn more](#)

Why is this important?
If your account is compromised, criminal hackers could switch off all Trend Micro protections. They could then gain access to your personal data, business secrets, and even banking information. All your data could be stolen, held for ransom, or destroyed. Trend Micro highly recommends you enable 2FA immediately to safeguard your account.

[Continue to 2FA Settings](#)

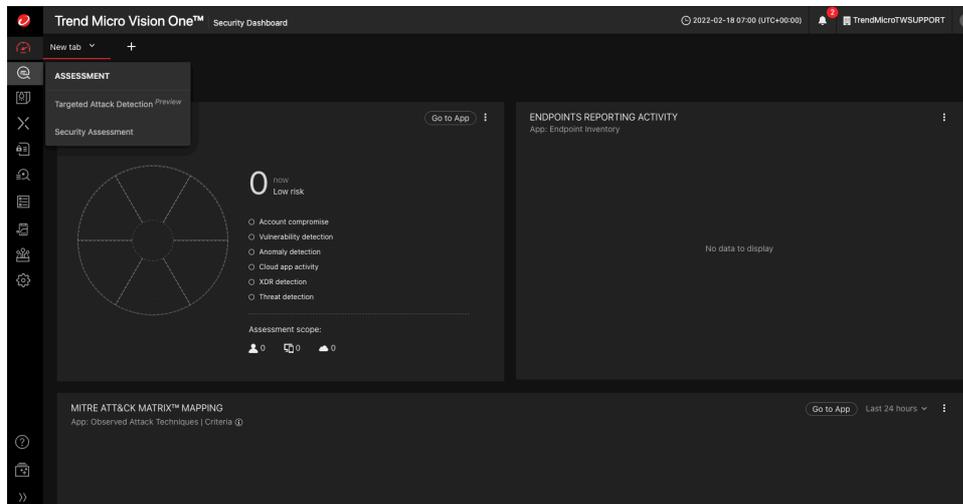
Do not show this message again

[Skip for now. I accept the risks](#)

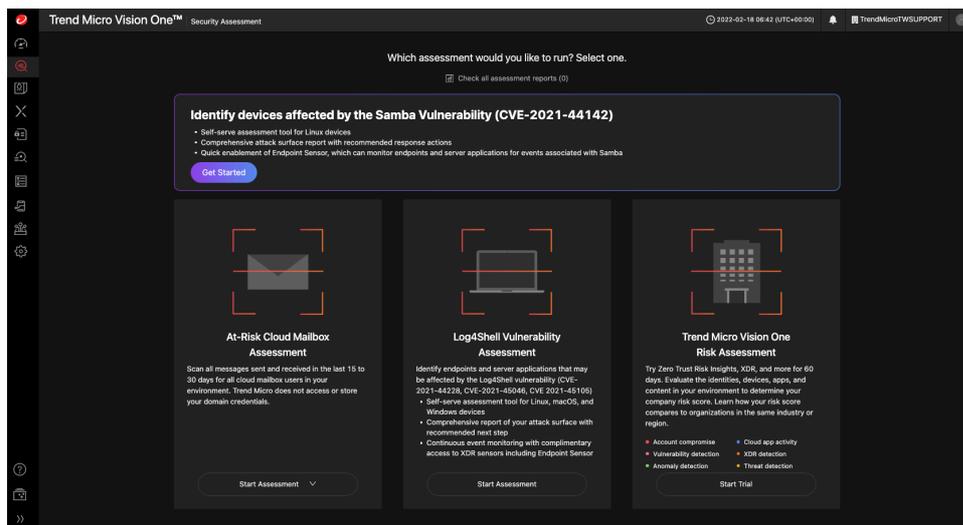
點擊左側功能 APP 此圖示



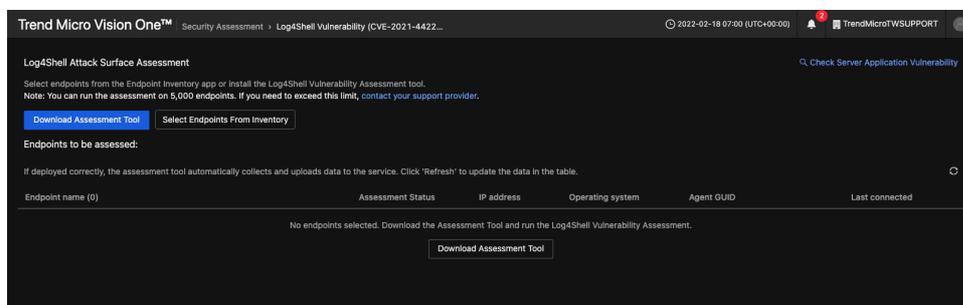
選擇”Security Assessment”開始進行檢測



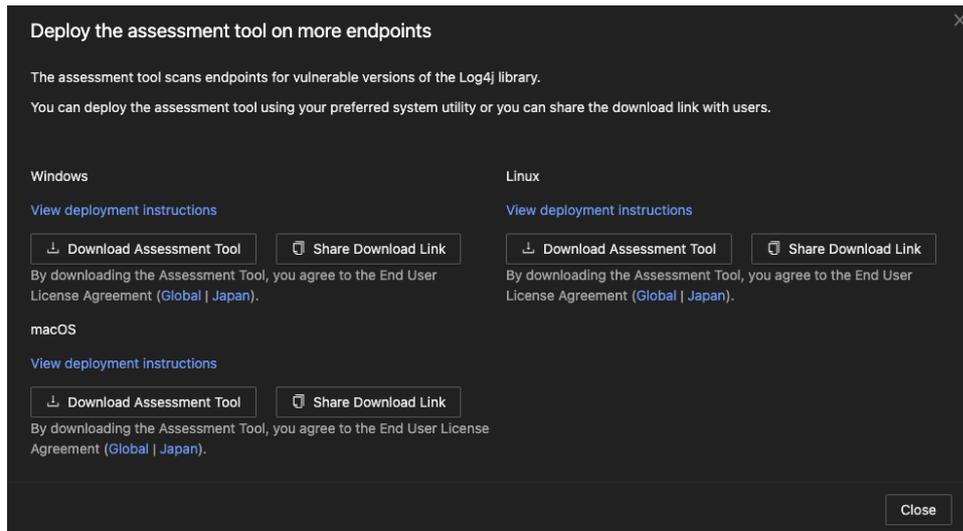
您可以依據您目前的需求進行檢測，以畫面中我們選擇”Log4Shell”弱點來進行檢測



選擇”Download Assessment Tool”



選擇需要檢測的作業系統平台來進行檢測



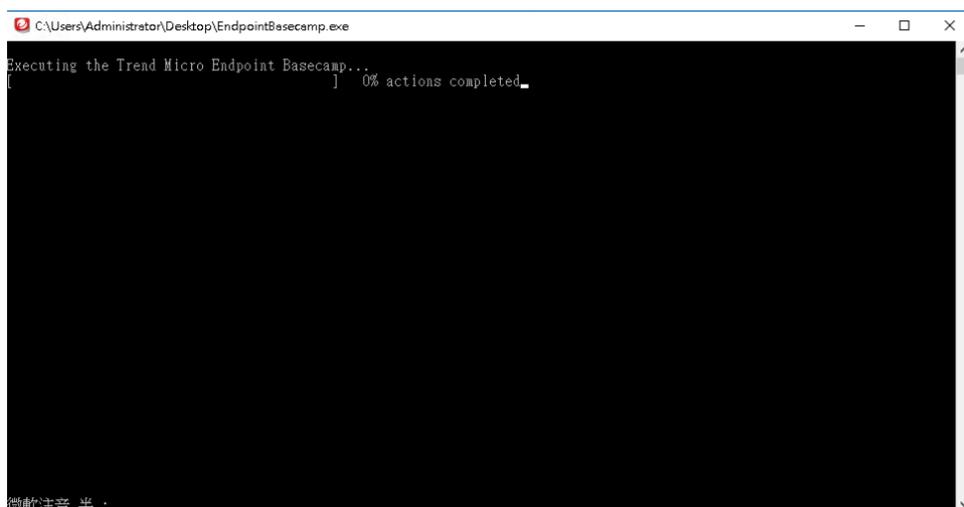
我們以 Windows 平台來舉例，您可以選擇下載 Assessment Tool 後分享安裝，或是分享下載連結給其他使用者下載安裝。

NOTE:請注意此工具僅能在貴公司環境中使用，若其他非貴公司環境中使用相同的檢測工具，會造成資料不正確的情況。

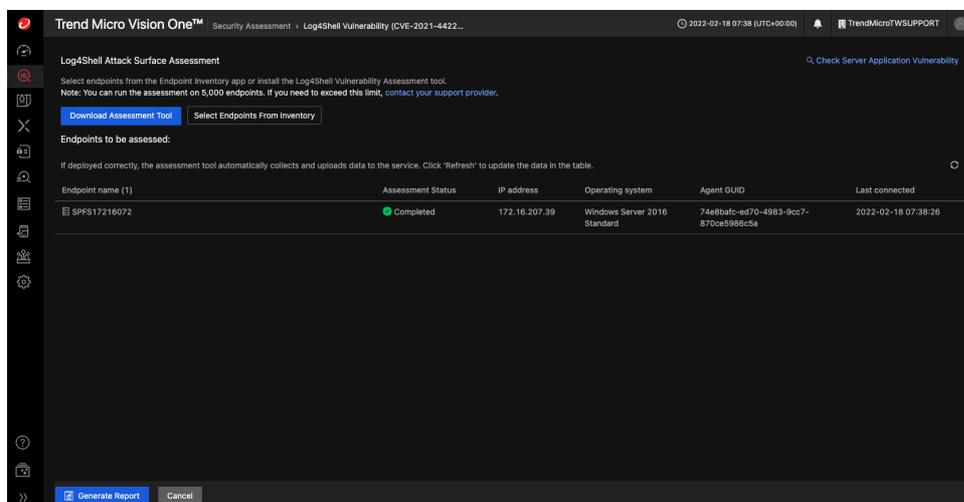
工具下載後，建議請使用系統管理者權限執行“EndpointBasecamp.exe”



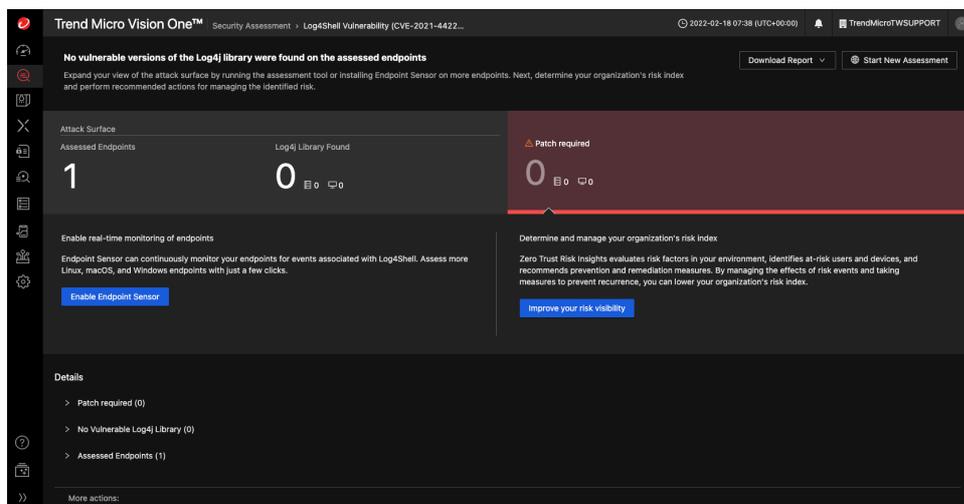
執行後會出現檢測視窗，請勿關閉該視窗。執行完畢後該視窗會自行關閉。



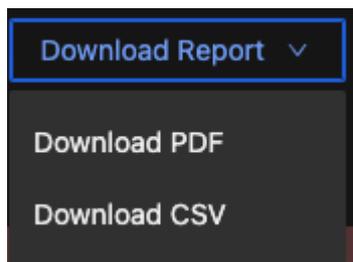
檢測完畢後將會出現在列表中，等待全數執行的主機都完成檢測



檢測完畢後，點擊下方“Generate Report”按鈕來產生報表，報表中可以清楚告知有哪些主機是需要進行安裝安全性修補程式。



您也可以點擊“Download Report”選擇您所需要的報表格式



PDF Report 樣式

No vulnerable versions of the Log4j library were found on the assessed endpoints
Expand your view of the attack surface by running the assessment tool or installing Endpoint Sensor on more endpoints. Next, determine your organization's risk index and perform recommended actions for managing the identified risk.

Attack Surface

Assessed Endpoints	Log4j Library Found	△ Patch required
1	0 <input type="checkbox"/> <input type="checkbox"/>	0 <input type="checkbox"/> <input type="checkbox"/>

Enable real-time monitoring of endpoints
Endpoint Sensor can continuously monitor your endpoints for events associated with Log4Shell. Assess more Linux, macOS, and Windows endpoints with just a few clicks.

Determine and manage your organization's risk index
Zero Trust Risk Insights evaluates risk factors in your environment, identifies at-risk users and devices, and recommends prevention and remediation measures. By managing the effects of risk events and taking measures to prevent recurrence, you can lower your organization's risk index.

Details

- ▽ Patch required (0)
- ▽ No Vulnerable Log4j Library (0)
- ▽ Assessed Endpoints (1)

<input type="checkbox"/> SPFS17216072	IP address: 172.16.207.39	Operating system: Windows Server 2016 Standard
---------------------------------------	---------------------------	--

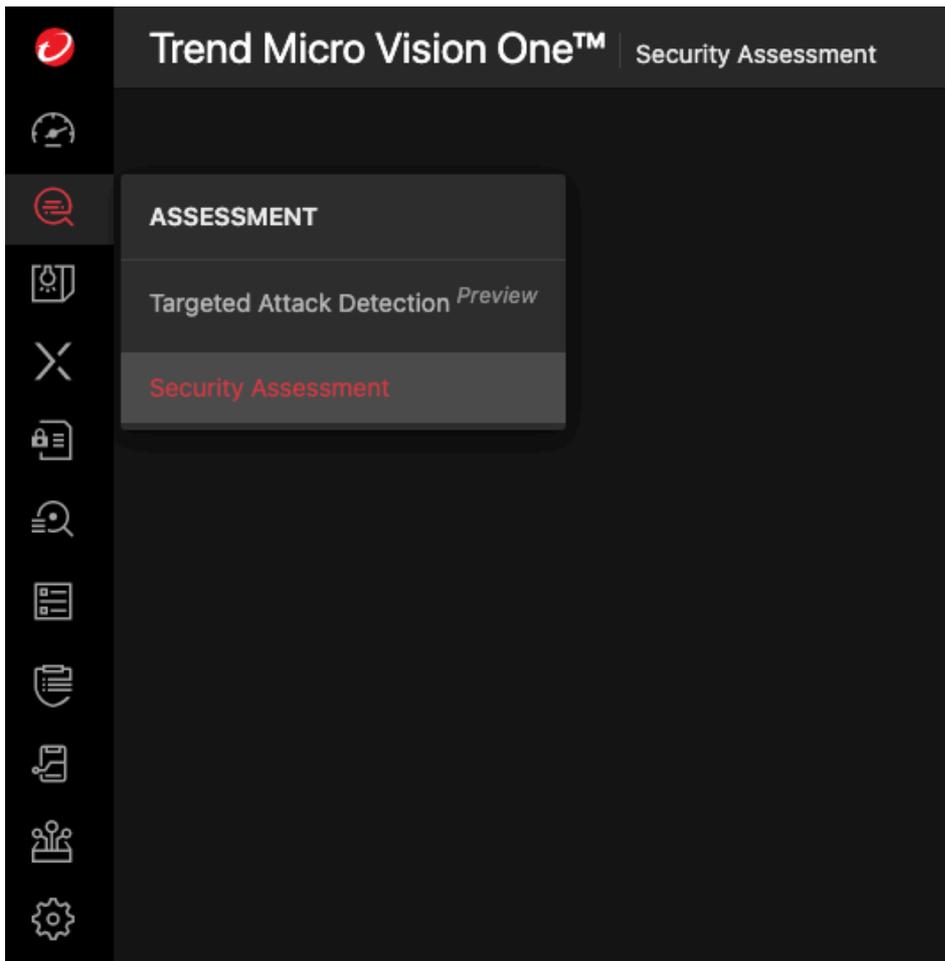
More actions:
Deploy XDR sensors to enhance your visibility

CSV Report 樣式

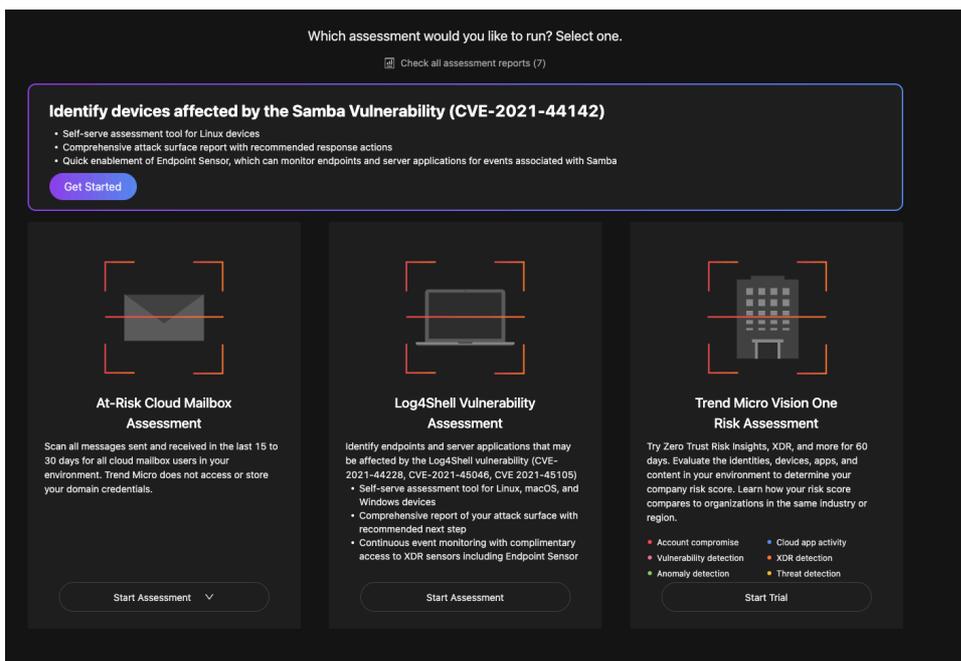
	A	B	C	D	E	F
1	hostname	ip address	file path	OS version	Last scan time	Status
2	SPFS17216072	172.16.207.39		Windows Server 2016 Sta	2022-02-18T07:38:12.000Z	Not Found
3						

正式客戶使用說明

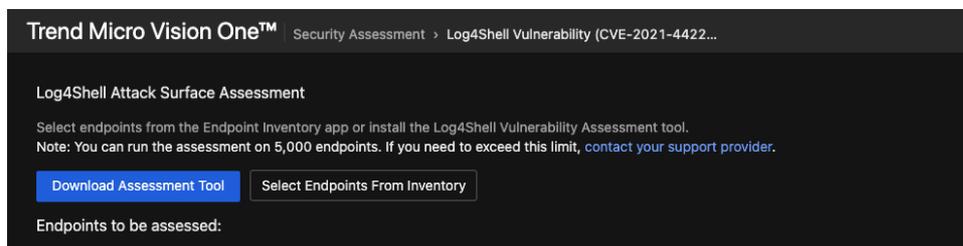
點擊左方 App 工作列，選擇到“Assessment | Security Assessment”



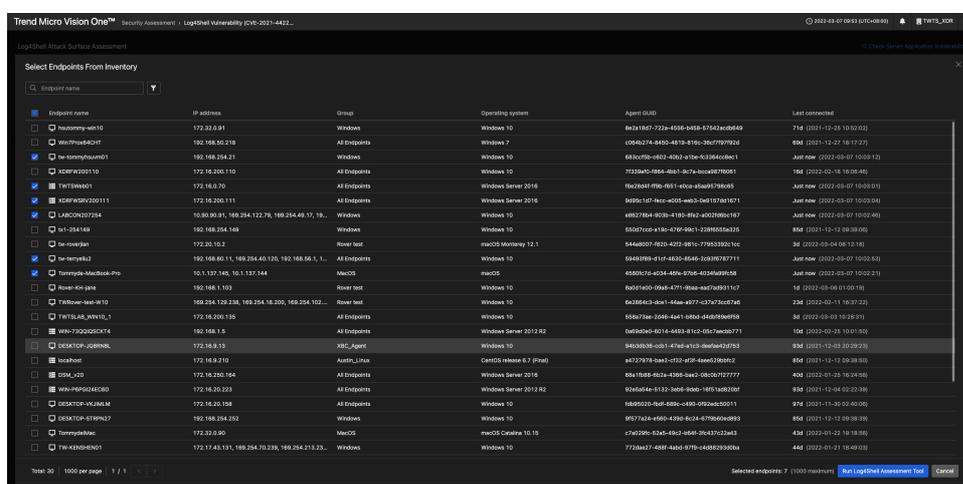
依照你的需求選擇檢測項目



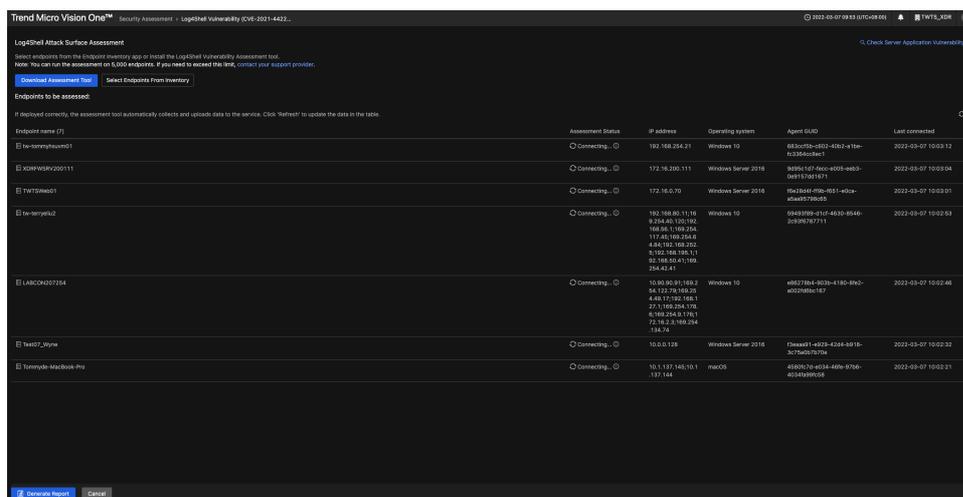
範例為使用 Log4shell 的檢測，點擊”Start Assessment”後，可選擇已經連線上 Vision One 平台中的 Endpoint Inventory 中的主機進行檢測。



選擇完畢後點擊”Run Log4J assessment Tool”



Vision One 平台即可開始進行相關檢測



完成檢測後，可以點擊”Generate Report”產出報表

Endpoint name (7)	Assessment Status
tw-terryellu2	Completed
Test07_Wyne	Completed
tommyde-macbook-pro.local	Completed
XDRFWSRV200111	Completed
TWTSWeb01	Completed
tw-tommyhsuvm01	Completed
LABCN207254	Completed

報表即可呈現檢測結果

Trend Micro Vision One™ Security Assessment | Log4Shell Vulnerability (CVE-2021-4422)

No vulnerable versions of the Log4j library were found on the assessed endpoints.

Expand your view of the attack surface by enabling the assessment tool or installing Endpoint Sensor on more endpoints. Next, determine your organization's risk index and perform recommended actions for managing the identified risk.

[Download Report](#) [Start New Assessment](#) [Give Feedback](#)

Attack Surface	Log4j Library Found	Patch required
Assessed Endpoints: 7	Log4j Library Found: 0	Patch required: 0

Enable real-time monitoring of endpoints
Endpoint Sensor can continuously monitor your endpoints for events associated with Log4Shell. Assess more Linux, macOS, and Windows endpoints with just a few clicks.
[Enable Endpoint Sensor](#)

Determine and manage your organization's risk index
Steps: Trust Risk Insights evaluates risk factors in your environment, identifies at-risk users and devices, and recommends prevention and remediation measures. By managing the effects of risk events and taking measures to prevent recurrence, you can lower your organization's risk index.
[Improve your risk index](#)

Details

- Patch required (0)
- No Vulnerable Log4j Library (0)
- Assessed Endpoints (7)

More actions:

- Deploy XDR sensors to enhance your visibility
Endpoint Sensor detects malicious or anomalous activities on monitored endpoints and servers.
[Enable in Endpoint Inventory](#)
- Protect and investigate with Trend Micro products
Trend Micro's security solutions help you detect, investigate, and respond to threats.