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:
United States
* Data center location:
Select V
I agree to the Terms of Service (Global I 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

🥏 IREND Trend Micro Vision One™			
	Verify Email Address	Trend Micro has sent a verification code to normalgatimuchysabo@itthrw.com. The code will earlie in 1022-02-18 14 50 24.	

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.

Jecum	y Assessment Service	
tello,		
Thank you for yo	r interest in Trend Micro. Type the following code to verify your email addr	ess.
/erification code:	JIR- 042638	
Note: This code v	ill expire on 02/18/2022 06:50:24(UTC+00).	
f you did not req	est a verification code, contact your support provider. Please retain this er	nail for future reference.
Best regards,		
rend Micro		

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



I hank you for registering for the Trend Micro Security Assessment Service. Using the Tren d Micro Vision One™ platform, this complimentary service offers insight into your attack su rface, identifies potential threats in your environment and provides a detailed, downloadabl e 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-d ays 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:	Send verification code
New password (j)	₹
Confirm password	<u>م</u>

Reset password				
Email address:	njomutgatmvdhyaxbo@nthrw.com			
Verification code:	8LJ -			
	If the email does not arrive in your inbox or spam folder, click here to resend (173s).			
New password (i)	ø			
Confirm password	ø			
		Submit		
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 UT	C+0.			
If you did not request a verification code, contact your s	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 ()		R		
Confirm password		œ		
			_	
			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	Sign In
Beyond the single vector Connecting email, endpoints, servers, cloud workloads, and networks provides a broader	Sign in
perspective and a better context to hunt, detect, and contain threats.	Account name
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.	Remember me
Integrated investigation and response	Continue
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 resoonse actions from a single	Need help signing in?
place.	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 protection alone can no longer be trusted to protect interne from unauthorized access. To adequately safeguard your Account, turn on two-factor authentication (2FA) immediat	s, password et accounts Trend Micro ely.
What is Two-factor Authentication (2FA)?	Why is this important?
What is Two-factor Authentication (2FA)?	Why is this important?
2FA lets you use your mobile device to confirm your identity when	If your account is compromised, criminal hackers could switch off all
What is Two-factor Authentication (2FA)?	Why is this important?
2FA lets you use your mobile device to confirm your identity when	If your account is compromised, criminal hackers could switch off all
signing into your Trend Micro Account. This added layer of security	Trend Micro protections. They could then gain access to your personal
What is Two-factor Authentication (2FA)?	Why is this important?
2FA lets you use your mobile device to confirm your identity when	If your account is compromised, criminal hackers could switch off all
signing into your Trend Micro Account. This added layer of security	Trend Micro protections. They could then gain access to your personal
prevents unauthorized access to your Trend Micro SaaS product	data, business secrets, and even banking information. All your data
What is Two-factor Authentication (2FA)?	Why is this important?
2FA lets you use your mobile device to confirm your identity when	If your account is compromised, criminal hackers could switch off all
signing into your Trend Micro Account. This added layer of security	Trend Micro protections. They could then gain access to your personal
prevents unauthorized access to your Trend Micro SaaS product	data, business secrets, and even banking information. All your data
consoles, even if your password is stolen.	could be stolen, held for ransom, or destroyed. Trend Micro highly

Continue to 2FA Settings

點擊左側功能 APP 此圖示	選擇"Security Accessment"開始進行檢測
Trend Micro Vision One [™] security Dashboard	© 2022-02-18 07:00 (UTC+00:00) 🗼 🦉 📲 TrendMicroTWSUPPORT 🛞
New tab Y +	
Targeted Attack Detection Preview Security Assessment	Ge to App : ENDPOINTS REPORTING ACTIVITY : Age: Endpoint Inventory
□ □	No data to display
MITRE ATTACK MATRIX" MAPPING Ago: Occerned Attack: Rechnices Criteria @	(Go to App) Last 24 hours v :

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

	Which assessment would you like to run? Select one.						
<u>(ف</u>)	I Check all assess						
	Identify devices affected by the Samba Vulnerability (C)	Identify devices affected by the Samba Vulnerability (CVE-2021-44142)					
	Self-serve assessment tool for Linux devices	Self-serve assessment tool for Linux devices					
	Comprehensive attack surface report with recommended response actions Quick enablement of Endpoint Sensor, which can monitor endpoints and server applications f	for events associated with Samba					
	Get Started						
		Ľ,					
	At-Risk Cloud Mailbox Log4Shell Vi	ulnerability Trend Micro	Vision One				
	Assessment Assess	ment Risk Asse	essment				
	Scal all messages set and received in the last 15 to benefity enclosities and sense 30 days for all coord messages set and received in the last 15 to benefity in elegibility of environment. Trend Micro does not access or store 2021-44229, (CF-2021-45 your domain credentials. Violation and access and access or store your domain credentials. Comparison and access access and access	y applications that may Try 2ren Trust Risk biolistics burkensbilly (CVC days, E valuate the identities 0446, CVZ 021-45105) content in your environment for Unixun, racco, and company risk score. Learn h compares to organizations i region.	XDR, and more for 60 devices, paps, and to determine your ow your risk score the same industry or Cloud sep settivy XDR stepsion				
		* Anomaly detection	Threat detection				
	Start Assessment V Start Asse	Start	Trial				

選擇"Download Assessment Tool"



選擇需要檢測的作業系統平台來進行檢測

Deploy the assessment tool on more endpoints					
The assessment tool scans endpoints for vulnerable versions of the Log4j library. You can deploy the assessment tool using your preferred system utility or you can share the download link with users.					
Windows	Linux				
View deployment instructions	View deployment instructions				
By downloading the Assessment Tool, you agree to the End User License Agreement (Global Japan).	By downloading the Assessment Tool, you agree to the End User License Agreement (Global Japan).				
View deployment instructions					
⊥ Download Assessment Tool					
By downloading the Assessment Tool, you agree to the End User License Agreement (Global Japan).					
	Close				

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

2	Trend Micro Vision One [™] Security Assessment > Log4Shell Vulneral	bility (CVE-2021-4422			() 2022-02-18 07:38 (UTC+00:00)	
	LogdShell Attack Surface Assessment Select enclosing from the Enclosed twentory say or install the Log4Shell Vulnerabil Note: You can run the assessment on 6,000 enclosing. If you need to exceed this lin Deventional Assessment Tool Select Enclosing From Inventory Enclosed to assessed:	ity Assessment tool. nit, contact your support provid				
1 1	If deployed correctly, the assessment tool automatically collects and uploads data to	o the service. Click 'Refresh' to	update the data in the	table.		
	Endpoint name (1)	Assessment Status	IP address 172.16.207.39	Operating system Windows Server 2016	Agent GUID 74e8bafc-ed70-4983-9cc7-	Last connected 2022-02-18 07:38:26
ų %				Standard	6700623000038	
© 1						
0						
>>	Generate Report Cancel					

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,

0	Trend Micro Vision One [™] Security Assessment > Log45Hell Vulnerability (CVE-2021-4422
(?) () ()	No vulnerable versions of the Logd jilbrary were found on the assessed endpoints Expand your view of the stack 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.
×∎ ଇ Щ	Attack Surface Assessed Endpoints 1 0 E 0 0 0 E 0 0
(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	Enable real-time monitoring of endpoints Endpoint Sensor can continuously monitor your endpoints for events associated with Log4Shell. Assess more Linux, mac55, and Windows endpoints with just a few clicks. Enable Endpoint Sensor Enable Endpoint Sensor Institle Endpoint
< 🗐 🛈	Details > Patch required (0) > No Vulnerable Log4] Lbrary (0) > Assessed Endpoints (1) More additions:

您也可以點擊"Download Report"選擇您所需要的報表格式



PDF Report 樣式

No uninerable versions of the Log & library were found on the second and winte				
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 organizations risk index and perform recommended actions for managing the identified risk.				
Attack Surface Assessed Endpoints Log4j Library Found 1 0 to the second	A Patch required 0 ₽0 ₽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. Determine and manage your organization's risk index. Zero Trugt 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 Logdj Library (0)				
✓ Assessed Endpoints (1)				
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

	А	В	С	D	Е	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"

Trend Micro Vision One ¹⁰ society Aussesses Lapteen Vincenze (1000-000)						
LogKhil Mtak Surtar Assessment 0, Orex Server Application Valenzani						
Select	t Endpoints From Inventory					
G. 6						
	Endpoint name	IP address		Operating system	Agent GUID	Last connected
	D hsutommy-win10		Windows	Windows 10	8e2a18d7-722a-4556-b458-57542acdb549	71d (2021-12-25 10:52:02)
	Win7Prost4CHT	192.168.50.218	All Endpoints	Windows 7	c084b274-8450-4819-816c-38cf7f97f92d	69d (2021-12-27 18:17:27)
2	C tw-tommyhsuvm01		Windows	Windows 10	683ccf5b-o602-40b2-a1be-fc3364cc8ec1	Just new (2022-08-07 10:08:12)
	C XD8FW200110		All Endpoints	Windows 10	7f339af0-f864-4bb1-9c7a-bcca967f6061	16d (2022-02-18 16:06:46)
2	III TWTSWeb01		All Endpoints	Windows Server 2016	16e28d4f-ff9b-f651-e0ca-a5aa95798c65	Just new (2022-08-07 10:08:01)
2	XDRFWSRV200111		All Endpoints	Windows Server 2016	9d95c1d7-fecc-e005-eeb3-be9157dd1671	Just new (2022-03-07 10:03:04)
2	LABCON207254	10.90.90.91, 169.254.122.79, 169.254.49.17, 19	Windows	Windows 10	e86278b4-903b-4180-8fe2-a002f96bc167	Just new (2022-03-07 10:02:46)
	🖵 tx1-254149	192.168.254.149	Windows	Windows 10	550d7ccd-a19c-476f-99c1-22816555a325	85d (2021-12-12 09:39:06)
	💭 te-roverjan		Rover best	macOS Monteney 12.1	544e8007-f820-4212-981c-77953352c1cc	3d (2022-08-04 08:12:18)
2	🖵 tw-terryelu2	192.168.80.11, 169.254.40.120, 192.168.56.1, 1	All Endpoints	Windows 10	59493f89-d1cf-4630-8546-2c93f6787711	Just new (2022-03-07 10:02:53)
2	Tommyde-MacBook-Pro		MacOS	mac05	45501c7d=e034-46fe-97b6-4034fe99fc58	Just new (2022-03-07 10/02/21)
	Rover-KH-jane		Rover test	Windows 10	8a0d1e00-09a8-4711-9baa-ead7ad9311c7	1d (2022-08-06 01:00:19)
	TWRover-test-W10		Rover test	Windows 10	6e2854c3-doe1-44aa-a977-c37a73cc67a6	23d (2022-02-11 16:37:22)
	TWTSLAB_WIN10_1		All Endpoints	Windows 10	558a73ae-2d46-4a41-b8bd-d4db189e6158	3d (2022-08-03 10:28:81)
	WIN-7399895CKT4	192.168.1.5	All Endpoints	Windows Server 2012 R2	0x69d0e0-6014-4493-81c2-05c7aecbb771	10d (2022-02-25 10:01:50)
					94b3db38-ocb1+47ed-a1c3-deefae42d753	98d (2021-12-03-20:29:25)
	III localhost		Austin_Linux	CentOS release 6.7 (Final)	a4727978-bas2-c132-af3f-4aee529bbfc2	85d (2021-12-12 09:38:50)
	III D5M_v20		All Endpoints	Windows Server 2016	65a1fb35-6b2a-4385-bae2-08c0b7127777	40d (2022-01-25 16:24:58)
	III WIN-PEPGI24EC6D		All Endpoints	Windows Server 2012 R2	92e5a54e-5132-3eb6-9deb-16f51ad8200f	984 (2021-12-04 02:22:38)
	DESKTOP-VKJINEM		All Endpoints	Windows 10	fdb95020-fbdf-589c-c490-0192edc50011	97d (2021-11-30 02:40:06)
	DESKTOP-6T8PN27	192.168.254.252	Windows	Windows 10	91577a24-e560-439d-8c24-6719b60ed893	854 (2021-12-12-09-38-39)
	D TommydelMac		Mac05	macOS Catalina 10.15	c7#029fc-52#5-49c2-b54f-3fc437c22#43	43d (2022-01-22 19:18:56)
	TW-KENSHEN01	172.17.48.131, 160.254.70.230, 160.254.213.23	Windows	Windows 10	772dae27-488f-4abd-9719-c4d88293d/ba	44d (2022-01-21 18-49-05)
Total	30 1000 per page 1 / 1 < →				Selected endpoints: 7	(1000 maximum) Run Logi Sheil Assessment Tool Cancel

Vision One 平台即可開始進行相關檢測

Trend Micro Vision One ⁵⁴ Security Assessment > LapeShell Vulnerability (CVE-2021-4422				() 2022-03-07 09 83 (UTC+08 00)		TWTS_XDR
Constant Average of the second average of th						
If deployed connectly the assessment tool automatically collects and unloads data to the service. Click 'Refresh' to undate the data in the table.						
Endpoint name (7)						
E te-sample and 1				683cc15b-c602-40b2-a1be- fc3364cc8ec1		
E xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx				9d95c1d7-feco-e005-eeb3- 0e9157dd1671		
E TWTSWeb1			Windows Server 2016	15e2854f-ff9b-f651-e0ce- a5ax95798c05		
Etwinyini2		192.168.80.11;16 9.254.40,120;192, 168.56,1;169.254, 117.45;169.254,6 4.84;192,168.252, 5;192,168.198,1;1 92,188.50,41;169, 254,42,41		59493789-01cf-4630-8546- 208876787711		
Енасонотия		10.90.90.91;169.2 54.122.79;169.25 4.49;17;192.168.1 27.1;169.254.178, 6;169.254.9.176;1 72.16.2.3;169.254 .134.74		68627854-9035-4180-8762- x0007695c167		
E Teat?_Jiyoa				f3eaaa91-e929-4244-b918- 3c75a0b7b70e		
E Terrinyde-MacBook-Pro				45801c7d-e034-46fe-97b6- 40341s99fc58		
(person band) and						

完成檢測後,可以點擊"Generate Report"產出報表

Endpoint name (7)	Assessment Status
The terry dia2	Completed
E Test07_Wyne	Completed
E tommyde-macbook-pro.local	Completed
E XDRFWSRV200111	Completed
E TVTSWeb01	Completed
C tw-tonmyhsuvm01	Completed
□ LABCON207254	Completed

報表即可呈現檢測結果

Trend Micro Vision One TM Security Assessment > Log45Net Vulnerability (2VIE-2021-4422	🔿 2222-43-47 66632 juite-66630 🌲 📑 TWT5_XXR 🔘
No vulnerable versions of the Logit (Brary were found on the assessed indipolets). Expand your rive of the attack surface by running the assessment tool or initialing triggent Sensor on more exclusions, best, adversive your arguitasters risk index and partorn more	Develand Napoli v 📄 🔮 Shel New Assessment 🖉 Shel New Assessment 🖉 Shell New Assessment 🖉 Shell New Assessment 🖉
Anach Surfae Anamad chigarth Saget (Sherry Fand 7 O Bo Geb	Anton meane O Bo ⇔a
Saak ne ére norbing af elgipan. Sagkart Searc av continual mohtr par edgalm for eens associate els LagtSet Jases non Lina, nació, ed Nickan engalm als jar a for dita. Frain Diagont Searc	Deemine and manage put organization (do shok 20m Twe for the highly a subury dia future to jour animone), Switch a scho sam and twicks, and assumed prevention and metabolis measures by managing the reflect of all assumed and all researce to prevent escence, you cal loan your application (do hole. Regression and metabolis
Details > Price majored (8) > No Varvendo Logi (1) > No Varvendo Trajante (7) > Assessed Trajante (7)	
Man and extense Design 2014 amounts the interact your widelity Register Service Match in address an extensional antibities on resolvent antipoletic and answer. Catella in Exploration Homotry Produce and extendingua with Yook (does producib) Hings (bursteen Manana Resolution(ESCERED)	