

Forcepoint

從資料分類到行為分析： Forcepoint 如何用 AI 守 護關鍵資料？

Ray Pai

北亞區技術顧問 | Taiwan | Korea | Japan |

資料安全 與 Gen AI

Generative AI and Data Security

如何在我的公司裡安全地
採用 AI？

AI 的使用有哪些資料安全風
險？

AI 在其他公司的
應用情況如何？

有哪些 AI 驅動的資料安全
產品可用？

如何利用 AI
管理資料安全？

如何使用 AI 來提高組織
的生產力？

如何保護 Gen AI 網站的使用



每天會有新的 AI 網站或工具出現！

Gen AI 使用可視性 (ChatGPT Enterprise)

公司採購AI工具提高生產力



Gen AI 的開放還是管制

Gen AI 網站自動識別與分類

Categories

Configure filtering actions and SSL decryption for web categories.

SSL decryption: ☒ The *Forcepoint LLC root certificate(s)* must be installed on the end user workstations.

Search

Quick select ...

Human Interests

Illegal or Unethical

Information Technology

Computer Security

Generative AI - Conversation

Generative AI - Multimedia

Generative AI - Text & Code

Hacking

Other AI ML Applications

Proxy Avoidance

Search Engines and Portals

Unauthorized Mobile Marketplaces

Web Analytics

Web and Email Marketing

Web and Email Spam

Web Collaboration

Web Hosting

Website Translation

Internet Communication

Generative AI - Text & Code

Action:

☐ Allow access

☐ Do not block

☐ Require user authentication

☐ Confirm

☐ Use Quota

☒ Block access

Block page: Upload Blocked

SSL decryption:

☒ Decrypt

☐ Do not decrypt



Gen AI 的開放還是管制

ChatGPT

Forcepoint detected content that violates corporate policy. Please do not reload the tab. Further actions on this page are currently blocked until this content is cleared. Close [X]

登入 註冊

貼上敏感資訊

我可以為你做什麼？

姓名 出生年月日 身分證統一編號 電話 地址 e-mail 台幣存款帳號 台幣金額 信用卡帳號

鄭智偉 661120 B204602960 04-3747683 台中縣神岡鄉大同路一段20號 girl77138@yahoo.com 041-23-123432-2-32 3457669 4770327189136670

邱春樹 660321 A123456789 02-27265896 台北市重慶南路一段38號

gary@mail.kenmark.com.tw 041-23-123432-2-33 3457669 4435223046072280

高欣儀 730101 Q105925140 02-89191568 台北市大同區承德路三段58號4樓之1

amelia@kenmark.com.tw 041-23-123432-2-34 3457669 4337451795127830

陳明哲 740705 F276527619 02 27221969 台北市大同區承德路三段58號4樓之1

附加 搜尋 推理

總結文字 幫我寫 制訂計畫 分析資料 分析圖像 更多

傳送訊息至 ChatGPT，即表示你同意我們的條款，並已閱讀我們的「隱私政策」。

Warning

Forcepoint DLP Endpoint 已阻止你將敏感資訊上載至遠端主機 CHATGPT.COM，因為您這樣做違反公司政策。

提供鑑識資料

387309	2025-03-27 21:34:31	GOOD/fpclin	臺灣身分證號碼; 姓名和臺灣手機...	Endpoint HTTPS	GEMINI.GOOGLE.COM	High	Blocked
387297	2025-03-27 21:34:26	GOOD/fpclin	臺灣身分證號碼; 姓名和臺灣手機...	Endpoint HTTPS	COPILOT.MICROSOFT.COM	High	Blocked
386621	2025-03-27 21:34:18	GOOD/fpclin	臺灣身分證號碼; 姓名和臺灣手機...	Endpoint HTTPS	CHATGPT.COM	High	Blocked
384193	2025-03-27 21:19:22	GOOD/fpclin	網站文字判斷	Endpoint HTTPS	CHATGPT.COM	High	Blocked
385113	2025-03-27 21:16:12	GOOD/fpclin	網站文字判斷	Endpoint HTTPS	FELLO.AI	High	Blocked
383440	2025-03-27 21:14:03	GOOD/fpclin	網站文字判斷	Endpoint HTTPS	NOTEBOOKLM.GOOGLE.COM	High	Blocked
383159	2025-03-27 21:10:27	GOOD/fpclin	網站文字判斷	Endpoint HTTPS	GEMINI.GOOGLE.COM	High	Blocked
383332	2025-03-27 21:08:41	GOOD/fpclin	網站文字判斷	Endpoint HTTPS	COPILOT.MICROSOFT.COM	High	Blocked
383277	2025-03-27 21:06:11	GOOD/fpclin	網站文字判斷	Endpoint HTTPS	CHATGPT.COM	High	Blocked

Incident: 387297 Severity: High Action: Blocked Channel: Endpoint HTTPS (encrypted)

Display: Violation triggers

Rule: 姓名和臺灣手機號碼

姓名 (Regular Expression) 23
羅志明, 鄭智偉, 黃宜芳, 黃佳偉, 符佩芬, 楊顯如, 詹大偉, 黃曉琳, 梁淑萍, 曾嘉宏, 邱春樹
臺灣市話號碼 (Regular Expression) 21
02-27622776, 02-22210731, 02-27265896, 02-86637388, 02-89904543, 02-89191568, 02-2311

Rule: 姓名和電子郵件地址

姓名 (Regular Expression) 23
羅志明, 鄭智偉, 黃宜芳, 黃佳偉, 符佩芬, 楊顯如, 詹大偉, 黃曉琳, 梁淑萍, 曾嘉宏, 邱春樹
Email Addresses (Script) 24
cde@ms50.hinet.net, f1rkt@yahoo.com.tw, fsts@yahoo.com.tw, aaaa@ms44.hinet.net, 566

Rule: 臺灣身分證號碼

Taiwan ID (Script) 24
Q105925140, A123456789, P259491034, P191101677, B204602960, V139049038, H26606791

Rule: 姓名和臺灣地址

臺灣地址 (Regular Expression) 23
台北市大同區承德路四段58號4樓之1, 台北市羅斯福路三段107巷11號3樓, 台北市大同區
姓名 (Regular Expression) 23
羅志明, 鄭智偉, 黃宜芳, 黃佳偉, 符佩芬, 楊顯如, 詹大偉, 黃曉琳, 梁淑萍, 曾嘉宏, 邱春樹

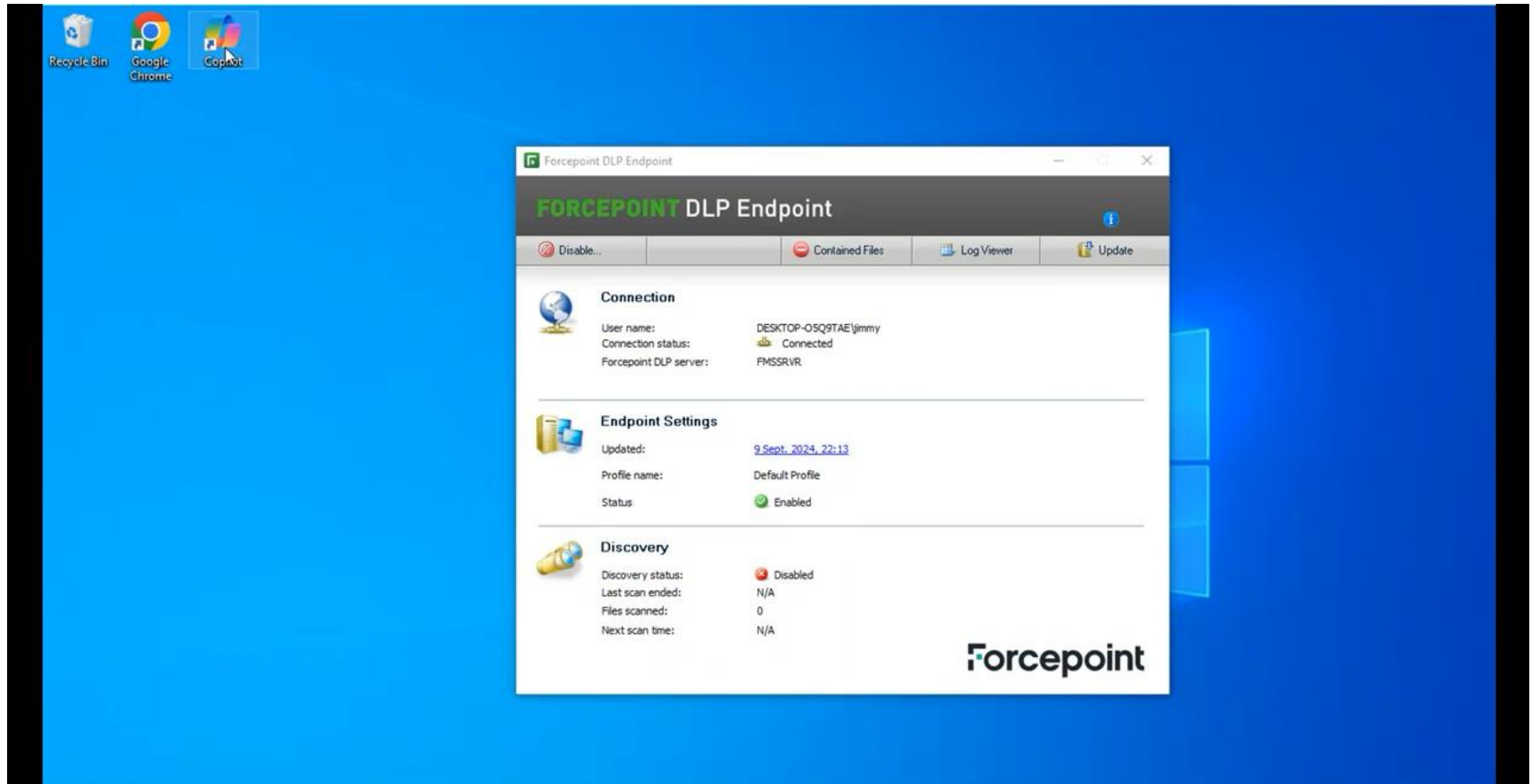
Forensics Properties History

Source: GOOD/fpclin
Destination: COPILOT.MICROSOFT.COM
Url: COPILOT.MICROSOFT.COM
File: Attachment (3.58 KB)

Event Time: 27 Mar. 2025, 9:34

DLP 偵測阻擋

Demo 1 GEN AI APP DLP



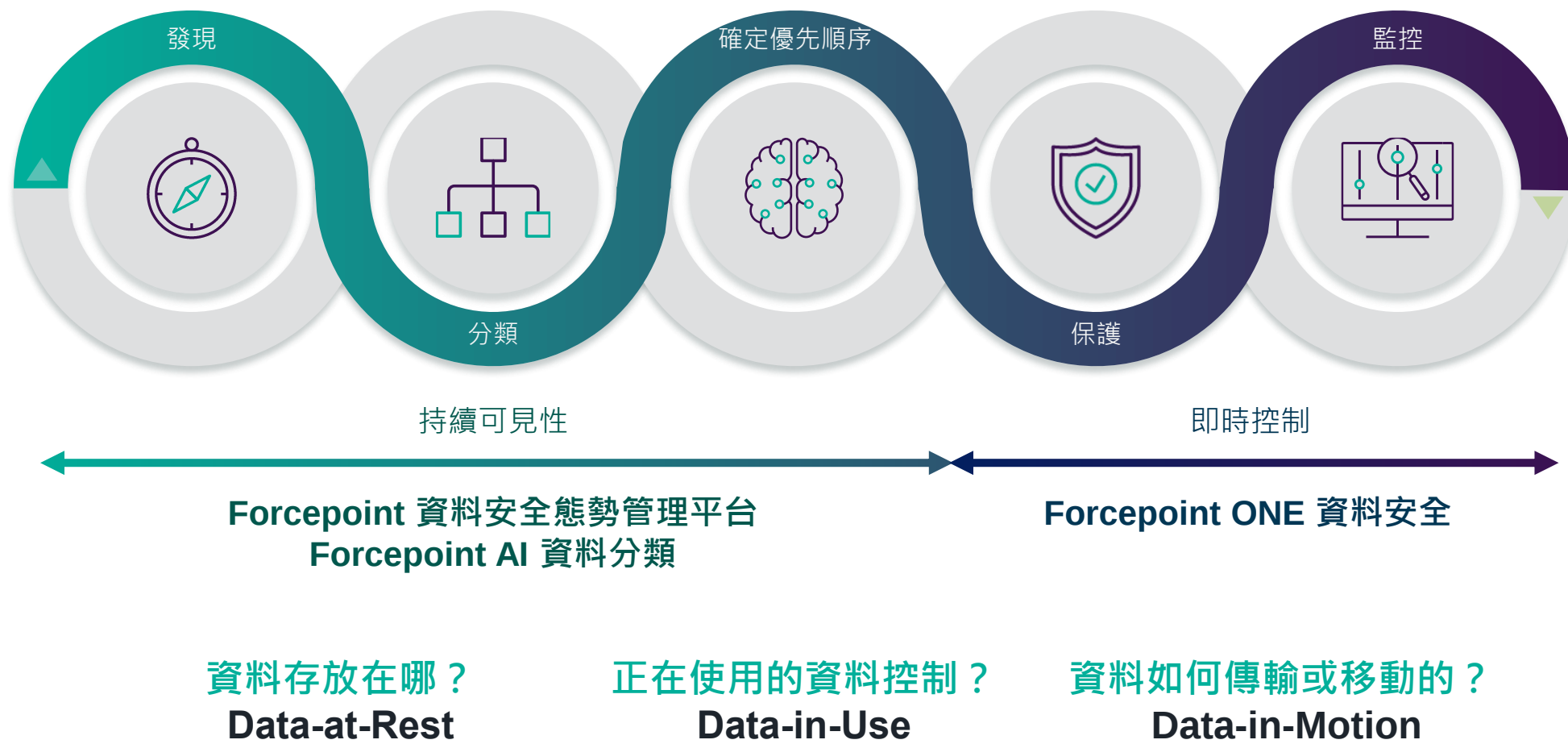
Demo 2 GenAI 使用可視性 (ChatGPT Enterprise)

The screenshot displays the ChatGPT Enterprise web interface. The browser's address bar shows the URL `chatgpt.com/g/g-n4f9lreoU-fp-pii`. The left sidebar contains a list of chat sessions: ChatGPT, APAC_CSE_GPT, FP_PII (selected), and Explore GPTs. Below this, a 'Today' section lists recent topics: PCI Compliance Overview, PCI Data Assistance, and CWSRF Loan Eligibility Overview. The main chat area features a header for 'FP_PII' by Kanishka Dubey, with a description: 'FP_PII will give reply to the prompts asked by looking into the files under knowledge.' A document titled 'PII_PCI_Data_Classified.docx' is attached to the chat. The input field contains the text 'I am sure you need this PII for testing'. At the bottom, a disclaimer states: 'Forcepoint sandbox workspace chats aren't used to train our models. ChatGPT can make mistakes.'

讓敏感資訊不再無所適從

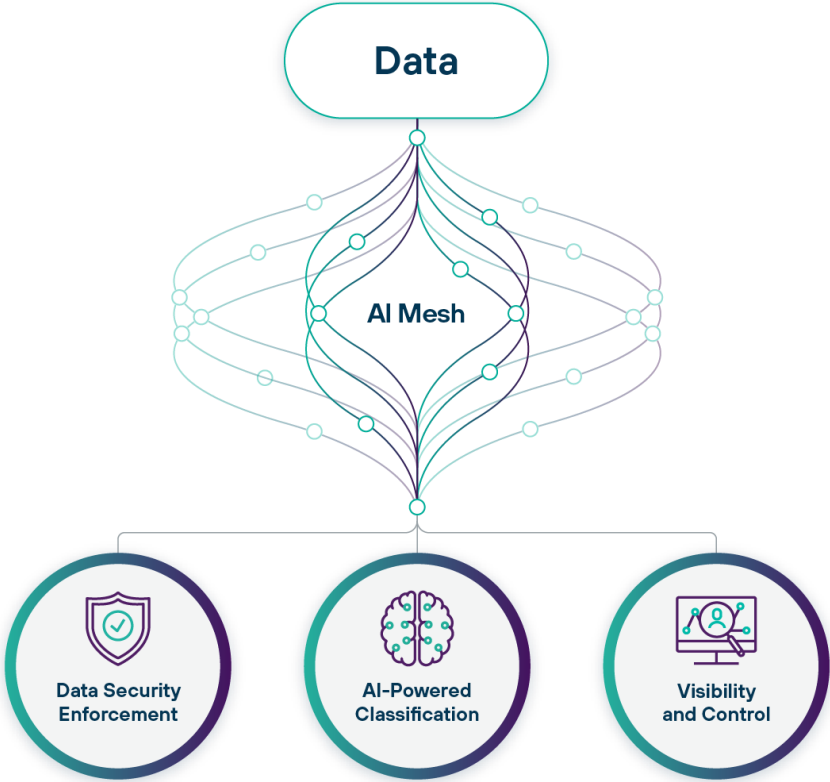
Forcepoint x Data x AI

Forcepoint 自動化保護資料的整個生命週期



關於資料盤點與分類

	傳統資料盤點與分類	Forcepoint AI 盤點與分類
分類方式	靜態規則、人工標記	AI + 機器學習，自動分類
數據可視性	通常侷限於內部伺服器	支援本地端、雲端、SaaS*
更新頻率	需人工維護	動態更新、即時適應
誤報與遺漏	規則難以涵蓋所有情境	AI 持續學習與優化



Forcepoint DSPM AI Mesh

準確、快速、可解釋、降低 TCO

資料識別的運用

LANDING AGENT admin

EXPORT

Classification Tags

Sensitive	HR Documents	Financial Documents	Legal Documents	Technical Documents	Business Documents	Marketing Documents
	CV PII Public	Accounting form General Business	Agreement/Contract General Business	Correspondence (Technical) PII Confidential	Asset inventory General Business	Market Research/Planning Confidential
	Correspondence (Employee) PII Confidential	Audit Confidential	Correspondence (Legal) Confidential	Presentation General Business	Audit Confidential	
	Employee record PII Confidential	Banking form General Business	NDA form PII General Business	Proposal General Business	Business plan Confidential	
	Incident report General Business	Financial agreement/Contract Confidential	Patent Highly Confidential	RFI Public	Correspondence (Business) PII Confidential	
	Performance review Confidential	Invoice/Purchase order General Business		RFP/RFQ Public	Customer/Vendor Record General Business	
	Recruitment PII Confidential	Quotation/Pricing General Business		Specification/Blueprint Highly Confidential	Internal document PII General Business	
Non-Sensitive	HR Documents	Financial Documents	Legal Documents	Technical Documents	Business Documents	Marketing Documents
	Browsing history General Business		Certificate/Permit General Business	Code General Business	Logistic data General Business	Advertisement/Product description Public
			License agreement General Business	Configuration General Business	Policy/Procedure General Business	Logo Public
			Terms/Conditions General Business	Guide/Manual General Business		Press Release Public
				Note/Log General Business		Written content/Draft General Business
				Report General Business		

Legend Non-business Non-business Public General Business General Business Confidential Confidential Highly Confidential

Categories

Sensitive Data

Sub - Categories

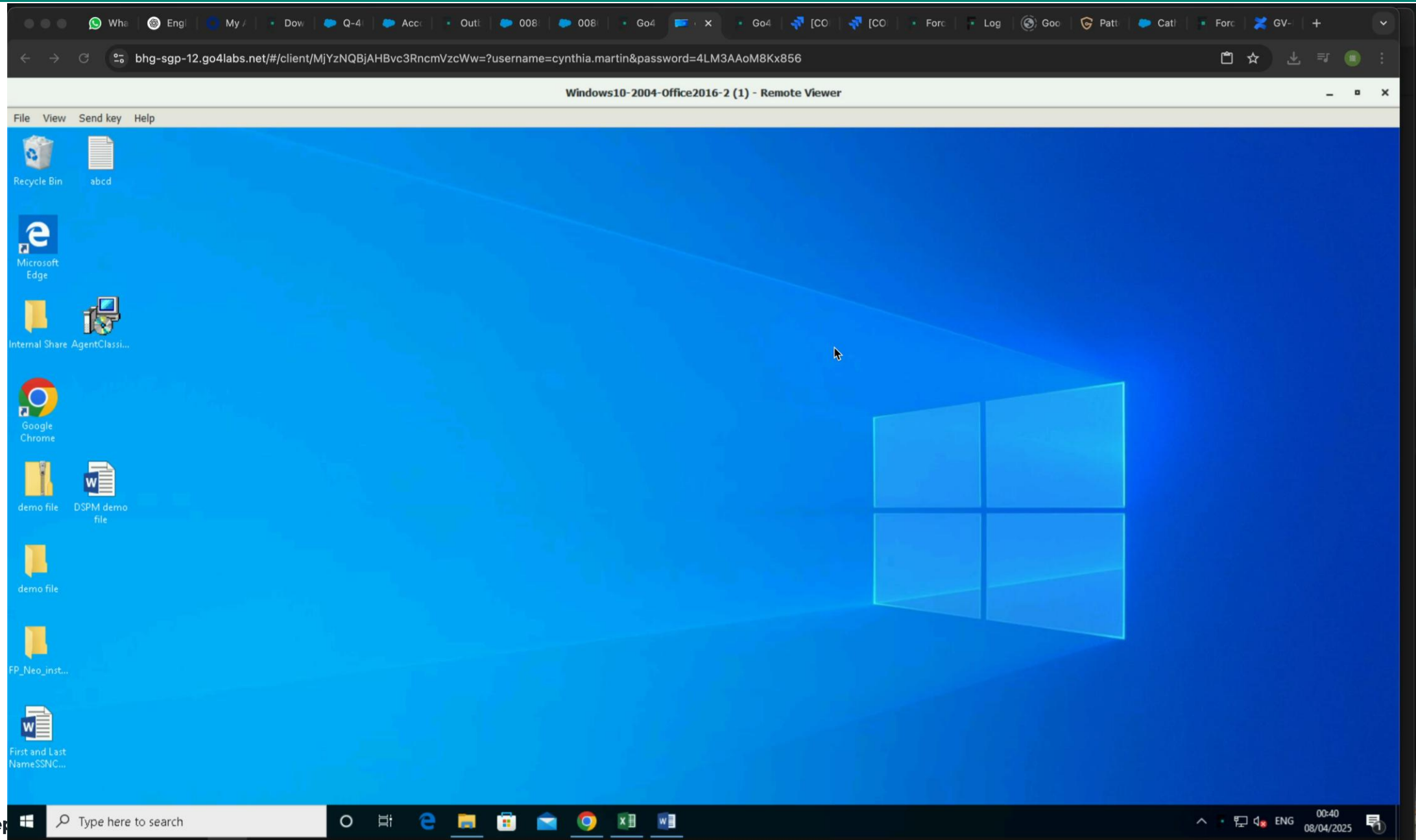
Non- Sensitive Data

DLP Tags

DLP Tags
Sensitive Data
Data Categories
Non- Sensitive

這些Tag適用於文件的保護級別。此資訊可以寫入文件Metadata中，以便與 Forcepoint Enterprise DLP 或 Forcepoint ONE DLP 整合使用。有價值的數據或必須保護的數據（只能使用 PII/PHI/PCI/特殊關鍵字）
第一級標籤稱為子類別，並包含更詳細，例如 Invoices、Quotations 和 Proposals（例如業務文檔）。
可用於描述文件內容的預定義標記集。應用於文檔的標記可以通過多種不同的方式進行構建。在 Forcepoint Data Visibility 中，我們有一組預設的標籤。這些標籤分為兩個級別，頂層稱為類別，是文檔（如 法律文檔、業務文檔）的高級分組，客戶可以廣泛修改。
所有其他資料（通常不含 PII/PHI/PCI/特殊關鍵字）

Demo 3 AI Classification With DLP



使用者行為 x Data x AI

AI 驅動的資料零信任

以人為本的動態資料保護 – 資料零信任

靜態規則 x 動態規則

	靜態規則 (Static Rule)	動態規則 (Dynamic Rule)
定義	事先定義好、不變的條件與對應處理方式	根據當下的使用者行為、環境狀況或風險即時計算條件與決策
決策方式	「如果符合 X，就做 Y」永遠依照固定規則處理	「如果使用者風險高、環境可疑，再決定是否執行」策略是可變動的
資料來源	靠靜態內容 (關鍵字、檔案型態、目的地等) 判斷	會參考行為分析、時間地點、風險分數、歷史模式等動態因子

TVBS 新聞網

92.4k 人追蹤

☆ 追蹤

釣魚簡訊騙卡號 黑幫101盜刷 狂買精品包

江昀蔓 王經綸

2025年4月11日 週五 下午8:38

LINE

f

台北市多間百貨日前報案有民眾盜刷，警方循線逮捕嫌犯，發現天道盟也涉案，先由一名男子傳送釣魚簡訊，誘騙民眾輸入卡號，黑幫再到精品店盜刷，過程中擔心傳送刷卡簡訊，還跟櫃姐裝窮，說刷卡額度低，要求分次刷卡。

刑事局九大三隊長邱承迪：「嫌犯他會針對消費金額上限，可能會跟櫃姐講說，我的消費金額有上限，可不可以協助做我分次的刷卡，來獲得比較高單價的商品。」

Forcepoint

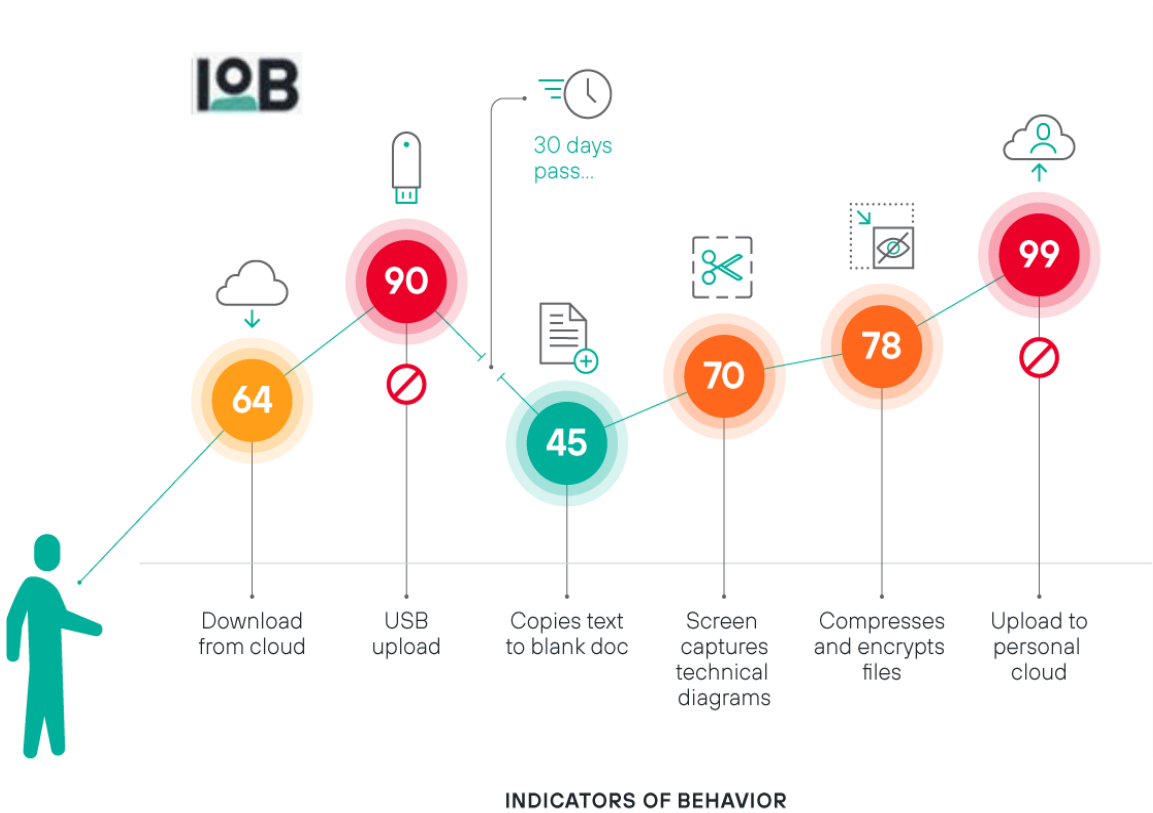
CYBERSEC 2025
臺灣資安大會

4/15 Tue - 4/17 Thu
臺北南港展覽二館

© 2025 Forcepoint

17

基於使用者行為的動態調整資料風險保護策略



單一使用者行為

使用者行為關聯性

異常偵測

Demo

Andy Patrick 計劃離開公司

[DLP] 他從 Gmail 發送了簡歷(CV)

[DLP] 他嘗試使用雲端列印服務列印簡歷(CV)

[RAP] 他嘗試**移除** Forcepoint Agent

[RAP] 他在Google上搜索「**駭客工具**」

[DLP][RAP] 他連接到公司 Share Folder 並將文件備份到 USB

[RAP] 他下載了更多資料並使用 7-Zip 進行加密

[DLP] [DLP] 他比平常更頻繁地將資料複製到USB

[RAP] 他刪除了 Windows Event logs

[DLP] 他下載了臺灣 VIP 資料並嘗試上傳到 Google Drive

[DLP] 然後他嘗試將臺灣 VIP 資料複製到 USB

[RAP] 他的USB許可權已從 Permit 更改為 **Block**





Recycle Bin



Microsoft
Edge



Demo



Google
Chrome

Forcepoint
Endpoint

Agent version: 23.12
23.12.0.86

About **Devices**

Endpoint bypass ▶

Connected devices (2)

QEMU QEMU HARDDISK USB Device Serial number: 1-0000:00:03.0-1	Permit
QEMU QEMU HARDDISK USB Device Serial number: 1-0000:00:07.0-1	Read only

Andy Patrick 是一般使用者，有 1 個個人 USB (只能讀) 和共用 USB

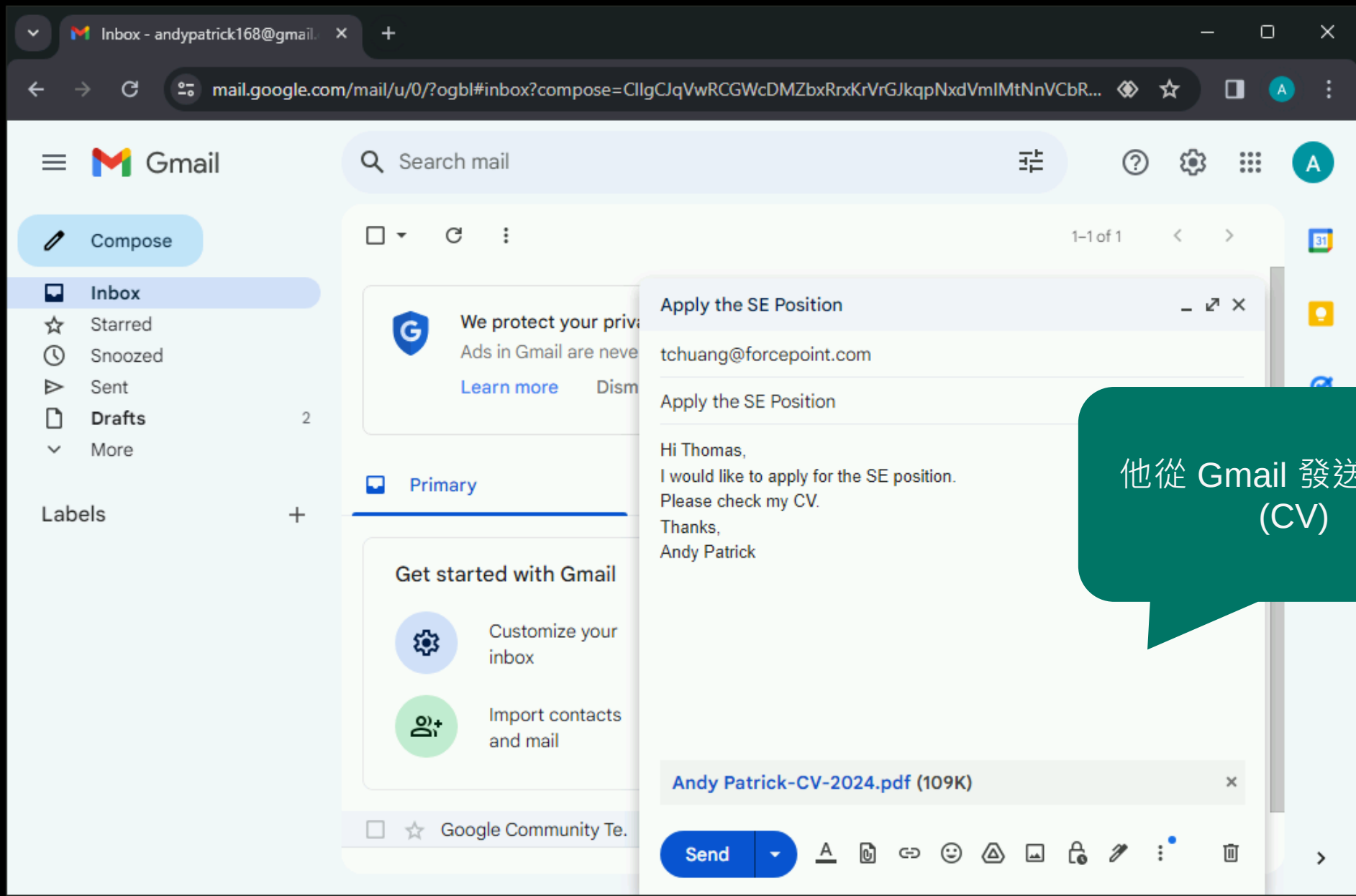
2 new notifications



ENG
INTL



13:45
07/03/2024



他從 Gmail 發送了簡歷
(CV)



Recycle Bin



Google Chrome



Microsoft Edge

Inbox - andypatrick168@gmail.com

コンビニで印刷 | 会員登録不要の

+

lite.printing.ne.jp/web

☆ □ A ⋮

印刷期限
プリント予約日 + 1日 /

かんたんnetprint

FUJIFILM

操作ガイド

店舗でのプリント方法

料金表

店舗検索

FAQ

お問い合わせ

コンビニでいつでもプリント！

セブン-イレブンのマルチコピー機なら、かんたん・きれい



1. 無料でファイル登録



2. QRコードを表示



3. コンビニでかざす

ご利用の際には必ず[利用規約](#)および[個人情報の取扱い](#)、[注意制限](#)をご確認頂き、同意してください。

他嘗試使用雲端列印服務
列印簡歷





Recycle Bin



Google Chrome



Microsoft Edge

Inbox - andypatrick168@gmail.com

コンビニで印刷 | 会員登録不要の

+

← → ↺

lite.printing.ne.jp/web

印刷期限
+ 1日 /

かんたんnetprint

プリントの設定をしてください

ファイルを選択

※用紙サイズ選択をリセットしました。
印刷可能なファイルの種類とサイズは[こちら/料金表](#)

☰ 用紙サイズ ②

☐ フォト用紙 L

☐ フォト用紙 2L

☐ 普通紙 A4

☐ 普通紙 A3

☐ 普通紙 B5

☐ 普通紙 B4

☐ はがき

カラーモード ②

☒ マルチコピー機でのプリント時に選択

☐ カラー

☐ 白黒

ちょっと小さめ ②

☒ しない

☐ する (像欠け防止)

暗証番号 ②

☒ 設定しない

☐ 設定する

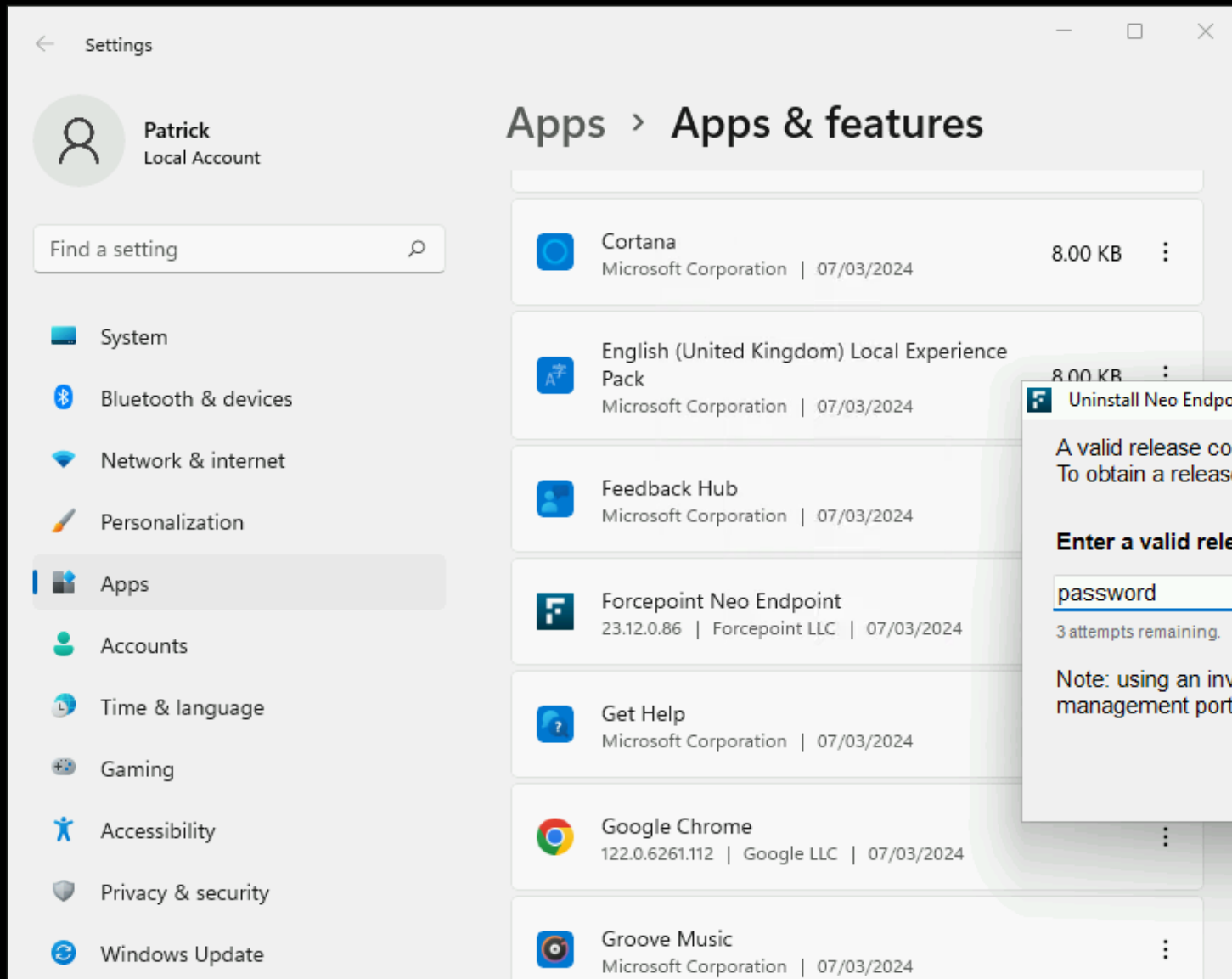
ファイルを選択

Blocked

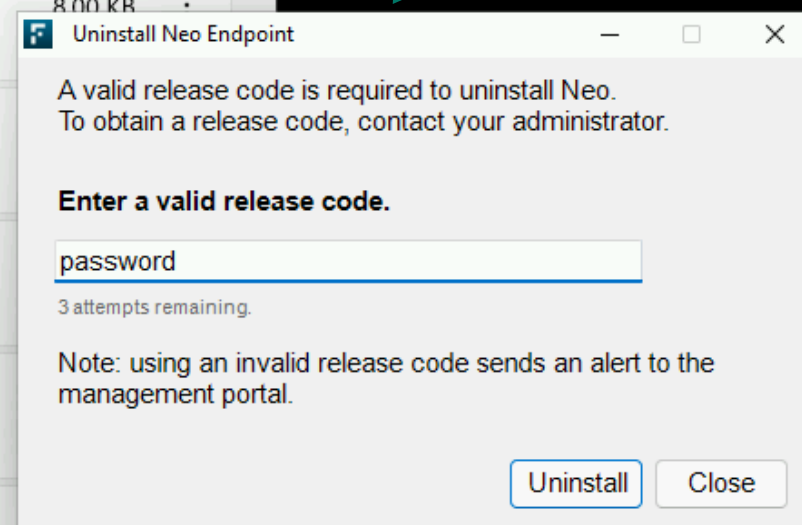
Forcepoint DLP Endpoint has blocked you from uploading sensitive information to the remote host lite.printing.ne.jp, because it is in violation of corporate policy.

公司政策是阻止列印服務。





他嘗試移除 Forcepoint Agent





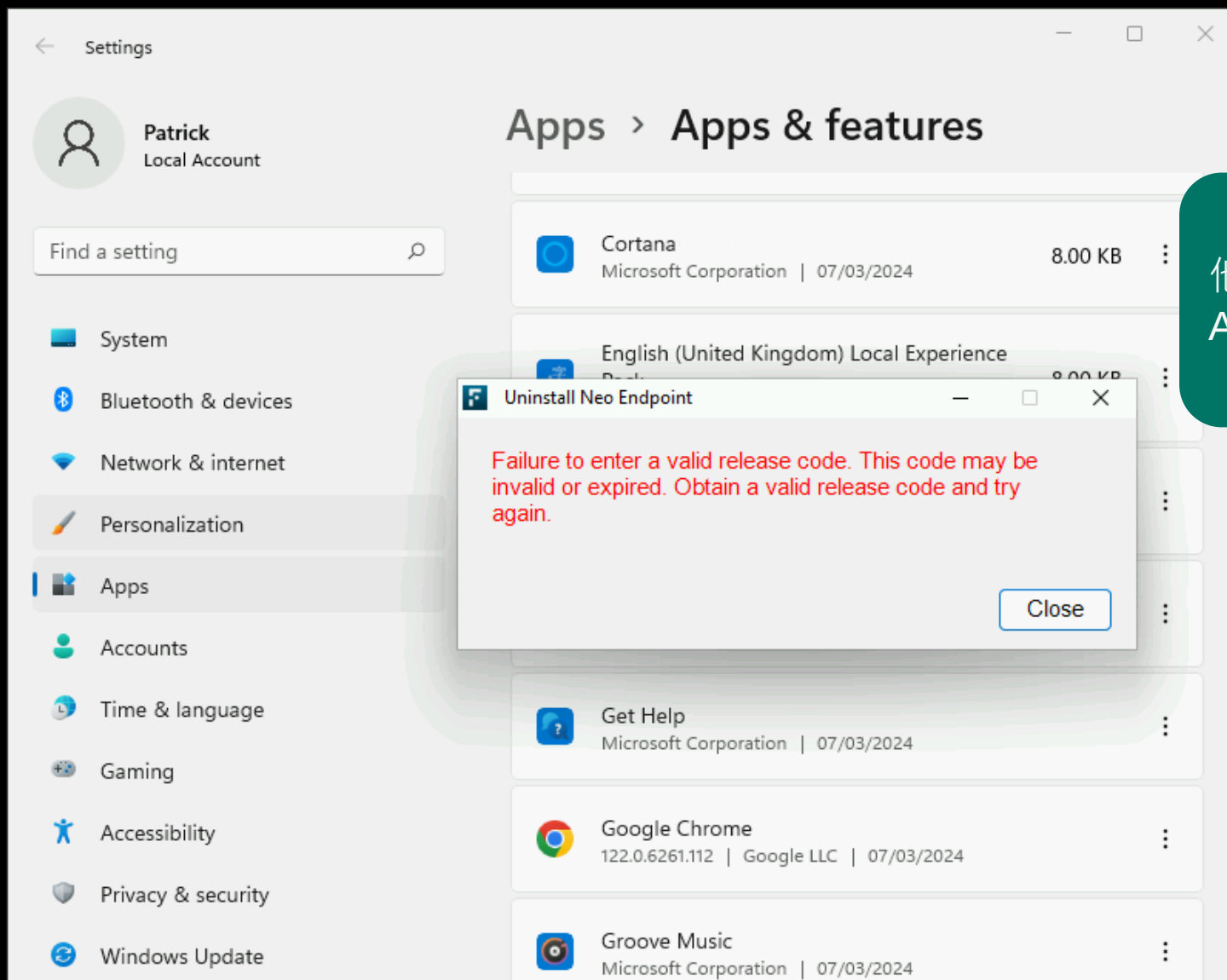
Recycle Bin



Google
Chrome



Microsoft
Edge



他無法移除 Forcepoint
Agent



ENG
INTL



14:10



07/03/2024



Recycle Bin



Google Chrome



Microsoft Edge

Inbox - andypatrick168@gmail.com

コンピで印刷 | 会員登録不要の

hacking tools - Google Search

+

← → ↺

google.com/search?q=hacking+tools&oq=hacking+tools&gs_lcrp=EgZjaHJvbWUyDggAEEUYJxg5GIAEGL

Google

hacking tools

× | 🎤 🔄 🔍

Images

Videos

Products

News

Building

Books

Finance

About 605,000,000 results (0.29 seconds)

Sponsored



SentinelOne

<https://www.sentinelone.com>

Singularity Platform

One Platform — Leading Enterprises Use Singularity To Prevent, Detect, and Respond to Cyber Attacks.

Sponsored



withsecure.com

<https://www.withsecure.com>

Cyber security tools

Essai gratuit de 30 jours — Arrêtez les menaces avancées avec la solution de cybersécurité de WithSecure™ Elements.

Sponsored

他在Google上搜索「駭客工具」



Apps

Network > 192.168.125.195 > Corp_Share > Apps

Name	Date modified	Type	Size
7z2401-x64	03/03/2024 17:19	Application	1,557 KB
ChromeSetup	03/03/2024 17:34	Application	1,345 KB

USB (D:)

USB (D:)

Name	Date modified	Type	Size
ChromeSetup	03/03/2024 17:34	Application	1,345 KB
7z2401-x64	03/03/2024 17:19	Application	1,557 KB

他連接到 公司 Share Folder 並將文件備份到 USB



Recycle Bin



Google Chrome



Microsoft Edge



Japan Data



Tor Browser



Tor Browser

Add to Archive

Archive: C:\Users\Patrick\Desktop\
Japan Data.7z

Archive format: 7z
Compression level: 5 - Normal
Compression method: * LZMA2
Dictionary size: * 16 MB
Word size: * 32
Solid Block size: * 4 GB
Number of CPU threads: * 4 / 4
Memory usage for Compressing: 656 MB / 6554 MB / 8192 MB * 80%
Memory usage for Decompressing: 18 MB
Split to volumes, bytes:
Parameters:

Update mode: Add and replace files
Path mode: Relative pathnames

Options
☐ Create SFX archive
☐ Compress shared files
☐ Delete files after compression

Encryption
Enter password:
Reenter password:
☐ Show Password
Encryption method: AES-256
☐ Encrypt file names

Options

OK Cancel Help

他下載了更多資料並使用
7-Zip透過密碼進行加密





USB (D:)

New ▾

Sort ▾ View ▾

← → ▾ ↑

USB (D:)

Name	Date modified	Type	Size
ChromeSetup	03/03/2024 17:34	Application	1,345 KB
7z2401-x64	03/03/2024 17:19	Application	1,557 KB
Japan Data.7z	07/03/2024 14:30	7Z File	44,987 KB

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- Music
- Videos
- OneDrive
- This PC
- USB (D:)
- USB FLASH (E:)
- Network

3 items

他比平常更頻繁地將資料複製到USB





Recycle Bin



Google
Chrome



Microsoft
Edge



Japan Data



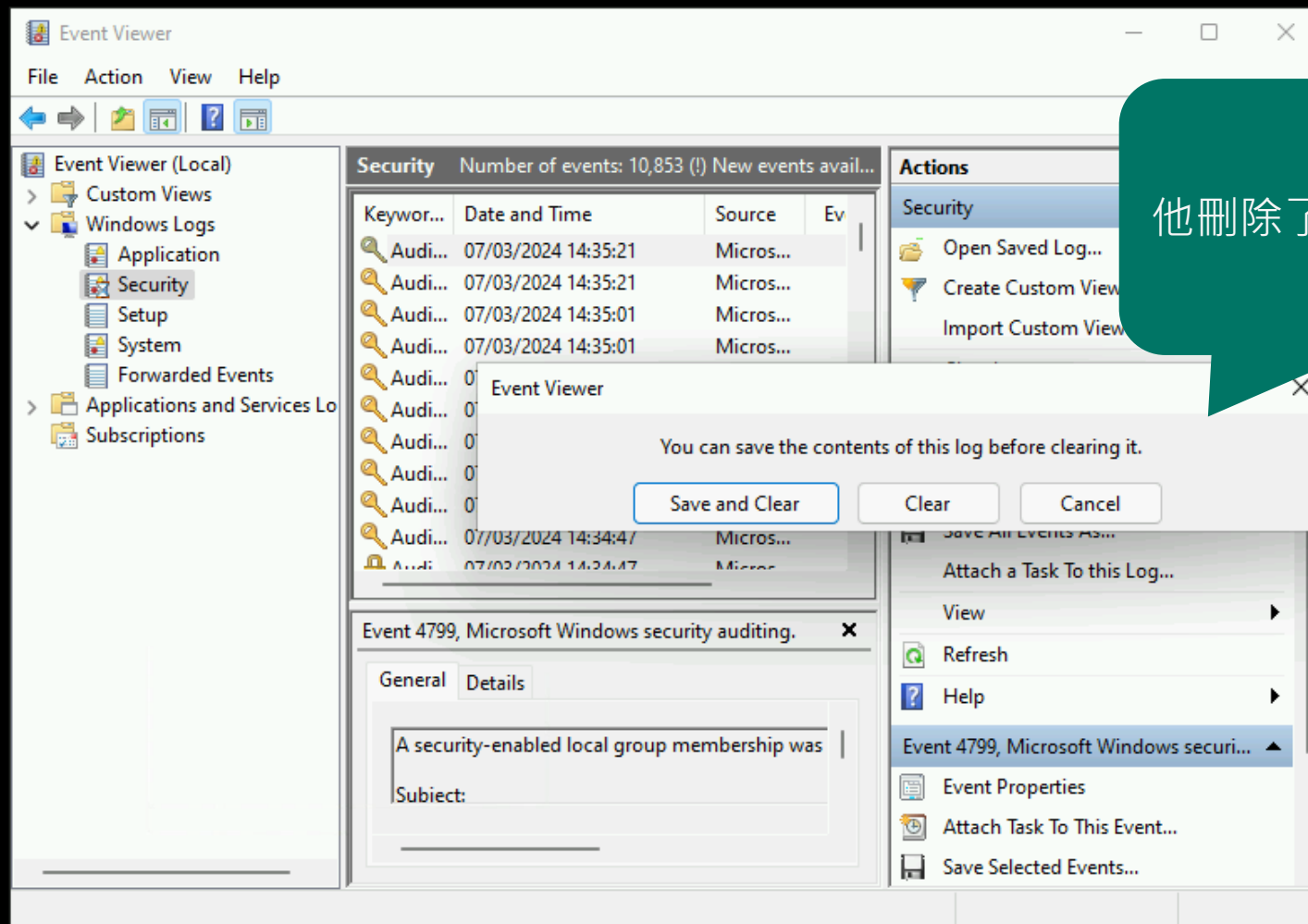
Tor Browser



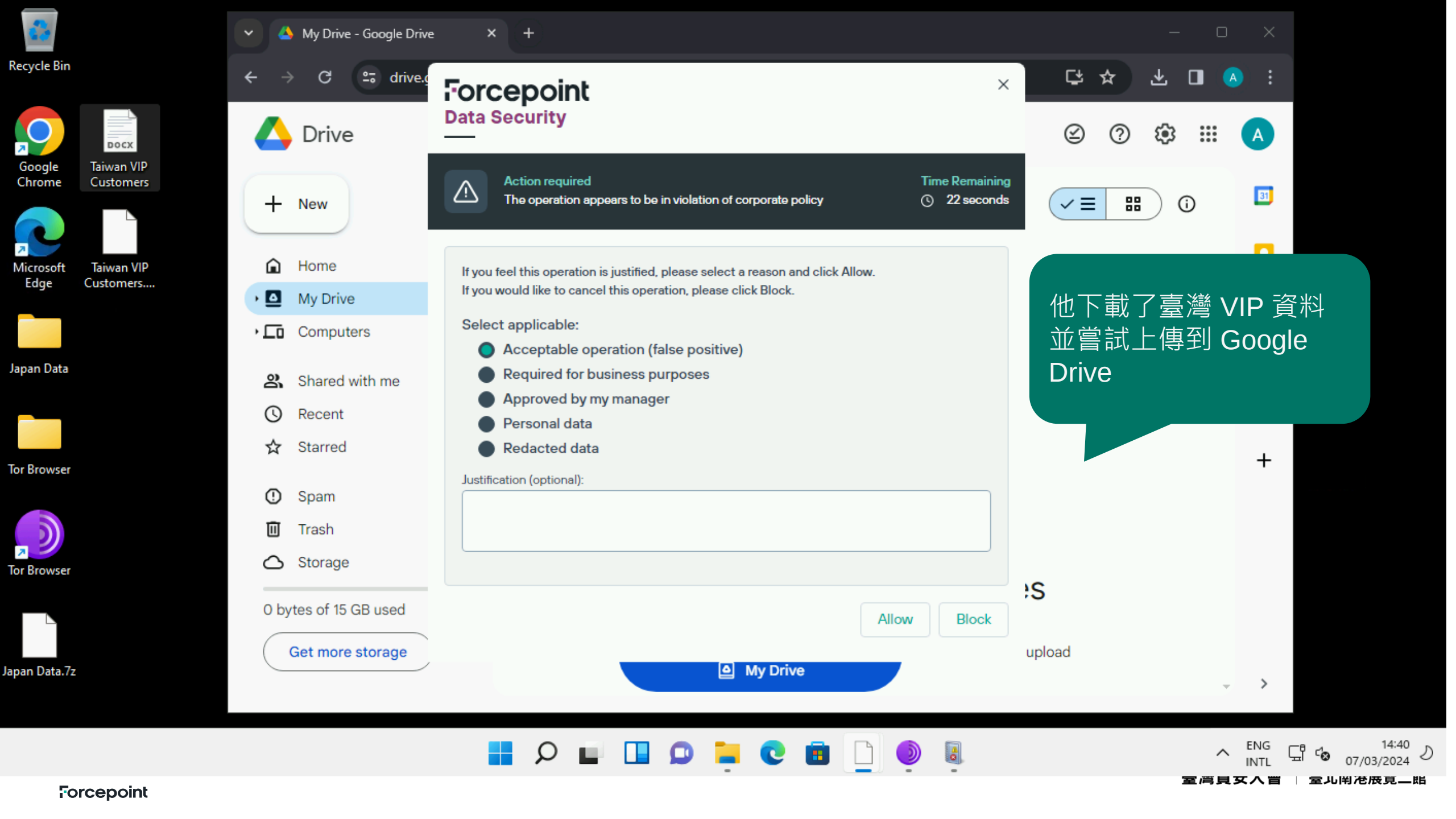
Tor Browser



Japan Data.7z



他刪除了 Windows 事件



Forcepoint
Data Security

Action required
The operation appears to be in violation of corporate policy

Time Remaining
22 seconds

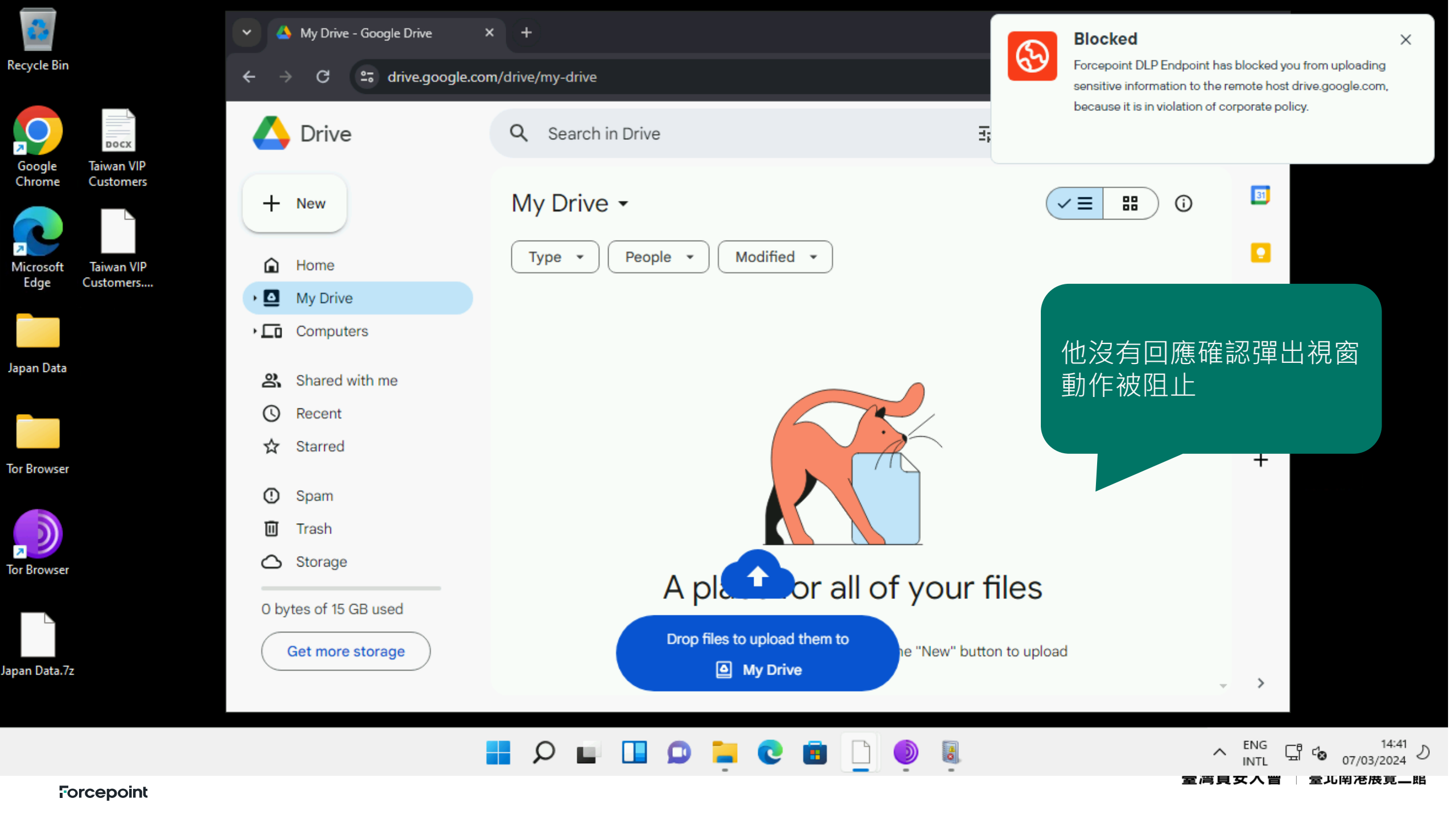
If you feel this operation is justified, please select a reason and click Allow.
If you would like to cancel this operation, please click Block.

Select applicable:

- ☒ Acceptable operation (false positive)
- ☐ Required for business purposes
- ☐ Approved by my manager
- ☐ Personal data
- ☐ Redacted data

Justification (optional):

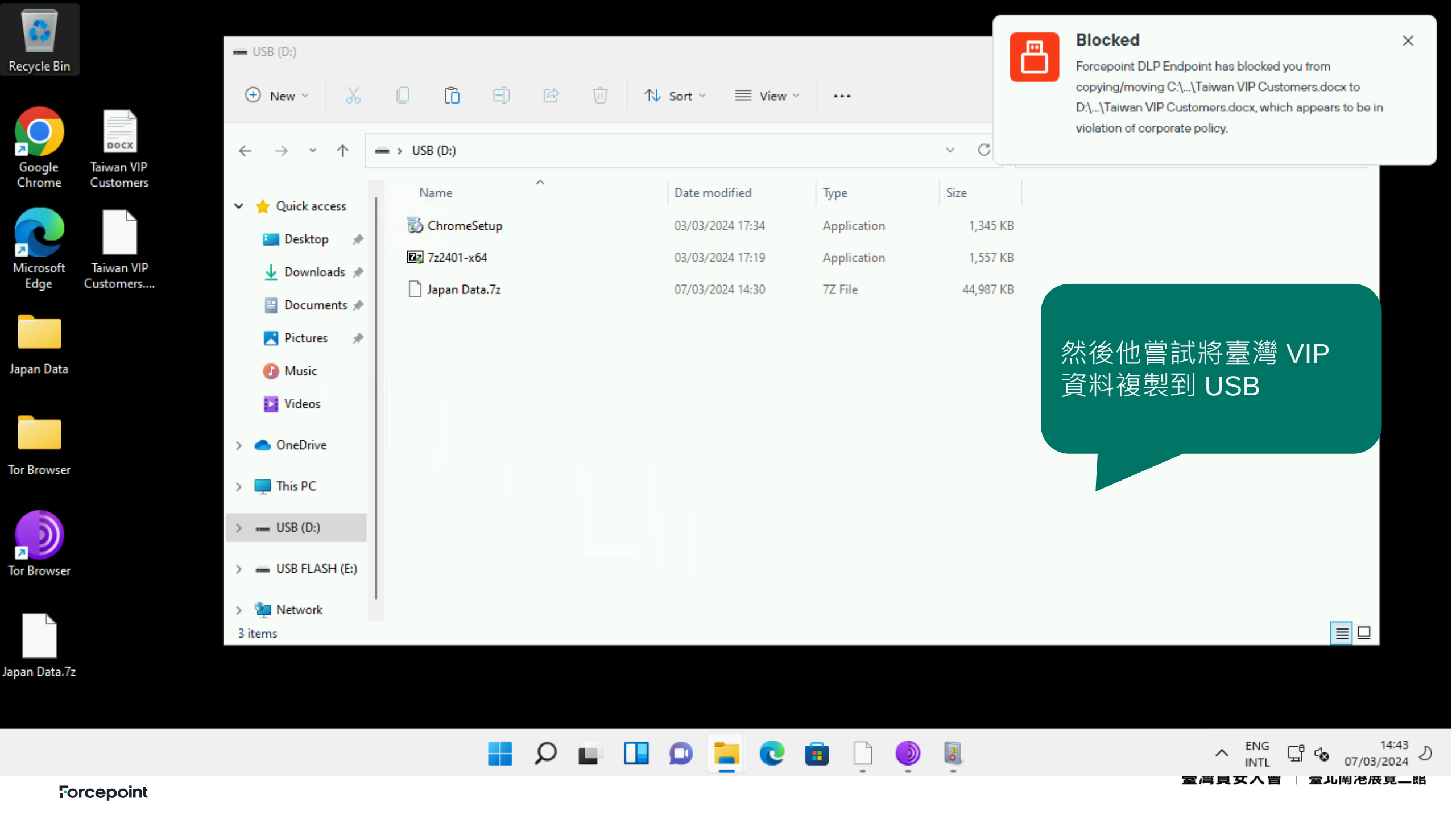
他下載了臺灣 VIP 資料
並嘗試上傳到 Google
Drive



**Blocked**

Forcepoint DLP Endpoint has blocked you from uploading sensitive information to the remote host drive.google.com, because it is in violation of corporate policy.

他沒有回應確認彈出視窗
動作被阻止



Blocked

Forcepoint DLP Endpoint has blocked you from copying/moving C:\...\Taiwan VIP Customers.docx to D:\...\Taiwan VIP Customers.docx, which appears to be in violation of corporate policy.

然後他嘗試將臺灣 VIP
資料複製到 USB

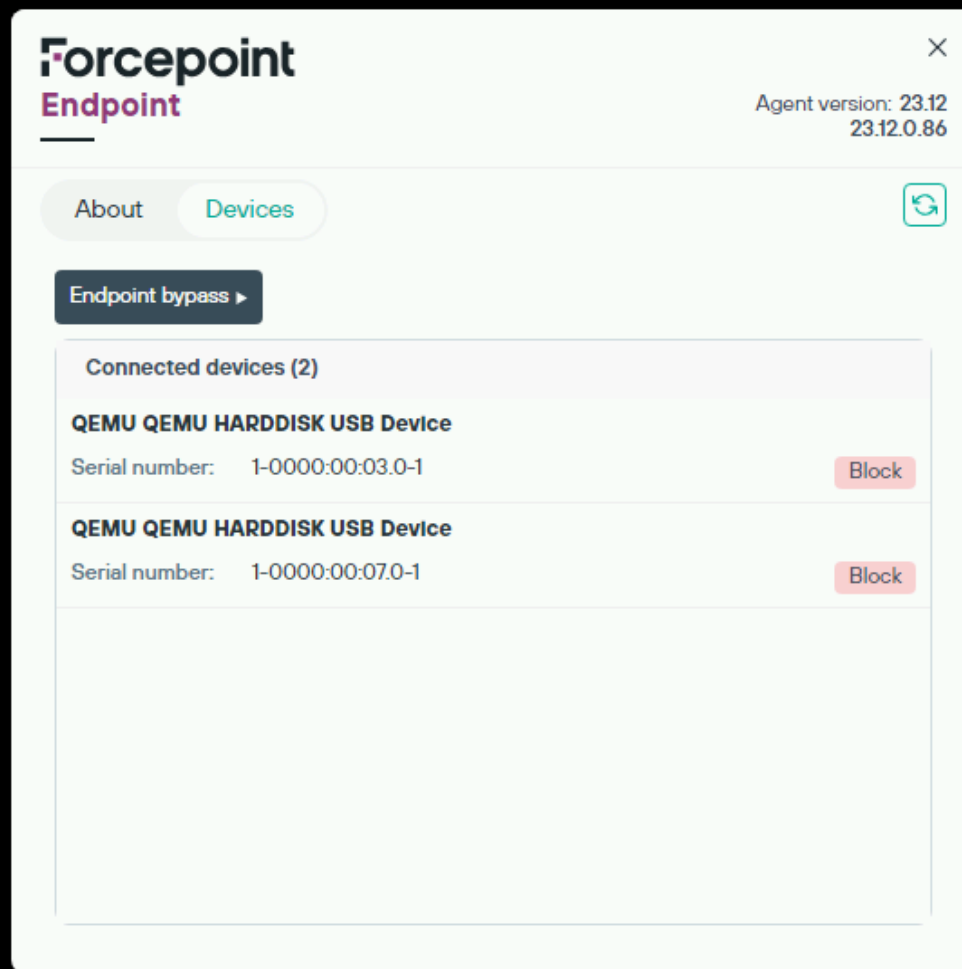
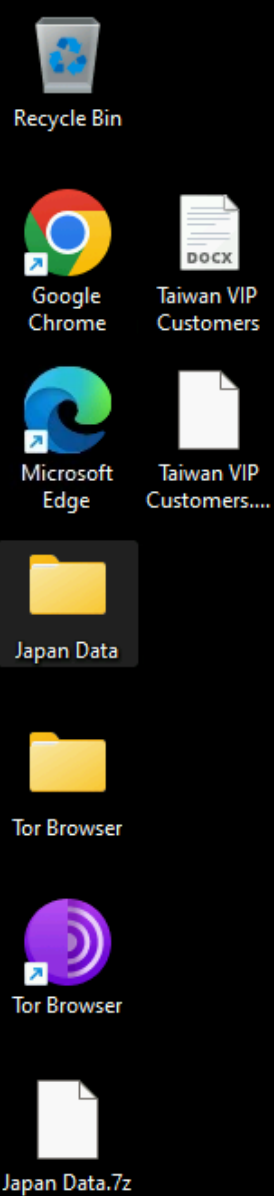


ENG
INTL



14:43
07/03/2024



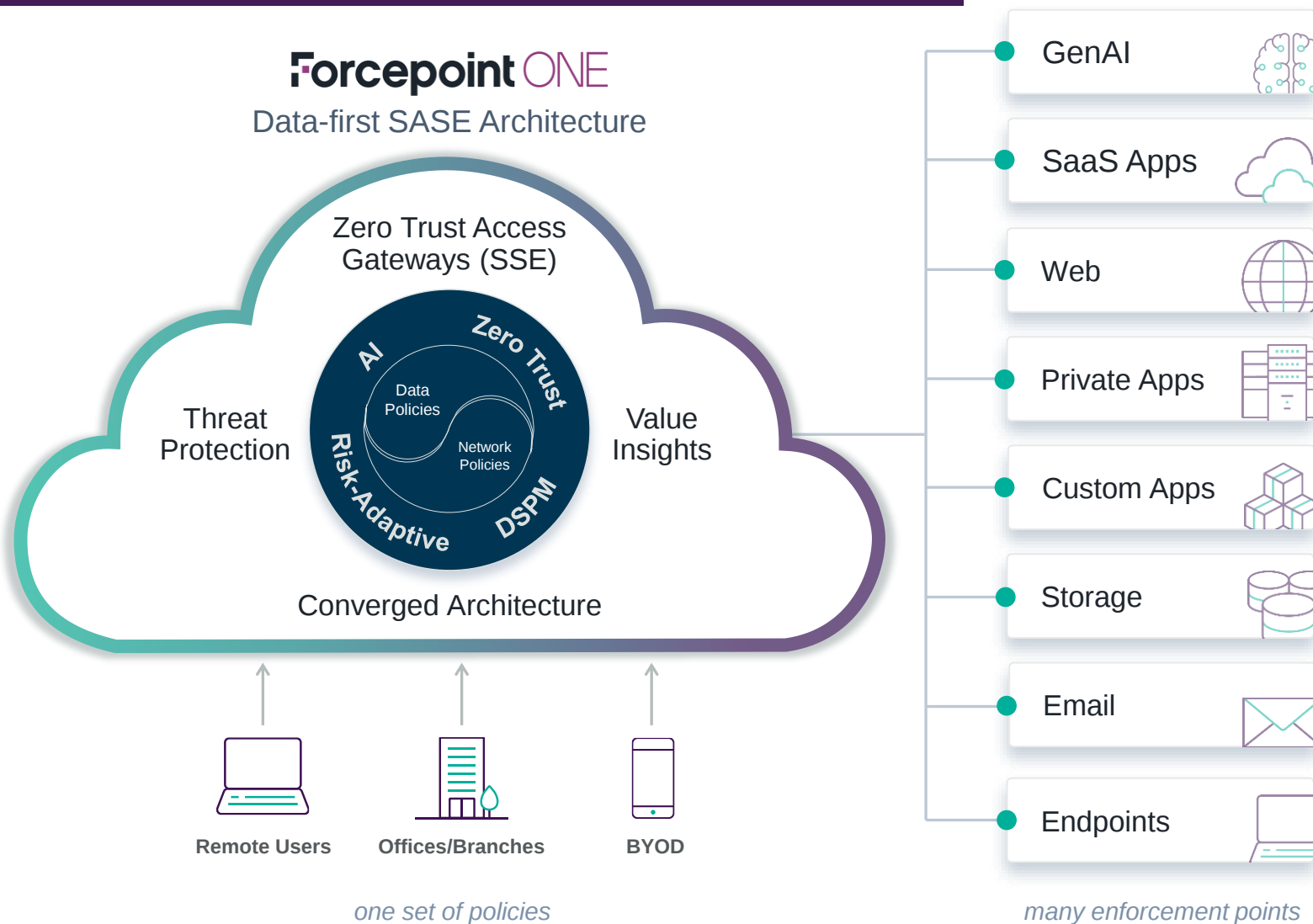


他的USB 裝置被 RAP 更改為 Block



Forcepoint 資料安全無所不在

建立集中管理的資料安全平台



Forcepoint

Data Security Everywhere

Empowering people to work anywhere,
with data everywhere

最經濟高效的雲數據安全方式

- 在雲端和網路中使用現有的DLP策略
- 在現有 FSM 控制台中進行管理
- 統一的政策管理
- 不虛中斷現有端點 DLP

感謝聆聽！！
ray.pai@forcepoint.com

展區攤位 P208

1F 展場平面圖

超級品牌・4單位展攤 2・1單位展攤

