Microsoft Security

AI時代的資安展望：挑戰與創新

吳子強 Vic Wu

台灣微軟 專家技術群總經理

這些是什麼？

Dall-E

GPT-3.5

OpenAI

Chat-4

ChatGPT

Codex

Azure OpenAI Service

Generative AI

2023年1月16日
Azure OpenAI 服務全球上市

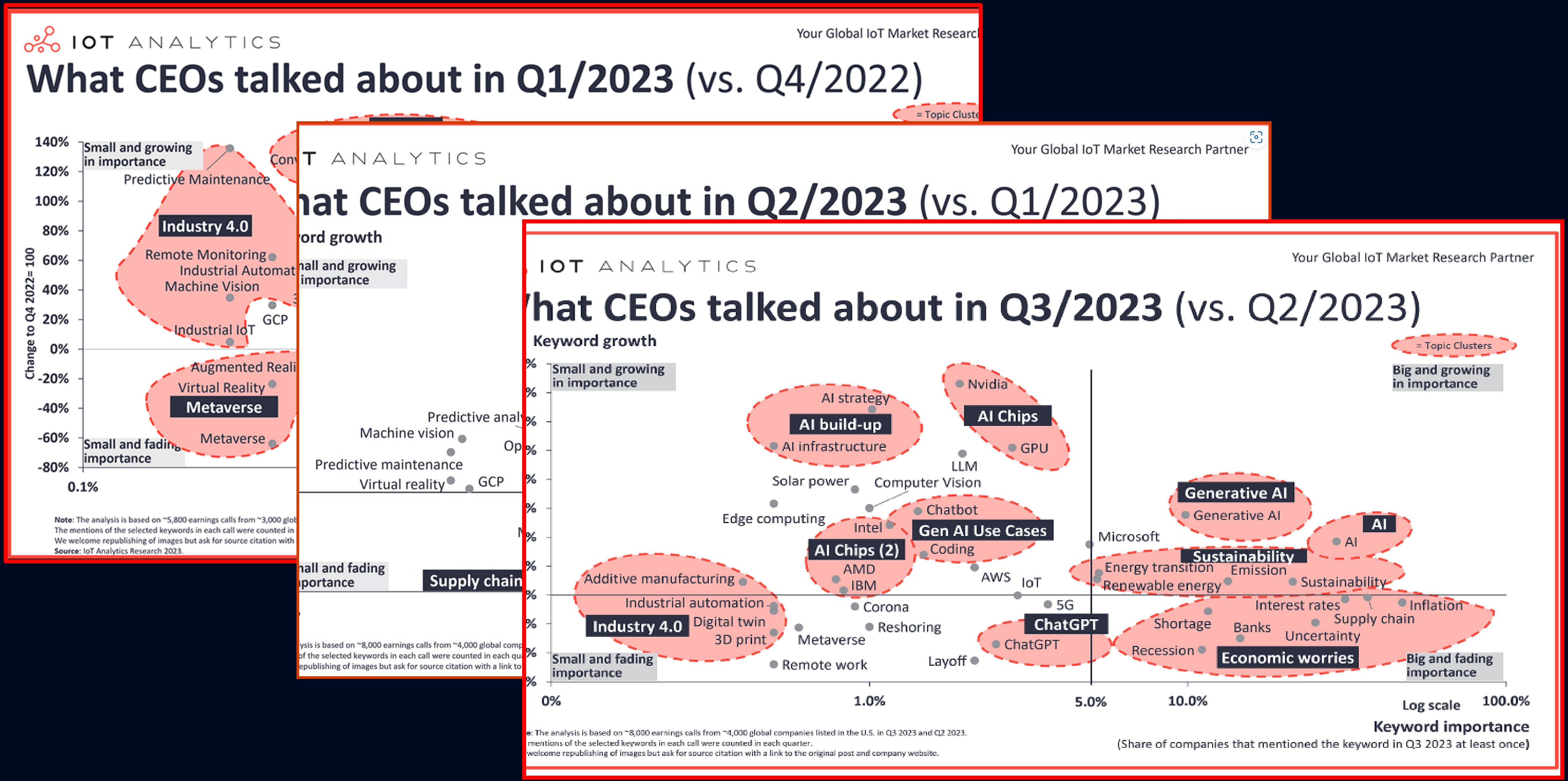
去年此時，
我們正在討論…

「人工智慧搜索是擔任 CEO 九年來公司發生的最重大事件，上一次顛覆性技術是雲端運算出來的時候。」

"It's a new race"

- Satya Nadella, Microsoft CEO
  Feb 8, 2023

2023 全球 4000 大企業財報會議調查
– ChatGPT / GenAI / GenAI Use cases 出現在會議談話中次數驟升



IOT ANALYTICS

Your Global IoT Market Researc

What CEOs talked about in Q1/2023 (vs. Q4/2022)

Note: The analysis is based on ~5,800 earnings calls from ~3,000 glob
The mentions of the selected keywords in each call were counted in
We welcome republishing of images but ask for source citation with
Source: IoT Analytics Research 2023.

T ANALYTICS

Your Global IoT Market Research Partner

hat CEOs talked about in Q2/2023 (vs. Q1/2023)

ord growth

ysis is based on ~8,000 earnings calls from ~4,000 global comp
of the selected keywords in each call were counted in each qu
epublishing of images but ask for source citation with a link to

IOT ANALYTICS

Your Global IoT Market Research Partner

/hat CEOs talked about in Q3/2023 (vs. Q2/2023)

Keyword growth

Keyword importance
(Share of companies that mentioned the keyword in Q3 2023 at least once)

e: The analysis is based on ~8,000 earnings calls from ~4,000 global companies listed in the U.S. in Q3 2023 and Q2 2023.
mentions of the selected keywords in each call were counted in each quarter.
welcome republishing of images but ask for source citation with a link to the original post and company website.

企業領導者怎麼看

65%

的領導者
制定了計畫

75%

的領導者在雲端建立所有未來的新產品和功能

82%

相信AI
將提升表現與效能

變動中的經濟情勢[1]

加速科技創新[2]

開啟新機遇[3]

1. IDC Whitepaper - How Public Cloud Strategies Help Companies Navigate Market Uncertainty
2. State of Cloud | Pluralsight
3. US AI Institute State of AI, 5th Edition (deloitte.com)

組織怎麼看

91% 的組織已將雲端納入策略中 [1]

79% 的組織將資安列為他們在雲端面臨的主要挑戰之一 [2]

87% 認為 AI 將帶來競爭優勢 [3]

1. IDC Whitepaper - How Public Cloud Strategies Help Companies Navigate Market Uncertainty
2. Flexera 2023 State of the Cloud | Report
3. MIT Sloan Management Review

員工怎麼看

64%

員工需要更多時間和精力來完成他們的工作

3.5X

在策略思考方面遇到困難

70%

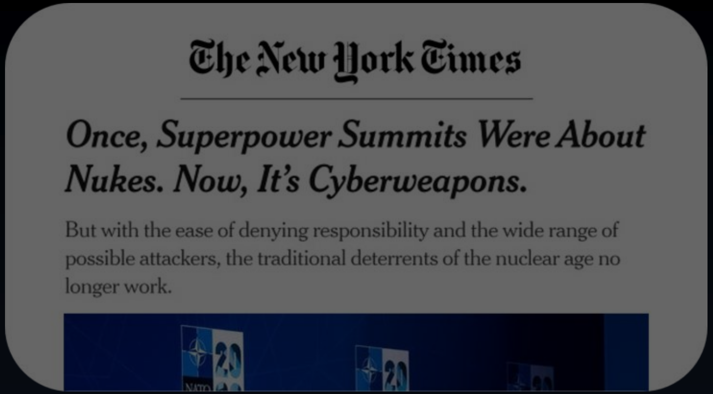
員工願意將工作委託給**AI**

2X

管理者正在考慮利用**AI**來提升生產力

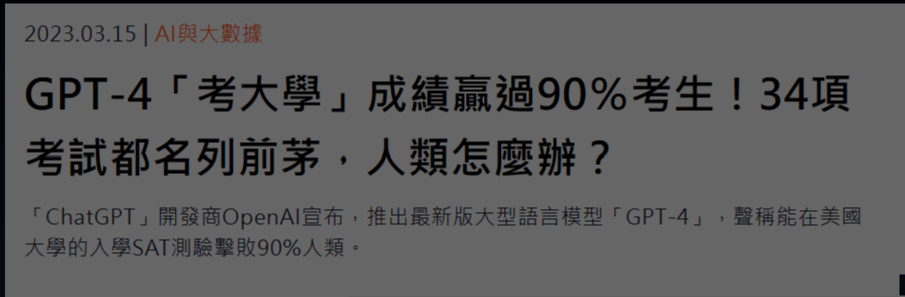
Source: 2023 Work Trends Index

AI 未來，已來
資安是我們這個時代的關鍵挑戰


The New York Times

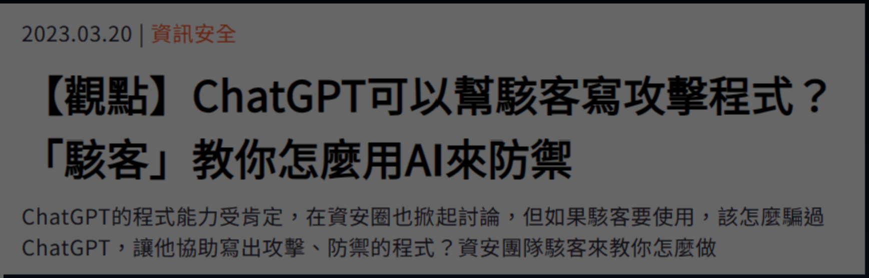
Once, Superpower Summits Were About Nukes. Now, It's Cyberweapons.

But with the ease of denying responsibility and the wide range of possible attackers, the traditional deterrents of the nuclear age no longer work.


2023.03.15 | AI與大數據

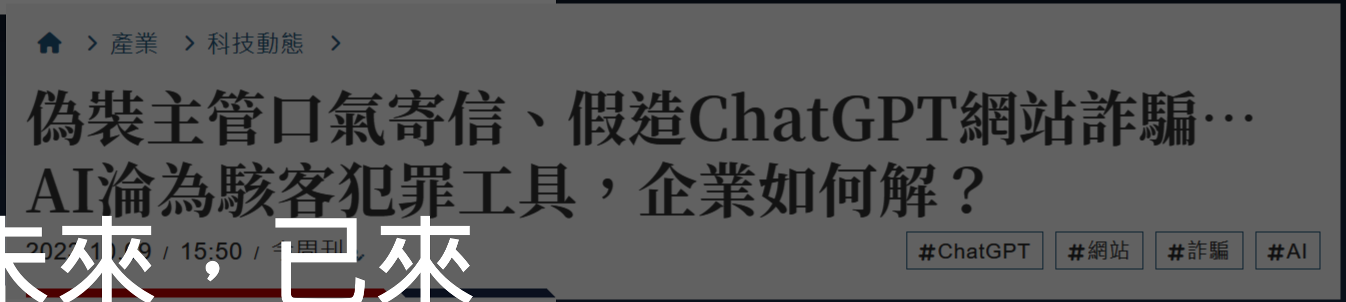
GPT-4「考大學」成績贏過90%考生！34項考試都名列前茅，人類怎麼辦？

「ChatGPT」開發商OpenAI宣布，推出最新版大型語言模型「GPT-4」，聲稱能在美國大學的入學SAT測驗擊敗90%人類。


2023.03.20 | 資訊安全

【觀點】ChatGPT可以幫駭客寫攻擊程式？「駭客」教你怎麼用AI來防禦

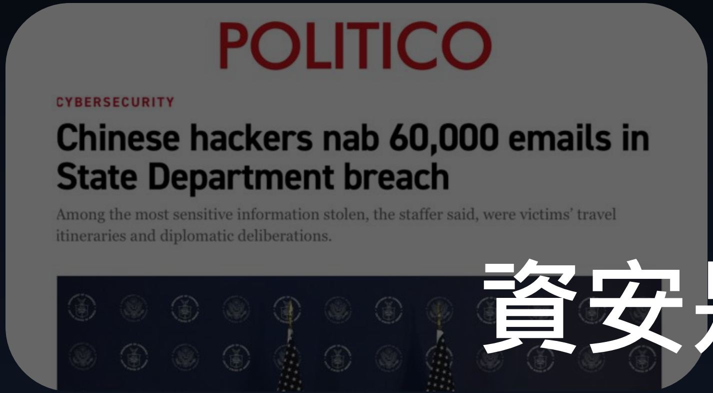
ChatGPT的程式能力受肯定，在資安圈也掀起討論，但如果駭客要使用，該怎麼騙過ChatGPT，讓他協助寫出攻擊、防禦的程式？資安團隊駭客來教你怎麼做


› 產業 › 科技動態 ›

偽裝主管口氣寄信、假造ChatGPT網站詐騙…AI淪為駭客犯罪工具，企業如何解？

15:50

#ChatGPT #網站 #詐騙 #AI


POLITICO

CYBERSECURITY

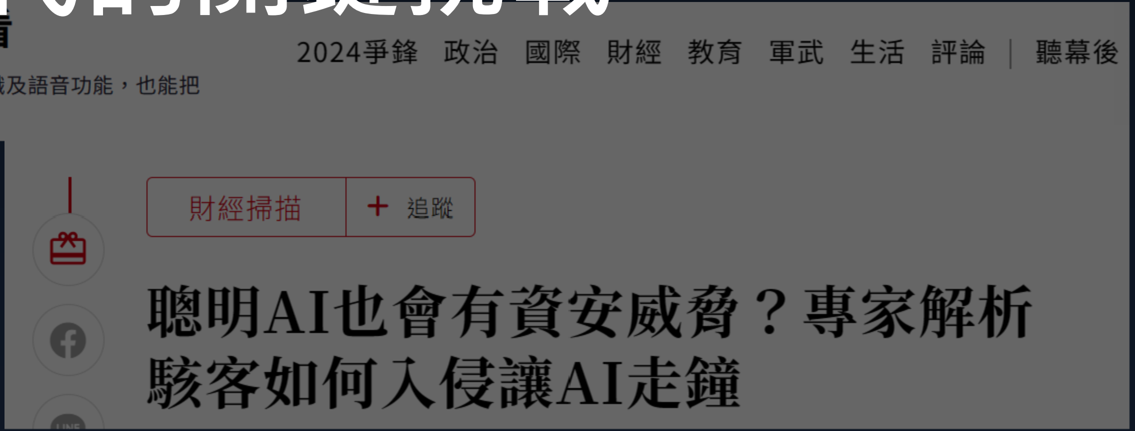
Chinese hackers nab 60,000 emails in State Department breach

Among the most sensitive information stolen, the staffer said, were victims' travel itineraries and diplomatic deliberations.

2023.09.28 | AI與大數據

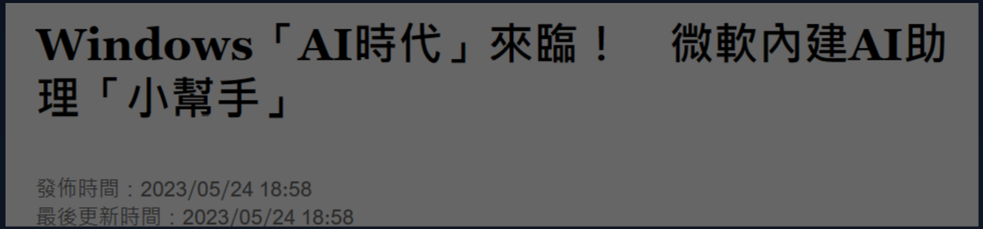
翻譯podcast，重磅更新一次看

ChatGPT重大更新！OpenAI宣布，ChatGPT將支援圖像辨識及語音功能，也能把podcast轉成其他語言，未來兩周內率先提供付費用戶體驗。

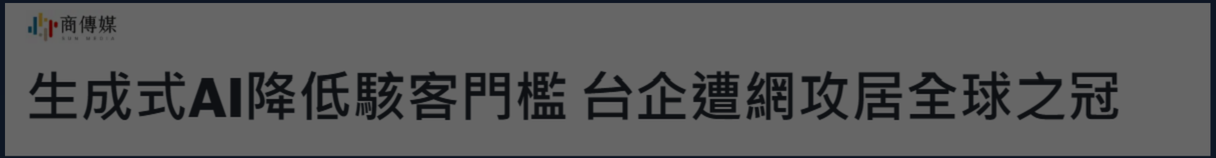

2024爭鋒 政治 國際 財經 教育 軍武 生活 評論 | 聽幕後

財經掃描 ＋ 追蹤

聰明AI也會有資安威脅？專家解析駭客如何入侵讓AI走鐘

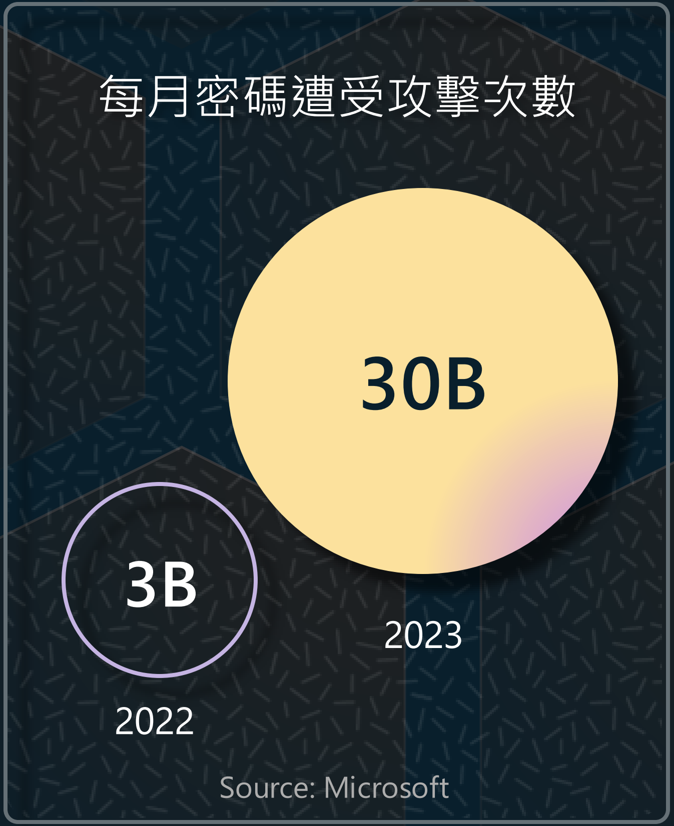

Windows「AI時代」來臨！　微軟內建AI助理「小幫手」

發佈時間：2023/05/24 18:58
最後更新時間：2023/05/24 18:58

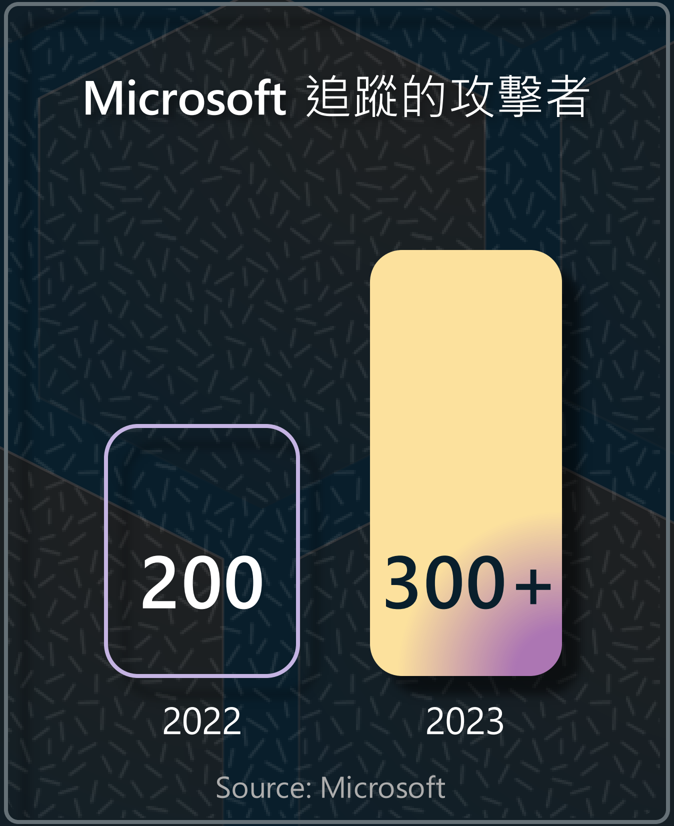

商傳媒

生成式AI降低駭客門檻 台企遭網攻居全球之冠

網路攻擊的複雜性、速度和規模都與日俱增

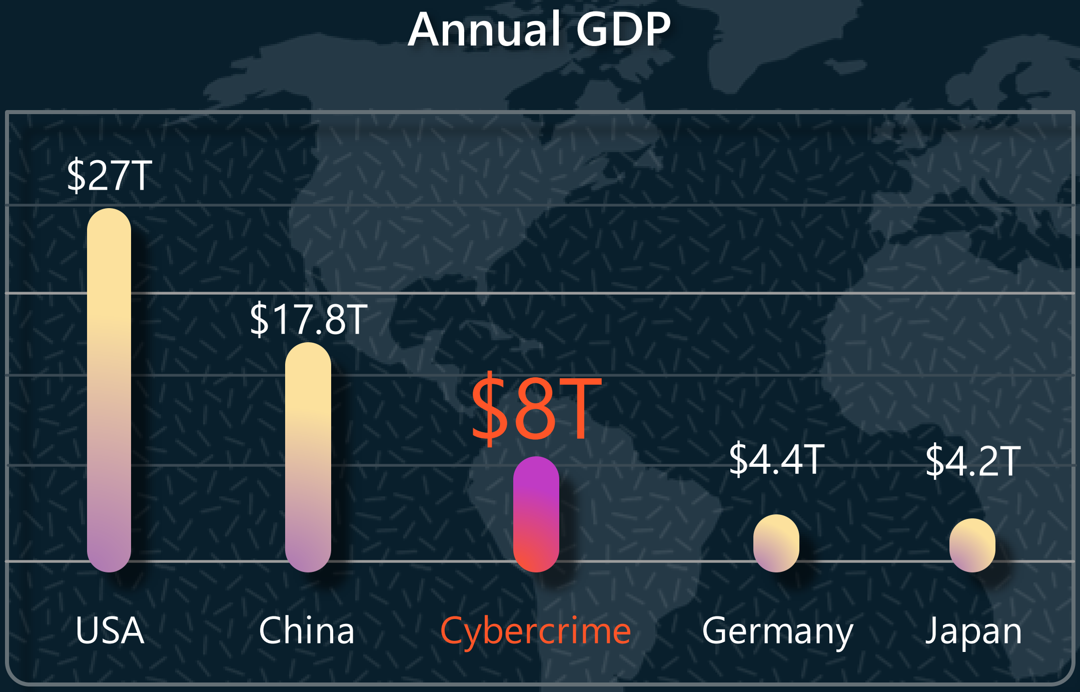


Source: Microsoft

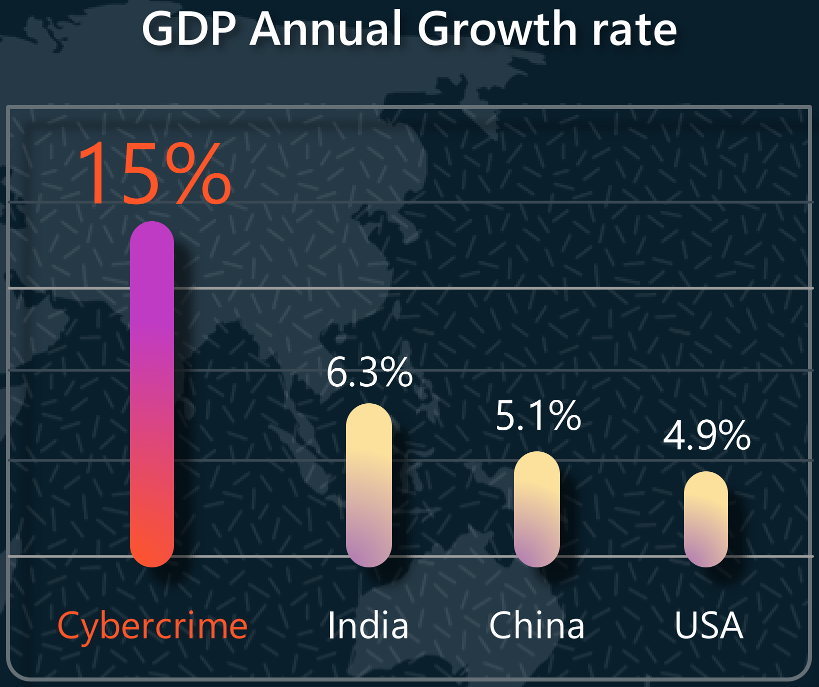


Source: Microsoft

如今，網路犯罪已成為世界第三大經濟體，並且增長迅速



Source: Statistica



Source: Statistica

資安營運複雜性也在增加

80

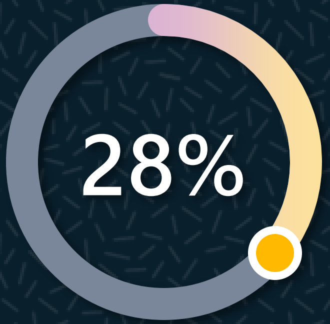
組織平均使用
80種資安工具

Source: Microsoft

3.4M

全球欠缺資安人才

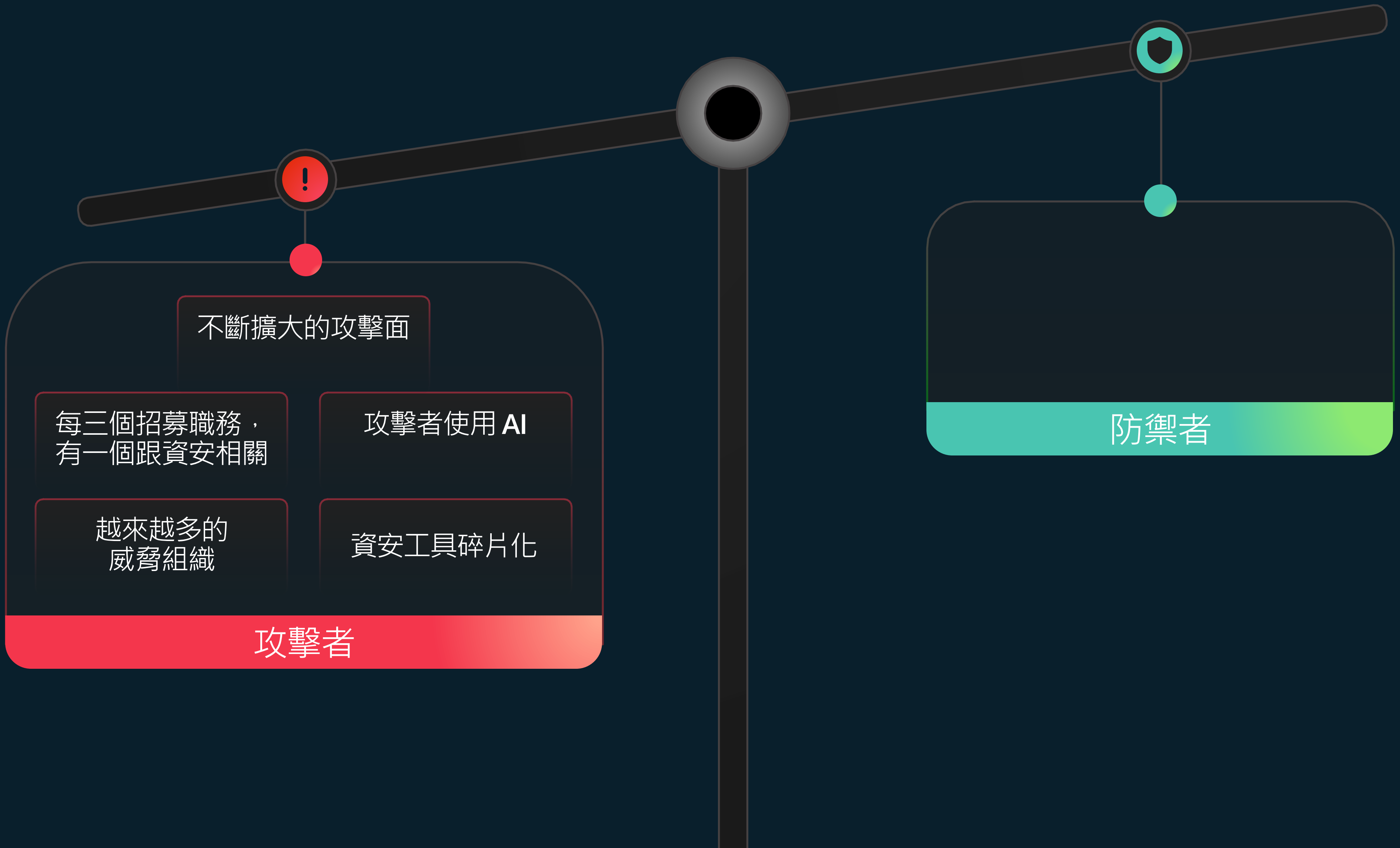
Source: (ISC)^2



企業領導者擔心
由於不當使用人工智慧
造成機敏資訊或IP外洩

Source: IDC

攻擊者具有不對稱優勢



不斷擴大的攻擊面

每三個招募職務，有一個跟資安相關

攻擊者使用 AI

越來越多的威脅組織

資安工具碎片化

攻擊者

防禦者

Microsoft 的優勢

大規模情資和威脅情報

最全面、整合的端到端保護

產業領先的
負責任且安全的 AI

數據和威脅情報

Microsoft 比任何人都更了解攻擊者的行為

78兆

每天偵測到的安全情資

1 萬名

資安和威脅情報專家

1 百萬名

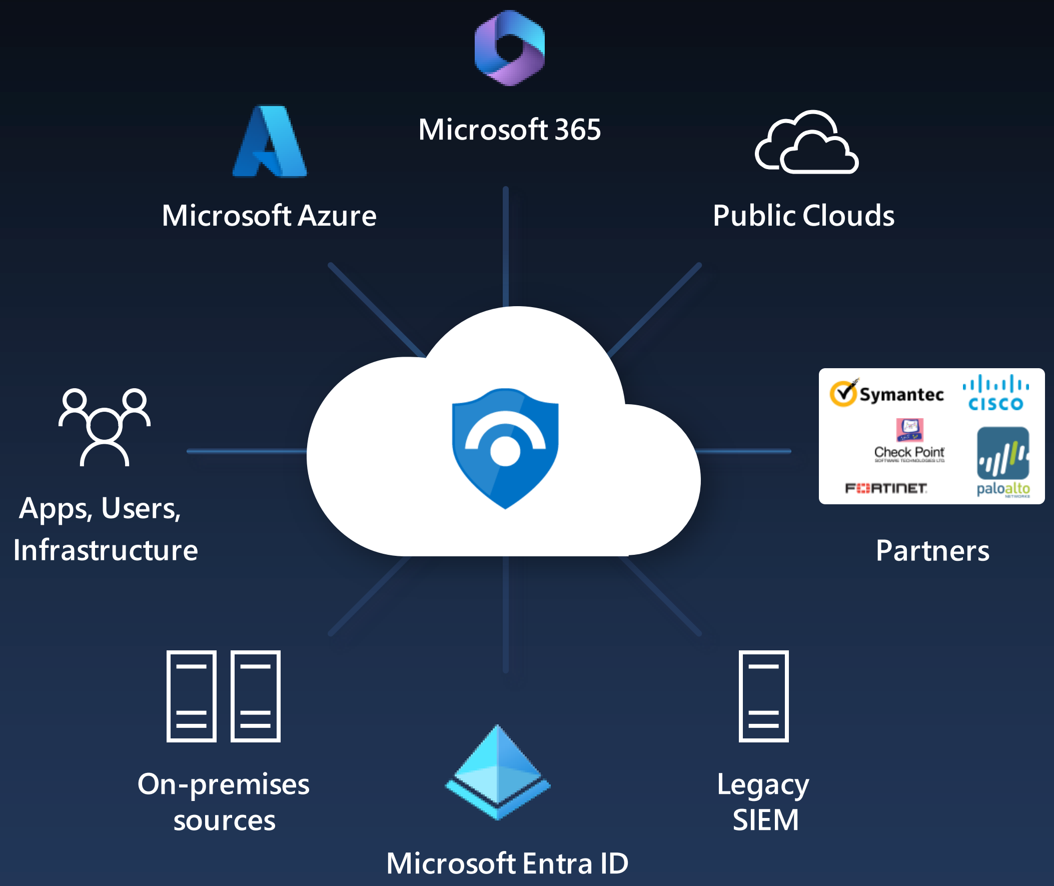
Microsoft 資安用戶

1 萬 5 千個

合作夥伴

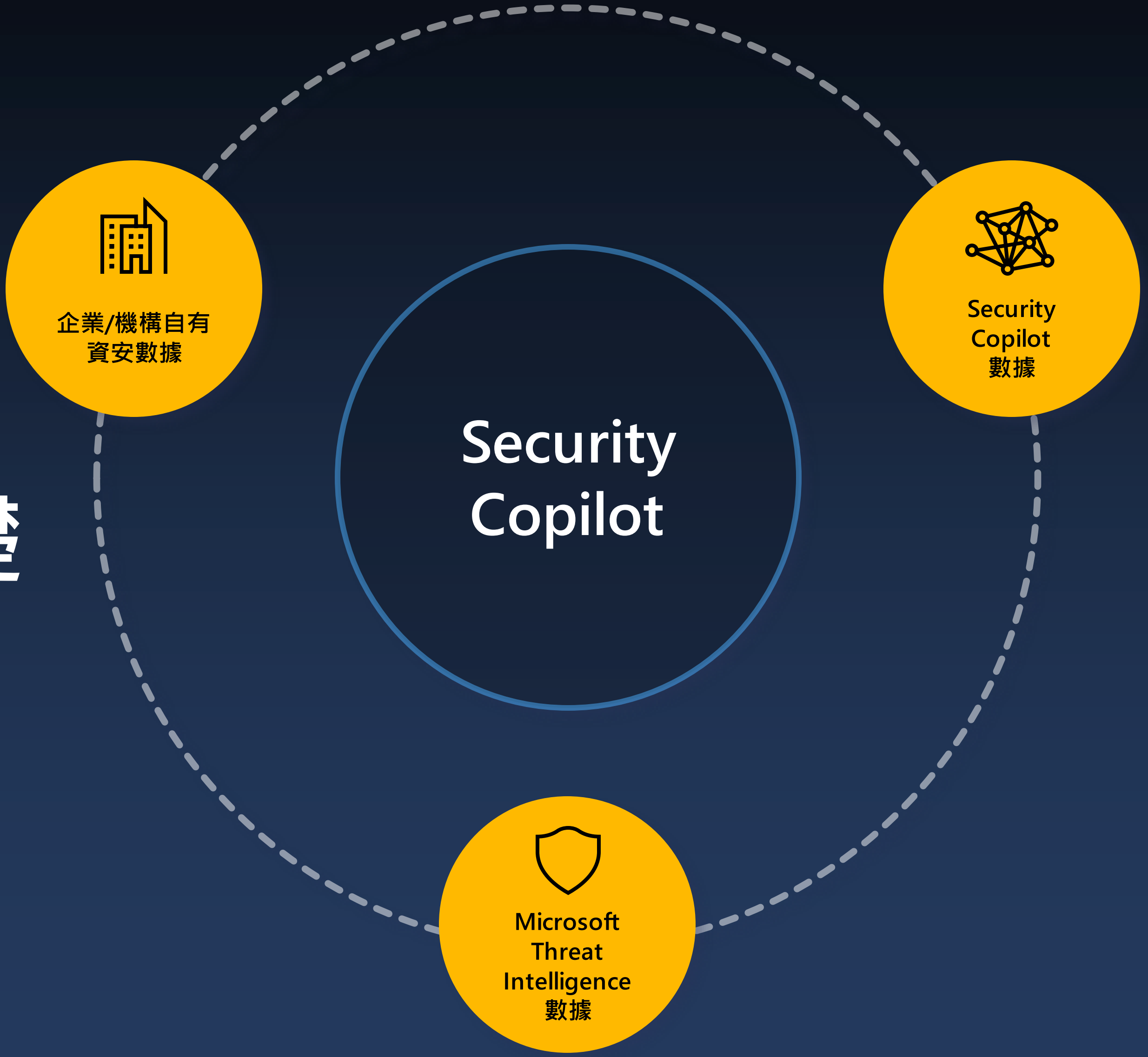
AI 應用在資安的優勢

- 效率：優先順序和自動化
- 速度：能夠即時瞭解特殊的威脅
- 規模：能夠處理大量數據



Microsoft Sentinel 平臺具有每天超過 10 PB 的擷取量

由組織內獨有的
資安數據作為分析基礎



在企業級資安環境下 透過 AI 助力企業增強防禦

資安分析師使用 **Copilot for Security** 之後...

速度提升

22%

資安分析師使用 **Copilot for Security** 之後...

準確性提高

7%

體驗過 **Copilot for Security** 的資安分析師中

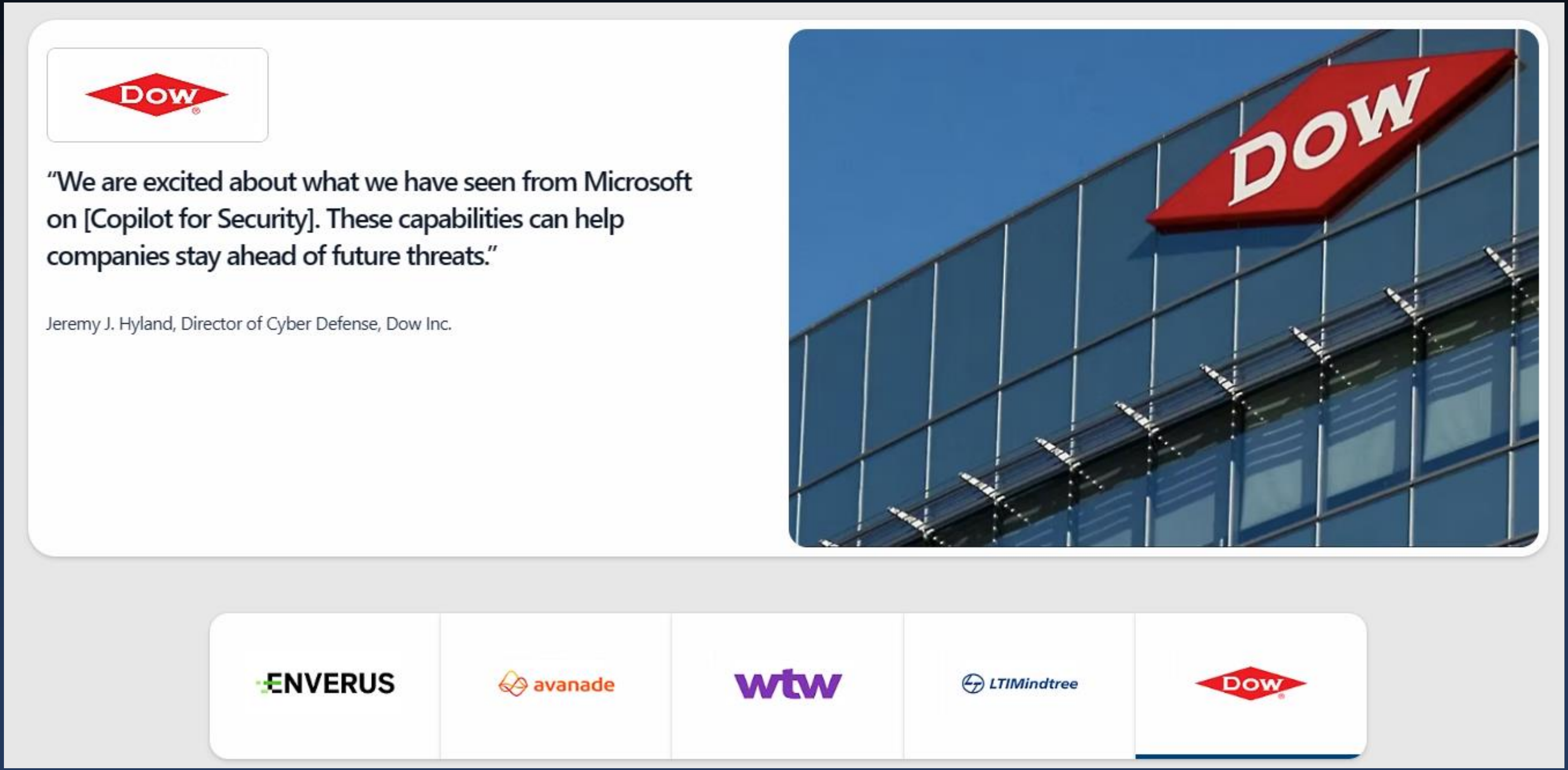
97%

表示他們未來會想要持續使用

Copilot for Security 已於4月1日正式推出

Source: Microsoft Copilot for Security randomized controlled trial (RCT) with experienced security analysts conducted by Microsoft Office of the Chief Economist, January 2024

早期採用 Copilot for Security 的客戶反饋



"We are excited about what we have seen from Microsoft on [Copilot for Security]. These capabilities can help companies stay ahead of future threats."

Jeremy J. Hyland, Director of Cyber Defense, Dow Inc.

隨著 AI 發展，機敏資料保護的重要性更加提升

影子 **AI** 的興起

58%

的組織擔心缺乏對未經批准使用
生成式人工智慧的可視性。

缺乏控制措施來保護 **AI** 共享的數據

43%

的組織表示，缺乏檢測和降低人工
智慧風險的控制措施是首要問題.[2]

監管複雜度增加

“By
2027

至少有一家全球性公司將因不遵守資料
保護或人工智慧治理法規而被監管機構
禁止其人工智慧導入。[3]

1. PRNews wire, portal 26 report, Nov 2023
2. Survey of 658 data security professions, Mar 2023, commissioned by Microsoft
3. Gartner® *Security Leader's Guide to Data Security*, Andrew Bales, Sep 2023. *GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.*

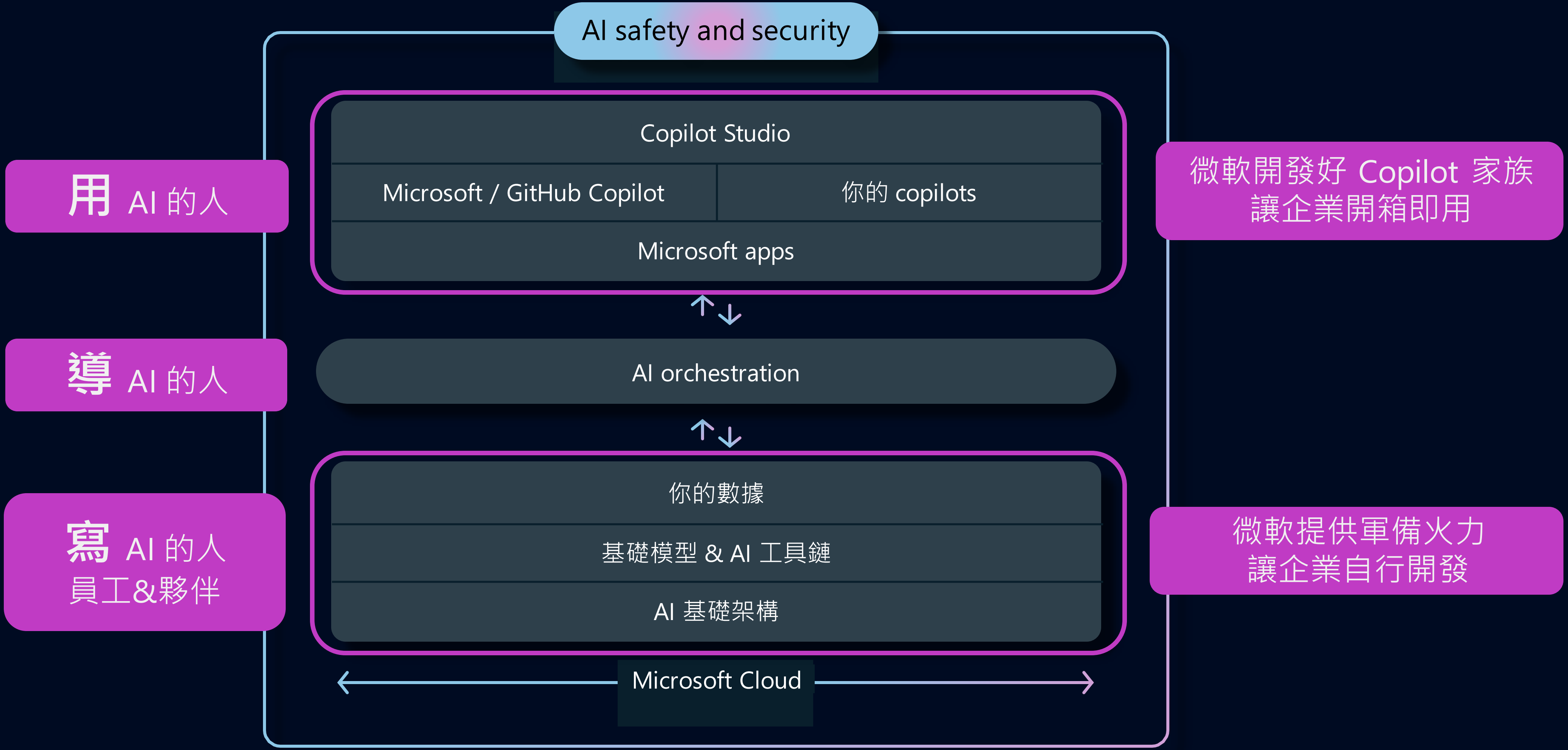
確保生成式 AI 的使用安全

瞭解 AI 的使用

保護 AI 使用或生成的資料

AI 治理

微軟提供完整平台，資安至上



AI safety and security

Copilot Studio

Microsoft / GitHub Copilot

你的 copilots

Microsoft apps

AI orchestration

你的數據

基礎模型 & AI 工具鏈

AI 基礎架構

Microsoft Cloud

用 AI 的人

導 AI 的人

寫 AI 的人
員工&夥伴

微軟開發好 Copilot 家族
讓企業開箱即用

微軟提供軍備火力
讓企業自行開發

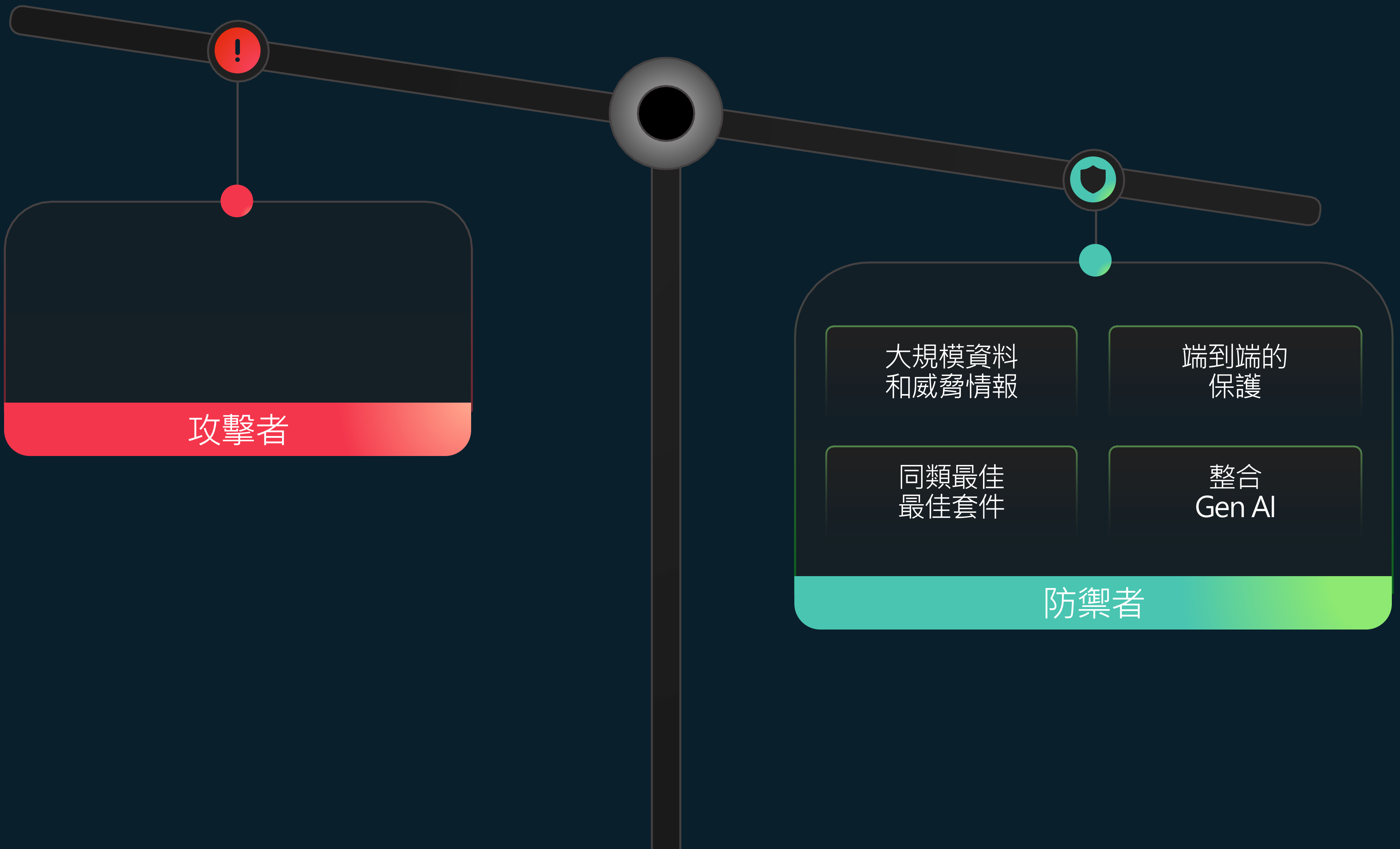
安全未來倡議：資安至上

Culture, governance, accountability

Highest urgency and expansion of scope

New operating model and processes

Microsoft 協助您將天秤向防禦者的方向傾斜



攻擊者

大規模資料
和威脅情報

端到端的
保護

同類最佳
最佳套件

整合
Gen AI

防禦者

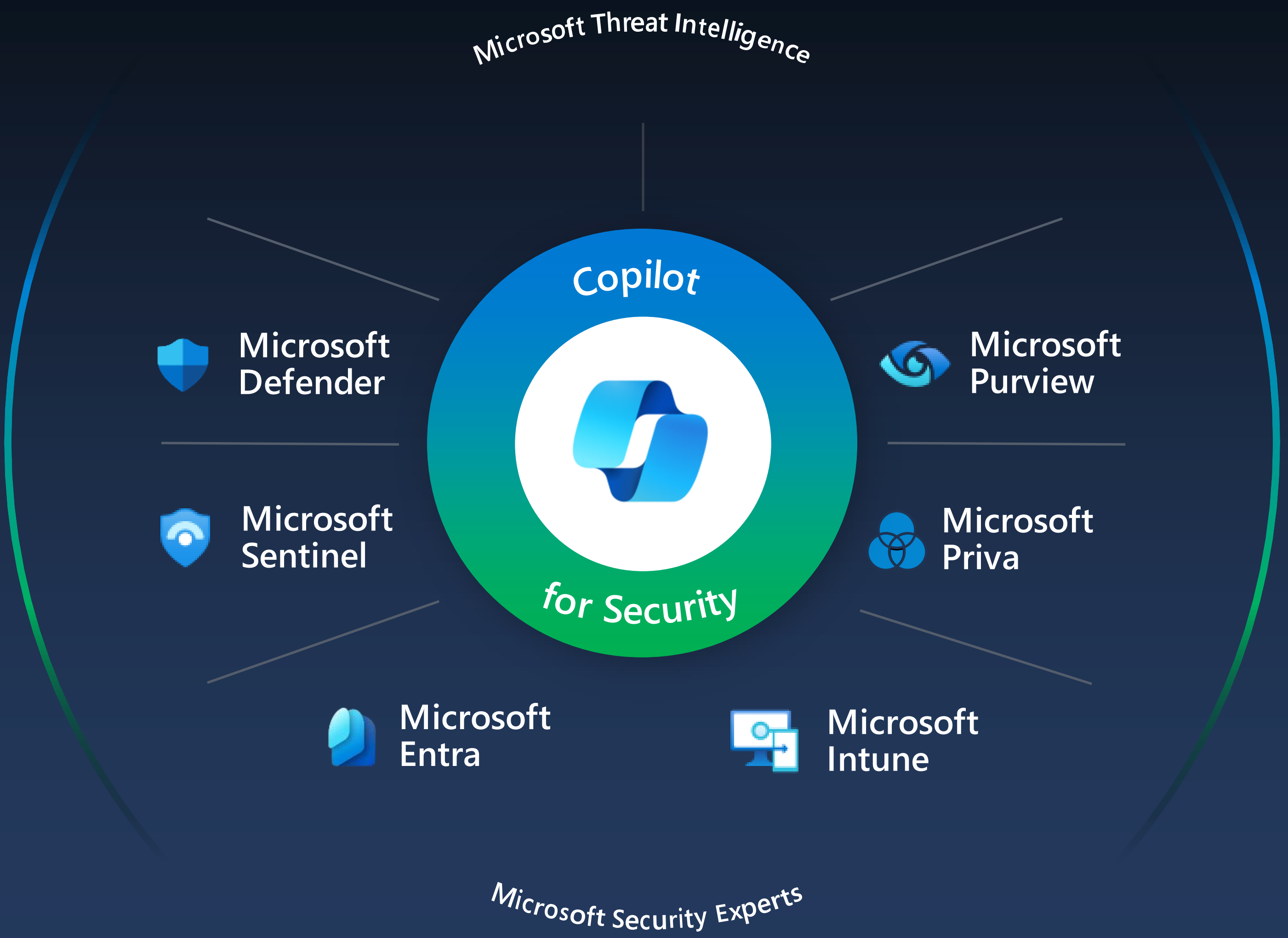
Microsoft 提供完整端到端的安全

跨雲

Cloud platforms

跨平台

Device OSs



微軟資安合作夥伴生態體系

Microsoft Security Service Partner – Modern Soc

eDC.

LOGICALIS
Architects of Change

更多微軟資安合作夥伴

AEB 宏碁資訊

精誠軟體服務
SYSTEX Software & Service

uniXecure

遠傳 FET

iTOP

中華資安國際
CHT Security

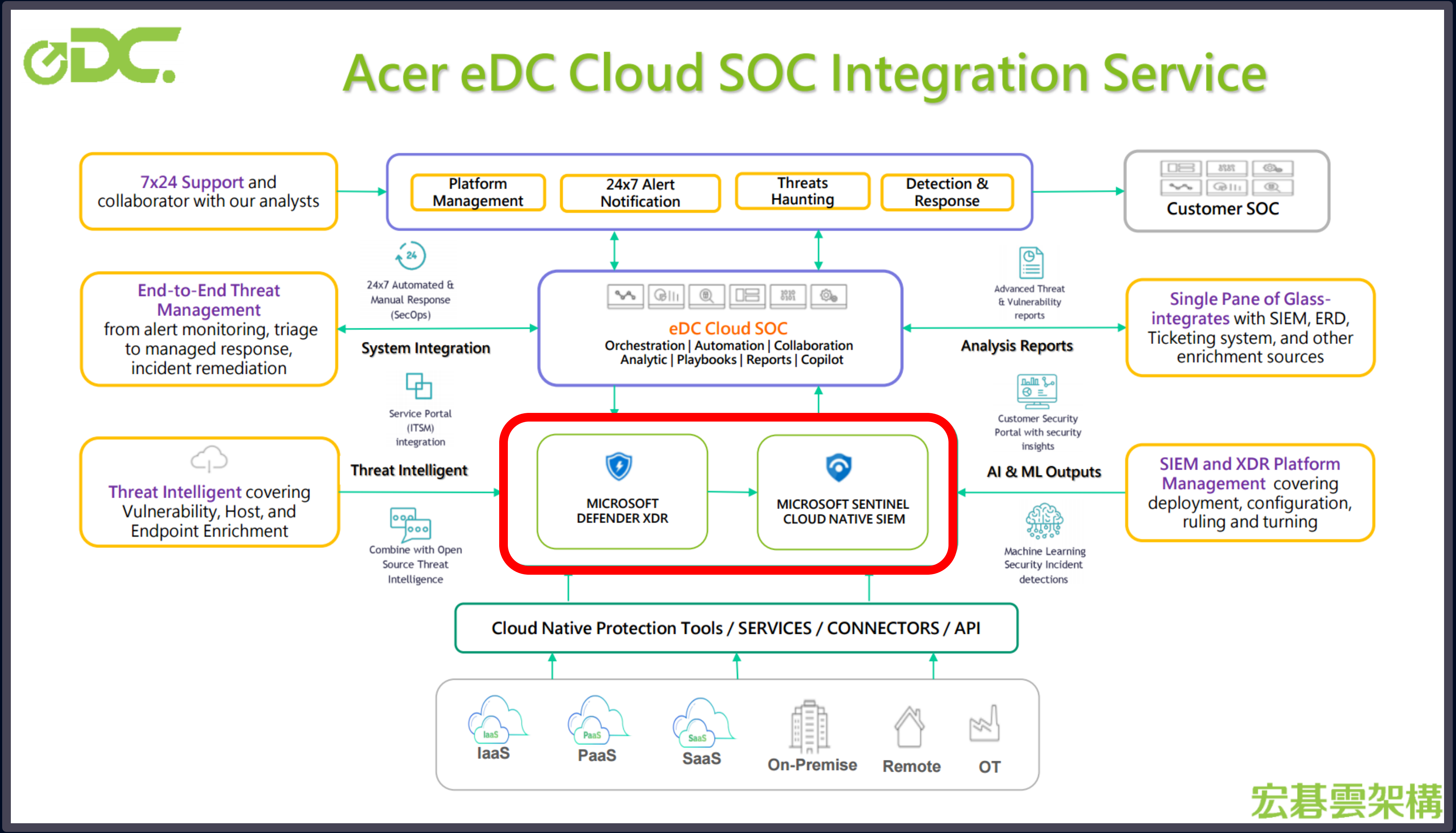
FREEDOM
SYSTEMS

eCloud
valley

中芯數據
Core Cloud Tech.

⋮

微軟資安合作夥伴生態體系



Acer eDC Cloud SOC Integration Service

7x24 Support and collaborator with our analysts

Platform Management | 24x7 Alert Notification | Threats Haunting | Detection & Response

Customer SOC

24x7 Automated & Manual Response (SecOps)

End-to-End Threat Management from alert monitoring, triage to managed response, incident remediation

System Integration

eDC Cloud SOC
Orchestration | Automation | Collaboration
Analytic | Playbooks | Reports | Copilot

Advanced Threat & Vulnerability reports

Analysis Reports

Single Pane of Glass-integrates with SIEM, ERD, Ticketing system, and other enrichment sources

Service Portal (ITSM) integration

Threat Intelligent

Threat Intelligent covering Vulnerability, Host, and Endpoint Enrichment

Combine with Open Source Threat Intelligence

MICROSOFT DEFENDER XDR

MICROSOFT SENTINEL CLOUD NATIVE SIEM

Customer Security Portal with security insights

AI & ML Outputs

SIEM and XDR Platform Management covering deployment, configuration, ruling and turning

Machine Learning Security Incident detections

Cloud Native Protection Tools / SERVICES / CONNECTORS / API

宏碁雲架構

安全性、合規性、身份和管理領域的領導者

Gartner

A leader in three

Gartner® Magic Quadrant™ reports

FORRESTER®

A leader in seven

Forrester Wave™ categories

IDC

A leader in seven

IDC MarketScape reports

Gartner and Magic Quadrant are registered trademarks and service marks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2024 Vendor Assessment, Doc #US50521223. January 2024
IDC MarketScape: Worldwide Modern Endpoint Security for Small and Midsize Businesses 2021 Vendor Assessment, Doc #48304721. November 2021
IDC MarketScape: Worldwide Advanced Authentication for Identity Security 2021 Vendor Assessment, Doc #US46178720, July 2021
IDC MarketScape: Worldwide eDiscovery Early Case Assessment Software 2022 Vendor Assessment. Doc #US48970222. October 2022

IDC MarketScape: Worldwide Unified Endpoint Management Software 2022 Vendor Assessment, Doc #US48325122. May 2022
IDC MarketScape: Worldwide Unified Endpoint Management Software for Small and Medium-Sized Businesses 2022 Vendor Assessment, Doc #US48325522. May 2022
IDC MarketScape: Worldwide Endpoint Management Software for Ruggedized/Internet of Things Device Deployments 2022 Vendor Assessment, Doc #US4Unified832532322. May 2022

Today more than ever…
let's secure the world together.