

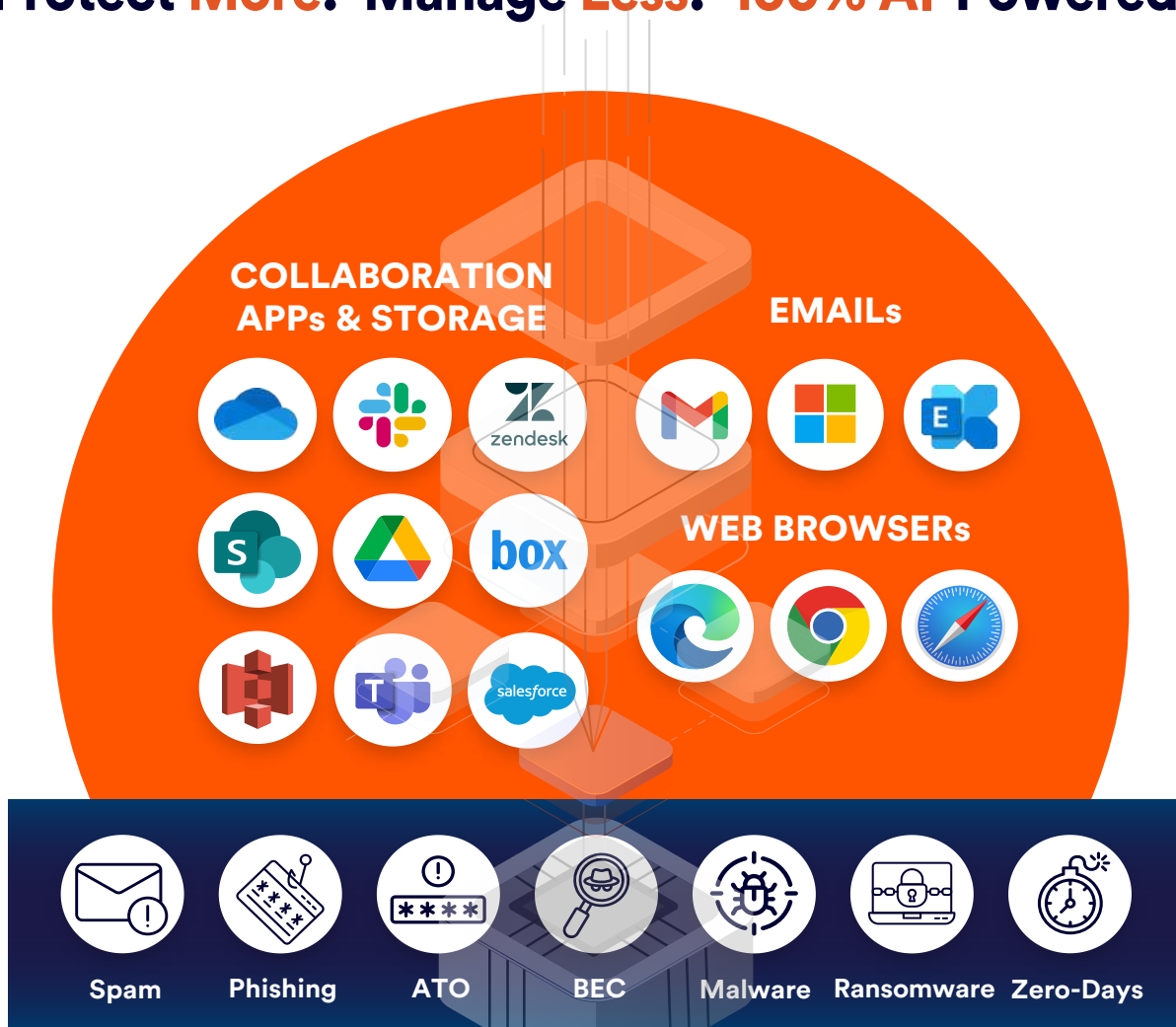


PERCEPTION  
POINT

Prevention as a Service  
進階威脅防禦資安服務

## Cybersecurity for the Modern Workspace

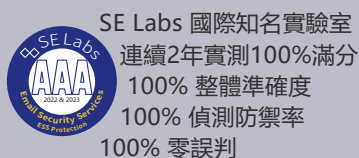
Protect **More**. Manage **Less**. 100% AI-Powered.



**One Platform One Click**  
**360° Channel Protection 100% Scanning**  
**Zero-Trust Managed Service**



**Gartner**  
2023 Market Guide  
Advanced Email Security &  
Collaboration Security  
連續 4 年榮獲代表性供應商



2023  
KuppingerCole  
Email Security  
Leadership Compass  
整體產業領導者



## 100% AI-Powered. 100% Scanning. 零信任終極達標

Perception Point 進階威脅防禦資安服務以 AI-Powered 各項專利技術提供 360°雲端協作管道威脅防禦，針對經由電子郵件、雲端程式、網頁瀏覽器及雲端儲存等協作管道入侵之各類型內容散播惡意攻擊，進行**零信任 100% Content Scanning**，並提供**原廠免費24/7 Incident Response 事件應變服務**，結合其獨家 AI 專利 GPThreat Hunter™，全球 IR 團隊平均回應速度鉅幅降低至17分鐘，為業界之最。

Perception Point 為備受全球各產業推崇的資安服務公司，連續兩年獲全球三大獨立資安產品/服務評估實驗室 SE Labs 評定為 100% 整體準確度、100% 偵測防禦率、100% 零誤判；連續四年獲 Gartner Market Guide 評選為 Advanced Collaboration Security & Advanced Email Security ICES 具代表性資安服務供應商；KuppingerCole 2023 Email Security Leadership Compass 評為整體產業領導者；2024 Gartner Peer Insights 獲 4.9 顆星。

Perception Point 以 AI 與 LLM 大型語言模型防禦生成式 AI 內容散播惡意攻擊，擁有 AI 演算專利 GenAI Decoder™，結合行為與內容基礎分析、NLP 自然語言處理、主旨歸類分析、影像辨識演算法，進行 100% Content Scanning，此對於識別複雜的商業電子郵件詐騙 (BEC)、偽冒攻擊、ATO 帳戶接管、垃圾郵件和其他社交工程威脅至關重要。

Perception Point 具備多重 AI 驅動99.95%精準度的Multi layers 偵測技術，**平均偵測速度15秒**。藉由其**專利遞迴拆解專屬反規避引擎**進行100%內容掃描、過濾、拆解，例如：QR Code 解析、URL深度逐層分析、加密檔案解密等，有助於偵測識別藏匿於內容或企圖規避傳統資安機制的進階惡意威脅，如：Quishing 攻擊、Macro巨集等。

Perception Point 次X世代**專利 HAP™ 動態偵測技術**，針對CPU指令縝密偵測分析，攔截零日與N日漏洞攻擊、勒索軟體、惡意 Office 巨集等，支援偵測 Mac 與 Windows 系統之漏洞攻擊。

**GPThreat Hunter™** 藉由 OpenAI GPT-4 模型所驅動的偵測分析能力，無需人為介入，能自主辨識從而解決大量複雜隱匿的惡意威脅，大幅突破傳統人工分析準確度，以100倍的速度偵測並阻絕各類新興攻擊手法與惡意威脅(如：電子郵件)，進而提升 IR 事件應變服務之效率。當 Perception Point 威脅防禦平台偵測到不明確的事件時，GPThreat Hunter™ 將自動啟動並彙整一套詳盡背景對照資料，包括問題項目之全文、來自偵測引擎的證據、及被演算法標記為可疑的項目，進一步由Perception Point持續累積訓練的客製定義多語言 (custom multilingual) LLMs進行分析，再遞交OpenGPT-4模型，由該模型提供即時的判斷結果，提供信心評分和判斷細節，此模型亦將自動隔離惡意威脅，並使系統對於未來類似攻擊產生自我防禦能力。結合多年累積的威脅應變專業智庫所提供的免費 24/7 IR 服務，平均可於17分鐘內協助客戶完成事件調查，顯著提升威脅偵測與事件處理效率。

## ALL Channels. ALL Threats.

### 99.95% Detection Accuracy

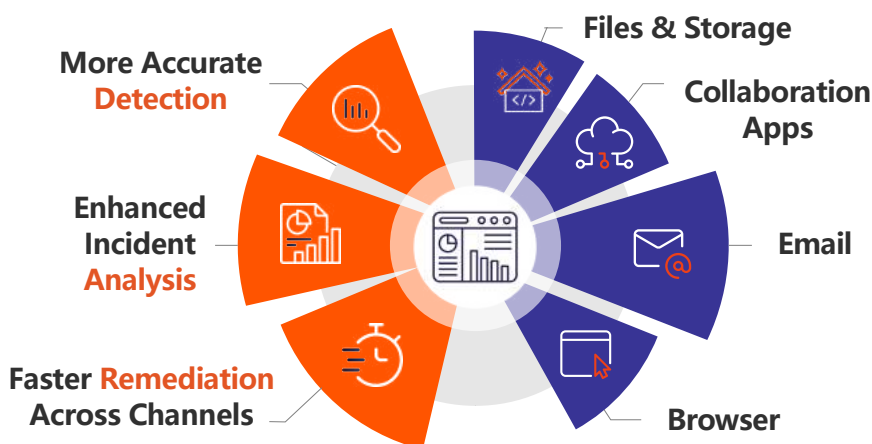
市場上最高威脅偵測率：BEC、Quishing、Phishing、ATO、Malware、0-Days...

### 100% Dynamic Scanning

完整動態即時掃描分析100%內容與物件，包括嵌入的檔案和超連結，Multi-Layers 縝密逐層偵測，確保不遺漏任何物件，達成零信任關聯防禦終極目標。

### 75% SOC Time Saving

IR事件應變服務，確保每一事件完整分析、處理和修復，節省SOC成本與時間。



# ONE Platform. 7 Layers of Security.

## 2 Anti-Evasion

### Recursive Unpacker

專利遞迴拆解反規避引擎拆解並傳送每一層隱藏於檔案、超連結、網址、執行檔內的惡意威脅至Multi-Layer中個別對應的引擎進行掃描及分析。

## 3 File Analysis

### Static Signatures

結合頂尖特徵檢測防毒引擎與專屬技術快速辨識高複雜度的特徵病毒。

## 4 Known Attacks

### Threat Intelligence

整合多個威脅情資來源與Perception Point內部情資，針對URL與檔案進行比對，並告警潛在或當前的惡意攻擊。

## 7 Dynamic Analysis

### Zero-days & Unknown Attacks

### Hardware-Assisted Platform (HAP™)

顛覆業界各類傳統的沙箱引擎與技術，採用 CPU-Level 數據指令演算分析，具備 Dropper、CFG 與 FFG 三種偵測機制。

## 1 Anti-Spam

### Spam Filter (Email only)

以 Reputation 及 Anti-Spam filters 快速辨識標記已接收的惡意電子郵件。

## 5 Payload-less Threats & Account Takeover

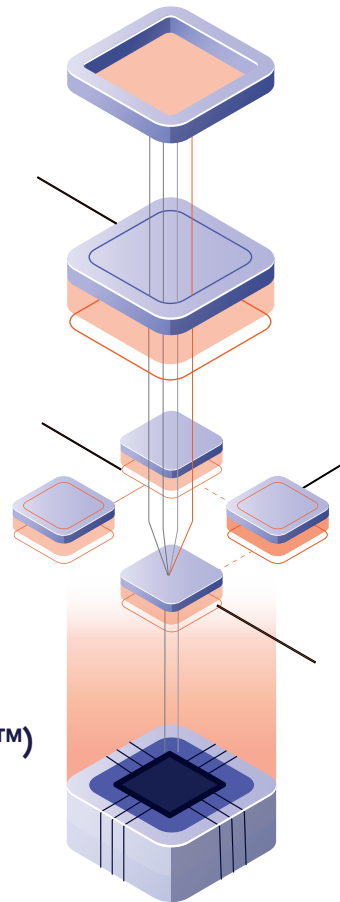
### BEC & ATO

獨有的三階段架構: 1. Large Language Models (LLMs) 2. 模型和分群演算法 3. 驗證協定，有效偵測辨識破解最難防禦的生成式AI商業電子郵件詐騙與 Thread Hijacking等惡意威脅。

## 6 URL analysis, AI & Image Recognition

### Anti-Phishing

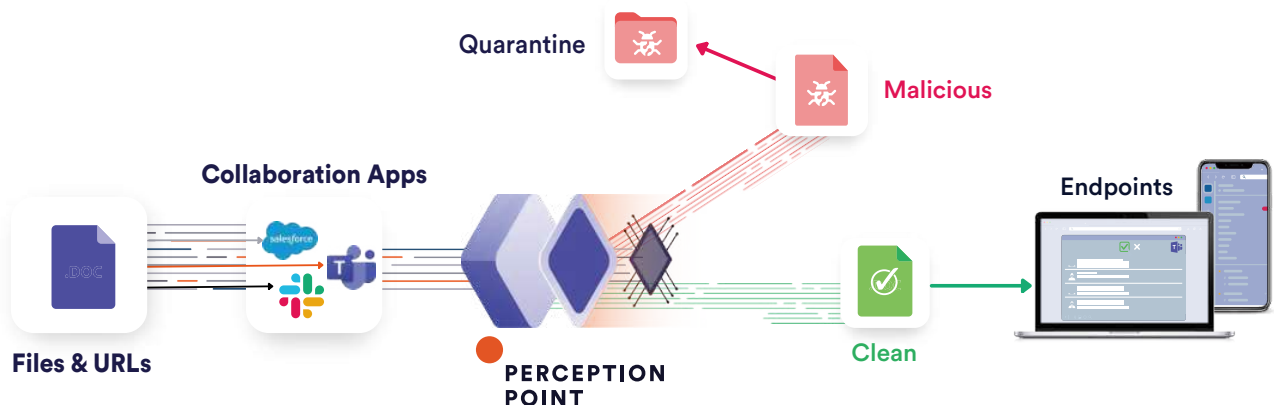
結合世界級 URL Reputation 引擎和原廠圖像辨識分析引擎，辨識偽裝技術和網路釣魚攻擊。



## Advanced COLLABORATION Security



Perception Point 資安防禦服務可動態偵測雲端協作管道中100%所有內容，於數秒內偵測攔截惡意的上傳、分享、更新的檔案或資料，Multi-Layer遞迴拆解與專利 HAP™ CPU-Level 數據指令演算分析技術能以秒計的速度層層拆解分析釣魚攻擊、複雜/日常型惡意程式或程式碼、零日/N日攻擊、APT進階持續性威脅，或任何惡意文件 (Office、PDF等)及網址，提供即時通訊軟體、檔案共享平台、雲端服務、CRM等各類管道深層縝密的資安防禦。



### ZERO-DAYS, N-DAYS & EVERY-DAYS

運用專屬反規避引擎，遞迴拆解深層偵測分析 Collaboration雲端協作管道內每一個分享的文件、檔案、執行檔、URLs等物件及每一層物件內隱藏之惡意威脅及零時差攻擊。

### MULTI-LAYER THREAT DETECTION

Multi-Layer動態即時偵測掃描及分析儲存空間100%內容，挖掘可能深層存在之各類已知/未知惡意威脅，並針對 Office 檔案藏匿的巨集、JavaScript、VBScript程式碼，進程式碼靜態分析。

### ARCHIVE SANITIZATION

針對上傳、分享、更新或歷史封存之檔案進行即時動態偵測分析，數秒內即可發現惡意威脅並立即進行隔離，以確保雲端儲存空間內無任何潛藏之未知惡意威脅。

### ONE-CLICK DEPLOYMENT

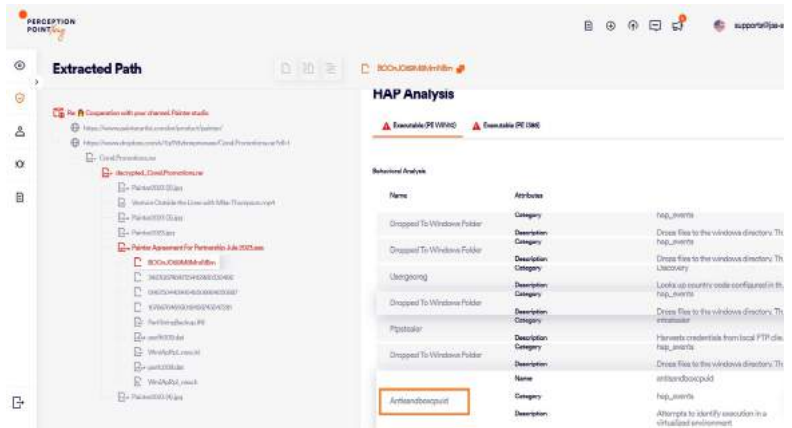
快速部署: 經由 API 一鍵即可完成設定，包括: SharePoint、Teams、Slack、Salesforce、Zendesk、OneDrive、Dropbox、Box、Google Drive & Amazon S3。

## Advanced EMAIL Security



Perception Point 進階電子郵件安全服務整合其多項領先業界之專利HAP™動態偵測、專利遞迴拆解反規避引擎、圖像識別等技術，並以創新的 LLM-based 偵測模型，協助世界各地不同規模的企業組織在使用 Microsoft 365、Google Workspace、任何雲端或自建電子郵件系統時，能有效對抗經由電子郵件散播的各類惡意威脅攻擊，特別是急速崛起的 GenAI-based 社交工程與BEC。

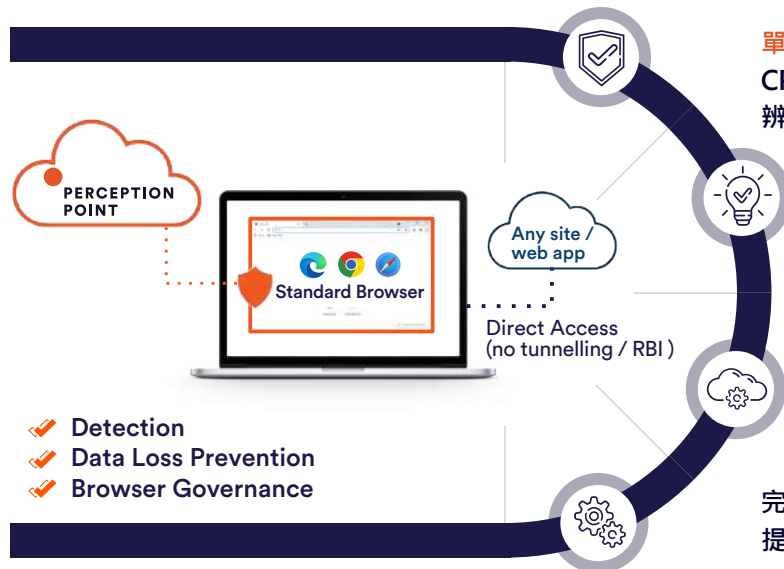
Perception Point 100% 掃描偵測郵件內容；經由 Recursive Unpacker 逐一拆解郵件之物件傳送至 Multi-Layer中個別對應引擎獨立掃描及分析，其 X-Ray Dashboard 可即時查閱經深層拆解之email物件，並快速搜尋每一層隱藏的檔案、超連結、網址、執行檔內的惡意威脅，特別是動態偵測所發現的零日漏洞、零時差攻擊及AntiSandbox規避行為等，皆可鉅細靡遺於儀表板內深度調查。



## Advanced BROWSER Security



Perception Point 為網頁瀏覽器提供一鍵部署的進階威脅偵測、資料外洩防護與瀏覽器合規治理。經由 Browser Extension瀏覽器擴充功能，即可擁有前所未有的動態偵測、阻擋與修復能力。可預防釣魚網站並阻擋惡意物件下載至前端裝置，如: 勒索軟體、惡意程式碼JavaScript及零日漏洞等攻擊，同時確保使用者的生產力及原生瀏覽體驗。



單一集中管控平台亦運用Multi-Layer與專利HAP™ CPU-Level動態偵測、專利遞迴拆解反規避引擎、圖形辨識及機器學習等技術，立即強化網頁瀏覽安全

相容於Edge、Chrome、Safari等瀏覽器，以及企業組織現行使用之Web Apps 與整體資訊生態環境

資料外洩防護控管 - 依網站分類控管網站訪問權限、檔案下載及上傳、特定檔案類型下載、網站資料剪貼、網站列印、機敏網站浮水印等

完備企業組織跨平台管道之關聯式聯合防禦機制，亦提供24/7 Incident Response事件應變服務

## 關於 Perception Point

Perception Point 為推行防禦即服務 (Prevention as a Service) 備受全球業界推崇的資安服務公司，同時經 Gartner 認可具備業界革命性技術。100%運用創新的各類 AI 技術，結合其獨家專利的次X世代HAP™遞迴拆解動態偵測技術，分析攔截經由電子郵件、雲端程式、網頁瀏覽及雲端儲存等協作管道之 Content-borne Threats 內容散播惡意威脅。GPThreat Hunter™ 更為一項以GPT-4模型所驅動的自主分析Incident Response 創新技術，有助其免費的24/7 IR全球服務速度鉅幅降低至17分鐘。Perception Point 由前以色列國防網路情報團隊於2015年所創立，客戶遍佈全球，其中包含許多 Fortune 500 大企業，橫跨眾多產業，如：公用事業、電信、科技、零售、食品、醫療保健、金融服務等。