DARKTRACE

資料

DARKTRACE 公司簡介

願景

Darktrace 應用人類免疫系統的原理，保護企業免受高階網絡威脅的侵擾。Darktrace 的願景是使用尖端技術幫助企業實時檢測網絡中的異常行為，並阻止這些行為發展成具破壞性的網絡攻擊。

Darktrace 功能

- 檢測網絡中出現的異常
- 了解實時的正常和異常行為
- 識別和抵抗內部和外部威脅
- 防禦範疇包括雲端、虛擬化環境和工業控制系統
- 建置的第一天起便能帶來價值

> 「習慣上，當我們尋求安全和自我保護時，盔甲和高牆會佔據我們的思緒。但慢慢地，我發現自己轉而思索醫學上、抗體對抗病毒的解決方式。
>
> 網絡安全仍然如此艱難的某部分原因在於威脅不需要像一架又一架坦克輾過你的防禦措施, 因為我們防護的系統脆弱得即使一隻螞蟻亦可進入並造成破壞。這意味著我們必須以不同的方式思考我們的安全。」
>
> 美國總統歐巴馬，**2016** 年

企業免疫系統

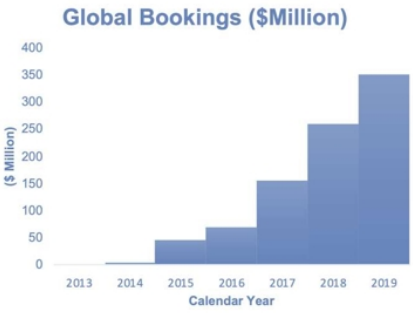
Darktrace 的企業免疫系統技術屢獲殊榮，擁有獨一無二的技術，即使網絡中最細微的威脅都能即時檢測和反應。企業免疫系統採用最先進的機器學習與數學演算法，能夠自動學習並了解每個使用者、設備與網路的「行為模式」，進而偵測出真正具有威脅的行為。這種自我學習技術為企業提供了對其網絡活動的全面可見性，使企業能夠主動應對威脅並降低風險。

為什麼機械學習和數學運算對網絡安全這麼重要？

使用高聳的網路圍牆來保護您資訊的傳統方法已經不足以防禦現今的巨大潛在威脅。理所當然的，網路中永遠存在著威脅。而我們透過劍橋大學數學專家開發的機械學習和數學演算法，能夠智能的偵測出各種有危險的事件，讓企業網絡安全得到完善的保障。Darktrace 的機械學習能夠動態和快速地自動建模和收集訊息，進而找出未知的潛在風險；而不是預先定義「不好」的行為，或依賴處理過往事件的經驗建立而成的資料庫。

關於Darktrace

- 創立於2013年，由劍橋大學的數學家及英國情報人員成立
- 依賴AI & ML專注於網路安全領域
- 英國公司，雙總部在劍橋及舊金山
- 2021年於倫敦證交所上市
- 全球超過四千個客戶, 40國有辦公室



44 OFFICES | **110** COUNTRIES | **1,600** EMPLOYEES | **4,000** CUSTOMERS | **$2bn+** VALUATION

WSJ Tech Companies to Watch 2017 · The Sunday Times Tech Track 100 2017 & HISCOX · Gartner 2015 CoolVendor · The Queen's Awards for Enterprise: Innovation 2016 · World Economic Forum Technology Pioneer 2015 · Bloomberg Business Innovators 2016 · Royal Academy of Engineering

Technical and Intelligence Experts

Darktrace擁有的智慧學習技術，與其背後龐大且複雜的推演統計運算，始於全球最頂尖數學家們與長期從事資訊安全技術的資深成員，其專業團隊組成與背景是與英國劍橋大學所共同研究、開發的成果，將安全防禦課題結合遞迴貝氏機率估測（Recursive Bayesian Estimation;RBE）理論，打造為企業免疫系統的核心，一舉超越現今各式的傳統防禦策略。

Darktrace的創始人來自英國軍情五處（MI5）與政府通訊總處（GCHQ）的資深成員，以及英國軍情五處的前總幹事Lord Evans。

Darktrace的安全團隊，是長期於英國軍情五處（MI5）與政府通訊總處（GCHQ），第一線效力國家資訊安全防禦的成員，對於網路攻擊與防禦之間擁有豐富之經驗，發掘與阻擋潛藏於民生資源、公共服務、核心建設等領域內，長期且複雜的攻擊行為，追蹤其幕後可能的組織與背景，並提出具體之防禦政策。Darktrace安全團隊成員目前更持續增加，其中不乏來自其他國家如國家安全局（NSA）、與中央情報局（CIA）的專家，並一齊為Darktrace的客戶提供最先進也最完善的安全防禦服務。

Darktrace價值驗證（Proof of Value，POV）計畫

Darktrace價值驗證計畫是一個特別的短期試用方案，透過建立於企業實際環境中之Darktrace EIS企業免疫系統，包含數位防禦系統與威脅展示平台，讓客戶完美體驗等同於現有Darktrace世界級大客戶所擁有的企業資訊環境解析，以及即時與最真實的網路威脅安全服務平台方案。

DARKTRACE

電子郵件

Darktrace/Email 能夠學習每位電子郵件使用者的「常態」行為，包括他們的關係、語氣和情緒、內容和連結分享模式，以及來自電子郵件內外的其他數千種訊號。

Darktrace AI 不斷發展，持續加強理解電子郵件通訊背後的人類行為，藉此發現異常的偏差情況，掌握電子郵件威脅，即使具有高度針對性或是前所未見的目標，也都能有效應對。

Darktrace/Email 重點特色：

- 無與倫比的偵測能力：相較於根據既往已知威脅進行訓練的電子郵件安全工具，Darktrace/Email 平均能夠提前 13 天偵測新型電子郵件攻擊。
- 強化資安團隊：平均事件解決時間從 1 小時縮短為 5 分鐘。
- 提升生產力：減少誤報，使客戶回報的真實商業郵件數量增加 14%。
- 減少資料暴露：每年平均阻止每位員工將四封關鍵商業電子郵件發送給不當的收件者。

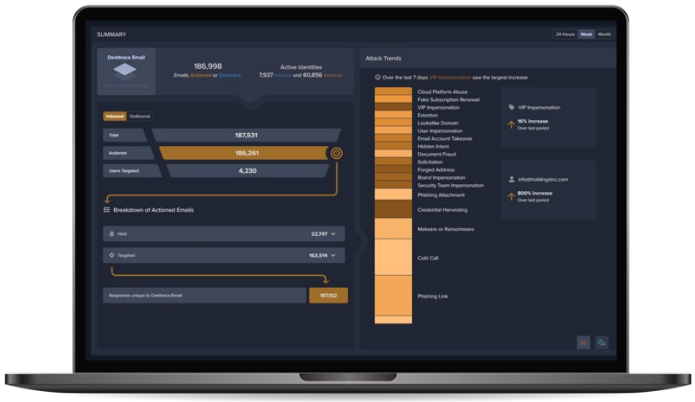


圖 1：Darktrace/Email 可保護您的收件匣、保護使用者帳戶並防止意外資料遺失，提供完整的電子郵件保護。

如欲進一步瞭解，請參閱部落格：「Darktrace/Email 操作實況：AI 驅動的電子郵件安全性為何是抵禦持續網路釣魚活動的最佳防禦措施。」

若想在您的環境中即時試用 Darktrace/Email，
請造訪 Innovation Series 頁面或聯絡您的 Darktrace 代表！

Darktrace/Email 的各項數據

2023 年 9 月 – 11 月

7.5M

Darktrace/Email 去年以最高置信度**偵測到的網路釣魚電子郵件**數量。

65% 通過 DMARC 驗證

46% 魚叉式網路釣魚

37% 發現使用新型社交工程技術

26% 包含超過 1,000 個字元的文字

3% 使用新註冊的網域

550K+ 內含惡意行動條碼數量

1. 相較於其他電子郵件安全技術提交 16 筆獨立情報的最早時間，Darktrace/Email 平均可提前 13 天發現實際作用中的網路釣魚酬載並予以回應。

生成式 AI 模型

過去這一年來，生成式 AI 和 LLM 工具已逐漸為大眾所熟悉，人們使用 OpenAI 的 ChatGPT 和 Google Bard 等工具處理一切事務，包括輔助網頁搜尋，以及使用 AI 功能提高工作場所效率等。

Enterprise AI 一項調查發現，56% 的美國員工承認在工作中使用生成式 AI，但只有 25% 表示所屬組織訂有生成式 AI 政策。[2]

企業希望採用新型生成式 AI 工具，但若無防護措施而貿然使用，將會提高智慧財產遺失或資料外洩風險，因此資安團隊必須在兩者之間取得平衡。

因此我們為 DETECT + RESPOND 開發了多種風險和法規遵循模型，協助組織自行開展生成式 AI 業務並執行自有政策，以減輕資料隱私或智慧財產遺失等顧慮。

前述模型為資安團隊提供了一種簡單方法，有利於執行組織專屬的風險和法規遵循政策。每間企業皆需執行各自的細節政策，因此客戶也可輕鬆新增自己的生成式 AI 工具清單進行監控。

如欲進一步瞭解，請參閱部落格：「生成式 AI：Darktrace AI 如何保護 8,400 名客戶免受安全和隱私風險。」

若想在您的環境中即時試用 RESPOND，
請造訪 Innovation Series 頁面或聯絡您的 Darktrace 代表！

雲端

雖然組織繼續採用雲端提高效率和靈活性，但這也為威脅攻擊者打開大門，提供刺探利用的全新途徑。

值得注意的是，雲端供應商不願採取共享責任的營運模式，表示組織必須仰賴自己的安全性程序，而不是由雲端供應商保護其資料。這可能十分困難，而 Gartner 預測到 2027 年以前，會有 99% 的雲端洩漏事件是由於客戶疏失、帳戶接管或配置錯誤等原因所造成。[3]

Darktrace/Cloud 使用自我學習 AI 技術，為多雲端環境提供完整的網路恢復能力，此外也提供架構感知、雲端原生回應、雲端保護和法規遵循以及部署靈活性。

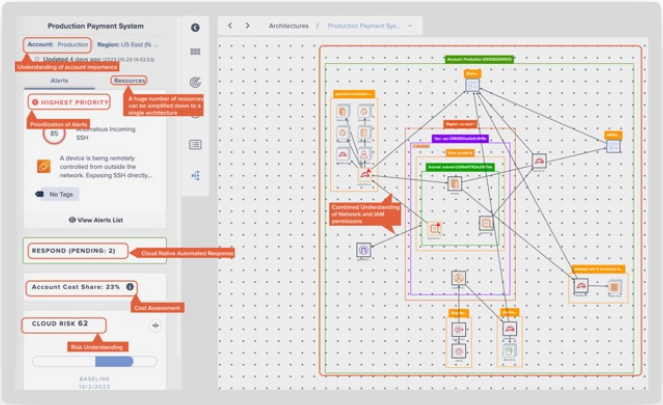


圖 2：Darktrace 可為雲端架構進行建模，並突顯相關風險。

- 立即瞭解您的雲端足跡，包括以**即時可見性**深入掌握雲端資產和架構，以及使用者和權限。
- 識別**錯誤配置、漏洞和法規遵循問題**，並根據真正的雲端風險確定行動優先順序。
- **雲端原生**偵測和回應功能可快速且大規模運作，保護網路環境安全無虞。
- 透過**攻擊面管理**和攻擊路徑建模掌握攻擊的關鍵途徑。
- **成本洞見**也讓您更充分瞭解資源分配，協助團隊確切掌握資源實況。

我們最新的 Darktrace/Cloud 產品方案目前支援 AWS，此外也即將推出 Azure 版本。

若要進一步瞭解，請參閱部落格：「保護雲端安全從瞭解雲端做起。」

若想在您的環境中即時試用 Darktrace/Cloud，
請造訪 Innovation Series 頁面或聯絡您的 Darktrace 代表！

2. 企業 AI，「意見調查：大部分美國員工已開始使用生成式 AI 工具，但公司政策仍未跟上腳步」，Doug Eadline，2023 年 9 月 18 日。

3. Gartner，「快速釋疑：我的雲端服務供應商能否抵禦網路威脅？」Charlie Winckless，2023 年 9 月 28 日。

附錄一：

Darktrace企業免疫系統EIS可以為您偵測的企業資訊網路異常行為舉例如下：

	異常行為	說明描述
1.	Remote access attack linked to dangerous malware RAT攻擊潛伏行為	偵測企業內部殭屍網路行為，發掘隱匿於企業環境內高複雜度、高隱匿性與多樣性的殭屍網路通訊
2.	Anomalous data transfer 異常數據傳輸行為	偵測企業可疑數據傳輸行為，尤其是包裝於一般應用程式外表下，卻對外產生異常連結與通訊
3.	Illegitimate access to database server 非法存取資料庫行為	偵測企業非法存取資料庫行為，尤其是額外的、異常的非加密連線，並分析存取來源與目的間相對關係，並研判其風險程度
4.	Unauthorized use of administrator credentials 未經授權卻使用管理員憑證行為	偵測是否有特權用戶，於特殊期間，發生非工作時間多次登入企業網路環境進行存取行為
5.	Fast travel indicating password compromise 單一帳號多點同時登入行為	偵測單一使用者帳號，卻於不同來源，且同一時間登入企業網路進行存取行為
6.	Connections to website linked to Advanced Persistent Threats 瀏覽網路時遭受APT攻擊行為	偵測使用者瀏覽知名社交網站時，經惡意導向至可疑的站台，可能遭遇APT針對性攻擊的行為
7.	Infection with ransomware 遭勒索軟體感染的行為	偵測使用者瀏覽網路後，遭勒索軟體植入後對主機異常使用與連線行為
8.	Domain Generation Algorithm 使用動態網域演算法的惡意行為	偵測企業主機對外連線，其連結對象為使用動態網域演算法，而產生之大量無效網域名稱行為
9.	Malicious web drive-by 惡意偷渡式攻擊行為	偵測使用者遭受的惡意偷渡式攻擊行為，於使用者電腦已遭受惡意程式感染時，它將竄改電腦設定，將您的正常連線導向一個惡意偽冒網站
10.	Port-scanning for internal company resources 企業內部資源及服務掃描行為	偵測企業內部不正常的資源、或服務的掃描行為
11.	Use of 'Tor' anonymizing network 使用Tor匿名網路連線行為	偵測企業內部是否存在使用Tor協定的網路通訊行為
12.	Peer-to-peer connections with the Far East 點對點的遠端通訊行為	偵測企業對外通訊時，發生連續且異常的點對點通訊行為
13.	Bitcoin mining 比特幣挖掘行為	偵測企業內部是否存在比特幣的挖掘行為，這行為可能牽涉主機間資源運用/濫用、中央控制（僵屍網路）等議題
14.	Attempted connections to non-existent domain names 大量嘗試聯結至不存在的網址行為	偵測企業主機對外連線，在一段時間週期內大量嘗試聯結到不存在的網址之行為，這行為經常被駭客用來隱藏惡意的流量
15.	Anomalous internal file transfers 反常的內部文件傳輸行為	偵測企業內部通訊作業間，使用者突然下載或存取超越日常數據量的行為
16.	Suspicious Java download 可疑的JAVA檔案下載	偵測使用者瀏覽網站時，突然遭導向至另一站台，並於背景自動下載.jar文件的行為
17.	Use of virtual Cyrillic keyboard 使用虛擬西里爾語鍵盤行為	偵測企業內部是否使用特殊虛擬鍵盤的網路通訊行為，這行為可能伴隨著駭客試圖以自己的語言進行攻擊滲透
18.	Suspicious file download using XOR obfuscation 使用XOR的可疑文件下載行為	偵測企業主機由網路下載檔案時，文件形式與內容不符，疑似為駭客偽裝或故意隱藏的攻擊行為
19.	Risk from 'bring-your-own-device' (BYOD) policies BYOD政策所帶來的風險行為	偵測企業開放BYOD時，駭客透過精心設計的電子郵件，崁入惡意的連結或附件所帶來的魚叉式攻擊行為