CrowdStrike 產品

CROWDSTRIKE

CROWDSTRIKE FALCON 端點偵測及回應 (EDR)

以快速、自動化與無可比擬的能見度，串流威脅偵測與回應生命週期

FALCON INSIGHT — 輕鬆簡單的 EDR

傳統端點安全工具有其盲點，無法偵測並阻止進階威脅。CrowdStrike® Falcon Insight™ 可提供整個組織的完全能見度，解決此問題。

Insight 會持續監控所有端點活動，並即時分析資料以自動識別威脅活動，藉此偵測並防範進階威脅發生。所有端點活動均會串流至 CrosdStrike Falcon® 平台，供安全團隊快速掃描並調查事件、回應警示，以及主動搜尋新威脅。

FALCON INSIGHT 就是 EDR 方面的領導產品

Forrester Wave™ 排名第一的領導產品：端點偵測及回應，2018

在 2018 年 MITRE 國家級模擬測試中，經追蹤及偵測進階攻擊之 MITRE ATT&CK™ 框架驗證

SC Magazine 的 2018 年「推薦首選」，SC Labs 在所有類別均給予五星評價

在 Gartner 2017 年端點偵測及回應技術與解決方案比較報告中，於所有評估的使用案例中獲得最高評分

主要優點

- 自動偵測進階威脅
- 搭配即時深度鑑識的快速調查
- 安心回應與修復
- 進行五秒企業搜尋
- 啟用 Falcon OverWatch™ 威脅搜尋服務
- 透過以 MITRE 為基礎的偵測框架，對複雜警示一目瞭然

主要產品功能

簡化偵測與解決方式

- **自動偵測攻擊者活動：** Insight 使用 IOA (攻擊指標) 自動識別攻擊者行為，並將優先警示傳送至 Falcon UI，消除耗時的研究與手動搜尋作業。CrowdStrike Threat Graph™ 資料庫會存放事件資料，即便面對數十億筆事件資料，也能於五秒內回覆查詢。
- **在單一畫面徹底分析整個攻擊：** 易於閱讀的流程圖可提供整體攻擊的情境資訊，讓調查快速又輕鬆。
- **加快調查工作流程：** 讓警示對映 MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) 框架，即使最複雜的偵測結果也能一目瞭然，藉此縮短分級警示所需時間，並加快優先順序的決定與修復。此外，符合直覺的 UI 可讓您快速切換操作，在數秒內搜尋整個組織。
- **取得情境資訊與情報：** 整合式威脅情報可提供整體攻擊的情境資訊，包括事發原因。
- **果斷回應：** 即時採取行動因應駭客，在發生入侵攻擊前便予以阻止。強大的回應動作可讓您遏止遭受入侵的系統並進行調查，即時回應功能可讓您直接存取受調查的端點。如此一來，安全回應者便能在系統執行動作，並以極高精準度消滅威脅。

即時獲得全領域能見度

- **即時觀察所有動作：** 立即能見度可讓您檢視駭客的活動，一舉一動都難逃法眼。
- **擷取威脅搜尋與鑑識調查的關鍵細節：** Falcon Insight 核心模式驅動程式會擷取超過 400 個原始事件與必要的相關資訊，以反向追蹤事件。
- **在數秒內獲得解答：** CrowdStrike Threat Graph™ 資料庫會存放事件資料，即便面對數十億筆事件資料，也能於五秒內回覆查詢。
- **為期 90 天的重新叫用：** Falcon Insight 會將完整的端點活動保留一段時日，無論您環境中具有少於 100 個端點或多於 50 萬個端點都沒問題。

立即實現價值

- **省時、省力、省錢：** 已啟用雲端的 Falcon Insight 由 CrowdStrike Falcon 平台提供，且不需要任何內部部署管理基礎架構。
- **部署只需數分鐘：** CrowdStrike 客戶可在一天內將雲端提供的 Falcon 代理程式部署至最高 7 萬個端點。
- **馬上運作：** Falcon Insight 在開始使用時即擁有無可比擬的偵測能力與能見度，無需重新開機、微調、設定基準或複雜的設定，安裝後即可執行、監控並加以記錄。
- **對端點無絲毫影響：** 端點上僅有一個輕量型代理程式，且會在 Threat Graph 資料庫中進行搜尋，因此不會對端點或網路造成任何影響。

防止「無聲侵略」並遏止入侵攻擊的力量

防範技術尚未完善。如果攻擊者有辦法突破貴組織的防禦，他們就能在數週或數月內隱藏蹤跡，因為安全團隊缺乏能見度與偵測工具來辨識入侵攻擊後的活動。這個「無聲侵略」的階段就是攻擊者的勝利，也是組織的潛在災難。Falcon Insight 可快速偵測、辨識，並讓您回應現有防禦措施無法偵測到的事件。

關於 CrowdStrike

CrowdStrike 是雲端提供的新一代端點保護的領導廠商。CrowdStrike 是業界領先唯一將新一代防毒軟體、端點偵測及回應 (EDR)，以及 24 小時全年無休管理式搜尋服務加以統整的公司，且僅透過單一輕量型代理程式就能提供，開創端點保護的革新局面。

如需更多資訊，請造訪
crowdstrike.com

CROWDSTRIKE

CROWDSTRIKE FALCON PREVENT™ NEXT-GENERATION ANTIVIRUS

將您的現有防毒解決方案更換為 CrowdStrike Falcon Prevent，立即享有更佳保護和效能

FALCON PREVENT：業界認可的舊版防毒軟體替代品

如果貴組織因為舊版軟體成效不彰，又複雜難懂而焦頭爛額，Falcon Prevent 在此為您提供鼎力協助。Falcon Prevent 作為業界最完整的防毒替代解決方案，可提供卓越的保護功能，並透過單一輕量型代理程式運作，無需持續更新病毒碼、內部部署管理基礎架構或複雜的整合就能完成。無論組織規模多麼龐大，都可在數分鐘內啟用和運作 Falcon Prevent。

經認證可取代舊版防毒軟體產品：AV-Comparatives 和 SE Labs 的獨立測試均認證 Falcon Prevent 的防毒功能。Falcon Prevent 亦通過 PCI、HIPAA、NIST 及 FFIEC 法規要求認證。

獲 Gartner 的 Magic Quadrant for Endpoint Protection Platforms 提名為前瞻者：前瞻的定位係根據創新的保護功能與簡化的部署模式。

主要產品功能

確保貴組織獲得完整保護，足以抵禦來勢洶洶的網路威脅

- **彌補舊版防毒軟體遺留的保護缺口：**Falcon Prevent 不僅是防毒軟體替代品，更是專門設計用於取代舊版防毒軟體解決方案，並為您的端點提供新的保護功能。Falcon Prevent 新增機器學習和行為分析功能，可阻止通常遭標準防毒軟體產品遺漏的無檔案惡意軟體、植入記憶體攻擊及其他進階技術。

主要優點

» 防止惡意軟體和勒索軟體感染

» 防止無檔案和植入記憶體攻擊

» 抵禦惡意軟體以外的攻擊

» 簡化無病毒碼保護和 SaaS 遞送作業

» 快速安心取代舊版防毒軟體

「越來越多組織開始尋找可較有效阻止現代進階威脅解決方案時，我相信 CrowdStrike Falcon 正是最佳解決辦法。」

— STEVE PHILLPOTT
WESTERN DIGITAL CORP. 資訊長

- **僅使用單一代理程式：**取得集中於單一代理程式的新一代最佳技術，包括機器學習、入侵封鎖、自訂白名單和黑名單、攻擊指標 (IOA)、攻擊屬性及廣告軟體封鎖。
- **完整的線上和離線保護：**Falcon Prevent 利用雲端和端點的保護技術，提供網路離線時的完整防護；且能在網路連線時有效運用雲端的額外功能。

快速輕鬆的部署

- **節省時間、心力與金錢：**雲端原生的 Falcon Prevent 是由 CrowdStrike Falcon® 平台所提供，不需要任何內部部署管理基礎架構。
- **以前所未有的速度部署：**雲端提供的 Falcon 代理程式可快速部署，經客戶回報可在單日內安裝多達 70,000 個代理程式。
- **立即運作：**立即提供無可比擬的防護功能。Falcon Prevent 致力於安裝後提供立即保護，不需要更新病毒碼、微調、基準化或複雜的設定。

近乎隱形

- **不會對端點造成任何影響：**從初步安裝到持續每日使用，Falcon Prevent 僅會使用極小的 20 MB 端點容量進行運作。
- **無須重新開機：**可任由端點持續運作，無須在安裝或更新期間重新開機。
- **無需經常進行繁瑣掃描或更新：**Falcon Prevent 使用的無病毒碼保護技術完全不需要執行使效能遲鈍的工作，例如更新病毒碼和掃描磁碟。

安心遷移

- **輕鬆轉換：**Falcon Prevent 可在您遷移時搭配防毒軟體流暢運作。

保護組織免於惡意軟體和入侵攻擊最輕鬆快速的方式

現今駭客的攻擊戰術不僅限於惡意軟體和入侵兩種方式。因此，Falcon Prevent 提供新一代防護功能，可抵禦此類不斷演進的工具和技術。

CROWDSTRIKE

CrowdStrike 為雲端提供新一代端點保護技術的領導廠商。CrowdStrike 是業界領先唯一將新一代防毒軟體、端點偵測及回應 (EDR)，以及 24 小時全年無休管理式搜尋服務加以統整的公司，且僅透過單一輕量型代理程式就能提供。

如需更多資訊，請造訪 crowdstrike.com

CrowdStrike 產品

CROWDSTRIKE

FALCON OVERWATCH
管理式威脅搜尋

找出隱藏的進階攻擊並加以遏止

FALCON OVERWATCH — 遏止大規模資料外洩

Falcon OverWatch™ 為 CrowdStrike 的管理式威脅搜尋服務，內建於 CrowdStrike Falcon® 平台。OverWatch 提供 24 小時全年無休持續進行的深度真人分析，不斷搜尋專門用於規避標準安全技術的匿名或新興攻擊者間諜技術。

OverWatch 的菁英團隊包含多位跨領域專家，能運用具有 CrowdStrike 豐富威脅情報的 CrowdStrike Threat Graph® 強大功能，持續搜尋客戶環境中的複雜威脅活動，並加以調查和提供建議。OverWatch 具備雲端規模遙測功能，以及 130 多個惡意團隊的詳細間諜技術，可提供無可比擬的能力，找出最為進階的攻擊並加以遏止。

「OverWatch 一週前與我聯絡，告訴我偵測到與已知伺服器挾持組織相關的活動。多虧有他們通知，讓我們得以著手處理該問題。OverWatch 的反應非常迅速，並表示：『對於此問題，我們可提供您已知資訊。』這樣的行動確實防止了我們任何一個伺服器被賣給垃圾郵件發送者或其他惡劣執行者的黑市使用。」

MarkSauer
TransPak 資訊技術總監

主要優點

找出隱藏的進階攻擊並加以遏止： OverWatch 團隊會持續搜尋，找出最隱蔽複雜的威脅並加以遏止；如果無法偵測無徵兆混入的任何一丁點威脅，哪怕只有 1% 的漏網之魚，都會造成入侵風險。

達到最佳效果與效率： OverWatch 能夠以最新的進階技術強化專業技術人員的技能，進而提供最佳結果。CrowdStrike 的菁英專家會使用雲端規模資料、自訂工具和最新的威脅情報，以前所未有的速度與規模進行搜尋作業。

可緊密延伸團隊： OverWatch 作為 Falcon 平台核心要素，可針對各種規模的組織提供不同結果，並以緊密延伸團隊的方式進行作業，大幅降低間接費用、複雜及成本。

FALCON OVERWATCH 管理式威脅搜尋

主要產品功能

專業人員 24 小時全年待命

- **攻擊者心態：**有效的威脅搜尋作業，需要具備以攻擊者角度思考的能力與專業知識。
- **跨領域專業知識：**OverWatch 雇用具備政府、執法機關、商業企業、情報界與國防單位等多種背景的菁英專家。
- **服務 24 小時全年無休：**發生複雜的入侵事件時，時間至關重要。駭客不眠不休發動攻擊，也不侷限於特定時區或地理位置。因此，您的威脅搜尋團隊亦不應受此限制。
- **持續警戒：**OverWatch 的持續主動作業每天每分鐘都會提供各項結果。
- **精確調整的回應：**OverWatch 每週皆可找出數以百計的潛在入侵威脅並加以回應。每排除一個威脅，都能協助團隊成員微調其技能與程序，確保成員隨時維持機警與工作成效。

雲端規模安全遙測

- **搜尋工具：**威脅搜尋作業不僅需要專業的搜尋人員，正確的工具也不可或缺。可擴充且有效的威脅搜尋作業需要存取大量資料，且能夠即時加以深入分析，瞭解是否有任何入侵跡象。
- **即時掌握資訊：**OverWatch 可有效利用專利 CrowdStrike Threat Graph 的雲端規模遙測功能，即時掌握廣泛且深入的資訊。
- **大量資料：**Threat Graph 每週會吸收數兆筆事件，在威脅活動出現時，提供 Falcon OverWatch 來自全球的廣泛即時威脅活動概觀。

最新威脅情報

- **威脅情境：**您無法偵測到不瞭解的威脅。
- **CrowdStrike 威脅情報：**此情報可提供來自 130 多個駭客的詳細即時間諜技術資訊，藉此強化 OverWatch 功能。
- **最新的 TTP：**現今使用的最新 TTP (戰略、戰術及程序) 深入資訊，確保能見度 OverWatch 的搜尋作業快速又有效。

Falcon 平台的流暢特色

- **團隊一心共同奮戰：**OverWatch 可以延伸 Falcon 平台與您團隊的方式進行作業，透過單一雲端原生主控台提供及時的威脅資訊。
- **根據情境傳送警示：**OverWatch 分析人員會提供包含情境詳細資料與全方位深入分析的警示，協助各組織更快速瞭解威脅並採取行動。

CrowdStrike 管理式威脅搜尋服務

Falcon OverWatch 透過即輔菁英人員的專業知識與雲端規模資料，持續搜尋過去可能無法偵測到的進階威脅。以下為符合貴組織特殊需求的兩種服務。

功能	Falcon Over Watch	Falcon Over Watch Elite
跨領域專家	X	X
持續警戒	X	X
雲端規模遙測	X	X
情報驅動	X	X
與 Falcon 平台流暢整合	X	X
根據情境傳送警示	X	X
電子郵件通知	X	X
指派的威脅分析人員		X
個人化入門指南		X
搜尋與調查指導	X	
例行環境檢查		X
主動調整		X
量身打造的威脅報告和簡報		X
回應建議、進階調查及情境支援		X
主動、保密聯繫通訊		X

關於 CrowdStrike

CrowdStrike® Inc. (那斯達克指數代號：CRWD) 為全球網路安全領導者，重新定義了雲端時代的安全，透過全新建立的端點保護平台抵禦入侵風險。CrowdStrike Falcon® 平台的單一輕量型代理程式架構利用雲端規模的人工智慧 (AI)，提供即時保護與企業內部完整資訊，防止線上和離線的端點攻擊。CrowdStrike Falcon 由專利的 CrowdStrike Threat Graph® 提供技術支援，每週從全球各地即時關聯超過 3 兆筆端點相關資訊，強化全球數一數二的進階資料平台，為您提供安全防護。

Start Free Trial
of Next-Gen AV

如需更多資訊，請造訪 www.crowdstrike.com

CROWDSTRIKE

FALCON DISCOVER
CROWDSTRIKE IT HYGIENE

Get real-time visibility into who and what is in your network. Instantly get an accurate inventory of the systems in your environment, of the software they are running and of how user accounts are being utilized.

FALCON DISCOVER — REAL-TIME VISIBILITY AND INVENTORY

For IT and Security teams who need to identify and track computers and applications on their network, Falcon Discover™ is the CrowdStrike™ IT hygiene solution. Falcon Discover monitors and inventories systems, application usage and user account usage in real time.

- **See who is on your network at all times** — The real-time system inventory gives you a view of all managed and unmanaged devices in the environment in a simple dashboard with drill-down options.
- **Find out what applications your users are running** — The real-time application inventory provides a view of all applications running in the environment via a simple dashboard with drill-down options. You can see what apps are CURRENTLY running on which hosts without impacting the endpoint. You can also determine when the application was originally launched and pivot to other endpoints running the same app to gain more context, finding usage per application or by host.
- **See where and how user accounts are being accessed across your environment** – Account monitoring provides visibility into the use of administrator credentials and password resets across the enterprise. Falcon Discover provides insight into logon trends (activities/duration) where credentials are being used, and password update information.

KEY BENEFITS

» Gain real-time and historical visibility into your assets and applications

» Be better prepared to face threats

» Identify rogue computers instantly

» Find unprotected systems

» Find out what applications your users are truly using

» See where privileged accounts are being accessed

KEY PRODUCT CAPABILITIES

BE READY TO FACE THREATS

- **Strengthen your security posture proactively** — Falcon Discover allows you to identify what is being utilized so you can ensure your best possible readiness to face attacks. By reporting unauthorized systems and applications in your environment, Falcon Discover enables you to improve your security posture by addressing security issues ahead of attacks.

- **Detect unwanted and vulnerable applications** — Detect whether unpatched or vulnerable applications are being used, so you can patch them before an attacker can take advantage.

- **Remediate unprotected and rogue systems** — The system inventory allows you to find and remediate unmanaged systems and also address systems that could be a risk on your network, such as unprotected BYOD or third-party systems.

- **Mitigate abuse of privileged accounts** — Monitor the usage and creation of administrator credentials across your enterprise and detect if they are being used inappropriately and out of context.

GO BEYOND SECURITY

- **Reduce licensing costs** — The real-time application inventory tells you how often and how long users run an application, enabling you to reconcile license costs with real needs.

- **Satisfy compliance requirements** — By fully automating the visibility and inventory required to ensure some compliance requirements, Falcon Discover helps you achieve, maintain and prove compliance obligations.

ENJOY IMMEDIATE TIME-TO-VALUE —

- **Save time, effort and money** — Cloud-based Falcon Discover is delivered by the CrowdStrike Falcon™ Platform and does not require any on-premises management infrastructure.

- **Immediately operational** — Falcon Discover can be deployed in hours and hits the ground running, monitoring and recording immediately upon installation without requiring reboots, query writing, baselining or complex configuration.

- **Zero impact on performance** — Inventory searches take place in the cloud and have zero impact on endpoints and the network.

PREVENTATIVE SECURITY AND BEYOND

Security starts with discovering where you're not protected, so you can close the gaps and be better prepared to face threats. Falcon Discover provides the visibility and information that security and IT teams need to ensure comprehensive defense against today's sophisticated threats.

CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered next-generation endpoint protection.CrowdStrike has revolutionized endpoint protection by being the first and onlycompany to unify next-generation antivirus, endpoint detection and response (EDR),and a 24/7 managed hunting service — all delivered via a single lightweight agent.

Learn more at **crowdstrike.com**

CROWDSTRIKE

CROWDSTRIKE FALCON X

CrowdStrike Falcon X integrates threat intelligence into endpoint protection, automating incident investigations and speeding breach response

CROWDSTRIKE FALCON X

MAKING PREDICTIVE SECURITY A REALITY

For cyber protection teams that are struggling to respond to cybersecurity alerts and don't have the time or expertise to get ahead of emerging threats, the CrowdStrike Falcon X™ solution delivers the critical intelligence you need, while eliminating the resource-draining complexity of incident investigations. Falcon X is the only solution to truly integrate threat intelligence into endpoint protection, automatically performing investigations, speeding response, and enabling security teams to move from a reactive to a predictive, proactive state.

With the unique cloud-native CrowdStrike Falcon® platform as a foundation, cyber protection teams can now automatically analyze malware found on endpoints, find related samples from the industry's largest malware search engine, and enrich the results with customized threat intelligence. This closed-loop system provides security teams with custom indicators of compromise (IOCs) to share with their other security tools as well as intelligence reporting that tells the complete story of the attack. With a complete understanding of the attack, your team is empowered to respond faster and orchestrate proactive countermeasures across your organization.

Falcon X and integrated threat intelligence is the next step for endpoint protection. It takes antivirus and endpoint detection and response alerts to the next level by not only showing what happened on the endpoint, but also revealing the "who, why and how" behind the attack. Understanding the threat at this level is the key to getting ahead of future attacks and raising the cost to the adversary.

Falcon X enables customers of all sizes to better understand the threats they face and improves the efficacy of their other security investments with actionable and customized intelligence to defend against future attacks, making proactive security a reality.

KEY BENEFITS

- Automates investigations into all threats that reach your endpoints
- Delivers custom IOCs to proactively guard against evasive threats
- Provides complete information on attacks to enable faster, better decisions
- Empowers your team with analysis from CrowdStrike® Intelligence experts
- Simplifies operations via seamless integration with the CrowdStrike Falcon platform

KEY PRODUCT CAPABILITIES

本案提供Falcon X版本

AUTOMATE AND SIMPLIFY INCIDENT INVESTIGATIONS

Seamless endpoint Integration:
Analyze high-impact threats taken directly from your endpoints that are protected by the CrowdStrike Falcon platform. Falcon X analysis is presented as part of the detection details of a Falcon endpoint protection alert. Security teams, regardless of size or skill level, will never miss an opportunity to learn from an attack in their environments.

Save time, effort and money:
Automate each step of a cyber threat investigation and reduce analysis time from days to minutes. Falcon X combines malware analysis, malware search and threat intelligence into a seamless solution.

Stop bad actors in their tracks:
CrowdStrike threat intelligence provides actor attribution to expose the motives, tools and tradecraft of the attacker. Practical guidance and proactive steps are prescribed so your team can deploy proactive countermeasures and get ahead of future attacks.

SHARE CUSTOM IOCs FOR SECURITY ORCHESTRATION

Defend against the most relevant threats
Focus your team on threats you actually encountered. Falcon X delivers custom IOCs that are derived from the automated analysis of threats taken directly from your endpoints. Custom IOCs include protection against the threat you just encountered plus related threats within the same campaign or malware family. This exclusive capability leads to a deeper understanding of the threat and a custom set of IOCs to defend against future attacks.

Gain access to CrowdStrike IOCs
Falcon X allows you to expand your defenses with real-time access to global IOCs delivered by CrowdStrike.

Easily integrate countermeasures
Protect against future attacks with IOCs that are easily consumed by your security infrastructure. A rich suite of APIs and pre-built tools enable easy orchestration with existing security solutions.

EMPOWER YOUR TEAM WITH CROWDSTRIKE THREAT INTELLIGENCE

Intelligence Reports	Receive trusted, in-depth threat intelligence reports from the global CrowdStrike Intelligence team, including real-time threat alerts, technical reports with expert analysis, and strategic reports outlining threats to industries, regions and infrastructure.
Threat Monitoring	Monitor the web for adversary activity against your organization to prioritize resources and effectively respond to impending cyberattacks.
Expert Malware Analysis	Escalate interesting malware samples to a CrowdStrike expert for deeper research or to get a second opinion.
Intelligence Support	The CrowdStrike team works to ensure it has a clear understanding of your intelligence requirements and that you are successfully onboarded. The team also performs quarterly reviews.
YARA/SNORT Rules	Keep ahead of the latest adversary threats and orchestrate your defenses with YARA and SNORT rules, created and validated by CrowdStrike experts.

FALCON X – PRODUCT OFFERINGS

There are two levels of Falcon X, enabling your organization to choose the option that best fits your needs and mission requirements.

Feature	Falcon X	Falcon X Premium
Endpoint Integration	X	X
Intelligence Automation	X	X
Custom Intelligence	X	X
Custom and Global IOCs	X	X
Intelligence Reports		X
Threat Monitoring		X
Intelligence Support		X
Expert Malware Analysis		X
YARA/SNORT Rules		X
Quarterly Briefings		X

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 2.5 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Start Free Trial
of Next-Gen AV

Learn more at **www.crowdstrike.com**