



# Harmony Endpoint

## 您所需的端點保護方案



Harmony Endpoint 是一款完整的端點安全解決方案，專注於幫助遠端辦公人員在目前日漸複雜的威脅環境中保持安全。Harmony Endpoint 有效防止迫在眉睫的端點威脅，如勒索軟體、釣魚攻擊或偷渡式惡意軟體，同時通過自主偵測與回應，快速、最大限度地降低入侵影響。

如此一來，企業只需一款高效且具有成本效益的解決方案即可獲得有力的端點保護。

### 主要產品優勢

全面端點保護：防止迫在眉睫的端點威脅

快速復原：自動檢測 90% 的攻擊、調查和修復任務，無須人員介入

降低總擁有成本：一款高效且富有成本效益的解決方案為您提供所需的一切端點保護

### 獨特的產品功能

進階式的行為分析引擎和機器學習算法在惡意軟體造成損害之前就將惡意程式隔離

高捕獲率和低誤報，確保安全效能和有效防護自動取證數據分析，提供有關威脅的詳細洞察

全面攻擊防護和修復，即時恢復任何受感染的系統

## 市場端點安全的領導解決方案



Harmony Endpoint 被 AV-TEST 評為企業端點保護領域的頂級產品

[瞭解更多](#)



Forrester Wave 將 Check Point 評為端點安全領導者

[瞭解更多](#)



Harmony Endpoint 在 NSS Labs 2020 年高級端點保護測試中獲得 AA 產品評級

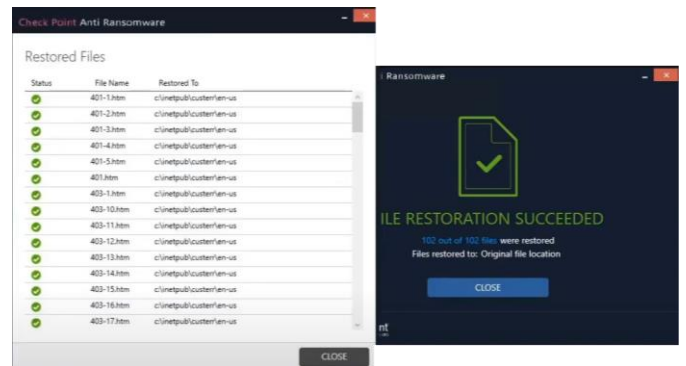
[瞭解更多](#)

## 運作方式

### 360 度的全方面端點保護

#### 防止迫在眉睫的端點威脅

- 即時阻擋來自 Web 瀏覽或電子郵件附檔的惡意軟體以免其侵入端點，不造成用戶生產力的任何影響。用戶通過電子郵件收到或通過 Web 瀏覽器下載的所有文件都將發送到威脅仿真沙箱進行檢測。另外，Harmony Endpoint 還可利用檔案清洗(CDR)對文件進行淨化，在毫秒間交付安全無虞的內容予用戶。
- 在離線模式也可以提供即時且全面性的保護，防止勒索軟體、惡意軟體和無檔案式攻擊。當檢測到異常或惡意行為，端點行為守衛(Behavior Guard)就會攔截並修復整個攻擊鏈，不殘留任何惡意攻擊痕跡。反勒索軟體功能可終止正在加密文件或嘗試入侵 OS 備份等勒索軟體行為，此外更自動恢復被勒索軟體加密的文件。Harmony Endpoint 確保備份空間的安全性，故僅有 Check Point 簽名執行序可以訪問的本地的備份空間。若惡意軟體試圖執行影子復制(Shadow-Copy)刪除，也不會丟失任何數據。
- Check Point 使用獨家 Zero-Phishing® 技術來防止用戶遭受釣魚攻擊，Zero-Phishing® 即時識別並即時阻擋用戶連線至釣魚網站，以防用戶密碼遭竊。Zero-phishing® 還可以進一步檢測外部網站上的是否與企業密碼重複使用情況，有效防止攻擊者執行撞庫攻擊。



#### 市場上最佳的「已知」和「未知」惡意軟體捕獲率

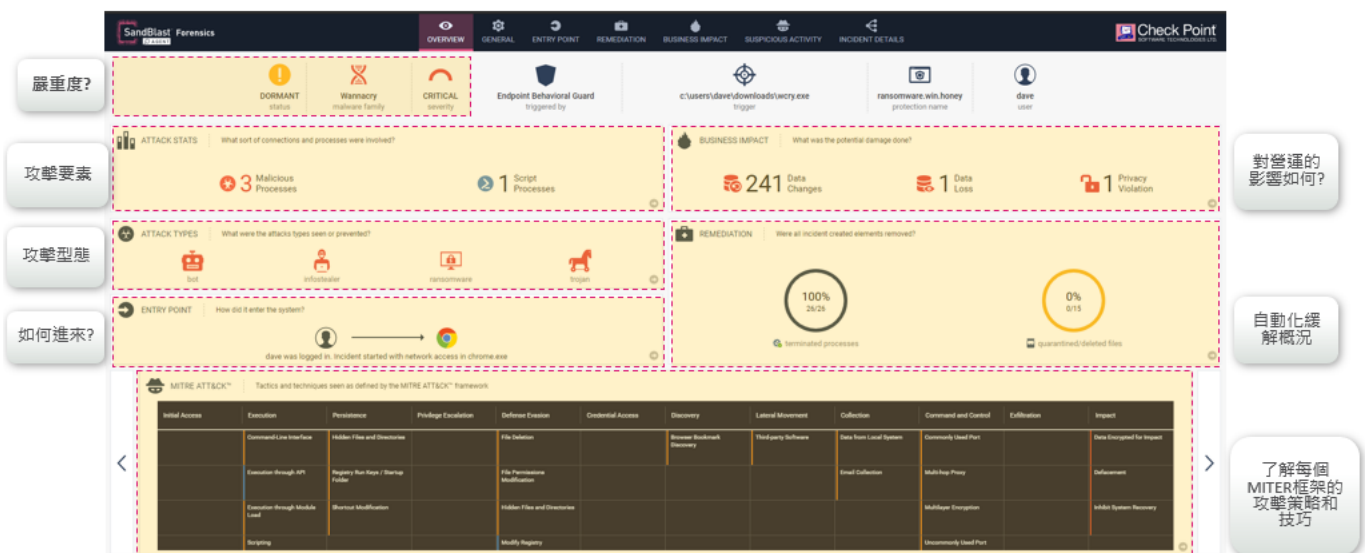
根據 2020 年 AV-TEST 企業端點保護和 NSS 高級端點保護實驗室測試的結果，Harmony Endpoint 是公認的技術先驅。Harmony Endpoint 採用 60 多個威脅防護引擎，並搭載全球最大的威脅情報平台 Check Point ThreatCloud™，可以提供市面上最高的威脅捕獲率。



## 加快恢復速度

### 自動執行 90% 的攻擊檢測、調查和修復任務

- 自動化攻擊控制和修復：市面上唯一可自動化並全面修復整個攻擊狙殺鏈的端點保護解決方案。當 Harmony Endpoint 檢測到攻擊後，受感染設備會被自動隔離以防止橫向感染移動，並恢復至安全狀態。
- 自動化鑑識報告：讓您詳細瞭解受影響資產、攻擊鍊及 MITRE ATT&CK™ 框架對應。鑑識報告記載端點事件，包括受影響文件、啟動的執行序、系統註冊表變化以及網絡活動。強大的攻擊診斷和可視化報告有助於管理人員採取後續補救措施，幫助事件應變團隊高效地診斷和解決攻擊。

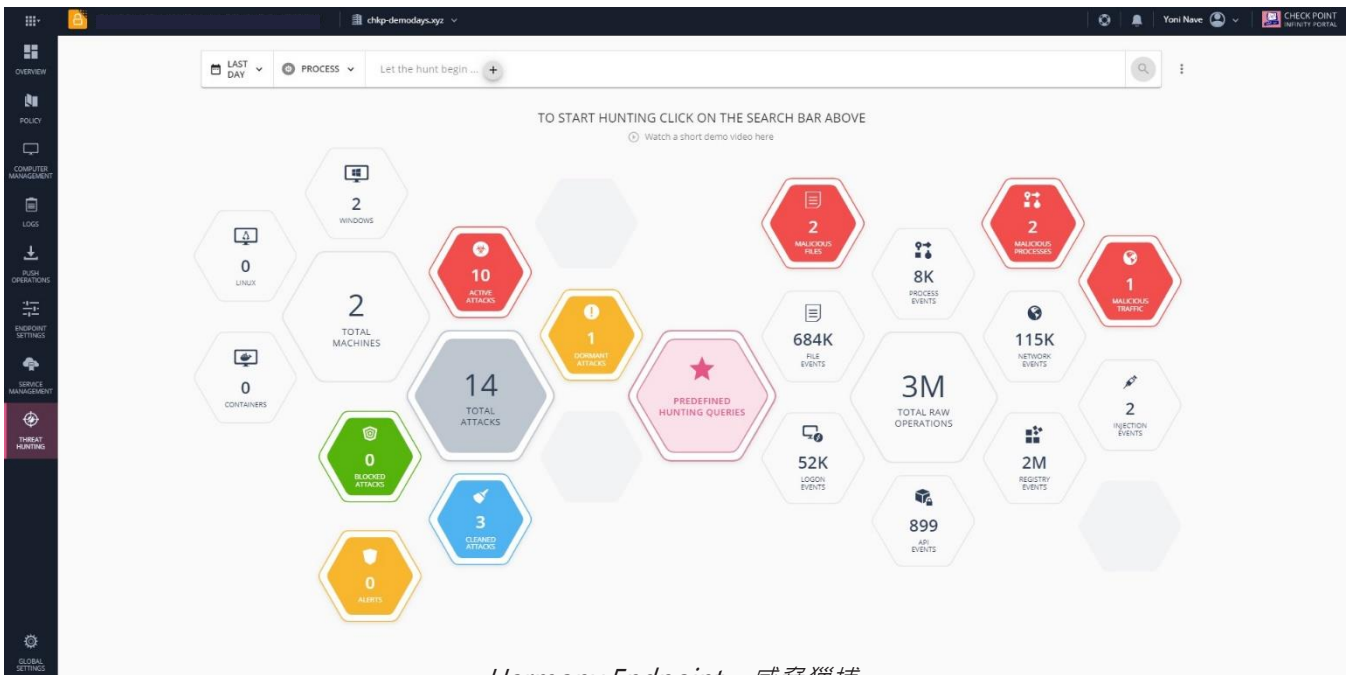


Harmony Endpoint 鑑識報告

使用 Check Point Harmony Endpoint 的最大優勢是，我們無需擔心對我們環境發起的勒索軟體攻擊。它可以讓我們放心無憂，而這對於我們而言至關重要。我們知道它就在守護著我們數據安全。

[IMC Companies 首席資安長 David Ulloa](#)

- 威脅獵捕：透過 ThreatCloud™ 從數億傳感器收集的全球共享威脅情報，來比對企業端點的執行紀錄，找到企業內部潛藏威脅。通過威脅獵捕功能，您可以設置查詢或使用預定義查詢語法深入挖掘可疑事件，並執行修復。



*Harmony Endpoint – 威脅獵捕*

自從我們部署了 Harmony Endpoint，將近一年內都沒有發生過一起因惡意軟體或勒索軟體引起的攻擊事件。

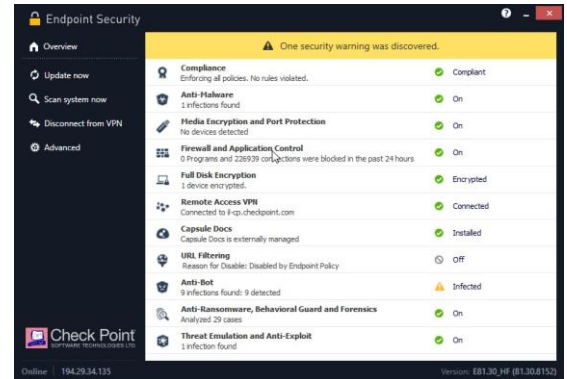
Mississippi Secretary of State 首席技術長 Russell Walker

## 最佳總擁有成本

一款高效且富有成本效益的解決方案為您提供所需的一切端點保護

Harmony Endpoint 提供 EPP、EDR、VPN、NGAV、檔案和 Web 瀏覽保護的單個代理引擎，幫助您企業簡化管理流程，降低總擁有成本。

極為靈活，滿足您的特定安全和合規要求。



- Harmony Endpoint 建立於本地或通過雲服務託管，強大易用的功能且支持快速部署，滿足您的要求
- 支援 Windows、macOS 和 Linux 作業系統
- VDI 功能，支援 VMWare Horizon、Citrix PVS/MCS
- Harmony Endpoint 安裝程序支援無縫升級和復原，對端點用戶而言，無需重啟設備，也不會遭受任何中斷
- 開發人員保護 - 保護開發人員不慎將密碼或金鑰外洩風險，無需整合持續集成/持續交付 (CI/CD) 或者集成開發環境 (IDE)

Check Point Infinity 是首個整合式安全架構，旨在解決連線需求增長和安全性不足所帶來的複雜問題，橫跨網絡、雲、端點、移動設備和物聯網提供全面保護和威脅情報。



“ Check Point Harmony Endpoint 是唯一一款高級端點保護解決方案。對我們而言，Harmony Endpoint 是最適合的高級端點保護解決方案。我們很快就在全球組織中部署了這款解決方案。管理控制台有一個非常直觀的用戶界面，使用起來非常簡單。”

[大型全球基礎設施企業高級安全分析師](#)

## 技術規格

HARMONY ENDPOINT 方案	
方案	<ul style="list-style-type: none"> <li>數據保護 – 包含全硬碟加密和可攜式媒體加密，包括存取控制和端口保護</li> <li>Harmony Endpoint 基礎版 – 包含防毒軟體、防範勒索軟體、阻擋零日釣魚攻擊、高級威脅防護以及端點偵測和回應 (EDR)</li> <li>Harmony Endpoint 高級版 – 包含 Harmony Endpoint 基礎版，以及威脅仿真(Threat Emulation)和威脅萃取(Threat Extraction)</li> <li>Harmony Endpoint 完整版 – 包含 Harmony Endpoint 高級版，以及數據安全 (全硬碟加密和可攜式媒體加密)</li> </ul> 注：端點合規性在所有套件中均有提供
作業系統	
支援的作業系統	<ul style="list-style-type: none"> <li>Windows Workstation 7, 8, and 10</li> <li>Windows Server 2008 R2, 2012, 2012 R2, 2016, 2018, 2019</li> <li>MacOS Sierra 10.12, MacOS High Sierra 10.13, MacOS Mojave 10.14, MacOS Catalina 10.15, MacOS BigSur 11.x</li> <li>Linux Ubuntu (16.04, 18.04, 20.04), Debian (9.12-10.10), RHEL (7.8-8.3), CentOS (7.8-8.3), Oracle (7.8-8.3), Amazon (2)</li> </ul>
跨電子郵件和 Web 進行檔案清洗 (CDR)	
威脅萃取	移除可能被惡意利用的內容，重建文件以消除潛在威脅，並在幾秒內向用戶提供處理後的乾淨檔案
威脅仿真	<ul style="list-style-type: none"> <li>借助威脅沙箱功能來檢測和阻擋電子郵件附件、已下載檔案與電子郵件附件的 URL 中發現的未知惡意軟體和 APT 攻擊行為。</li> <li>提供多種 Windows 作業系統環境及各種不同類型的文件 (包括 MS Office、Adobe PDF、Java、Flash、執行檔和存檔等) 模擬</li> <li>發現 SSL 和 TLS 加密通信中隱藏的威脅</li> </ul>
集中化管理	
雲端 & 本地管理	<ul style="list-style-type: none"> <li>Harmony Service (透過雲端主機進行服務)</li> <li>Harmony Appliance (在本地端建立一台管理主機)</li> </ul>
NGAV：運行時檢測和保護	
防勒索軟體	<ul style="list-style-type: none"> <li>威脅防護 - 持續監控勒索軟體行為，並識別非法文件加密和無簽名情況</li> <li>檢測與隔離 - 通過鑑識分析識別勒索軟體攻擊的所有元素，予以隔離</li> <li>數據恢復 - 自動從備份區中恢復加密文件，確保完整業務持續性</li> </ul>
防漏洞利用	<ul style="list-style-type: none"> <li>保護攻擊者對合法軟體漏洞攻擊所產生的衝擊</li> <li>藉由程式在運行時來識別可疑的記憶體操作以檢測漏洞是否遭利用</li> <li>即時阻擋遭惡意利用的執行序，並自動化修復整個攻擊鏈</li> </ul>
行為守衛	<ul style="list-style-type: none"> <li>主動檢測執行序的惡意行為並即時阻擋</li> <li>即時辨識、分類和阻擋惡意執行序，透過最小執行程序樹的模擬</li> </ul>
Web 保護	
零日釣魚保護	<ul style="list-style-type: none"> <li>即時阻擋未知的釣魚網站</li> <li>對網站中的可疑元素進行靜態和啟發式檢測</li> </ul>
公司密碼保護	檢測外部網站上的是否與企業密碼重複使用情況
URL 過濾	<ul style="list-style-type: none"> <li>輕量級瀏覽器插件，即時允許/阻擋用戶訪問的網站</li> <li>根據企業內部資安政策建立用戶之網路連線行為過濾</li> <li>提供 HTTPS 流量的完整可視性</li> </ul>
威脅獵捕	
威脅獵捕	收集端點上的所有原始事件和檢測到的事件，主動進行威脅獵捕並深入調查事件

## 為何選擇 Harmony Endpoint ?

現今，端點安全在遠端辦公的作用日益重要。鑑於 70% 的網絡攻擊都始於端點，提供最高安全級別的全面端點保護對於避免安全漏洞攻擊和數據洩露至關重要。

Harmony Endpoint 是一款完整的端點安全解決方案，專用於幫助遠端辦公人員在目前日漸復雜的威脅環境中保持安全。Harmony Endpoint 解決方案可以防止迫在眉睫的端點威脅，如勒索軟體、釣魚攻擊或偷渡式惡意軟體，同時通過自主偵測與回應快速、最大限度地降低入侵影響。

如此一來，企業只需一款高效且富有成本效益的解決方案即可獲得所需的有力端點保護。

Harmony Endpoint 是市場上首個專門針對用戶、設備和訪問打造的統一安全解決方案 Check Point Harmony 產品套裝的一部分。Harmony 集六款產品於一身，可以為所有人提供毫無漏洞的卓越安全性和簡便性。它不僅能保護設備和上網免受駭客攻擊，還可確保對企業應用程序的零信任訪問，所有這些只需一款易於使用、管理和購買的解決方案即可實現。

瞭解更多：<https://www.checkpoint.com/products/advanced-endpoint-protection/>

### 全球總部

5 Ha' Solelim Street, Tel Aviv 67897, Israel | 電話：972-3-753-4555 | 傳真：972-3-624-1100 | 電子郵件：info@checkpoint.com

### 台灣分公司

台灣台北市松山區敦化北路205號7樓 | 電話：886 2 2719 9030 | 傳真：886 2 2719 9070

[www.checkpoint.com](http://www.checkpoint.com)