Kaspersky® Endpoint Security for Business

保護貴企業最重視的資產

IT 安全預算無法永遠反應持續增加的業務需求和與日俱增的威脅程度。資源必須經過優化，才能滿足現今 - 以及日後的挑戰。不過該怎麼做，才能找出適合的安全解決方案 - 一個可以保護您 IT 基礎結構的每個元素不受最先進的網路威脅影響，以及可以在不斷改變的環境中確保業務連續性，而不會讓您超出預算的安全解決方案？

請試著詢問我們的客戶。**Kaspersky Endpoint Security for Business** 提供的全方位適性化安全防護可以配合貴企業擴充，透過全套最先進的技術來保護貴企業的連續性與資產。結果不言可喻。

領先全球的安全情報已內化成為我們的一部分，並且協助我們建立決策。做為一家獨立公司，使我們更加靈活、多元思考，而且行動更加迅速，以對抗和抵禦不分來源或目的的網路威脅。這也是我們的產品和解決方案能夠提供其他供應商無法提供真正網路安全水準的原因。

Common Criteria

Ready for GDPR

可以放心交給它的真正網路安全

結合多層次防護方法的先進技術，可以在效能和有效防護間取得完美平衡。卡巴斯基實驗室在 Gartner 2018 年端點防護平台重要功能的每個使用案例中被評選為前 3 大供應商。

保護端點、伺服器和閘道
全球歷經最多測試考驗以及獲獎項目最多的安全防護技術可協助強化防護，同時將誤判率降到最低 - 保護容器、伺服器和閘道，以及每個端點。

簡化安全管理和委派
整合式網頁主控台整合了 Active Directory 以及角色型存取控制 (RBAC) 和可自訂儀表板，因此可以因應團隊成員的職責簡化存取。

降低複雜度和整體擁有成本
不須費心即可保持在最新狀態，即使是 Windows 版本之間的移轉或升級至我們端點防護產品的未來版本。

強化系統並提高生產力
主機入侵防範和雲端式異常、網頁、裝置和應用程式的控制都可以減少您的攻擊面，並可協助控制企業資源 (即使位於您的 IT 防護網外部)。

全年無休保護弱點以減少攻擊進入點
透過 150 多種軟體應用程式的支援，我們的弱點監控和修補程式管理可以為所有最廣泛使用的業務應用程式提供全方位的防護。

將作業系統和軟體部署工作自動化來節省時間
在分公司或家庭辦公室設定全新工作站，能夠以遠端和自動化的方式完成。您也可以推出和安排新的應用程式在下班時間自動安裝。

找出更多攻擊和入侵 - 即使沒有定期更新
我們的輕量化雲端模式可以提供最佳的防護，也能把對 PC 資源和網際網路頻寬使用的影響降到最低。無特徵碼元件甚至可以在沒有頻繁更新的情況下偵測威脅，並且可以透過新世代靜態 (前置執行) 和動態 (後置執行) 機器學習 (ML) 進行強化。

我們的知識就是您的力量

由全球頂尖的專家所建立的適性化安全防護，可以把對資源和管理負荷的影響降到最低。防護和 ML 型技術可以找出和封鎖端點威脅，不分來源或目標。此外，即使您遭到攻擊，也可以將惡意行動復原，因此您的使用者可以繼續工作。

小錯誤不該變成大問題

可以保護多變的環境和輕鬆擴充，而不需要廣泛規劃，即使在異質 IT 基礎結構中，也可以讓您自由變更任何預先定義的設定以及選擇適應新功能的時機。

數位轉型中的寧靜

我們已經將 EDR 代理程式的部署、修補程式管理、攻擊後復原，以及軟體發佈等處理程序自動化，您不需要費心處理。我們在獨立測試和分析評論中一致的高效能，代表我們的產品有口皆碑 - 這是您可以信任的真正網路安全。

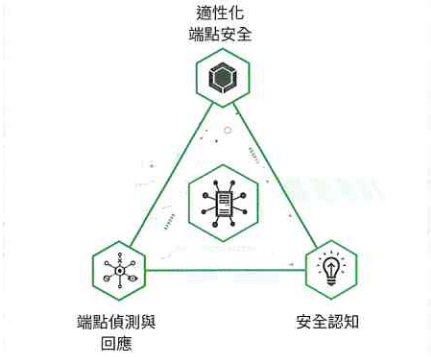
三個漸進式功能套件

Kaspersky Endpoint Security for Business 的工具和技術能夠以智慧的方式在漸進式防護層中達到均衡，以滿足貴企業發展過程中每個階段對於持續發展的安全與 IT 需求。

如需更多詳細資料，請參閱我們涵蓋每個防護層的個別資料表 -「標準」、「進階」和「全方位」。

支援與服務

我們的營運範圍超過 200 個國家，全球擁有 35 間辦公室，全年無休致力於提供全球支援，我們的維護服務合約 (MSA) 支援套件亦表現出此特性。我們的專業服務團隊隨時待命，確保您可以從您的解決方案中獲得最大的優勢、協助您進行部署，以及在發生重大事件的期間提供支援。



如需系統需求，請參閱知識庫

除了端點防護以外 - 目前與未來

我們的技術以無可比擬的即時威脅情報和機器學習來源為基礎持續發展，可以讓您保護貴企業最重視的資產不受 Crypto Miner 和最新最複雜的網路威脅影響。

受到和您一樣的決策制定者認可

忘了行銷炒作 - 聽聽已經升級至 Kaspersky Endpoint Security for Business 的使用者有哪些建議，以及他們所享有的好處：

- 始終如一的傑出防護 - 輕鬆的一步升級可確保您永遠保持在最新狀態，並且為對抗最新網路威脅做好準備
- 容易使用和集中管理 - 一部伺服器、一個網頁主控台、一個單一代理程式
- 更深入的元件整合 - 在內部打造，擁有數十年的頂級評等和獨立驗證經歷
- 單次購買即可擁有所需要的一切 - 成本和授權簡單明瞭。

品質檢查員
產業 製造業
角色 基礎結構和營運
廠商規模 <50M 美元
最後更新 2018 年 10 月 25 日
https://kas.pr/epp-ref2

「可以快速建置的完整安全防護。」

請您親自見證

我們對於研發高度重視，讓我們可以將資源部署在最重要的地方、提供具有成本效益的防護技術，以及將諸多技術創新整合到我們的產品。請您親自體驗真正的網路安全！造訪這個網頁，**即可體驗完整版本的** Kaspersky Endpoint Security for Business。

更大的願景 - Kaspersky IT Security Solutions for Business

端點防護固然重要，但只是個開始。不論您是否採行同級最佳或單一來源的安全策略，卡巴斯基實驗室都有適用於混合式雲端基礎結構，以及可以和老舊 Windows XP 系統搭配使用或單獨運作的產品供您選擇，而不會犧牲效能效率或是讓您放棄選擇的自由。請造訪我們的網站以深入了解。

卡巴斯基實驗室
尋找鄰近的銷售夥伴：www.kaspersky.com/buyoffline
Kaspersky for Business：www.kaspersky.com/business
企業網路安全：www.kaspersky.com/enterprise
IT 安全新聞：business.kaspersky.com/

真正的網路安全
#HuMachine

www.kaspersky.com

台灣聯繫人：台灣銷售總監 黃茂勳 eden.huang@kaspersky.com

kaspersky BRING ON THE FUTURE

Kaspersky Sandbox

進階偵測功能可以防止未知和規避式威脅 - 不需要雇用 IT 安全專家

現在先進的網路攻擊能夠癱瘓公司，並且對財務和商譽造成破壞。金融資產和交易機密遭竊、因服務中斷而喪失客戶的信任，以及複雜的威脅所造成的諸多其他負面影響，都會對企業的踏實穩健及宏開駿業造成嚴重影響。若要防止快速發展的網路攻擊，針對保護周邊網路 (防火牆、電子郵件、網頁閘道、Proxy 伺服器)，以及工作站和伺服器 (具備基本功能的防毒保護和端點防護平台等級解決方案) 所設計的傳統工具已經不敷使用。這正是有遠見的公司必須認真考慮使用專業工具來偵測、調查與回應複雜事件的原因。

Kaspersky Sandbox 解決方案非常適合：

- 沒有專屬的安全團隊可以將 IT 安全人員分派到 IT 部門的公司。
- 不希望負擔額外 IT 安全資源的小型企業。
- 基礎結構分佈在各地，而且沒有 IT 安全專家駐點的大型企業組織。
- 必須確保全職 IT 安全分析師全心處理重要工作的公司。

二十多年來，卡巴斯基持續為各個規模、產業，以及 IT 安全成熟度的公司打造防護工具。因為持續不斷的研發，以及在威脅獵捕、調查和回應方面的進步，讓卡巴斯基始終在最前線對抗網路犯罪。

卡巴斯基對抗複雜威脅的產品和服務組合包括：

- Kaspersky Anti Targeted Attack：可以在網路層偵測和調查複雜威脅與針對性攻擊的先進解決方案。
- Kaspersky Endpoint Detection and Response：可以偵測、調查和回應鎖定工作站與伺服器之複雜威脅的解決方案。
- Kaspersky Threat Intelligence Portal：提供雲端沙箱的存取權限，以及 APT 威脅的分析報告和其他服務。

不過，若要有效利用這些解決方案與服務，公司必須擁有一個具備適當經驗和專業知識的成熟 IT 安全部門。全球缺乏經過訓練可以解決複雜威脅的專家，以及雇用這些專家的成本，通常是阻擋公司獲得這些解決方案與服務的主要原因。

採用專利技術 (專利號碼 US 10339301B2) Kaspersky Sandbox 可協助企業組織對抗數量和複雜度持續增加，並且可以繞過現有端點防護的現代威脅。Kaspersky Sandbox 讓 Kaspersky Endpoint Security for Business 的功能更加完備，使企業組織能夠大幅提高其工作站與伺服器的防護水準，得以防止過去未知的惡意程式、新型病毒和勒索軟體、零日入侵程式等 - 而不需要高度專業的資訊安全分析師。

這讓小型企業免於付出招募和雇用這些高價值專家的必要開支。對於擁有分散式網路大型企業，這也有助於將其成本最佳化，在減輕其安全分析師人工作業的工作量之餘，還可以有效保護其遠端辦公室。

提供和部署選項：
Kaspersky Sandbox 是以 ISO 映像檔提供，內含預先設定的 CentOS 7 和所有必要的解決方案元件。Kaspersky Sandbox 可以部署在實體伺服器或 VMware ESXi 的虛擬伺服器上。

整合：
- SIEM 系統可以接收 Kaspersky Sandbox 所偵測的相關資訊。這項資訊會按照一般事件流程透過 Kaspersky Security Center 傳送。
- 因為 API 是在 Kaspersky Sandbox 中執行，可以和其他解決方案加以整合，所以能夠將檔案傳送至 Kaspersky Sandbox 進行掃描，並向其要求檔案評價。

擴充性
此解決方案的基本配置可以支援多達 1,000 個受保護的端點，因此可以輕鬆擴充，為大型基礎結構提供持續防護。

叢集
多部伺服器可以組成叢集來提高容量和實現高可用性。

授權
Kaspersky Sandbox 是以軟體裝置提供授權。一個授權內含對多達 1,000 位 Kaspersky Endpoint Security for Business 使用者的支援。

運作方式

Kaspersky Sandbox 可以利用我們的專家最佳實務來對抗複雜威脅和 APT 等級的攻擊，而且可以和 Kaspersky Endpoint Security for Business 緊密整合。Kaspersky Sandbox 可以透過我們整合的原則式管理主控台 Kaspersky Security Center 進行管理。

Kaspersky Endpoint Security for Business 代理程式會向位於 Kaspersky Sandbox 伺服器上的分析結果共用作業快取要求可疑物件的資料。如果物件已經完成掃描，Kaspersky Endpoint Security for Business 便會收到物件的分析結果，並且套用一或多個修復選項：

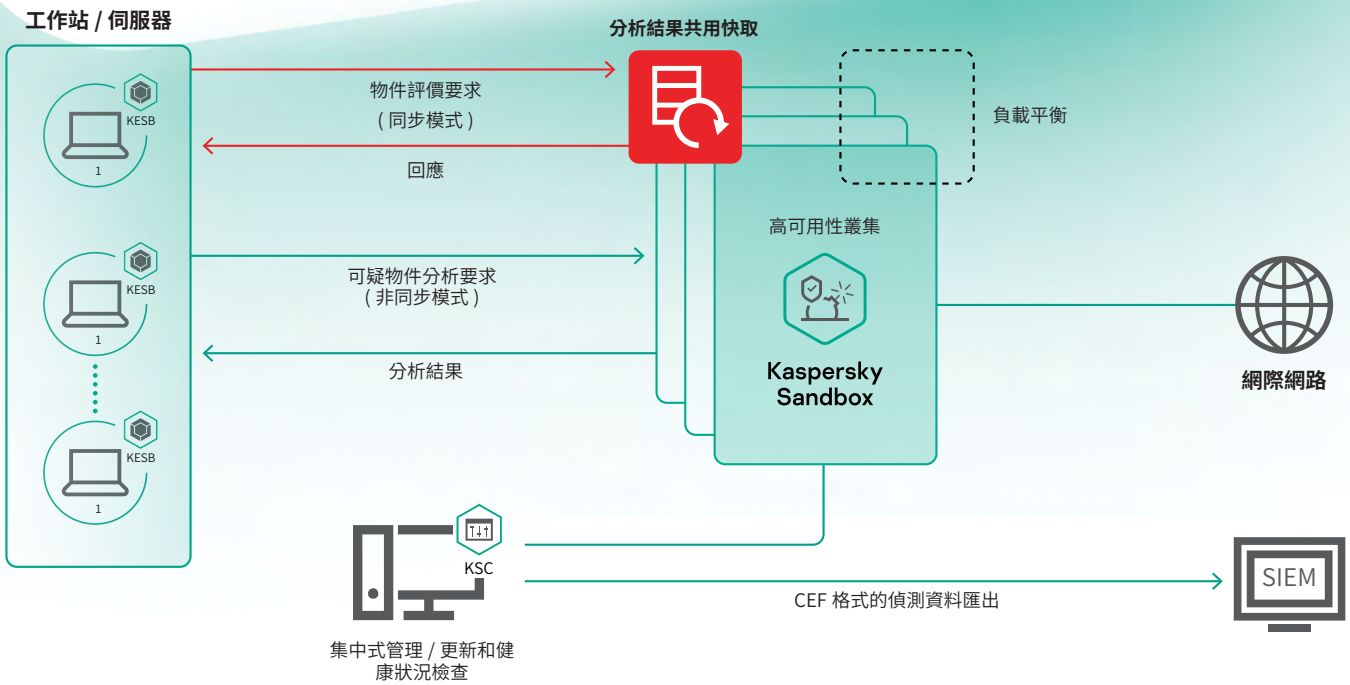
- 移除或隔離
- 通知使用者
- 開始關鍵區域掃描
- 在管理的網路中搜尋其他電腦上的已偵測物件。

如果無法從快取中取得物件評價的分析結果，Kaspersky Endpoint Security for Business 代理程式會將可疑檔案傳送至沙箱並等候回應。沙箱會收到掃描該物件的要求，此時測試的物件會在與實際基礎結構隔離的環境中執行。

檔案掃描會在配備各種工具的虛擬機器中執行，這些工具可以模擬一般的工作環境 (作業系統 / 已安裝應用程式)。為了偵測惡意物件，沙箱會執行行為分析並收集和分析產物，如果物件執行惡意行動，沙箱會將其辨識為惡意程式。在進行沙箱分析期間，Kaspersky Sandbox 會將分析結果指派給物件。

一旦完成物件的模擬程序，產生的分析結果就會即時傳送至分析結果的共用作業快取，讓安裝 Kaspersky Endpoint Security for Business 的其他主機可以快速取得已掃描物件的評價資料，而不需要再次分析相同的檔案。這個方法可以確保快速處理可疑物件、降低 Kaspersky Sandbox 伺服器的負載，以及提高威脅的回應速度和效率。

Kaspersky Sandbox 是 Kaspersky Endpoint Security for Business 重要的新增解決方案。Kaspersky Sandbox 會自動封鎖進階、未知和複雜的威脅，而不需要額外的資源，並且可以讓 IT 安全分析師專心處理其他工作。



網路威脅新聞：www.securelist.com
IT 安全新聞：business.kaspersky.com
適用於中小型企業的 IT 安全：kaspersky.com/business
適用於企業的 IT 安全：kaspersky.com/enterprise

www.kaspersky.com

台灣聯繫人：台灣銷售總監 黃茂勳
eden.huang@kaspersky.com

我們久經考驗。我們獨立自主。我們公開透明。我們承諾打造一個更安全的世界，以科技改善我們的生活。這正是我們要保護這個世界，無論你我都能擁有這個世界帶來無窮機會的原因。實現網路安全，讓明天更加安全。

在此深入了解：kaspersky.com/transparency

久經考驗。
公開透明。
獨立自主。

Kaspersky Endpoint Detection and Response

為回應進階威脅與現代的網路攻擊，企業持續改善其安全策略。對網路犯罪者而言，端點仍是主要的目標─不過現在的威脅可以避開傳統的端點安全防護措施、中斷關鍵業務流程、讓生產力降低，以及增加營運成本。

延遲導致金錢損失

相較於立即做出回應，在事件探索之後的一星期才進行復原，導致企業損失的金額會**超過200%**。

卡巴斯基實驗室企業 IT 風險調查

Kaspersky EDR 非常適合希望實現以下目標的企業組織：

- 自動威脅辨識與回應─而不會讓業務中斷
- 利用先進的技術改善端點可視性與威脅偵測，包括 ML (機器學習)、沙箱、入侵指標 (IoC) 掃描與威脅情報
- 改善安全防護─利用容易使用的企業解決方案來改善事件回應
- 建立整合且有效的威脅獵捕、事件管理及回應流程。

協助符合法務遵循：

透過內部部署的 Kaspersky Private Security Network 分享即時威脅情報。

- 透過 KPSN 整合，沒有仰賴雲端和資料外流的疑慮。
- 所有的鑑識資料都會集中儲存在企業自有環境中的 Kaspersky EDR。

主動追蹤威脅：

將全年無休的威脅獵捕服務卡巴斯基託管防護新增至 Kaspersky EDR 部署，即可讓企業存取全球威脅研究。
此外，卡巴斯基實驗室的威脅研究人員可以：

- 檢閱企業環境中所收集的資料；
- 快速通知企業的安全團隊─如果偵測到惡意活動；
- 提供回應與修復處理方式的建議。

產品特性

適性化威脅回應

Kaspersky EDR 內含多種自動回應功能，可以協助企業避免使用傳統的修復處理程序─例如抹除和重新安裝映像所導致的昂貴停機和生產力損失。

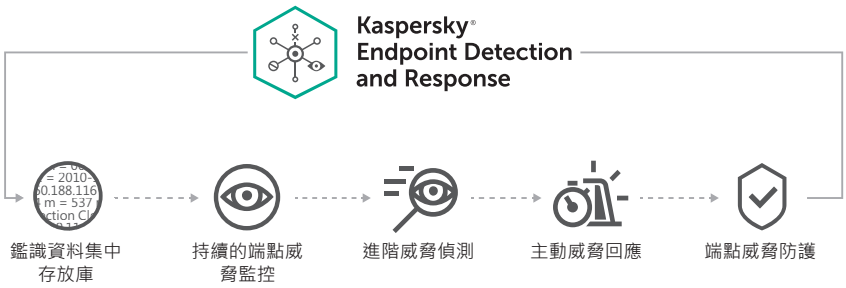
主動威脅獵捕

有了使用集中化資料庫，以及入侵指標 (IoC) 搜尋的快速搜尋功能，Kaspersky EDR 可以徹底改變安全防護工作流程。您的安全團隊可以主動狩獵威脅，而不需要等候警示─主動掃描端點找出異常訊號及安全漏洞。

直覺的網頁介面

Kaspersky EDR 的瀏覽器型介面非常容易使用，可以為安全人員提供下列各項操作的整合可視性與控制能力：偵測、調查、防止、警示與報告。

因為可以透過單一介面監測與控制多種功能，所以您的安全團隊能夠以更有效的方式和更高的效率執行安全工作─而不需要在各種工具和多個主控台間來回切換。



快速找出並遏止進階威脅

Kaspersky Endpoint Detection and Response (Kaspersky EDR) 可以協助企業進行偵測、調查與回應：

- 改善對所有端點的可視性
- 自動處理手動回應的工作
- 改善調查的功能

...而且相容於傳統的端點安全解決方案。

Kaspersky EDR 可以協助安全團隊─以及經驗較少的回應負責人─以網路回應專家的精準度，將端點分類。有了 Kaspersky EDR，貴組織即可：

- 有效「監控」威脅─超越惡意程式
- 有效「偵測」威脅─利用先進的技術
- 集中「彙總」鑑識資料
- 快速「回應」攻擊
- 透過探索的威脅「防止」惡意行動

...這些全都可以透過強大的網頁介面執行，讓調查和反應更加容易。

使用案例：

- 即時主動研究的入侵證據—包括入侵指標 (IoC) —範圍遍及整個網路
- 快速偵測與修復入侵漏洞—在入侵者造成重大破壞與業務中斷之前進行
- 整合 SIEM —協助建立警示和端點活動間的關聯
- 驗證其他安全解決方案找到的警示與潛在事件
- 以無縫的工作流程進行事件的快速調查與集中管理—範圍涵蓋數千個端點
- 將日常作業自動化—協助將手動工作減到最少、空出資源，以及減少「警示過多」的可能性。

進階端點安全防護

卡巴斯基實驗室在端點防護方面展現出持續領先的地位，原因在於我們將以下五個重要元素結合至單一解決方案：

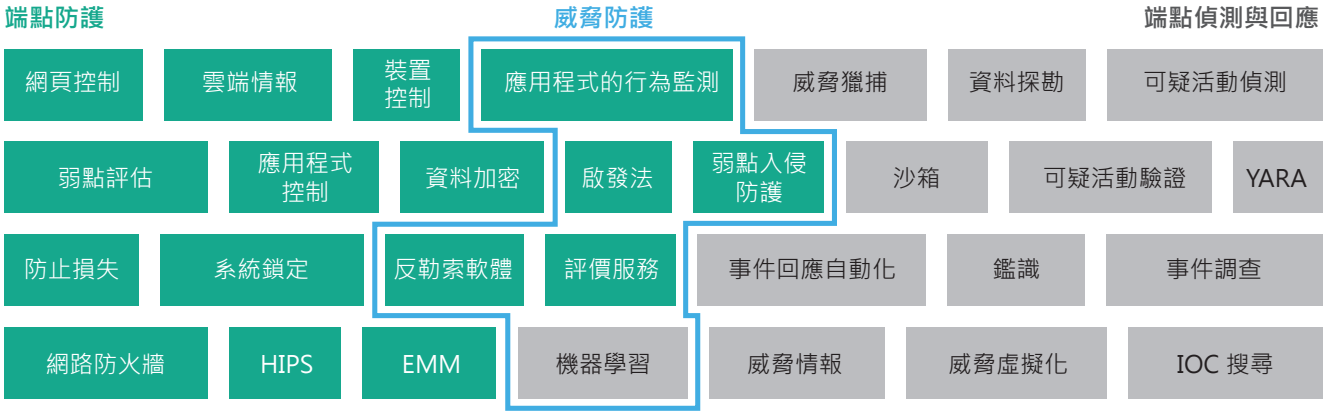
- 強大的新世代防惡意程式引擎—內含機器學習
- 端點偵測與回應 (Kaspersky EDR)
- 全年無休的威脅獵捕服務—卡巴斯基託管防護服務
- 即時威脅情報的存取權—透過 Kaspersky Security Network
- 先進的端點控制 (裝置 / 網頁 / 應用程式、加密等)。

為傳統端點提供安全防護

因為 Kaspersky EDR 相容於來自各種不同供應商的多種傳統安全防護產品，而且也可以配合企業現有的端點安全防護運作，協助增加：

- 新世代功能—用於進階偵測與防護；
- 集中式偵測與回應流程。

...企業不需要更換現有的安全解決方案。



在隔離的虛擬環境中進行物件分析

Kaspersky EDR 內含內部部署的進階沙箱，可以自動擷取任何端點中的任何檔案進行深度分析。Kaspersky EDR 有效為企業提供內部病毒實驗室—而不會將任何資料傳送到網路外部。

進階偵測—包含機器學習

Kaspersky EDR 的機器學習引擎—針對性攻擊分析器 (TAA)，可以建立端點行為的基準狀態。這可以提供用來探索入侵如何發生的歷程記錄。此外，建立鑑識資料、威脅情報和安全引擎分析結果的關聯性，將有助於偵測異常訊號。

企業整體的商業優勢：

降低成本

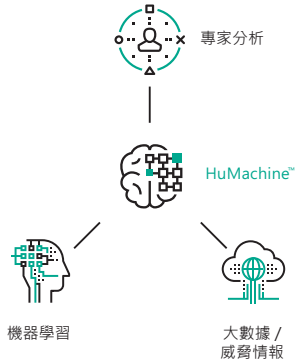
- 將手動工作自動化—在威脅偵測與回應期間
- 協助加快威脅遏止的速度—可節省金錢與資源
- 讓 IT 與安全人員有時間處理其他工作
- 協助將調查期間的業務中斷次數減到最少

提升投資報酬率

- 實現高效率的工作流程
- 縮短威脅辨識與回應的時間
- 強制建立端點記錄、警示檢閱和調查結果的文件，協助符合法務遵循—(PCI DSS 等)

緩解攻擊風險

- 協助排除安全防護缺口，並減少攻擊的「暫留時間」
- 簡化威脅分析與事件回應
- 為現有的安全防護提供威脅驗證



卡巴斯基實驗室
企業網路安全：www.kaspersky.com/enterprise
網路威脅新聞：www.securelist.com
IT 安全新聞：business.kaspersky.com/

真正的網路安全
#HuMachine

www.kaspersky.com

台灣聯繫人：台灣銷售總監 黃茂勳 eden.huang@kaspersky.com