Kaspersky® Hybrid Cloud Security

適用於混合式雲端的可靠防護與無邊界協調流程

企業採用雲端的主要挑戰：

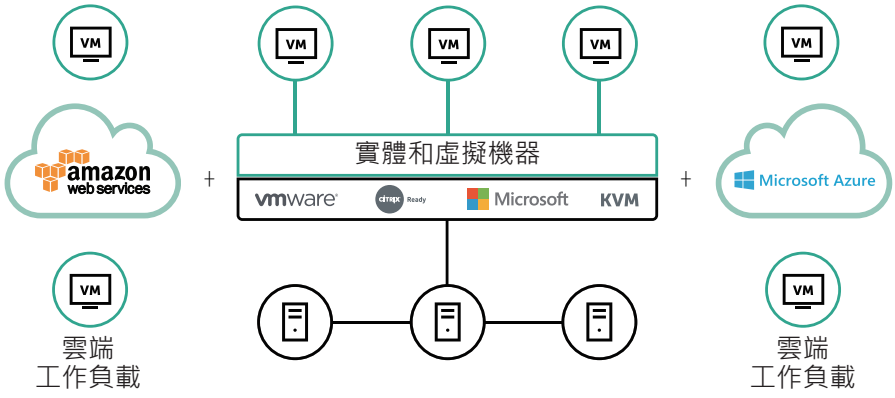
- 基礎結構的複雜度日益增加，導致透明度降低
- 單一產品罕有多層次的防護方式 (可靠防護的關鍵)
- 傳統的重量級安全功能會佔用寶貴的系統資源
- 定址方法和獨立控制會造成額外的系統管理和安全挑戰
- 惡意程式與勒索軟體會攻擊虛擬以及實體端點
- 無法為個人資料防護建置適當的網路安全措施，可能會導致法律問題。

為什麼選擇 Kaspersky Hybrid Cloud Security ？

- 專為實體、虛擬和雲端工作負載所設計
- 適合所有類型工作負載的整合多層次安全功能
- 為 AWS 和 Azure 公用雲端提供一致、自動化與靈活的安全功能
- 利用完整的安全工具組合協助承擔共同責任
- 可以在整個混合式雲端執行無縫安全協調流程
- 根據眾多獎項和獨立測試，這是通過最多測試，安全性最高的防護 [1]
- 採用贏得客戶信任和肯定的技術，其中包括 Gartner Peer Insights 頒發的白金客戶獎 (Platinum Customer Award)。

對每個力求靈活和效率的企業而言，虛擬化已經成為主要的方法。雲端運算自然是下一個步驟。虛擬化可以擺脫複雜基礎結構的支援限制，並且可以提供過去無法企及的效率水準。不過，雲端應用有其風險和複雜度，其中部分為歷來首見，部分則是自實體機器留存至今。

Kaspersky Hybrid Cloud Security 可以為任何階段或形式的雲端應用提供整合安全功能。Kaspersky Hybrid Cloud Security 適用於雲端移轉以及原生雲端的形式，無論是在內部部署、資料中心，或是公用雲端中執行，都能保護您的實體和虛擬工作負載。因為 Kaspersky Hybrid Cloud Security 的應用程式在建立時考慮到虛擬化和伺服器的特性，所以可以針對目前和未來最先進的威脅提供完美平衡的防護，而不會減損系統效能。



主要優勢

可以保護雲端應用—而不會降低防護水準

- 專利的技術和我們獲獎的網路安全引擎，可以保護您所有的工作負載—實體、虛擬，或是雲端式工作負載。
- 搭載機器學習的多層次即時防護，可以防止您的資料、處理程序和應用程式遭到新興威脅攻擊。
- 整體考量的資料安全防護方法，有助於降低與資料防護法規相關的法律及商譽風險。

1 測試係指一系列卡巴斯基實驗室產品，採用和 Kaspersky Hybrid Cloud Security 中使用的相同威脅防護技術。

Kaspersky Humachine ™方法

Kaspersky HuMachine ™將大數據威脅情報、機器人機器學習功能，以及和人類專家經驗無縫融合，因此可以提供多種優勢以及效率更高的防護。將各項元素予以結合，即可將個別元件強化為效率更高的有效整體。

確保能夠從資源和投資獲得最大收益

- 無代理程式和代理程式型防護，可以保護一般及軟體定義網路中的虛擬化資產，而不會對效能造成影響。
- 與原生的公用及託管雲端安全防護整合，有助於以最少的資源使用量來保護您的應用程式、作業系統、資料流和使用者工作區。
- 實體和虛擬資源的單點視圖管理，可以節省採用與維護期間的人力。

無論混合式基礎結構採用哪種配置，都能提供完整的可視性與控制能力

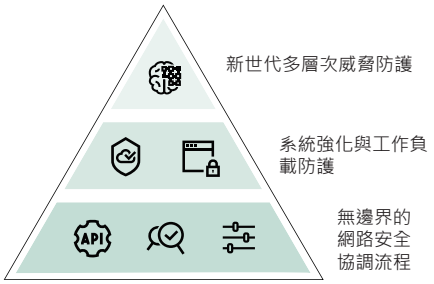
- 管理能力和安全協調流程可以跨多個雲端順暢執行。
- 可以為所有地點的所有工作負載提供防止最先進威脅的完整可視性、控制能力和整體防護。
- 可以讓您更輕鬆在混合式雲端直接進行安全服務佈建和原則式操作。

功能

搭載 HuMachine 的多層次威脅防護

卡巴斯基的新一代惡意程式防護採用多個主動式安全防護層，能夠阻止最廣泛的網路攻擊，防止這些攻擊威脅到您的關鍵業務工作負載。

- **全球威脅情報**可以提供威脅現況的即時狀態資料，即使狀態發生變化，也能隨時確保您的防護。
- **機器學習：**全球威脅情報的大數據會交由結合機器學習演算法和人類專業知識的功能處理，以在最低的誤判率下達到可靠的高偵測水準。
- **網頁及郵件威脅防護**可以讓虛擬和遠端桌面安全運作，保護這些桌面不受電子郵件式或網頁式威脅的影響。
- **檔案完整性監控**有助於確保關鍵系統元件和其他重要檔案的完整性。
- **記錄檢查**會掃描內部記錄檔文件，以獲得最佳的操作衛生。
- **行為分析**可以監控應用程式及處理程序，防止無主體惡意程式或指令碼式惡意程式等進階威脅。
- **修復引擎**可以將雲端工作負載中所做的任何惡意變更復原 (如有必要)。
- **弱點入侵防護**提供可以有效防止第一波攻擊的防護，同時確保完美相容於受保護的應用程式，對其效能的影響最小。
- **反勒索軟體功能**可以保護虛擬工作負載，防止將關鍵業務資料用於勒索的任何企圖，因此可以將受影響的文件復原至加密前的狀態，以及封鎖遠端啟動的加密。
- **網路威脅防護**可以偵測並防止網路型入侵威脅侵入雲端式資產。



適用於任何雲端的整合安全功能

公用雲端
- Amazon Web Services (AWS)
- Microsoft Azure

私人資料中心
- Vmware NSX
- Microsoft Hyper-V
- Citrix XenServer
- KVM
- Proxmox

VDI 環境
- Vmware Horizon
- Citrix XenDesktop

實體伺服器
- Windows
- Linux

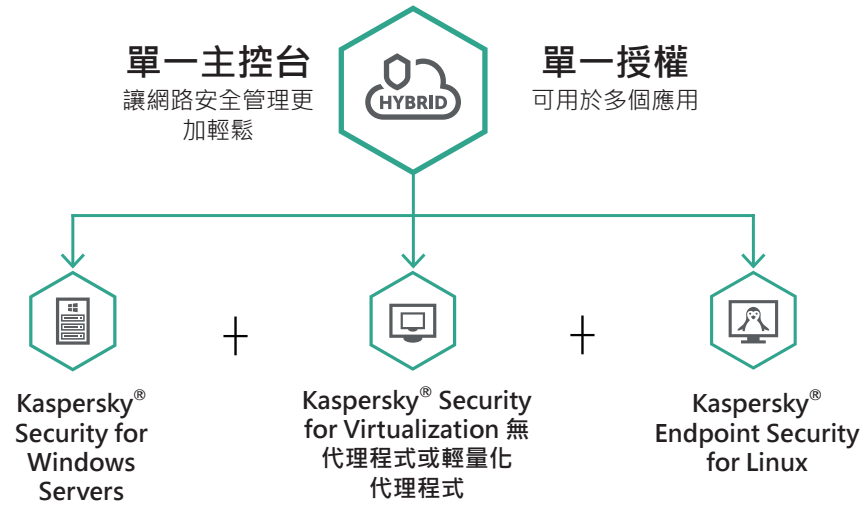
系統強化可以提高恢復力

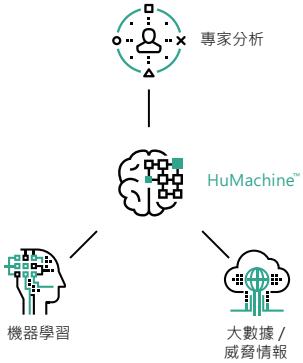
- **應用程式控制**可讓您將所有的混合式雲端工作負載鎖定為預設拒絕模式，使系統能夠充分強化，讓您可以限制應用程式只能在合法和信任的範圍內執行。
- **裝置控制**可以指定能夠存取個別雲端工作負載的虛擬化裝置。
- **網頁控制**可以規範虛擬和遠端桌面使用的網頁資源，以降低風險並提高生產力。
- **主機入侵防範系統 (HIPS)** 會將信任的類別指派給已啟動的應用程式，讓您可以限制這些應用程式對關鍵資源的存取，以及限制這些應用程式的功能。

無邊界的可視性

- Kaspersky Security Center 的**整合安全功能**管理可以協助您在整個基礎結構、端點及伺服器—亦即辦公室、資料中心和雲端—實現單點檢視的安全防護系統管理。
- 雲端 API：可以和公用 AWS 與 Azure 環境無縫整合，實現基礎結構探索、自動化安全代理程式部署和原則式管理，並且可以讓您更輕鬆進行庫存與安全防護的佈建。
- **彈性的管理選項**具有多重租用的功能、權限型帳戶控制以及角色型存取控制，讓您能夠靈活運用，同時兼顧來自單一伺服器的整合協調流程優勢。
- **SIEM 整合**：在 IT 成熟度較高的基礎結構中，安全資訊及管理系統可以做為公司網路安全各個方面的整合窗口—跨整個混合式 IT 網路。

Kaspersky Hybrid Cloud Security 提供多種業界認同的獲獎安全技術，可支持和簡化您的 IT 環境轉型。Kaspersky Hybrid Cloud Security 可以為您從實體到虛擬 (以及雲端) 的移轉提供保護，而可視性與透明度則可保證安全協調流程毫無破綻。





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/
我們獨特的方法：www.kaspersky.com/true-cybersecurity

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