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：

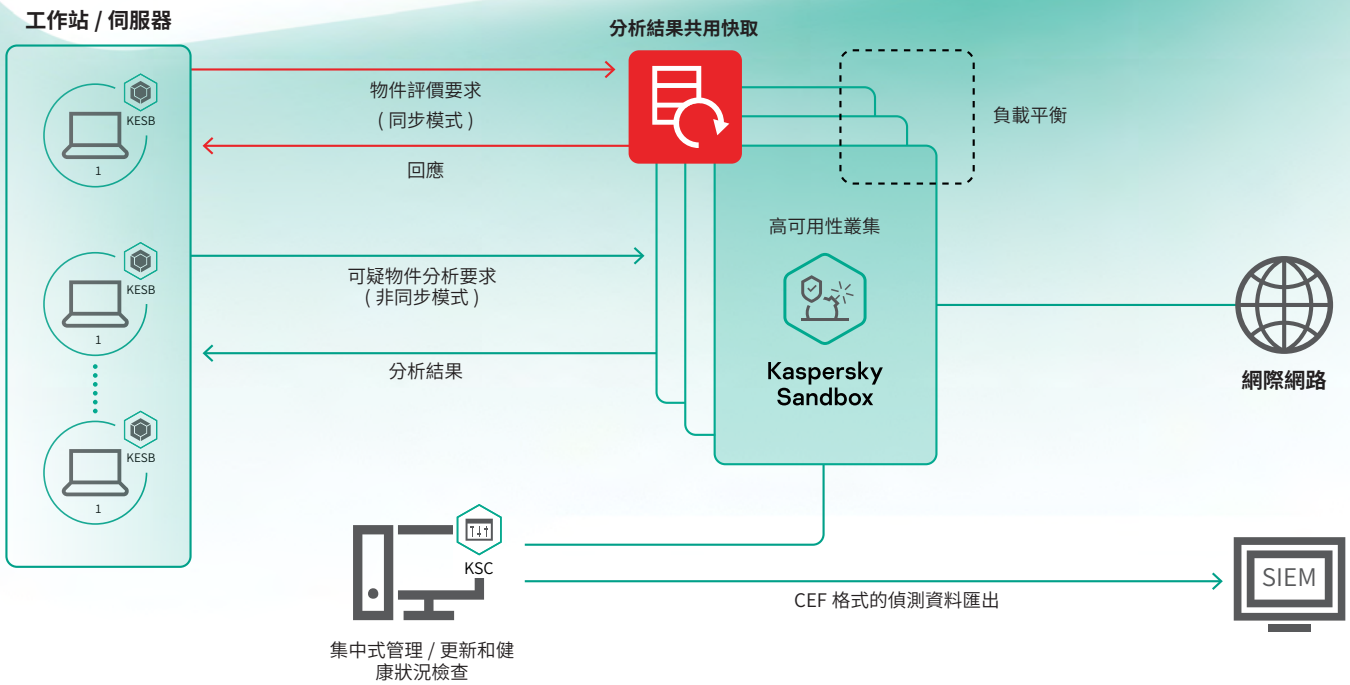
- 移除或隔離
- 通知使用者
- 開始關鍵區域掃描
- 在管理的網路中搜尋其他電腦上的已偵測物件。

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。