Kaspersky Next EDR Optimum

將您的端點防護提升到新的水準，並正面應對規避式威脅

kaspersky

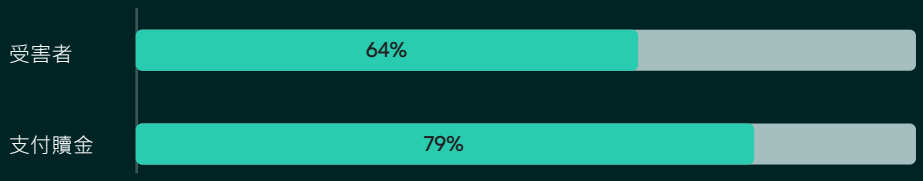
Kaspersky Next EDR Optimum

64% 的企業組織已成為勒索軟體攻擊的受害者。

當然，79% 支付贖金給攻擊者。

企業主管如何看待勒索軟體威脅，卡巴斯基，2022 年 5 月

現在正是提高防護水準的時候。辨識、分析和抵禦為規避傳統防護所設計的威脅。



挑戰

規避偵測的威脅

規避式惡意軟體、勒索軟體、間諜軟體和其他威脅越來越聰明，會在其攻擊中利用合法的系統工具和其他先進技術，來避開傳統偵測。

勒索軟體即服務

現在的駭客可以購買便宜的現成工具並攻擊任何人，竊取資料、破壞基礎結構，以及要求持續增加的贖金。

資源有限

基礎結構變得更加複雜和多樣化，而時間、金錢和人員等資源卻不足。這是昂貴貨架軟體應運而生的絕佳機會。

「我們重視卡巴斯基的全方位解決方案、可靠性，以及迅速提供的服務和支援。他們能夠保證我們 IT 環境的可用性。」

NEO 的 CISO Marcelo Mendes

閱讀案例研究

我們如何提供協助

Kaspersky Next 是我們的旗艦產品線，其設計可以協助您輕鬆建立更好的安全性。無論是尋找基本的 EDR 功能，還是安排未來採用 XDR，Kaspersky Next 以無與倫比的網路安全記錄為基礎，提供適應性和強大的雲端原生防護，只需點擊幾下即可開始使用。

Kaspersky Next EDR Optimum 提供容易使用的進階偵測、簡化的調查與自動回應功能，有助於辨識、分析和抵禦規避式威脅。

進階防護

我們的進階偵測機制包括行為分析和機器學習。

這些功能全都可以和簡單的視覺化分析工具與快速回應行動結合，讓您可以充分了解威脅及範圍，並且在造成任何損害之前阻止攻擊。

利用雲端探索和封鎖功能以及 MS Office 365 Security，在端點和雲端完成攻擊面的縮減。

單一解決方案

新世代端點安全和簡單的 EDR 整合，可以強化筆記型電腦、工作站、伺服器、雲端工作負載和虛擬環境的防護。

此外只需單一主控台，即可在雲端或內部進行部署和管理。

簡單高效率

我們在建立 Kaspersky Next EDR Optimum 時考慮到較小型的網路安全團隊，這些團隊希望將事件回應能力升級，並發展專業知識，但沒有太多空閒時間。

我們將大多數的任務自動化與最佳化，因此您只需將時間用在處理重要的事情上。此外，我們也為您和您的 IT 團隊，提供充分利用全新安全功能所需的培訓。

現在您可以：

- 事先**預防網路威脅**
- **保護您的系統**和資料不受規避式威脅影響
- 在對方有所行動之前**發現目前的威脅**
- **識別**您端點中的**規避式威脅**
- **了解威脅**並快速分析
- 以快速的自動回應**避免損害**
- 利用簡易的工具**節省時間和資源**
- **保護每一個端點**：筆記型電腦、伺服器、雲端工作負載
- **使用專業檢視**或專家檢視主控台**工作**，您可以自由選擇！

現在您擁有：

- 新世代端點安全
- 以機器學習為基礎的**進階偵測功能**
- **入侵指標** (IoC) 掃描
- **目視調查**與分析工具
- 所有必要資料都在**單一警示卡**中
- **內建回應**指南與自動化
- **單一雲端或內部部署主控台**與自動化
- 支援您所有的**工作站、虛擬和實體伺服器、VDI 部署，以及公用雲端工作負載**
- **經過完整產品培訓的** IT 安全人員

找到這些問題的答案，在最關鍵的時刻

我是否遭到攻擊？

- 根據機器學習**套用進階偵測**
- 從 securelist.com 或其他資料來源**下載和掃描 IoC**，以找出進階威脅

事情是怎麼發生的？

- 以**視覺化流程樹**分析威脅
- 以**深入分析圖**了解其行動
- **了解其根本原因及**基礎結構中的**進入點**

我該如何抵禦威脅？

- **利用多種回應選項**，隔離主機、防止檔案執行或移除檔案
- **掃描其他主機**是否有已分析威脅的任何跡象
- 在發現威脅 (IoC) 時跨主機**自動套用回應**

那麼其他威脅呢？

- **新世代端點安全**可以立即阻止大部分的威脅
- **自動減少您的攻擊面**並調整您的原則
- **控制**使用者可以使用的**應用程式和裝置**

未來我該如何防止這種情況？

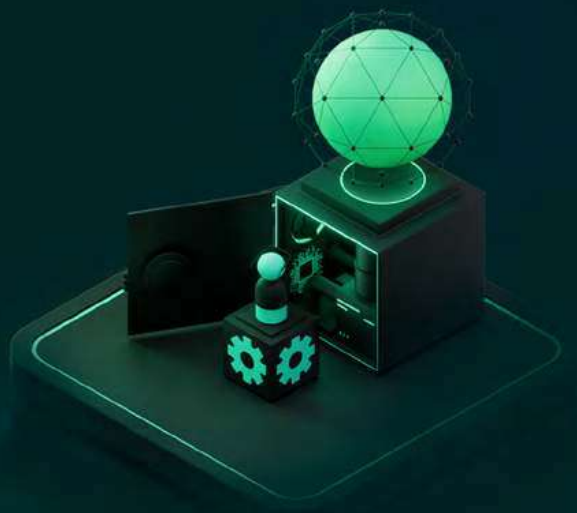
- **運用習得的資訊**，了解要封鎖的 IP 和網站、要修改的原則，以及要培訓的員工
- **建立防護規則以防止**未來此類威脅
- **保護您的雲端，探索、限制和封鎖存取**，以防止未經授權存取雲端資源、服務、即時訊息等
- **獲得** MS SharePoint Online、OneDrive 和 Teams 的**可視性與控制**

我該如何才能更充分利用？

- **使用**警示卡中的**回應指南**
- **存取我們的威脅情報入口網站**與最新的 TI
- 透過威脅分析與回應**發展您的專業知識**
- **從內建的培訓**和認證**獲益**，其中包括在模擬環境中的互動式作業

我該如何挪出時間來完成這一切工作？

- **將弱點和修補程式管理自動化**，保護您端點的關鍵方法
- 針對所有員工遠端**管理原生加密**，確保企業資料安全
- **將耗時的安全與 IT** 管理工作**自動化**



Kaspersky Next EDR Optimum

建立您的防護
透過基本的調查與回應來提高安全性

如果您需要
- 強化可視性與回應功能
- 擴大雲端安全防護
- 企業級控制功能

[1] 入侵指標

Kaspersky Next - 您的前瞻性安全防護

Kaspersky Next EDR Optimum 是 Kaspersky Next 產品系列的其中一部份，可以根據您最重要的網路安全需求，透過 EDR 的透明度與速度，以及 XDR 在三個簡單產品層中的強大工具組，提供強大的端點防護與控制功能。隨著需求增加，您可以輕鬆從一種產品切換為另一種，快速升級您的安全功能。

更多產品特性

Kaspersky Next 各產品層提供：

Kaspersky Next EDR Foundations

為您的網路安全打造強大核心最直接的方式。

- **強大的機器學習型端點防護**
- **自動修復**
- **多項自動化功能**
- **靈活安全控制**
- **EDR 根本原因分析工具**

Kaspersky Next EDR Optimum

建立針對規避式威脅的防護與專業知識。

- **基本 EDR 功能提供可視性、分析與回應**
- **強大的端點防護**
- **強化控制、修補程式管理及雲端安全**
- **IT 的網路安全培訓**

Kaspersky Next XDR Expert

防止貴企業受到最複雜與先進的威脅影響。

- **與您現有的安全基礎結構無縫整合**
- **對威脅的即時可視性與深入見解**
- **進階威脅偵測**
- **跨資產關聯**
- **自動回應**

為什麼選擇卡巴斯基？

我們是一家全球性的私人網路安全公司，全球有數千名客戶及合作夥伴，致力於公開透明和獨立自主。25 年來，我們持續利用我們參與最多測試、獲獎項目最多的技術，來打造工具和提供服務，以確保您的安全。

IDC

IDC MarketScape 2021 年全球企業現代端點安全性供應商評估

重要參與者

防毒測試

進階端點防護：勒索軟體防護測試

100% 防護

Radicati Group

進階持續威脅 (APT) 市場象限

頂尖參與者

進一步深入了解

如需進一步了解 Kaspersky Next EDR Optimum 如何解決網路威脅，同時為您的安全團隊提供支援並輕鬆運用您的資源，請造訪 https://go.kaspersky.com/next。

進一步了解 Kaspersky Next EDR Optimum

Kaspersky Next EDR Optimum

Kaspersky Next EDR Foundations　深入了解

Kaspersky Next XDR Expert　深入了解

進一步了解 Kaspersky Next：
https://go.kaspersky.com/next

利用我們互動工具中的簡短調查，選擇最適合您的產品層：
https://go.kaspersky.com/Kaspersky_Next_Tool

網路威脅新聞：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

kaspersky.com

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