



Kaspersky Next

前瞻性安全防護

為什麼現今的安全營運更加困難：

41% 的企業組織認為是威脅現況快速改變所致

40% 認為是攻擊面持續擴大¹

Kaspersky Next 將強大的端點防護與控制功能，和 **EDR** 的透明度與速度及 **XDR** 的可視性與強大工具整合在三個簡單的產品層中。選擇您現在所需的工具，並於準備就緒時輕鬆切換。

您面臨



持續發展的攻擊

勒索軟體、惡意軟體和資料外洩持續發展，利用複雜的技術來避開偵測，並透過企業電子郵件入侵、供應鏈攻擊和弱點來入侵您的基礎結構。



擴大攻擊面

遠距工作、邁向雲端和行動辦公都讓人驚嘆不已。不過，這為駭客創造許多新的入侵方式，以及更多需要監控的地方。



資源有限

發起攻擊從未如此廉價，但保護自己需要大量資源，而且需求很可能超出預算。這讓 TCO 的重要性更勝以往。



日益嚴格的法規

GDPR、CCPA、PCI DSS 和資料外洩揭露需求，在安全和報告方面為安全部門帶來極大的壓力。



複雜度持續增加

IT 和網路安全基礎結構往往不會化繁為簡和更加封閉，這些基礎結構會快速發展，每個新工具都會新增新的伺服器、主控台並進行整合，以利控制和維護。



那麼...如何才能運用自如？

大量的專案、緊急工作、創新，以及不間斷的電話與會議，網路安全專家有許多工作要處理。新的工具和升級應該要讓您有更多時間可以運用，而不是占用您的時間。

¹ SOC 現代化與 XDR 的角色，企業策略集團，2022 年

協助近在眼前

51% 的現有工具難以偵測和調查進階威脅¹

Kaspersky Next 是卡斯基的全新產品線，在強大的端點防護支援下，利用 EDR 和 XDR 來強化您的安全防護。Kaspersky Next 可以協助您保護您的攻擊面，並且在造成損害前將其消滅。



安全創新

Kaspersky Next 是以我們屢獲殊榮的端點安全為基礎構建而成，可以涵蓋您所有的基礎結構，並且可以協助您以最少的資源無縫快速移轉到 EDR 和 XDR。



利用機器學習 打造而成

我們的產品使用多種偵測技術，其中的關鍵是機器學習，甚至是複雜和全新威脅亦可提供有效偵測和修復的支援。



完美契合

網路安全沒有通用解決方案。這就是 Kaspersky Next 有三個產品層的原因：從基礎端點防護到發展專業知識，到讓您的專家配備先進的工具。

主要優勢

- 防止貴企業受到多種類型的威脅影響，以及避免損失和干擾
- 選擇最符合您獨特需求的產品層
- 可以隨著您的安全需求增加和發展，從某一層輕鬆移轉到下一層
- 根據您的需求和資源，從每一層的 EDR 功能獲益
- 利用全方位的開放式 XDR 控制您的整個基礎結構
- 在每一層產品中獲得無可比擬的機器學習式端點防護
- 從雲端或內部部署管理您的安全
- 有了例行網路安全任務的自動化功能，您可以將更多時間用於其他重要專案

防護結構

根據您最重要的網路安全需求，Kaspersky Next 提供三個產品層。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。



Kaspersky
Next



Kaspersky Next
EDR Foundations

建議使用情況
IT 團隊處理安全問題

價值
確保保護您的所有端點

主要特性：

- 端點防護
- 根本原因分析
- 安全與 IT 管理



Kaspersky Next
EDR Optimum

建議使用情況
小型網路安全團隊

價值
透過簡化的調查與回應來提高安全性

主要特性：

- 進階端點防護
- 雲端防護
- EDR 指南與自動化



Kaspersky Next
XDR Expert

建議使用情況
大型網路安全團隊或 SOC

價值
您安全專家的主要專業工具

主要特性：

- 全功能 EDR
- IRP 工作流程和警示彙總
- ML 和進階偵測

¹ SOC 現代化與 XDR 的角色，企業策略集團，2022 年

使用案例

69% 的攻擊僅持續 2 天 (平均)¹

Kaspersky Next 解決您的關鍵網路安全問題。



Kaspersky Next
EDR Foundations



保護您的端點

利用我們屢獲殊榮的端點防護引擎自動防止惡意軟體、勒索軟體和其他大規模威脅。



Kaspersky Next
EDR Optimum



快速回應

只需按一下滑鼠即可回應出現的規避式威脅，或是輕鬆建立自動化任務來反擊。回應時間是有效安全的其中一項關鍵指標。



Kaspersky Next
XDR Expert



應對複雜的威脅

當貴公司成為進階或複雜攻擊的鎖定目標時，您必須讓您的專家配備最強大的工具和資訊。彙總、資料分析和進階偵測是關鍵。



獲得可視性

透過根本原因分析來調查威脅，並快速判斷範圍。不再猜測，了解您的威脅。



發展專業知識

並非每個人從一開始就需要複雜且強大的 EDR，但您必須從某個地方開始著手。單一套件中的可視性、分析與回應，可以在您的 EDR/XDR 發展過程中提供協助。



跨資產安全

從來自多個資料來源的資料中找出交叉關聯，與第三方產品整合並將例行任務自動化，讓您的專家能夠準確、快速和系統性獵捕及回應威脅。



減少攻擊面

使用裝置、網頁與應用程式控制並保護您的行動裝置，以減少攻擊者入侵您系統的方式。



雲端安全

探索、限制和封鎖對雲端資源、服務、即時訊息等未經授權的存取。獲得 MS SharePoint Online、OneDrive 和 Teams 的可視性與控制。



劇本

具有多個預設劇本的自動化與協調可以縮短您的平均回應時間，甚至可以在進階威脅發展之前先行阻止。

¹ 事件回應分析師報告，卡巴斯基，2022 年

產品內容

了解每個產品層中的特定主要特性。



端點防護

檔案、網頁和郵件防毒軟體、網路防護、AMSI、弱點入侵防護、修復、行為偵測、HIPS



安全管理

防火牆、網頁、裝置、應用程式控制、行動裝置防護與管理



IT 形式

弱點評估、修補程式管理、資料抹除、軟體 / 硬體庫存、第三方應用程式及作業系統安裝、遠端連線



加密

加密和加密管理



雲端安全

雲端探索及封鎖、MS Office 365 安全性、資料探索



教育

IT 系統管理員的網路安全培訓



基本 EDR 功能

根本原因分析、入侵指標掃描、端點回應



進階 EDR 功能

蒐集遙測、威脅獵捕、攻擊指標 (IoA) 偵測、MITRE ATT&CK 對應



XDR 功能

警示彙總、沙箱、AD 整合、TI 擴充、第三方連線程式、強化的調查工具、記錄管理和資料湖、全自動回應、劇本、威脅偵測和交叉關聯



	專業檢視	雲端	雲端	不適用
管理主控台	簡化、容易管理使用者人數上限：2500			
可在雲端或內部部署的兩種檢視下使用：	專家檢視	雲端及內部部署	雲端及內部部署	內部部署
	詳細、可自訂雲端使用者人數下限：300			

請參閱對應的產品特性清單，以了解您所選主控台類型中特定功能的可用性。

¹ 可用功能：弱點評估、軟體 / 硬體庫存

² 可用功能：雲端探索

³ 可用功能：根本原因分析

進一步提升您的安全水準

43% 的企業組織將保護日益複雜的技術環境成本，視為主要的 ITSec 挑戰¹

外部專業知識或其他服務有助於進一步提升您的安全水準。

以下是我們推薦可以進一步強化您對 Kaspersky Next 體驗的一些服務。



考慮託管安全

Kaspersky Managed Detection and Response

- 針對規避式威脅的全天候託管防護
- 可以配合每個產業部門和組織需求靈活調整
- 具成本效益且成本合理的 IT 安全投資



停止浪費時間

Kaspersky Professional Services

- 避免錯誤設定，並將執行的影響降到最低
- 卸載評估、部署、維護並適時最佳化
- 獲得卡巴斯基產品升級和移轉的協助
- 基本服務套件或自訂專案



獲得專家支援

Kaspersky Premium Support

- 獲得最高的投資報酬率，並避免人力吃緊
- 優質支援專線
- 專屬的卡巴斯基技術專家
- 更長的重大問題支援時數

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

[深入了解](#)



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

[深入了解](#)



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

[深入了解](#)

¹ 2022 年 IT 安全經濟學，卡巴斯基，2022 年

我們的身分

卡斯基是一家全球性的網路安全公司，全球有超過 250,000 名企業客戶。過去 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，以確保我們客戶的安全。我們致力於透明度和獨立性。

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



Info-Tech

2023 年端點防護冠軍



G2

2023 年秋季企業最佳投資報酬率預估



進一步深入了解

如需進一步了解 Kaspersky Next 可以如何協助貴企業在安全的環境中拓展，請造訪：<https://go.kaspersky.com/next>。

進一步了解 [Kaspersky Next](#)



**Kaspersky
Next**



**Kaspersky Next
EDR Foundations**

深入了解



**Kaspersky Next
EDR Optimum**

深入了解



**Kaspersky Next
XDR Expert**

深入了解

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

© 2024 AO 卡斯基實驗室。
註冊商標及服務標誌均為其各自擁有者的財產。
台灣聯繫人：銷售總監 黃茂勳 eden.huang@kaspersky.com.tw

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

