Kaspersky Next XDR Expert

無可比擬的見解。全方位防護。

kaspersky

企業網路安全的複雜度

網路威脅現況讓企業組織在專注於核心業務營運的同時，將網路安全保持在最高水準變得極具挑戰性。再加上持續擴大的攻擊面、法規需求，以及通用技能的差距，就不難理解為什麼現代企業面臨如此巨大的壓力—以及為什麼如此多的網路攻擊可以成功。

51%

的公司難以利用現有工具偵測和調查進階威脅

68%

的公司其網路曾遭到針對性攻擊，並直接導致資料外洩

每年

6 兆美元

：全球網路犯罪者的年度成本

每天偵測到

400 000

個新的惡意軟體

資料來源：Kaspersky、PurpleSec、CybersecurityVentures

Kaspersky Extended Detection and Response

完整可見性。無可比擬的防護。

作為 Kaspersky Next 產品線的其中一部份，我們推出 **Kaspersky Next XDR Expert**，這款解決方案可以體現卡巴斯基的 XDR 方法，以及提供公司安全性的全方位視圖。

Kaspersky XDR 是一款強大的網路安全解決方案，可以防止複雜的網路威脅。這款解決方案會利用包括端點、網路和雲端資料在內的多種資料來源，提供完整的可視性、關聯與自動化。

Kaspersky XDR 源自 Kaspersky Anti-Targeted Attack 平台，從 2016 年的原生 XDR 發展到 2023 年的開放式 XDR，可以提供全方位的安全視圖。Kaspersky XDR 可以透過開放式單一管理平台輕鬆管理，提供全面的內部部署安全性，以確保客戶的敏感性資料保留在自有的基礎結構內，同時滿足資料主權的需求。

開放式 XDR

開放式 XDR 解決方案採用可以和多種資安產品搭配使用的設計，讓企業組織可以整合各種來自不同供應商的安全產品，進而提供更高的彈性與不受供應商限制的功能。

原生 XDR

原生 XDR 解決方案通常可以搭配供應商自有的安全工具生態系統順暢運作，提供整合程度更高和一體化的體驗。這些解決方案是專門為了搭配使用製作，可以在供應商的安全產品套件中提供深度整合、自動化，以及簡化的工作流程。

關鍵技術

我們提供開放式 XDR 作為**單一開放式平台**—建立網路安全產品統一生態系統的通用工具。Kaspersky XDR 的核心是我們的頂尖解決方案— Kaspersky Unified Monitoring and Analysis Platform、Kaspersky Next EDR Foundations 及 Kaspersky Endpoint Detection and Response Expert。如需進階網路管理，可以額外選擇 KATA。

監控與分析

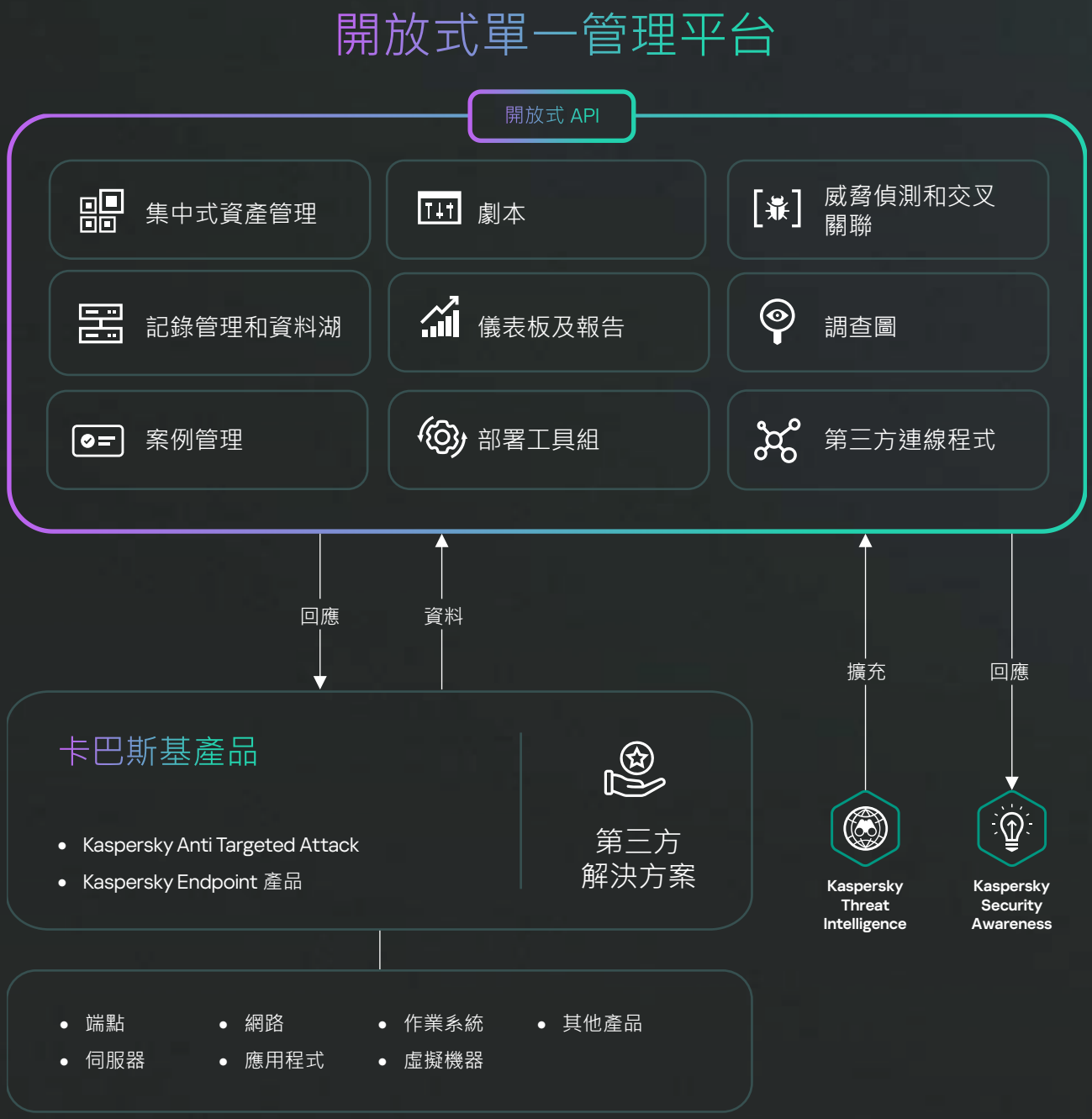
提供記錄的集中收集與分析、安全事件的即時關聯，以及事件的及時通知。內含一組現成的關聯規則，以及對 Kaspersky Threat Intelligence 服務豐富產品組合的存取權限，可以辨識威脅、攻擊和 IoC 並排定其優先順序。

端點防護

提供強大的端點防護，可以防止勒索軟體、惡意軟體和無檔案攻擊。在內部部署或雲端，我們的端點防護會使用機器學習和行為分析，來保護執行任何主要作業系統的所有類型端點。

端點偵測與回應

為企業組織的所有端點提供全方位的可視性與優秀的防護。威脅獵捕與探索功能經過卡巴斯基獨特且廣泛的威脅情報強化，加上例行任務、引導式調查流程和可自訂偵測的自動化，全都有助於快速解決事件。



功能強大，效益顯著

來自第三方的即時資料融合

可以將來自第三方來源的資料整合，這項功能整合的資料來源不僅限於端點，而且可以透過即時交叉關聯強化。

自動回應和修復

將遭到入侵的端點隔離或獨立、封鎖惡意活動，以及修復弱點，可以減少手動工作和回應時間。

同級最佳 EPP / EDR

卡巴斯基是公認的全球領導廠商，為全球的 EPP / EDR 解決方案立下基準。Kaspersky EDR 在全球的傑出表現屢獲殊榮，而且積極參與國際刑警組織和 MAPP 等國際委員會。

無可比擬的擴充性

Kaspersky XDR 能夠在單一執行個體上支援內含數十萬個端點的負載，在確保高可用性的同時，全力即時追蹤威脅。

資料主權

Kaspersky XDR 是少數提供全方位內部部署 XDR 解決方案的其中一家供應商，可以確保客戶的敏感性資料保留在其自有的基礎結構內，同時滿足資料主權的需求。

無縫與緊密整合卡巴斯基的產品

產品之間的互動達到第三方解決方案無法企及的程度，採用統一的支援系統和無縫整合的設計。

支援 MSSP 形式的多租戶模式

為成熟的租戶提供 XDR 即服務—某個租戶使用者無法看到其他租戶的資料，而主系統管理員 (MSSP) 可以為所有用戶端建立偵測與回應處理程序。

進階安全情況自訂與全基礎結構資料分析

讓使用者能夠設定複雜的安全情況，而且還能分析其整體基礎結構中的資料。

整合功能

和 Kaspersky XDR 搭配使用的多種整合方式可以提供**統一和情境化的潛在威脅視圖**，為您的安全團隊提供需要的所有工具和資訊，以保護貴組織不會受到網路犯罪者攻擊。

該產品的整合功能包括接收來自其他系統和裝置的資料 (記錄)，以及在其他產品中設定自動回應的能力。Kaspersky XDR 可以和卡巴斯基與第三方產品進行多種立即可用的整合。Kaspersky XDR 也可以新增其他整合，這些整合可以由 Kaspersky Professional Services 開發，或是由合作夥伴或客戶自行開發 (包括使用可連線產品的 API 功能)。Kaspersky XDR 可以和來自不同領域和不同供應商的系統整合，並且支援多種通訊協定和資料格式。

依安全領域區分

端點安全

- EPP 及 EDR 解決方案

網路及網頁與電子郵件安全性

- 電子郵件防護
- 網路偵測與回應 (NDR)
- 防火牆 (FW) 及次世代防火牆 (NGFW)
- 統一威脅管理 (UTM)
- 入侵偵測系統 (IDS)

雲端安全

- 雲端存取安全性代理程式 (CASB)
- 雲端工作負載防護平台 (CWPP)

威脅情報

- 網路威脅情報 (CTI)

身分識別安全性

- 身分識別和存取管理 (IAM)
- 特權存取管理 (PAM)

OT / IoT 安全 / 安全認知

依傳輸類型區分

- TCP
- UDP
- Netflow
- sflow
- nats-jetstream
- kafka
- HTTP
- SQL
  - SQLite
  - MSSQL
  - MySQL
  - PostgreSQL
  - Cockroach
  - Oracle
  - Firebird
- 檔案
- 1c-log 及 1c-xml
- Diode
- FTP
- NFS
- WMI
- WEC
- SNMP
- SNMP-TRAP
- VmWare API

依資料類型區分

- XML
- Syslog
- Csv
- JSON
- SQL
- IPFIX
- CEF
- Netflow 5
- Netflow 9
- KV

依供應商區分

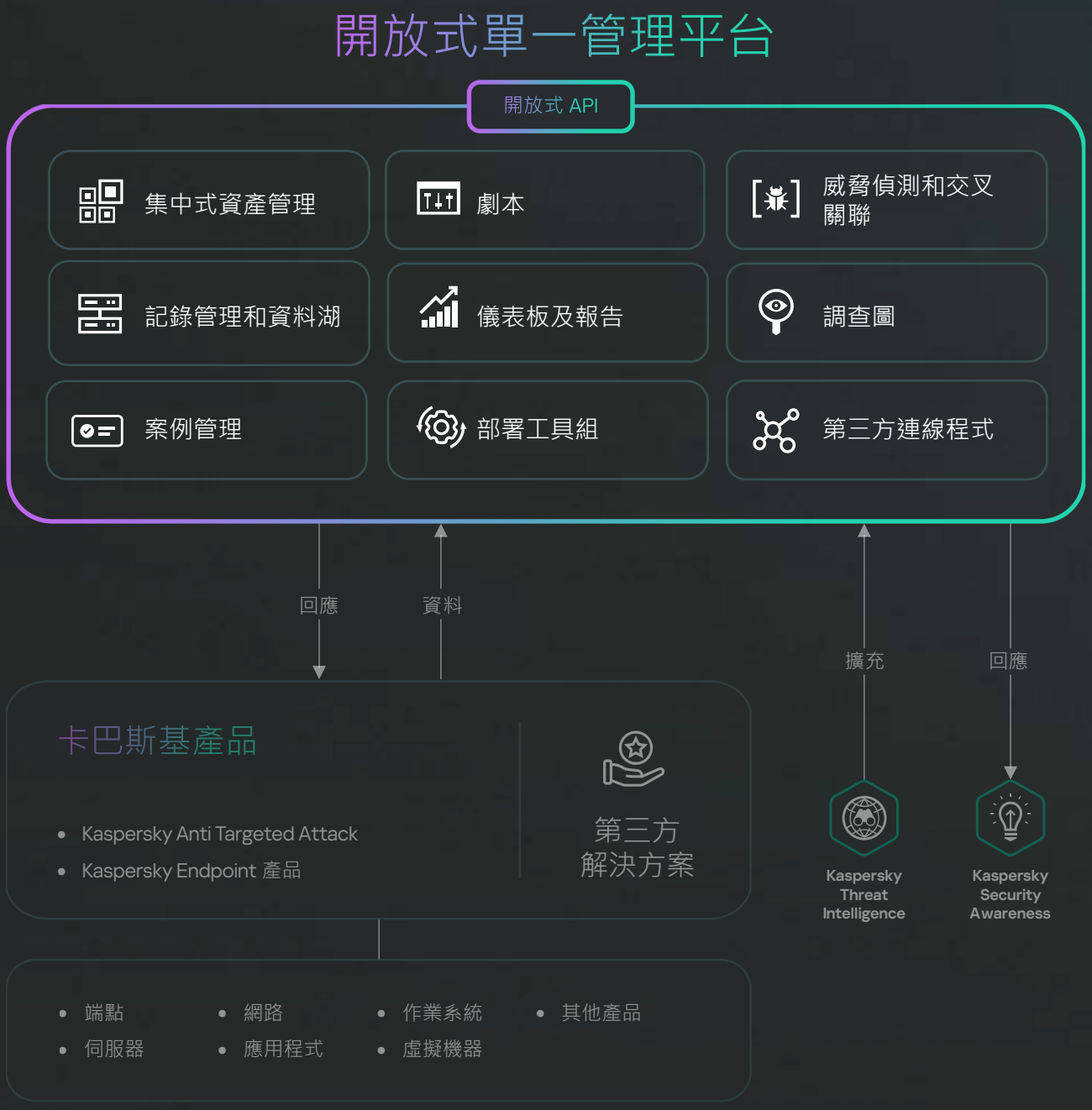
- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilo
- Ayehu
- Barracuda
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- CheckPoint
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- DeepInstinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- Eset
- F5 BigIP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- 華為
- IBM
- Ideco
- Illumio
- Imperva
- Orion Soft
- Intralinks
- Juniper
- Kemptechnologies
- Kerio
- Lieberman
- MariaDB
- Microsoft
- MikroTik
- Minerva
- NetIQ
- NetScout
- Netskope
- Netwrix
- Nexthink
- NIKSUN
- Oracle
- PagerDuty
- Palo Alto
- Penta Security
- Proofpoint
- Radware
- Recorded
- ReversingLabs
- SailPoint
- SentinelOne
- Sonicwall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro
- Trustwave
- VMWare
- Vormetric
- WatchGuard — Firebox
- Winchill Fracas
- Zettaset
- Zscaler 等

我們提供的產品

Kaspersky XDR 有兩種選擇。

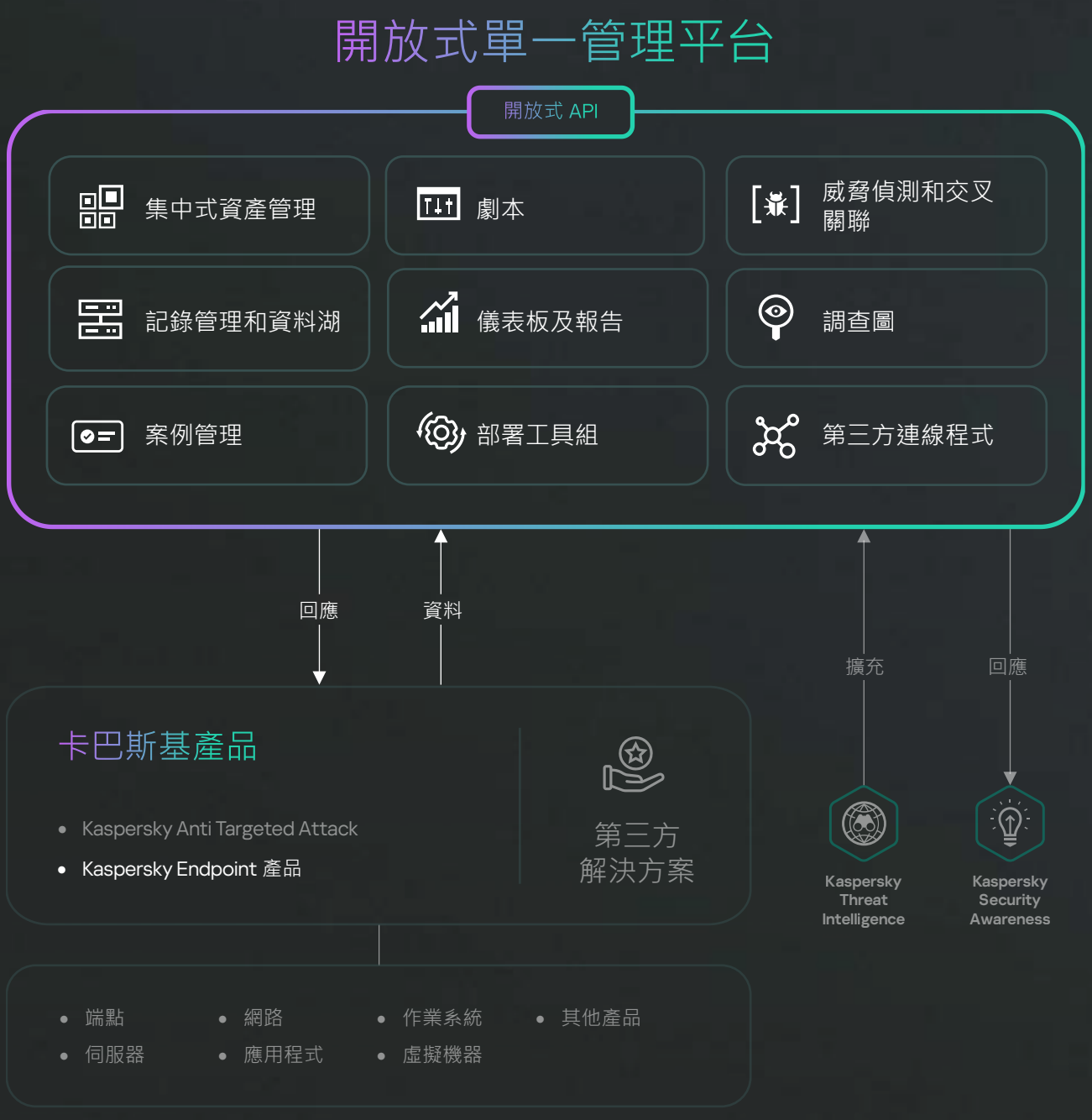
Kaspersky XDR Core

Kaspersky XDR Core 適合已經擁有端點和 EDR 解決方案，但不想改用其他端點和 EDR 解決方案，偏好利用關聯性引擎、自動回應和第三方連線程式擴充功能的客戶。



Kaspersky Next XDR Expert

Kaspersky Next XDR Expert 結合同級最佳的端點防護，以及 Kaspersky EDR Expert 的進階偵測功能、關聯性引擎和自動回應。您可以新增第三方連線程式來整合所有資料。



輔助感應器帶來的額外價值

Kaspersky XDR 支援無縫整合，目標為保護特定資產所設計的輔助感應器，可以將其無縫整合到 XDR，以提供額外的價值層，以及將 XDR 轉換為一體化的平台，為分析師提供涵蓋所有整合解決方案的集中式工作區。

Kaspersky XDR 不僅可以透過 EDR 提升您的防護，也可以提供彈性整合的功能，因此客戶可以隨時將產品新增到生態系統。

		Kaspersky XDR Core	Kaspersky Next XDR Expert
開放式單一管理平台及其元件	交叉關聯性引擎 • 第三方連線程式 • 記錄管理和資料湖 • 威脅偵測和交叉關聯 • 資產管理 • 儀表板及報告	●	●
	XDR 元件 • 案例管理 • 回應自動化與協調 (劇本) • 調查 • 部署工具組 • 開放式 API	●	●
Kaspersky Endpoint 功能 *	自動、半自動及手動偵測		●
	在受保護的端點間進行監控		●
	威脅遏制		●
	復原選項		●
	行動裝置防護與管理		●
	雲端探索及封鎖		●
	MS O365 安全性、資料探索		●
	IT 系統管理員的網路安全培訓		●

* 功能的可用性會因建置方法而有所不同

Kaspersky XDR Core

Kaspersky Unified Monitoring and Analysis Platform

XDR 元件

Kaspersky Next XDR Expert

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Next EDR Foundations

Kaspersky Endpoint Detection and Response Expert

XDR 元件

導入 Kaspersky Next

Kaspersky Next EDR Foundations

適合每個人強大的安全防護

保護您的所有端點

如果您需要

- 強大的端點防護
- 基本安全控制
- 徹底自動化

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

Kaspersky Next XDR Expert

讓您的專家更上層樓

防止貴企業受到最複雜與先進的威脅

如果您需要

- 進階威脅偵測
- 無縫整合
- 強大的威脅獵捕工具

為什麼選擇 Kaspersky XDR

參加最多測試。獲獎項目最多。卡巴斯基防護。

卡巴斯基是一家成熟的全球網路安全公司，擁有豐富的安全專業知識。過去 25 年來，我們持續保護世界各地的企業組織，我們的產品和服務獲得無數的獎項和榮譽。在 2013 年到 2022 年間，卡巴斯基的產品：

827
參加 827 項獨立測試及評鑑

587
獲得 587 項第一名

685
獲得前三名的成績

在 2023 年，卡巴斯基獲得頂尖的全球技術研究與顧問公司 ISG 評選為 XDR 解決方案市場的領導廠商。ISG 將「領導廠商」定義為擁有全方位的產品和服務，以及代表創新實力和競爭穩定性。

深入了解

Kaspersky Extended Detection and Response

提出示範申請

www.kaspersky.com

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

#kaspersky
#bringonthefuture