Kaspersky Next

新一代 安全

kaspersky

1

偵測率

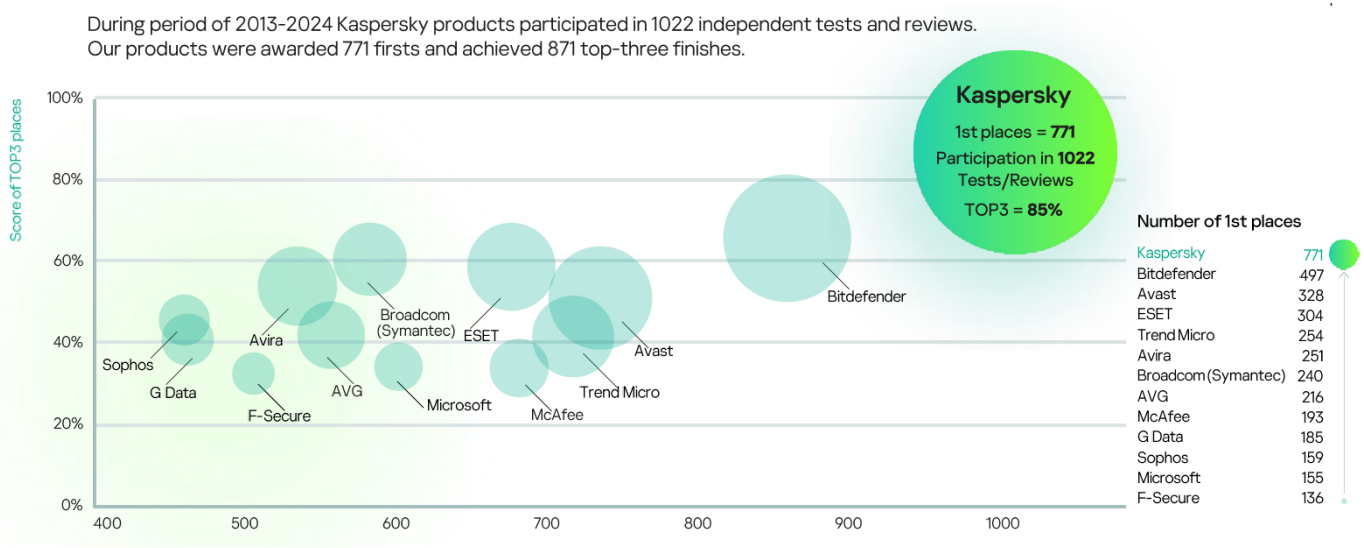
管理

全方位技術開發

資安情資

We are Kaspersky

1. 2013~2024參加獨立評測最多，偵測率第一，前三名比例最高。



2. 協助台灣客戶將更新主機移往新加坡、荷蘭等非敏感國家。

(三)卡巴斯基更新主機的資訊流向

卡巴斯基的更新伺服器位於許多國家與區域，包括加拿大、荷蘭、德國、法國、中國、香港、墨西哥、新加坡等。卡巴斯基的產品初始值會自行選擇最近且高可用度的伺服器來提供軟體更新，卡巴斯基用戶更可依自選需求設置特定位置的更新主機。**卡巴斯基亦於 2020 年開始將台灣用戶的產品更新初始值從香港轉移至新加坡，目前台灣客戶僅會向新加坡、荷蘭、德國、法國與加拿大的更新主機更新軟體、病毒碼與卡巴斯基安全網路資料庫(Kaspersky Security Network)，以保障客戶的隱私與下載安全。**相對於在台灣仍有營利的全球資安業者，卡巴斯基更主動對台灣客戶承擔資安廠商應負的責任。

3. AVTEST 評測，對抗勒索病毒防禦率最高。

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Advanced Endpoint Protection: **Ransomware Protection test**

Date of report: September 30, 2021

The three assessment scenarios were independently developed and executed by the test lab:

- Real-World ransomware attacks user files on local system
- Real-World ransomware attacks user files on remote shared folder
- Proof of Concept ransomware attacks user files on local system

During the test, the products were expected to detect ransomware activity and its files, block it, roll-back any changes to user files (the other words, to protect all user files) and eliminate the threat from the targeted system. Only these results were considered a true success and the relevant solution was given a credit in each test case.

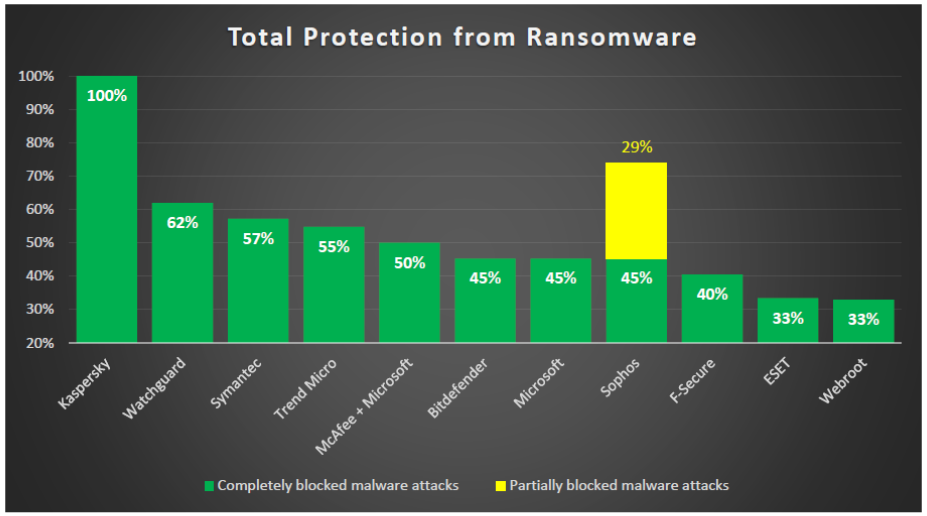


Figure 1. Total ransomware protection by different products basing on all three scenarios.
"Completely blocked" means that ransomware was detected, and all user files were protected.
"Partially blocked" means that ransomware was detected, but some user files were lost (not protected).
Arranged by "completely blocked" values.

AI

機器學習

情資模型訓練

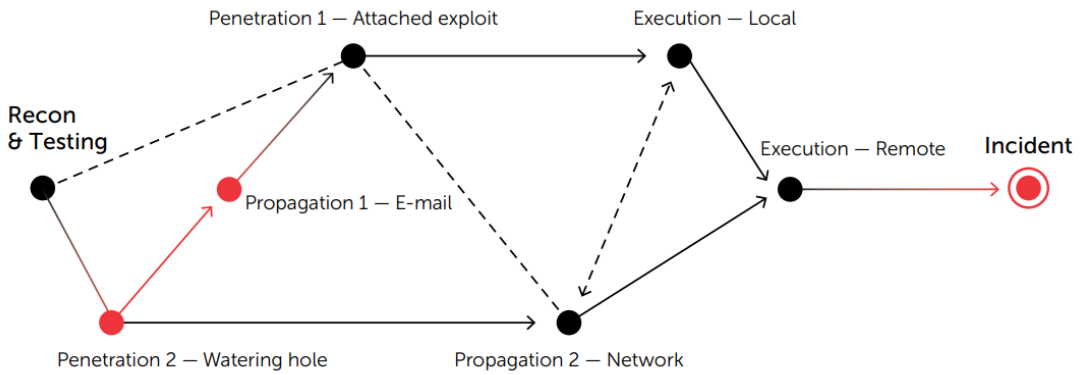
智能SOC

現今面對的挑戰

利用合法工具和無檔案式威脅 實施惡意攻擊 → 隱藏和躲避

需面對 有利益性的惡意攻擊（例如流行度高的勒索軟體） → 影響重大

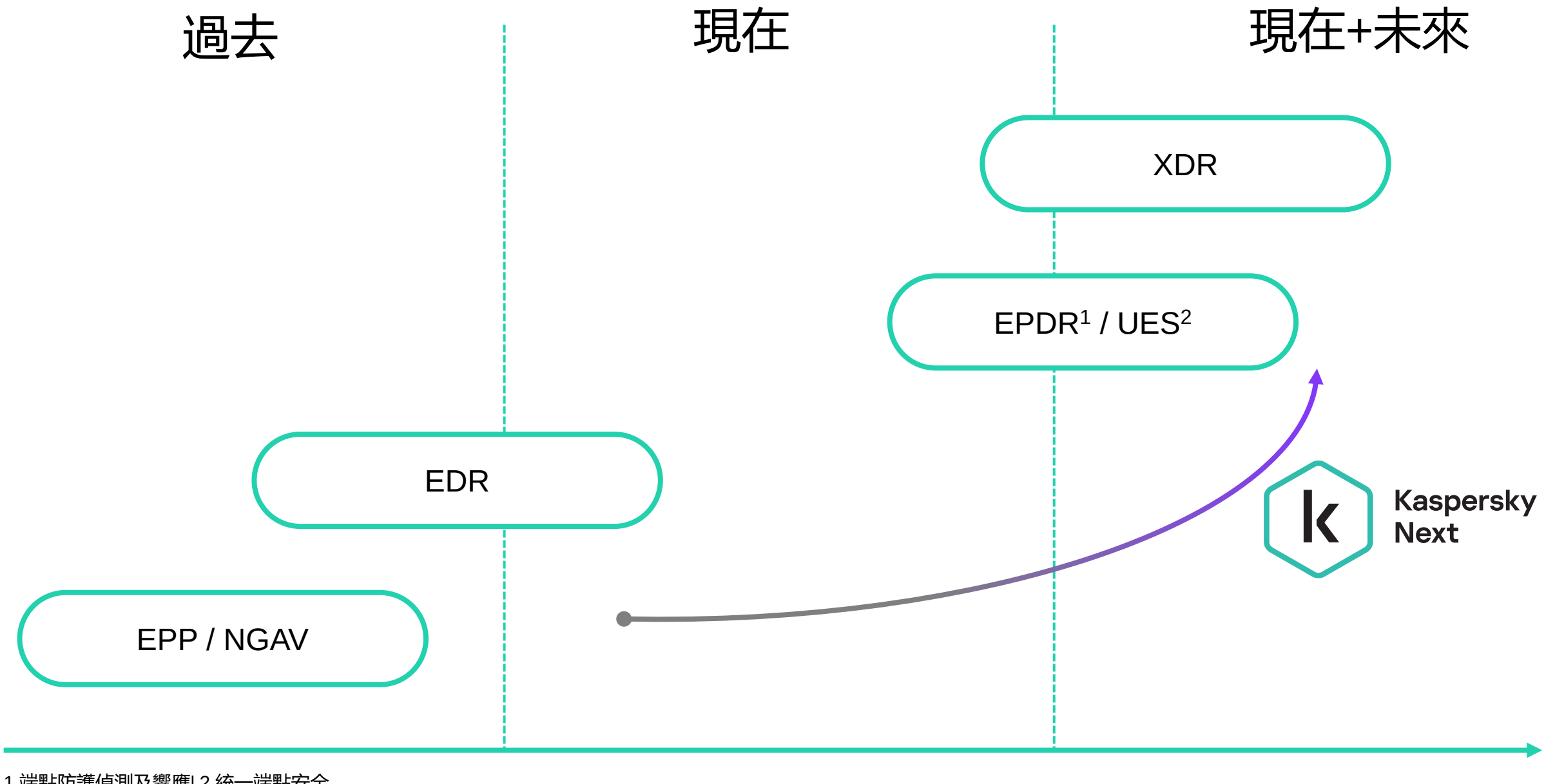
採用多重攻擊鏈階段 → 複雜持續性長



企業意識到：

- 威脅數量上升
- 攻擊場景日益複雜
- 威脅的財務影響
- 必須解決的合規性問題

端點防護（EPP）需要包含EDR的功能

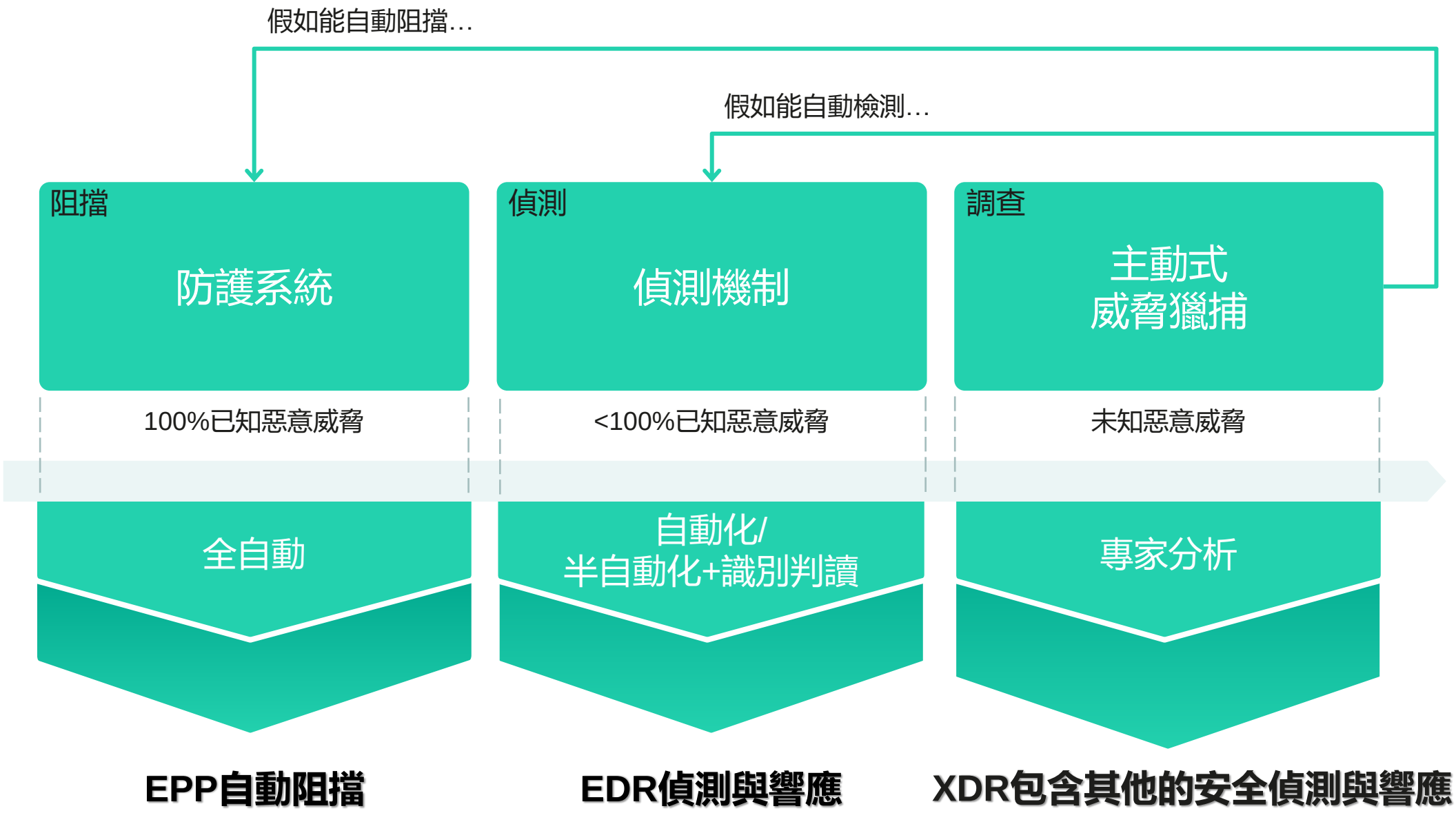


1 端點防護偵測及響應| 2 統一端點安全

Kaspersky Next

新一代安全

Kaspersky Next 從 EDR基礎功能延展至XDR架構



Kaspersky Next 產品價值定位

Kaspersky Next

在强大的端點防護機制下，利用 EDR 和 XDR 提高安全及優化維運

Kaspersky Next EDR Foundations

為每個人提供強大的安全防護

防護所有端點

1、提供企業基本安全需求
2、減少攻擊面威脅
3、增加可視性

Kaspersky Next EDR Optimum

加强防禦

通過必要的調查和響應措施提高對未知風險的安全性

1、提供企業自動化響應機制
2、定期清查內部可疑主機
3、提供主機安全加固功能

Kaspersky Next XDR Expert

擴展至其他安全防護範圍

防護您的企業免受最複雜，最新的網路威脅

1、提供整合端點及其他安全機制平台
2、整合端點外的安全防護機制

Kaspersky Next EDR Foundations：確保您所有端點的安全

Kaspersky Next EDR Foundations

為每個人提供強大的安全防護

防護您的所有端點設備

如果您需要

- 強大的端點防護
- 提供基本安全控制
- 最大程度的自動化

Kaspersky Next EDR Foundations：基礎防護

卡巴斯基
NEXT
EDR基礎版

來自網站的惡意內容

來自郵件的惡意內容

來自網路的威脅攻擊

橫向感染的威脅

網頁防護及網頁控制

控制對可疑資源和惡意檔案的網路存取。

郵件威脅防護

掃描接收和發送的電子郵件附件。

網路威脅防護

監控網路流量已發現攻擊活動。

防火牆

阻止未經授權的設備連接。

防護設備通訊的安全

Kaspersky Next EDR Foundations：進階防護技術

對抗現代化威脅的先進技術：

- Ransomware
- Fileless attacks
- Spyware and Infostealers
- Other evasive threats

漏洞利用防禦

跟蹤易受攻擊的應用程序運行的可執行檔案並阻止可疑活動。

AMSI 防護

允許掃描來自第三方應用程序（PowerShell、WMI、Office 巨集等）的腳本和其他對像。

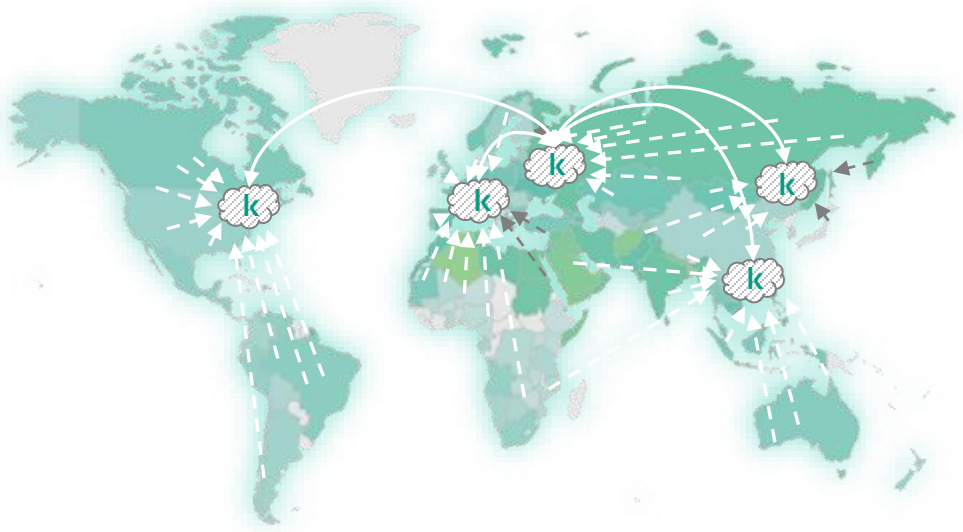
行為檢測

ML 算法在執行的最階段檢測應用程序行為中以前未知的惡意模式。

修復引擎

讓您回滾操作業系統中惡意軟體執行的操作。對勒索軟體尤其有效。

防護已知和新的惡意威脅變種病毒



檔案威脅防護

借助病毒防護資料庫、卡巴斯基安全網路雲服務和啟發式分析來預防惡意軟體。

KSN 服務每天檢測到超過 30 萬個新威脅

40% 的卡巴斯基用戶成功受到 KSN 服務的防護，當離線 AV 資料庫中未檢測的威脅

KSN

接收有關惡意軟體和可疑行為的匿名資訊。這種即時資料有助於快速響應新惡意軟體，同時降低"誤報"率。

豐富的分析資料，以阻止已知和新的惡意軟體

管控外接裝置

BadUSB 攻擊防護

防止受感染的 USB 設備模擬成鍵盤。

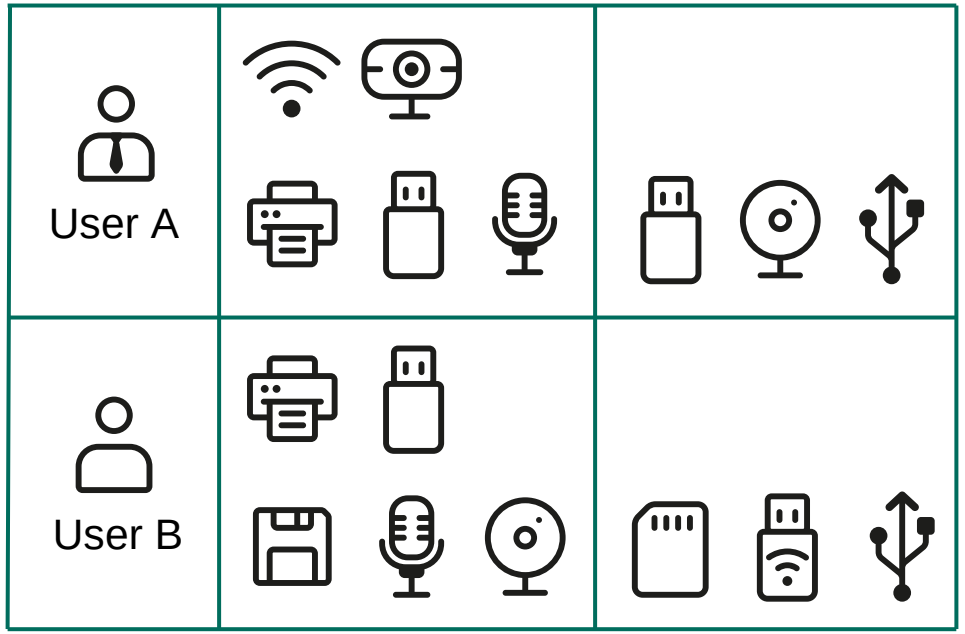
Hidden keyboard

設備控制

管理對連接到機器的設備存取

通過以下方式控制設備

- Device ID
- Device model
- Type of the device
- Connection bus



受信任的

不受信任

管控應用程式的啟動和執行和存取

應用程式控制*

管理用戶裝置上應用程式的啟動。

白名單

- Golden Image
- Office applications
- Browsers
- Business
- Other trusted

Allow

黑名單

- Remote administration
- Hacking tools
- High risk
- Other untrusted

Deny

主機入侵防護

防止應用程式在作業系統上執行潛在的危險操作。

按應用程序群組定義權限

Trusted → Low Restricted → High Restricted → Untrusted

控制對作業系統資源的存取：

- System files
- Startup settings
- Security settings
- System services

控制對個人資料的存取:

- Files
- Browser data
- Mail clients data
- Corporate messengers

根據KSN自動/手動分類限制不必要的應用程式啟動和存取

*要在伺服器上啟用應用程式控制，需要NEXT-Optimum

防護技術總結

管控外部存取

管控本機及外接設備、瀏覽網頁、開啟應用程式時，免可能帶來的攻擊入侵及資料外洩的風險。

減少攻擊面威脅

使用基本的漏洞評估和應用程式控制，對應用程式的啟動及其關鍵系統資源及用戶資料存取進行管控

防範已知和進階威脅

使用多個靜態和行為分析引擎阻止已知或未知攻擊

採用多層次防護機制防護設備

Kaspersky Next EDR Optimum：自動化 EDR 元件及功能

Kaspersky Next EDR Optimum

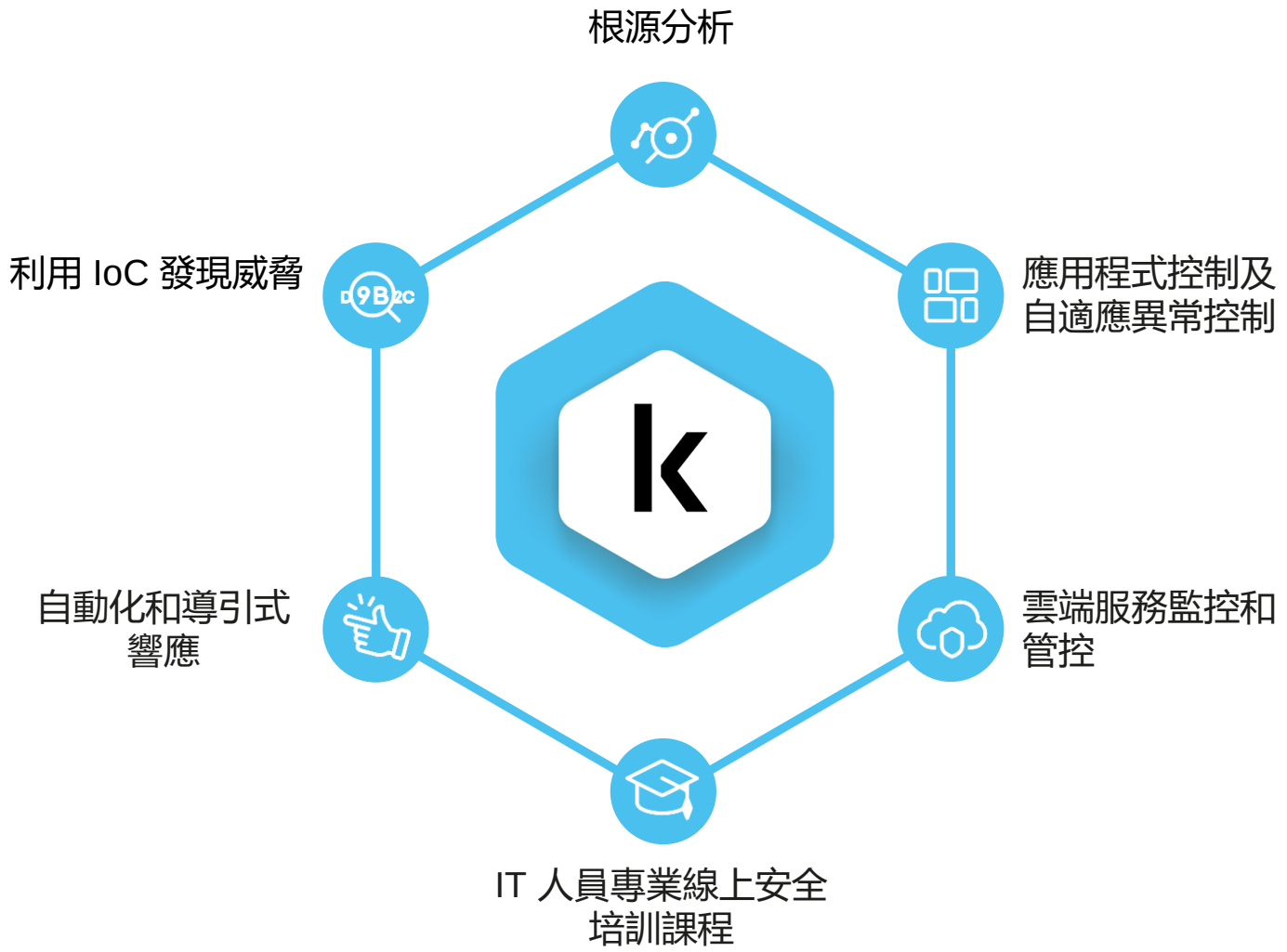
加强防禦

透過必要的調查和響應措施提高安全性

如果您需要

- 增强可視性和響應功能
- 擴展雲端服務安全
- 減少攻擊面風險

包含卡巴斯基 Next EDR 基礎版功能



[1] Indicator of Compromise

Kaspersky Next EDR Optimum：加强保固系統

系統強化

應用程式、網路和設備控制。

自適應異常控制

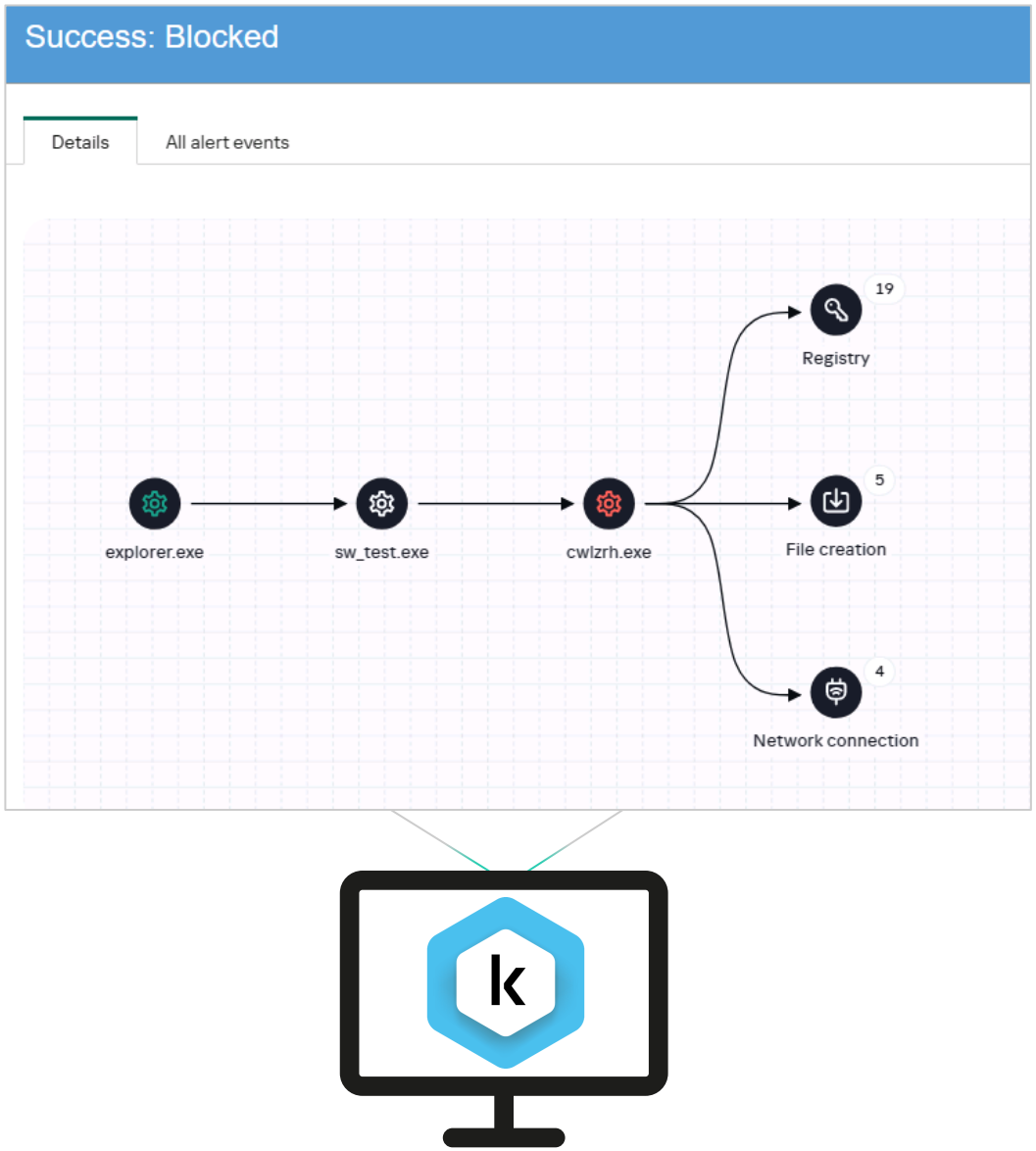
有助於自動根據用戶行為調整系統強化的 AI機器學習 演算法。

漏洞和補丁管理

作業系統和應用程式漏洞檢測和優先級排序。

自動分發補丁和更新。

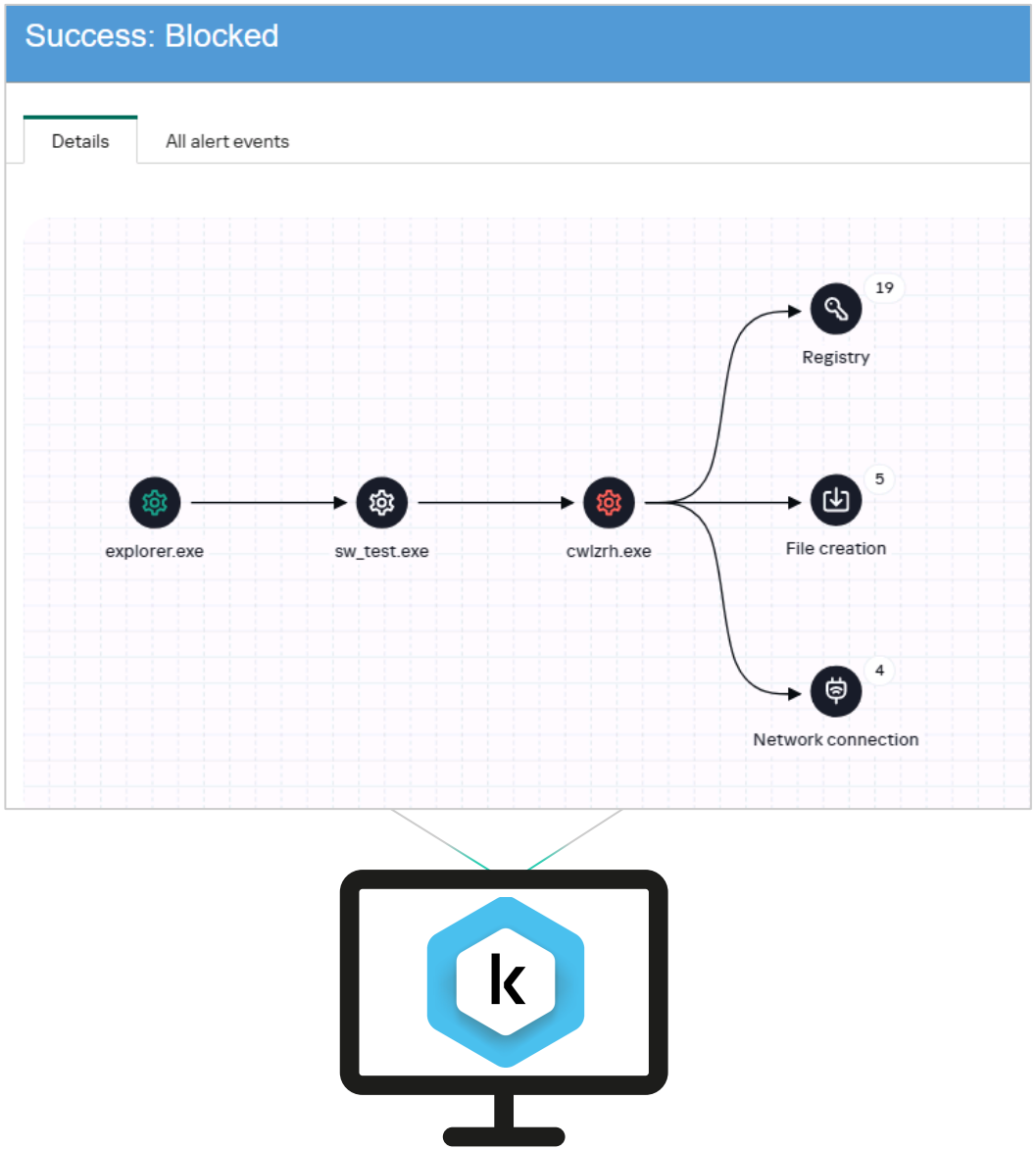
Kaspersky Next EDR Optimum：威脅行為及根源分析



預防攻擊並在攻擊鏈中將其可視化

- 機碼修改
- 惡意檔案載入
- 程序啟動
- 網路連接
- 代碼注入

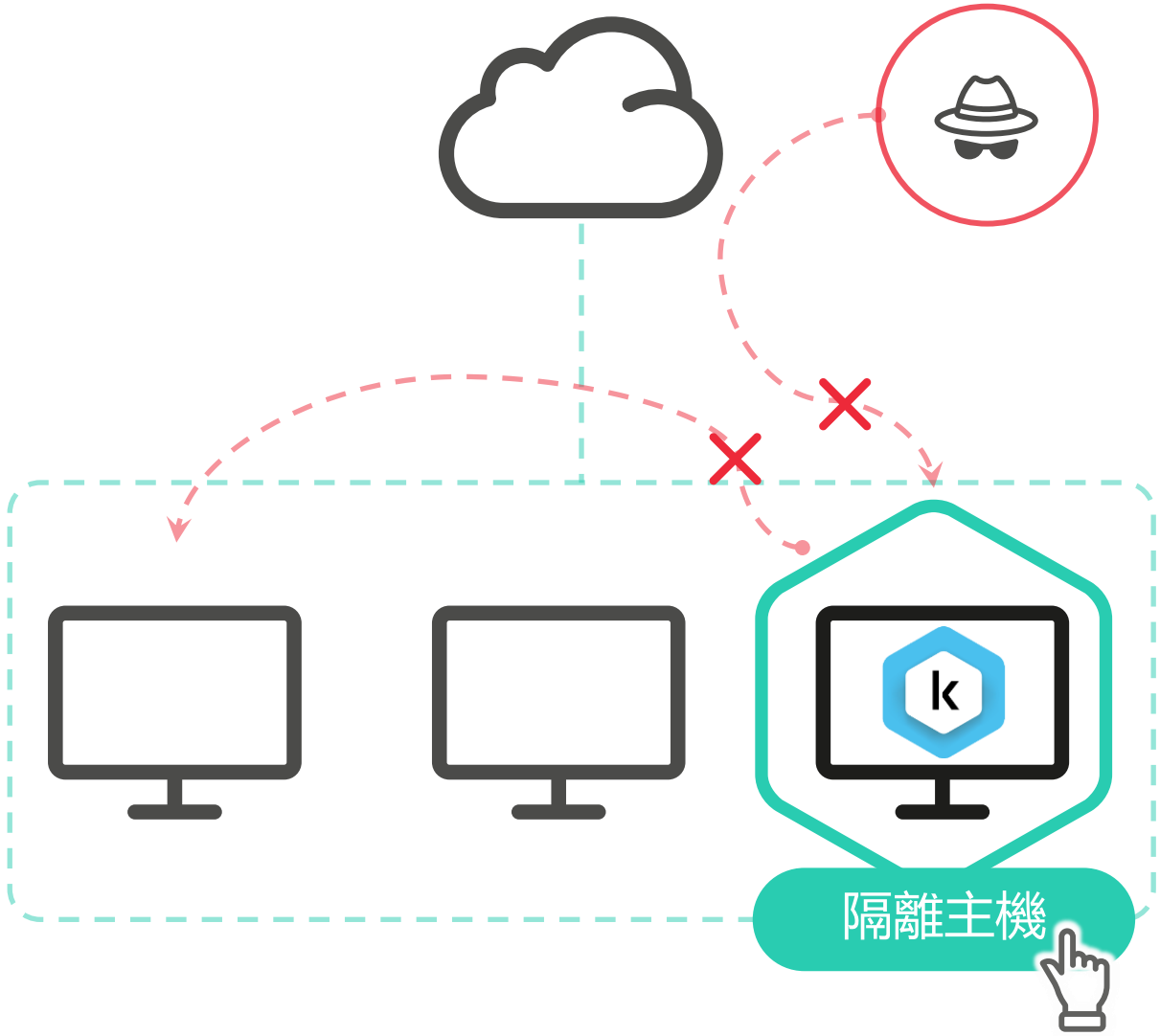
Kaspersky Next EDR Optimum：“一鍵式”自動響應



響應選項包括:

- 將主機與網路隔離
- 隔離檔案
- 禁止檔案執行
- 搜索內部其他設備是否有相同威脅
- 整合威脅情報了解更多資訊

“一鍵”將受感染主機與網路隔離



– 點擊隔離

– 一鍵將受攻擊的主機與網路隔離。從管理控制台本地或遠程恢復

– 阻止 C&C 通信

– 最大限度地降低橫向移動對其他機器的風險，併阻止對設備的遠程惡意命令

– 調查時間

– 使用網路隔離期作為調查時間，并在需要時停止隔離

防護技術總結

應用廣泛的 EPP 和 EDR 功能

利用內置的 卡巴斯基 Next EDR 基礎安全功能。使用額外的系統強化和漏洞管理功能

阻止複雜的攻擊

獲得自動複雜的攻擊預防開通過所有設備進行監控

調查

使用自動取証報告，通過單一管理控制台研究整個攻擊鏈的所有細節

響應

使用來自攻擊方或第三方的 IOC，以最少的資源阻止未來的攻擊，或通過 “跨端點” 響應查找過去的証據

Kaspersky Next XDR Expert：使用XDR做為事件調查平台

Kaspersky Next XDR Expert

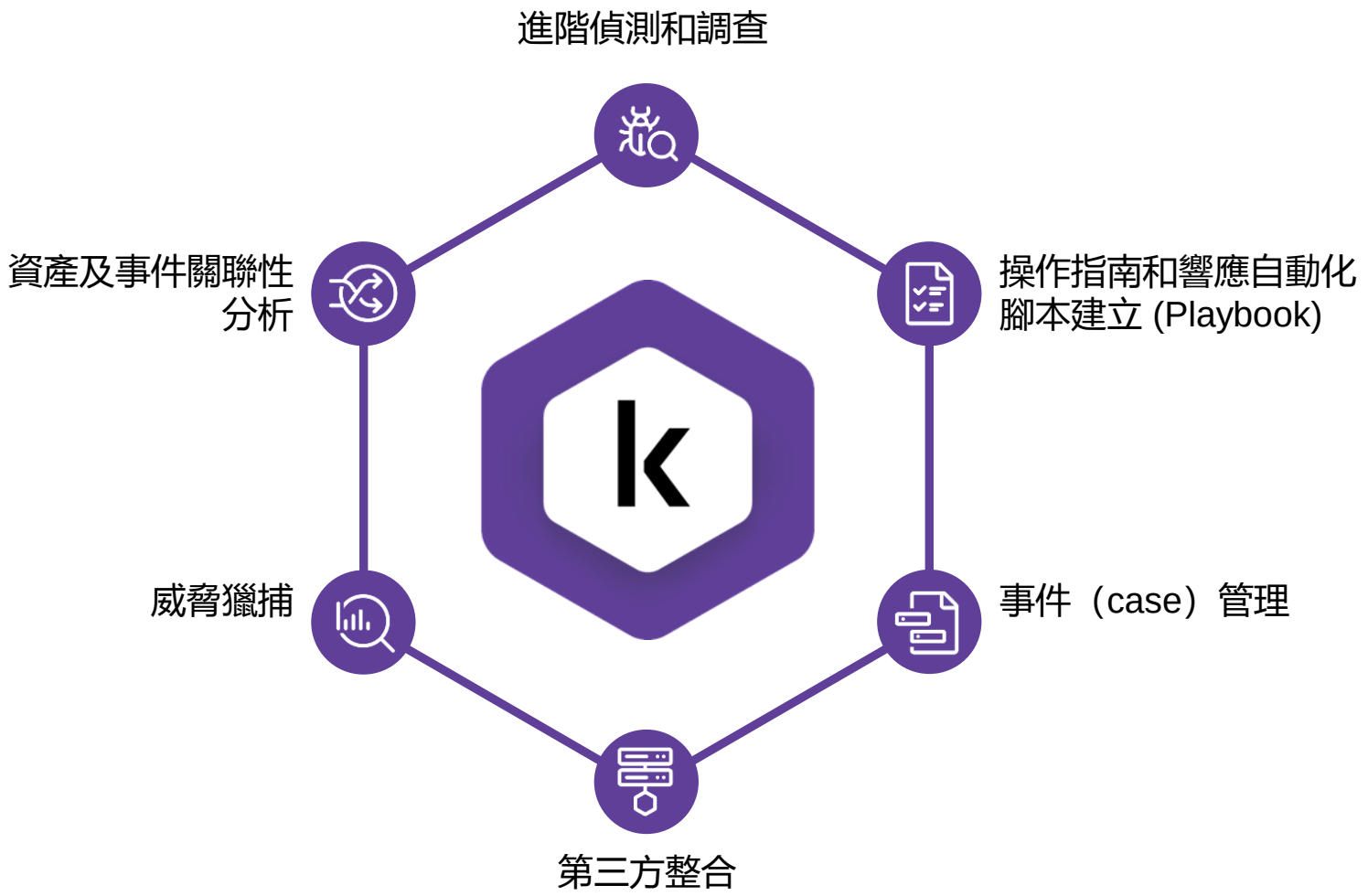
專家用的響應工具平台

防護您的企業偵測最複雜、最進階的威脅

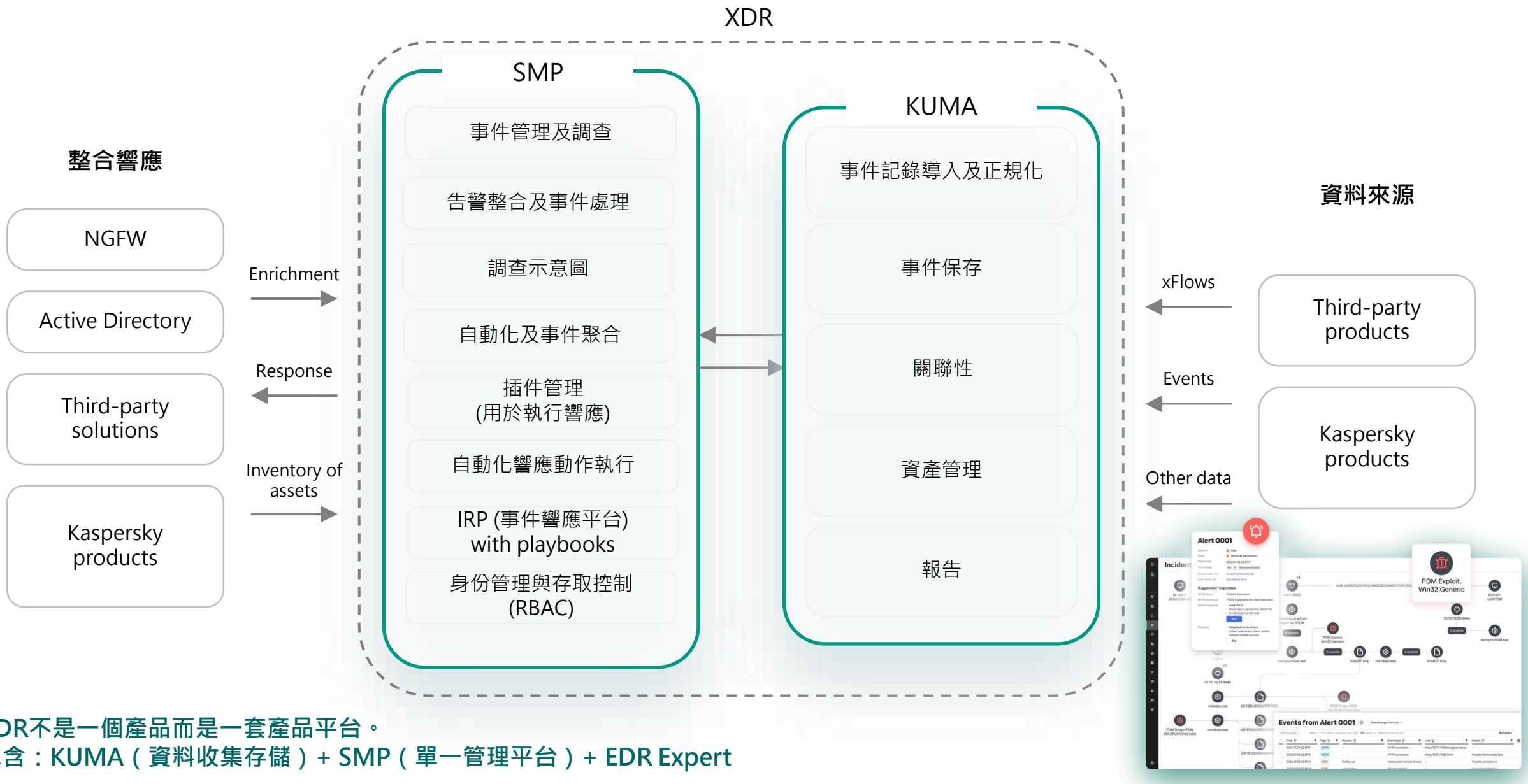
如果您需要

- 進階威脅偵測
- 整合其他安全產品事件
- 強大的威脅獵捕工具

包含 Kaspersky Next EDR Optimum 功能



Kaspersky Next XDR Expert :事件響應與關聯分析平台析



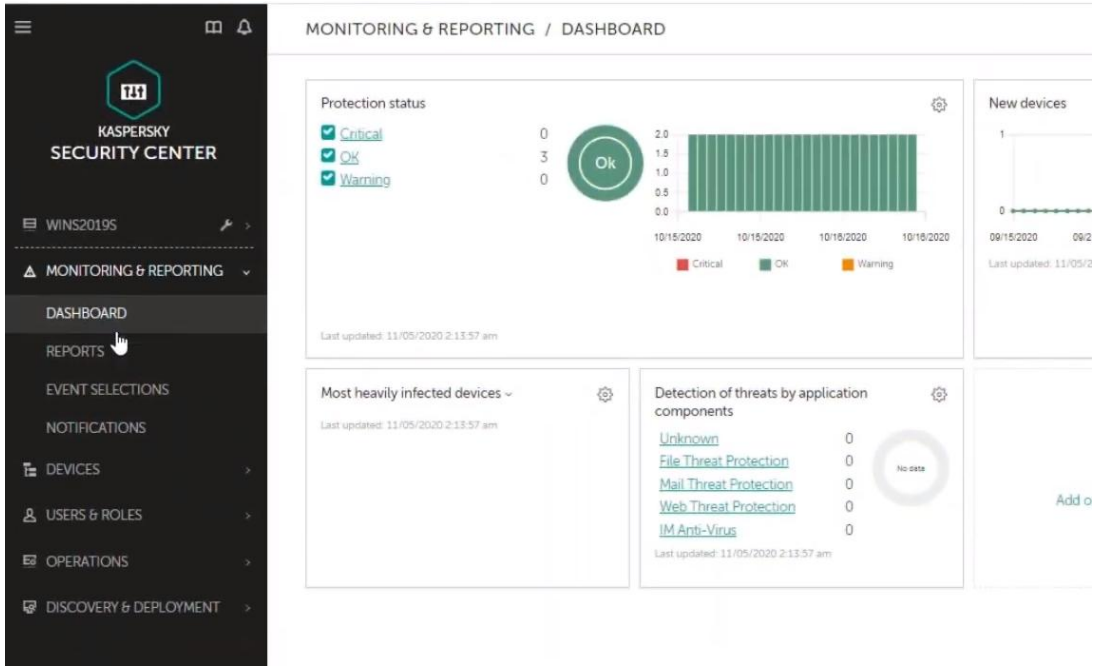
XDR不是一個產品而是一套產品平台。
包含：KUMA（資料收集存儲）+ SMP（單一管理平台）+ EDR Expert

產品內容

產品授權分級功能比較

	Kaspersky Next EDR Foundations	Kaspersky Next EDR Optimum	Kaspersky Next XDR Expert
端點防護 檔案、 網路和郵件防病毒、網路防護、AMSI、漏洞利用防禦、修復、行為偵測、HIPS	✓	✓	✓
安全管理 防火牆、網路、設備、應用控制、雲發現	✓	✓	✓
行動裝置防護和管理 防護、控制和管理	✓	✓	✓
IT 管理工具 安裝軟體漏洞評估、補丁管理、資料清除、SW/HW 清單、第三方應用程式和作業系統遠端安裝部署管理	✓ 漏洞評估, 軟硬體清單	✓	✓
加密 加密和加密管理		✓	✓
雲端防護 雲發現、MS O365 的安全性、敏威資料發掘	✓ 只有雲發現	✓	✓
安全人員技能養成 針對 IT 管理員的網路安全培訓		✓	✓
基本 EDR 功能 根源分析、IoC 掃描、端點響應功能	✓ 只有根源分析	✓	✓
進階 EDR 功能 收集遙測資料、威脅獵捕、入侵跡象（IoA）檢測、MITRE ATT&CK 對應			✓
基本 XDR 功能 告警事件聚合、事件案件管理、落地沙箱、AD整合、TI 威脅情報整合			✓
進階 XDR 功能 交叉關聯分析、第三方連接器、Playbook、調查圖、事件管理和資料湖			✓

支援使用雲端管理平台的選項



Expert視圖

雲端管理平台界面與原有本地卡巴斯基管控中心Web控制台相似。

- 雲端管理作為主要管理中心，本地KSC作為從屬管理服務器，可實現跨不同國家/地區且沒有Internet 網路的環境下集中統一管理
- 亦可採用原有管理方式，本地集中管理所有卡巴斯基Next產品。

	Kaspersky Next EDR Foundations	Kaspersky Next EDR Optimum	Kaspersky Next XDR Expert
雲端管理. **Expert 視圖** 最少用戶數量 = 300	✔	✔	-
本地管理. **Web Console 視圖**	✔	✔	✔

真實用戶案例範例

一切都是從”中獎(勒索)”開始

用戶 A： 零售連鎖公司 我希望它能正常工作

Kaspersky Next
EDR Foundations

功能

- 基本的端點安全
- 只有 IT 人員
- 預算低

需求：

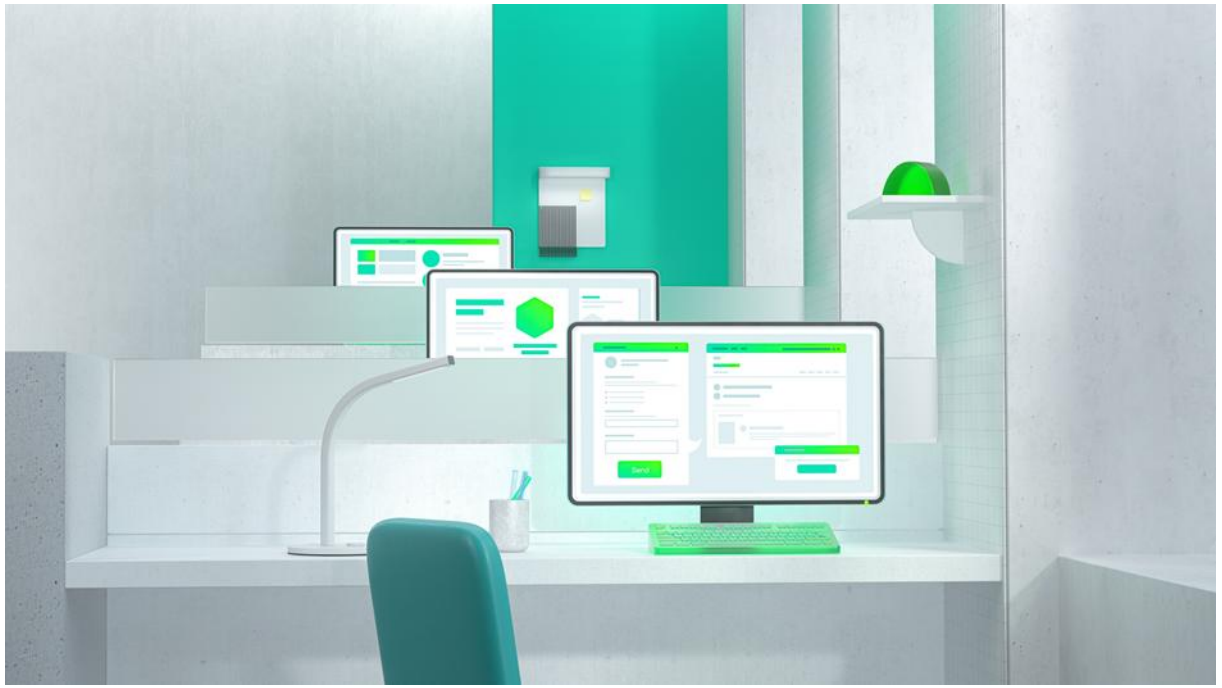
- 強大的安全性
- 維護簡單
- 低成本

Next Step：

- KESS 嵌入式安全
- KMDR 管理偵測與回應
- KUMA 輕型安全監控中心

用戶 B：政府單位 我想輕鬆建立安全保障

Kaspersky Next
EDR Optimum



功能：

- 端點安全
- 小型 IT 安全團隊
- 中低預算

需求：

- 開發專業知識和流程
- 高度自動化
- 專家建議指導

Next Step：

- KMDR 管理偵測與回應
- KATA 針對式攻擊防禦平台
- KUMA 安全監控中心

用戶 C：金融單位 需要為我的內部專家提供事件響應平台

Kaspersky Next
XDR Expert

功能：

- 複雜的環境
- 多種安全工具
- 專業的 IT 安全團隊
- 中高預算

需求：

- 强大的檢測、分析和響應能力
- 集中管理
- 降低複雜性

Next Step：

- 卡巴斯基 資安情資
- 卡巴斯基 安全服務
- 卡巴斯基 資安人員培訓

拋開意識形態

你需要的是 技術強悍的方案

卡巴斯基 Next
新一代安全

kaspersky