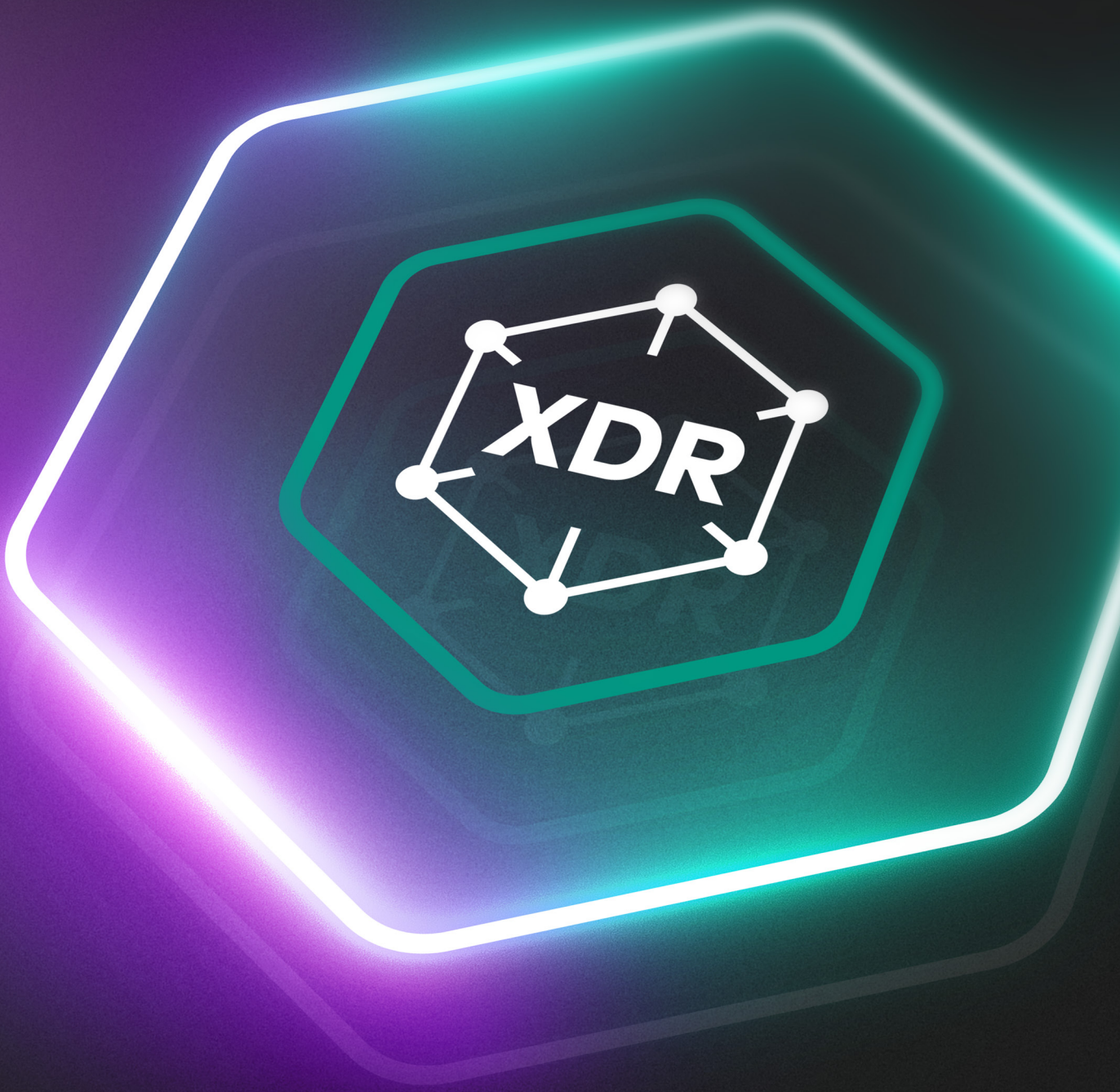


Kaspersky Extended Detection and Response

رؤية لا تضاهى.
الحماية الكاملة.

واجهوا المستقبل بأمان kaspersky

Kaspersky Extended Detection and Response

الرؤية الكاملة حماية لا مثيل لها.

يُعد Kaspersky XDR حلاً قويًا للأمن الإلكتروني يكافح التهديدات الإلكترونية المتطورة. ويوفر الرؤية الكاملة والارتباط والأتمتة، ويستفيد من مجموعة متنوعة من مصادر البيانات، بما في ذلك بيانات نقطة النهاية والشبكة والبيانات السحابية.

تطور هذا الحل من منصة Kaspersky Anti-Targeted Attack باسم Native XDR في عام 2016 إلى Open XDR في عام 2023، وهو يوفر رؤية شاملة للأمان. ويوفر Kaspersky XDR، الذي يمكن إدارته بسهولة من خلال منصة الإدارة الفردية المفتوحة، أمانًا شاملاً داخل المؤسسة، ويضمن بذلك بقاء بيانات العملاء الحساسة ضمن البنية التحتية الخاصة بهم مع تلبية متطلبات سيادة البيانات.

Open XDR

تم تصميم حلول Open XDR للعمل مع مجموعة واسعة من منتجات الأمان، مما يسمح للمؤسسات بدمج منتجات أمان متنوعة من مصادر مختلفة، ويؤدي إلى توفير المزيد من المرونة والقدرات المستقلة عن البائعين.

Native XDR

تعمل حلول Native XDR عادة بسلاسة مع النظام البيئي لأدوات الأمان الخاص بالبائع، مما يوفر تجربة أكثر توحيدًا وتماسكًا. وقد صُممت هذه الحلول خصيصًا للعمل معًا، ويوفر ذلك التكامل العميق والأتمتة وسير العمل المبسط ضمن مجموعة منتجات الأمان الخاصة بالبائع.

التقنيات الرئيسية

نقدم Open XDR كمنصة واحدة مفتوحة - أداة عامة لإنشاء نظام بيئي موحد لمنتجات الأمن الإلكتروني. ويتضمن Kaspersky XDR في قلبه حلولنا الرائدة Kaspersky Unified Monitoring and Analysis Platform - Kaspersky Endpoint Security for Business وKaspersky Endpoint Detection and Response. ولإدارة الشبكة المتقدمة، يمكن اختيار حل KATA كخيار إضافي.

المراقبة والتحليل

يوفر الجمع المركزي والتحليل الخاص بالسجلات وربط أحداث الأمان في الوقت الحقيقي والإخطار بالحوادث في الوقت المناسب. ويتضمن مجموعة جاهزة من قواعد الارتباط وإمكانية الوصول إلى المجموعة الغنية من خدمات Kaspersky Threat Intelligence لتحديد التهديدات والهجمات ومؤشرات الاختراق وترتيب أولوياتها.

تعقيد الأمن الإلكتروني للشركات

يضفي مشهد التهديدات الإلكترونية صعوبة بالغة لكي تبقى المؤسسات على دراية بأمنها الإلكتروني مع التركيز على عمليات الشركة الأساسية. ويمكن أن نضف إلى هذا المزيج مساحة الهجوم دائمة التوسع والمتطلبات التنظيمية وفجوة المهارات العالمية، ومن السهل معرفة سبب تعرض الشركات الحديثة لضغوط كبيرة، ولماذا تنجح العديد من الهجمات الإلكترونية

51%

من الشركات تكافح لاكتشاف التهديدات المتقدمة والتحقيق فيها باستخدام الأدوات الحالية

68%

من الشركات تعرضت لهجوم موجه على شبكاتها وتعرضت لفقدان البيانات كنتيجة مباشرة له

6 تريليون دولار

التكلفة السنوية العالمية للجرائم الإلكترونية

400000

من البرامج الضارة يتم اكتشافها كل يوم

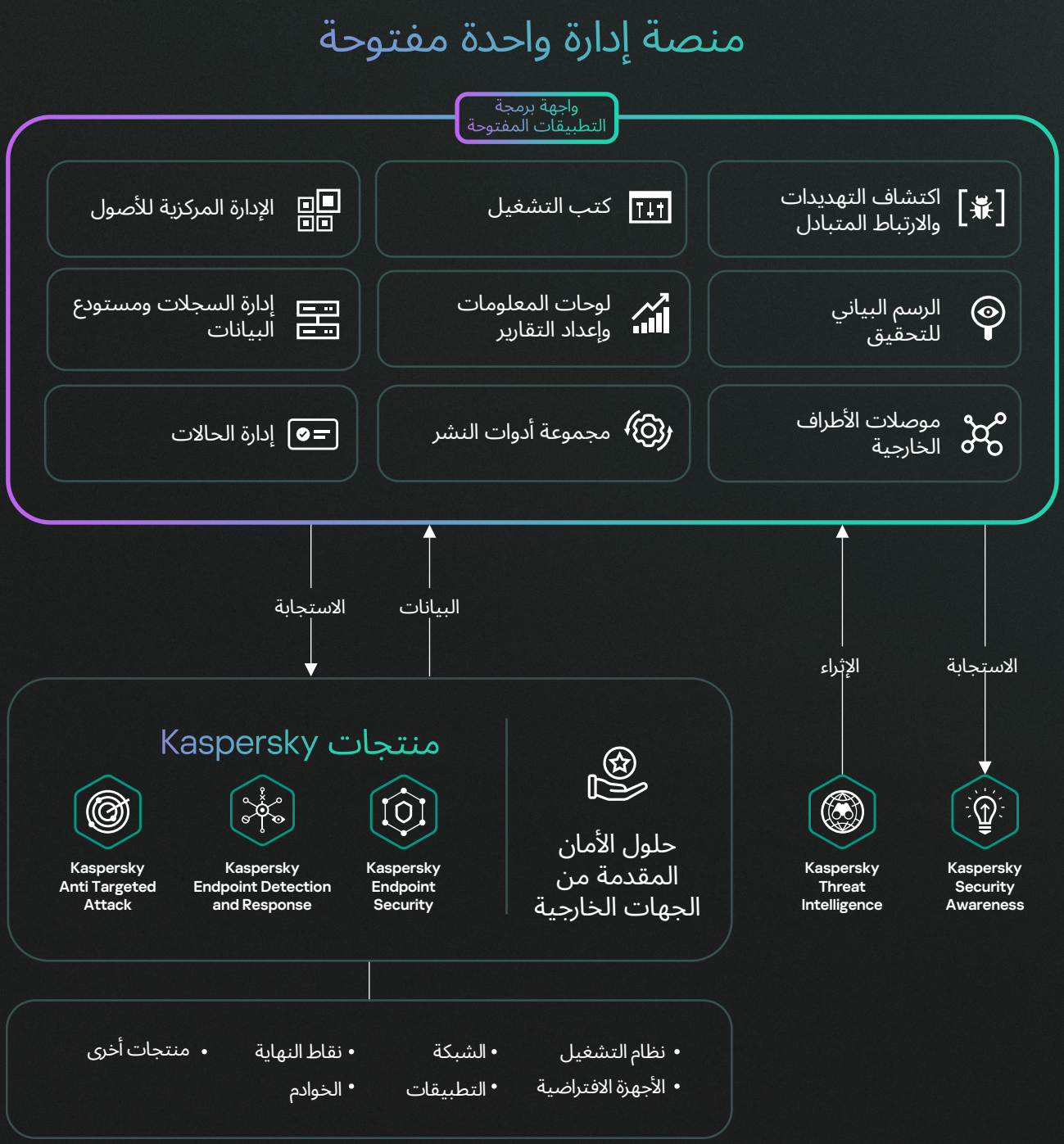
المصادر: Kaspersky وPurpleSec وCybersecurityVentures

حماية نقطة النهاية

توفر حماية قوية لنقطة النهاية، وتحمي من برامج طلب الفدية والبرامج الضارة والهجمات الخالية من الملفات. وسواء داخل الشركة أو في السحابة، تستخدم حماية نقاط النهاية التعلم الآلي وتحليل السلوك لحماية جميع أنواع نقاط النهاية التي تعمل على أي نظام تشغيل رئيسي.

Endpoint Detection and Response

يوفر الحل رؤية شاملة ودفاعات فائقة عبر جميع نقاط النهاية الخاصة بالمؤسسة. وتعمل عمليات البحث عن التهديدات واكتشافها بشكل محسّن بفضل معلومات التهديدات الفريدة وواسعة النطاق من Kaspersky، بالإضافة إلى أتمتة المهام الروتينية وعمليات التحقيق الموجهة والاكتشافات القابلة للتخصيص، على تعزيز تقديم حل سريع للحوادث.



ميزات قوية، فوائد كبيرة

دمج البيانات في الوقت الحقيقي من الأطراف الخارجية

تتجاوز القدرة على دمج البيانات من مصادر خارجية مجرد نقاط النهاية ويتم تعزيزها من خلال الارتباط المتبادل في الوقت الحقيقي.

الاستجابة والمعالجة الآليتان

عزل نقاط النهاية المعرضة للخطر أو فصلها، وحظر الأنشطة الضارة، ومعالجة الثغرات الأمنية، مما يقلل الجهد اليدوي ووقت الاستجابة.

EPP/EDR الأفضل في فئتها

نظرًا لأنها شركة رائدة عالميًا، تضع Kaspersky معيارًا لحلول منصة حماية نقطة النهاية (EPP) /اكتشاف نقطة النهاية والاستجابة لها (EDR) في جميع أنحاء العالم. ويتفوق حل Kaspersky EDR على نطاق عالمي، مدعومًا بالجوائز والمشاركة النشطة في اللجان الدولية مثل الإنتربول وMAPP.

قابلية توسع لا تضاهي

نظرًا للقدرة على دعم الأحمال التي تشمل مئات الآلاف من نقاط النهاية في مثيل واحد، يتتبع Kaspersky XDR التهديدات بجدية في الوقت الحقيقي مع ضمان التوافر العالي.

سيادة البيانات

تعد Kaspersky XDR أحد البائعين القلائل الذين يقدمون حل XDR شاملاً داخل المؤسسة، مما يضمن بقاء البيانات الحساسة للعملاء ضمن بنيتهم التحتية مع تلبية متطلبات سيادة البيانات.

الدمج السلس والقوي عبر منتجات Kaspersky

يصل التفاعل بين المنتجات إلى مستوى لا تستطيع حلول الجهات الخارجية الوصول إليه، ويتميز بنظام دعم موحد وتصميم متكامل بسلاسة.

تعدد المؤسسات التي تُمكن سيناريوهات مقدمو خدمات الأمن المدارة

يتم توفير XDR كخدمة مع مستأجرين شاملين - لا يستطيع مستخدم لدى أحد المستأجرين رؤية بيانات المستأجرين الآخرين، بينما يستطيع المسؤول الرئيسي (مقدمو خدمات الأمن المدارة) إنشاء عمليات الاكتشاف والاستجابة لجميع العملاء.

تخصيص سيناريو الأمان المتقدم وتحليل البيانات على مستوى البنية التحتية

تمكين المستخدمين من تكوين سيناريوهات الأمان المعقدة مع القدرة الإضافية على تحليل البيانات عبر بنيتهم التحتية بالكامل.

قدرات الدمج

توفر المجموعة الواسعة من عمليات الدمج التي تعمل مع Kaspersky XDR رؤية موحدة وسياقية للتهديدات المحتملة، مما يمنح فريق الأمان الخاص بك جميع الأدوات والمعلومات التي يحتاجونها لحماية مؤسستك من أي شيء يرسله إليك مجرمو الإنترنت.

تشمل إمكانات دمج المنتج القدرة على تلقي البيانات (السجلات) من الأنظمة والأجهزة الأخرى، بالإضافة إلى إعداد استجابات تلقائية في المنتجات الأخرى. ويأتي Kaspersky XDR مزودًا بمجموعة واسعة من عمليات الدمج المبتكرة مع منتجات Kaspersky ومنتجات الجهات الخارجية. ويمكن أيضًا إضافة عمليات دمج إضافية يمكن تطويرها إما بواسطة Kaspersky Professional Services أو بواسطة الشركاء أو العملاء أنفسهم (بما في ذلك استخدام إمكانيات واجهة برمجة التطبيقات (API) للمنتجات القابلة للاتصال). ويمكن الدمج مع أنظمة من مجالات مختلفة وبائعين مختلفين، ويتم دعم العديد من البروتوكولات وتنسيقات البيانات.

حسب مجال الأمان

أمان نقطة النهاية

- حلول EPP وEDR

أمان الشبكات والويب والبريد الإلكتروني

- حماية البريد الإلكتروني
- اكتشاف الشبكة والاستجابة لها (NDR)
- جدران الحماية (FW) وجدران الحماية من الجيل التالي (NGFW)
- إدارة التهديدات الموحدة (UTM)
- أنظمة اكتشاف الاختراق (IDS)

أمان الخدمات السحابية

- وسطاء أمان الوصول إلى السحابة (CASB)
- منصات حماية عبء العمل السحابي (CWPP)

المعلومات المتعلقة بالتهديدات

- معلومات التهديدات الإلكترونية (CTI)

أمان الهوية

- إدارة الهوية والوصول (IAM)
- إدارة الوصول المميز (PAM)

الوعي الأمني بأمان التكنولوجيا التشغيلية / إنترنت الأشياء

حسب نوع النقل

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

حسب نوع البيانات

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

حسب البائع

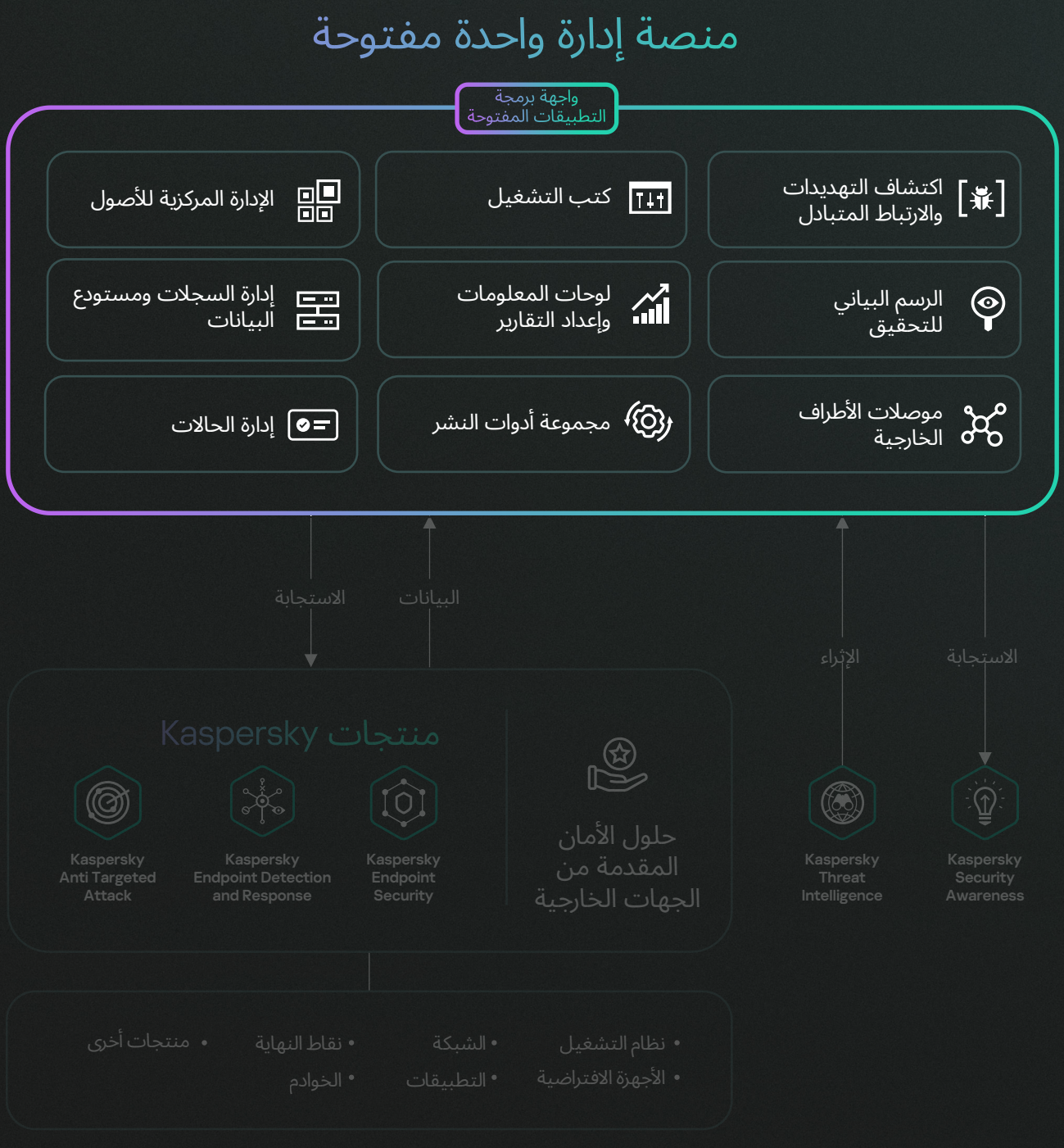
- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilo
- Ayehu
- Barracuda
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- CheckPoint
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- DeepInstinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- Eset
- F5 BigIP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- Huawei
- 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 & etc

الميزات التي نقدمها

يتوفر Kaspersky XDR في خيارين.

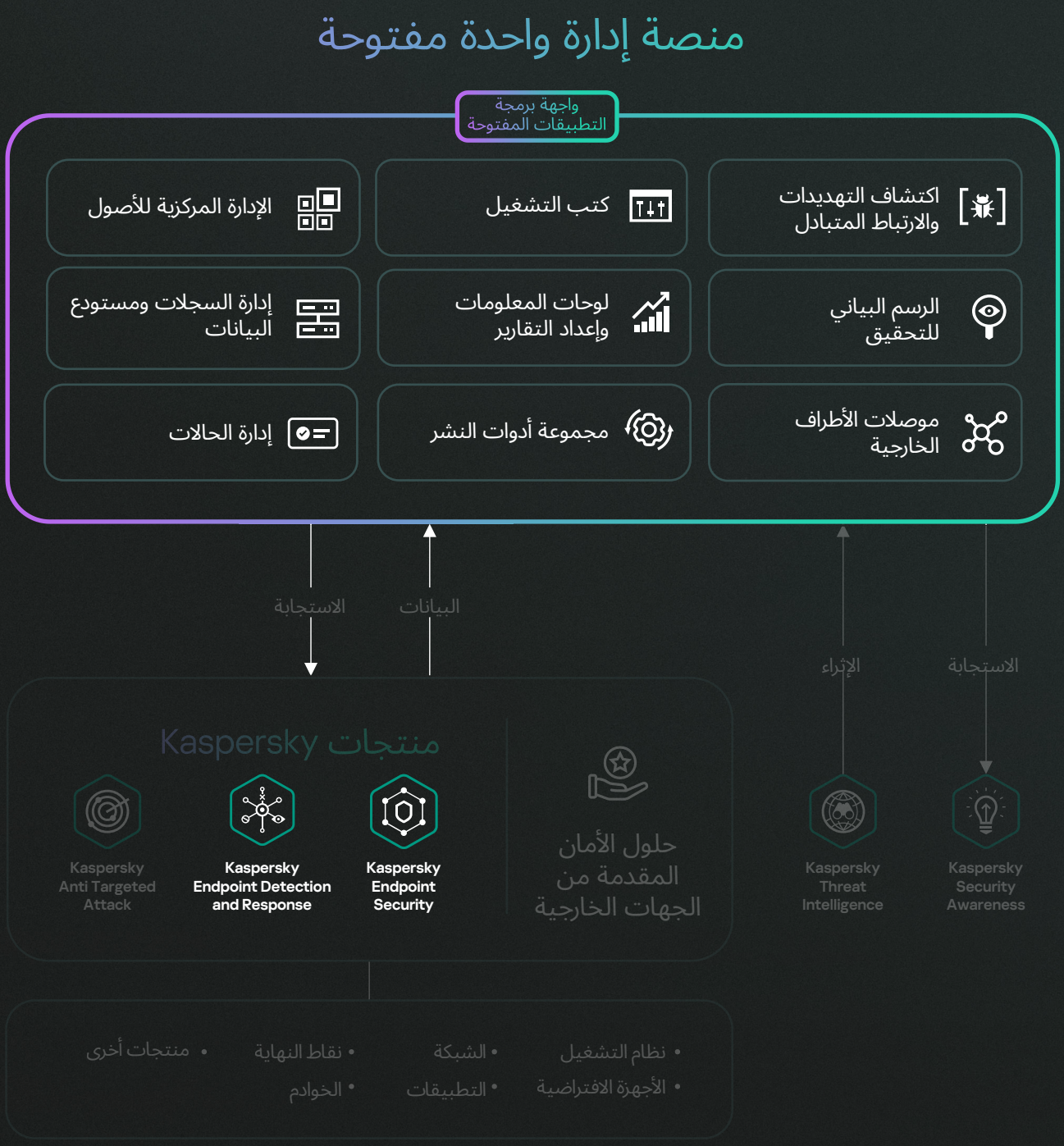
KasperskyXDR Core

يتم تخصيص Kaspersky XDR Core للعملاء الذين يمتلكون بالفعل حلول نقاط النهاية وEDR ولا يريدون استبدالها، ويفضلون توسيع الوظائف باستخدام محرك الارتباط والاستجابات الآلية والموصلات من جهات خارجية.



Kaspersky XDR Expert

يجمع Kaspersky XDR Expert بين حماية نقطة النهاية الأفضل في فئتها وإمكانيات الاكتشاف المتقدمة التي يتمتع بها Kaspersky EDR Expert، وهو محرك ارتباط واستجابات آلية. ويمكن إضافة موصلات الجهات الخارجية لسحب جميع البيانات معًا.



القيمة المضافة مع أجهزة الاستشعار التكميلية

يدعم Kaspersky XDR الدمج السلس لأجهزة الاستشعار التكميلية المصممة لحماية أصول محددة، والدمج بسلاسة في XDR لتوفير طبقة إضافية من القيمة، وتحويل XDR إلى منصة متماسكة تمنح المحللين مساحة عمل مركزية تغطي جميع الحلول المدمجة.

ولا يعمل Kaspersky XDR على تعزيز دفاعاتك من خلال EDR فحسب، بل يوفر أيضًا إمكانات دمج مرنة، بحيث يستطيع العملاء إضافة منتجات إلى النظام البيئي في أي وقت.

		Kaspersky XDR Core	Kaspersky XDR Expert
منصة الإدارة الواحدة المفتوحة ومكوناتها	محرك الارتباط المتبادل (مدعوم من KUMA) • موصلات الأطراف الخارجية • إدارة السجلات ومستودع البيانات • أكتشاف التهديدات والارتباط المتبادل • إدارة الأصول • لوحات المعلومات وإعداد التقارير	●	●
	مكونات XDR • إدارة الحالات • أتمتة الاستجابة والتنسيق (كتب التشغيل) • التحقيق • مجموعة أدوات النشر • واجهة برمجة التطبيقات المفتوحة	●	●
وظائف Kaspersky EDR وKESB	الاكتشاف الآلي وشبه الآلي واليدوي	●	
	المراقبة عبر نقاط النهاية المحمية	●	
	احتواء التهديد	●	
	خيارات الاسترداد	●	

Kaspersky XDR Core

- Kaspersky Unified Monitoring and Analysis Platform
- مكونات XDR

Kaspersky XDR Expert

- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Endpoint Security for Business
- Kaspersky Endpoint Detection and Response
- مكونات XDR

Why Kaspersky XDR

خاضعة لأكبر عدد من الاختبارات. حائزة على أكبر عدد من الجوائز. حماية KASPERSKY.

Kaspersky شركة عالمية راسخة في مجال الأمن الإلكتروني وتتمتع بسجل حافل من الخبرة الأمنية. وقد وفرنا الحماية للمؤسسات في جميع أنحاء العالم لأكثر من 25 عامًا وحصلنا على عدد لا يحصى من الجوائز والأوسمة لمنتجاتنا وخدماتنا. بين عامي 2013 و2022، حصلت منتجات Kaspersky على ما يلي:

685

حققت أحد المراكز الثلاثة الأولى

587

حققت المركز الأول 587 مرة

827

شاركت في 827 اختبارًا ومراجعة مستقلة

في عام 2023، حصلت Kaspersky على لقب الشركة الرائدة في سوق حلول XDR من قبل شركة ISG العالمية الرائدة في مجال الأبحاث والاستشارات التقنية. وتُعرّف ISG "الرواد" بأنهم من يمتلكون عرضًا شاملاً للمنتجات والخدمات ويمثلون قوة مبتكرة واستقرارًا تنافسيًا.

معرفة المزيد

Kaspersky Extended Detection and Response

طلب عرض توضيحي

#kaspersky
#bringonthefuture

me.kaspersky.com