Kaspersky Endpoint Detection and Response

واجهوا المستقبل بأمان kaspersky

أصبح مجرمو الإنترنت أكثر تطورًا وقدرة على تجاوز الحماية الحالية بنجاح. يمكن أن يتعرض كل مجال من مجالات عملك للمخاطر، مما يؤدي إلى تعطيل العمليات الحيوية للأعمال التجارية، والإضرار بالإنتاجية وزيادة تكاليف التشغيل.

عزز دفاعات نقطة النهاية الخاصة بك أولاً

بالنسبة لمجرمي الإنترنت، تعد نقاط النهاية للشركات مكان التقاء البيانات والمستخدمين وأنظمة الشركة معًا لإنشاء إجراءات العمل وتنفيذها، وبالتالي تظل الهدف الأساسي. لحماية نقاط النهاية ولمنع استغلالها كنقاط دخول إلى البنية الأساسية، يجب أن تستعرض فِرق أمن تقنية المعلومات لدى مؤسستك الوسائل بهدف تعزيز عمليات الأمن الحالية. تنفيذ الدورة الكاملة لحماية نقطة النهاية، بدءًا من حظر التهديدات التلقائي ووصولاً إلى الاستجابة السريعة والمناسبة للحوادث المعقدة، يتطلب تقنيات وقائية تكمّلها قدرات دفاعية متقدمة.

يوفِّر Kaspersky Endpoint Detection and Response (EDR) أمانًا قويًا ورؤية شاملة عبر كل نقاط النهاية على شبكة الشركة ويوفر كذلك دفاعات فائقة، مما يتيح أتمتة المهام الروتينية لاكتشاف التهديدات المعقدة والهجمات الشبيهة بالتهديدات المستمرة المتقدمة وتحديد أولوياتها والتحقيق فيها والقضاء عليها.

باستخدام Kaspersky EDR، يمكن لمؤسستك:

- **مراقبة** التهديدات بكفاءة – التي تتجاوز البرامج الضارة
- **اكتشاف** التهديدات بشكل فعال – باستخدام التقنيات المتقدمة
- **تجميع** البيانات الأولية وتقارير البيانات بشكل مركزي
- **الاستجابة** السريعة للهجمات
- **منع** الإجراءات الضارة من خلال التهديدات المكتشفة

... كل ذلك عبر واجهة ويب سهلة الاستخدام تعمل على تيسير عمليتي البحث والتفاعل.

أهم الميزات

- يُحسِّن Kaspersky EDR الأنظمة الأساسية لحماية نقاط النهاية (EPP) الخاضعة لأكبر عدد من الاختبارات والحائز على أكبر عدد من الجوائز – Kaspersky Endpoint Security for Business - مع إمكانات EDR الفعّالة، مما يزيد من تعزيز مستويات الأمن الإجمالي لديك. يعمل وكيل واحد على توفير الحماية التلقائية من التهديدات الشائعة والحماية المتقدمة من الهجمات المعقدة من أجل تسهيل معالجة الحوادث والحد من متطلبات الصيانة. لا يوجد أي عبء إضافي على نقاط النهاية أو أي تكاليف إضافية، بل يمكنك ببساطة التأكد من أن محطات العمل والخوادم لديك محمية بالكامل من أكثر التهديدات المتطورة والمستهدفة.
- يقلل Kaspersky EDR من الوقت اللازم لجمع الأدلة الأولية، ويقدم تحليلًا وافيًا للقياس عن بُعد ويزيد من أتمتة عمليات EDR، مما يقلل أوقات الاستجابة الإجمالية للحوادث دون الحاجة إلى جذب موارد أمن تكنولوجيا المعلومات الإضافية.
- يمكن استيعاب Kaspersky EDR في نظام **Kaspersky Anti Targeted Attack Platform**، حيث يجمع بين إمكانات EDR واكتشاف التهديدات المتقدمة على مستوى الشبكة. يملك المتخصصون في أمن تقنية المعلومات كل الأدوات التي يحتاجون إليها لإجراء اكتشاف التهديدات المتعدد الأبعاد على مستوى نقطة النهاية والشبكة، مع تطبيق تقنية رائدة وإجراء عملية تحقيق فعالة وتقديم استجابة مركزية سريعة، وكل ذلك عبر حل واحد.

Kaspersky EDR والتسليمات الرئيسية من تقرير IDC بشأن توفير الأمن لنقاط النهاية لعام 2020*

- سيؤدي حل الأنظمة الأساسية لحماية نقاط النهاية الضعيف إلى تدمير قيمة أداة EDR

  تقدم Kaspersky دفاعات قوية كاملة لنقاط النهاية (EPP + EDR) عبر وكيل واحد

- وهكذا أصبح الأشخاص والوقت مقياس عائد الاستثمار الجديد لأدوات EDR

  تطبق Kaspersky مستويات عالية من الأتمتة على المشكلات المعقدة، مما يوفر الوقت الثمين لخبراء الأمن لديك

- يجب أن يستفيد EDR من البيانات الموجودة خارج نقاط النهاية

  تعزز Kaspersky فعالية EDR من خلال إضافة اكتشاف متقدم للتهديدات عبر البريد والويب وإمكانية الرؤية من خلال أداة واحدة

* IDC PERSPECTIVE, Endpoint Security 2020:
إعادة ظهور حماية نقاط النهاية والمصير المحتوم لـ EDR

يعد Kaspersky EDR مثاليًا إذا كانت مؤسستك تريد:

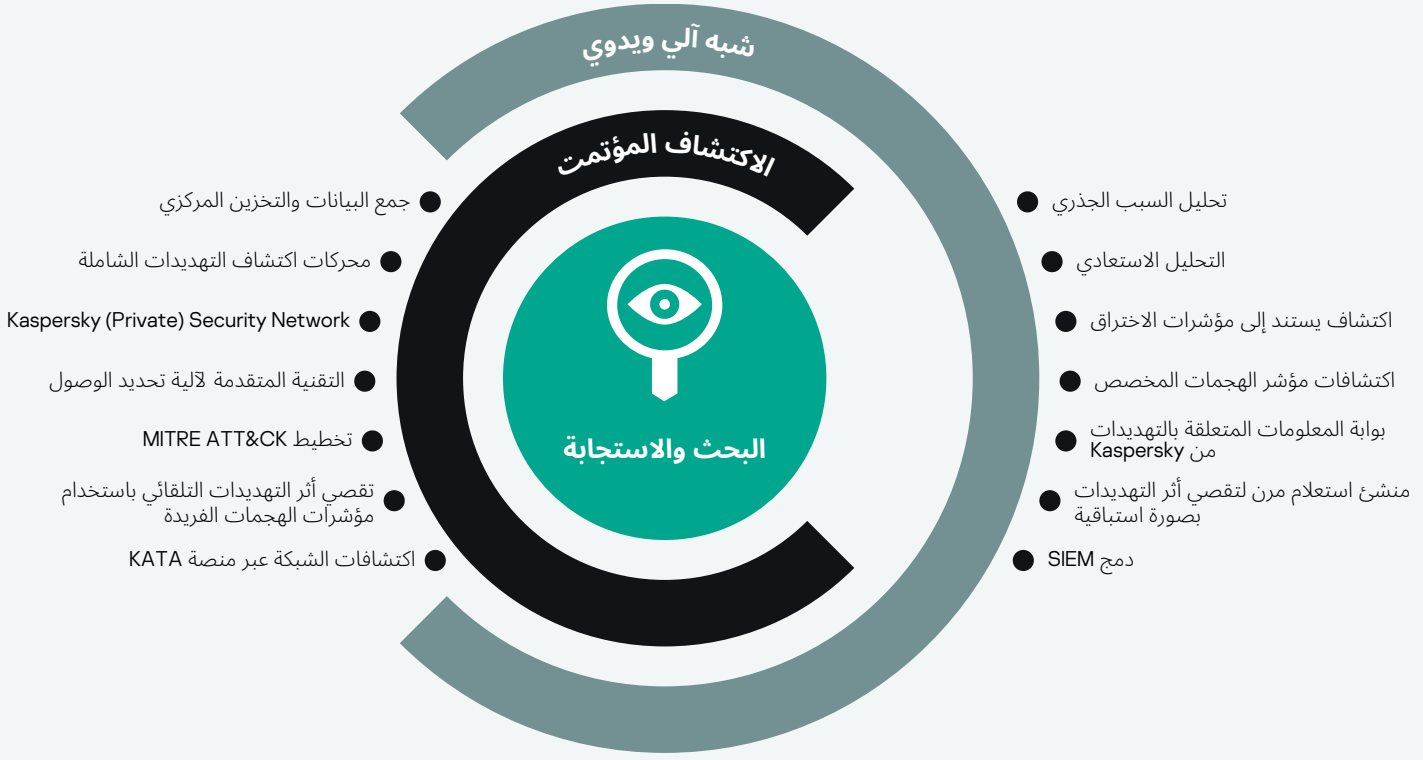
- ترقية الأمان باستخدام حل مؤسسي يسهل استخدامه بهدف الاستجابة للحوادث
- أتمتة تحديد التهديدات والاستجابات – دون انقطاع الأعمال أثناء التحقيقات
- تعزيز رؤية نقطة النهاية واكتشاف التهديدات عبر التقنيات المتقدمة
- فهم التكتيكات والأساليب والإجراءات (TTPs) المحددة التي يستخدمها الجهات التي تشن التهديدات لتحقيق أهدافها، وتمكين الدفاعات الأكثر فعالية وتخصيص موارد الأمان
- إنشاء عمليات موحدة وفعالة للبحث عن التهديدات وإدارة الحوادث والاستجابة لها
- زيادة كفاءة مركز عمليات الأمن (SOC) الداخلية – لا تضيع وقتهم في تحليل سجلات نقطة النهاية عديمة الجدوى
- تقديم المساعدة اللازمة للامتثال من خلال فرض سجلات نقطة النهاية واستعراض التحذيرات والوثائق المتعلقة بنتائج التحقيق

الكشف السريع عن التهديدات الأكثر تعقيدًا واحتواؤها

يوفر **Kaspersky EDR** مستويات عاليةٍ لنقاط النهاية ويزيد من كفاءة مركز عمليات الأمن (**SOC**)، مما يوفر اكتشافًا متقدمًا للتهديدات ويوفر الوصول إلى البيانات بأثر رجعي، حتى في المواقف التي يتعذر فيها الوصول إلى نقاط النهاية المخترقة أو عندما يتم تشفير البيانات أثناء الهجوم. قدرات التحقيق المعززة من خلال مؤشرات الهجوم الفريدة (**IoAs**) وتعزيز **MITER ATT & CK** ومنشئ الاستعلام المرن، بالإضافة إلى الوصول إلى قاعدة معارف بوابة **Threat Intelligence Portal** - كل ذلك يسهل البحث عن التهديدات والاستجابة السريعة للحوادث، مما يؤدي إلى الحد من الأضرار والوقاية منها.

حالات الاستخدام:

- بحث استباقي عن أدلة تُثبت الاختراقات على شبكتك بالكامل
- الكشف السريع عن الاختراقات ومعالجتها – قبل أن يتسبب المخترِق في أضرار وتعطيلات كبيرة
- تحقيق سريع وإدارة مركزية للحوادث عبر الآلاف من نقاط النهاية مع سير عمل سلس
- التحقق من صحة التحذيرات والحوادث المحتملة التي جرى اكتشافها عن طريق الحلول الأمنية الأخرى
- أتمتة العمليات الروتينية – للمساعدة في تقليل المهام اليدوية، وتحرير مواردك وتقليل احتمالية "التحذيرات الزائدة"



فوائد أعمال Kaspersky EDR عبر المؤسسة:

- تساعد في القضاء على الثغرات الأمنية وتقليل "مدة مكون" الهجوم
- أتمتة المهام اليدوية أثناء اكتشاف التهديدات والاستجابة لها
- إتاحة الوقت للعاملين في تكنولوجيا المعلومات وأمن تكنولوجيا المعلومات للقيام بمهام أخرى بالغة الأهمية
- تبسط تحليل التهديدات والاستجابة للحوادث
- تقليل الوقت المستغرق للتعرف على التهديدات والاستجابة لها
- تساعد على تمكين الامتثال الكامل

وإذا كنت تريد المزيد ... Kaspersky Managed Detection and Response

تشير إضافة دفاعات تُدار بالكامل ومصممة بشكل فردي على مدار الساعة إلى Kaspersky EDR إلى أنه يمكن الحفاظ على موارد أمن تكنولوجيا المعلومات لديك عن طريق إلغاء تحميل مهام المعالجة المتعلقة بالحوادث إلى Kaspersky، أو اللجوء إلينا للحصول على مشورة متخصصة والاستفادة من خبراتهم في مجال مواجهة التهديدات عندما يحتاج فريقك الداخلي إلى متخصصين أمنيين مؤهلين بشكل كافٍ لتلبية سيناريوهات محددة.

لمعرفة المزيد حول Kaspersky EDR، تفضل بزيارة:

kaspersky.com/enterprise-security/endpoint-detection-response-edr

Gartner peerinsights customers' choice 2020™

ترشح شركة Gartner Peer Insights Kaspersky Top Vendor لحلول EDR لعام Customers' Choice 2020

تعد Kaspersky واحدة من 6 موزّدين فقط في جميع أنحاء العالم يحصلون على تقدير Gartner Peer Insights Customer Choice الخاص بحلول Endpoint Detection and Response في عام 2020، والحصول على أعلى تقييمات لأي مورد لخدمتنا ودعمنا هو ثناء العميل النهائي لـ Kaspersky EDR.

إخلاء مسؤولية Gartner

تتضمن Gartner Peer Insights Customers' Choice الآراء الشخصية الخاصة بمراجعات المستخدم النهائي الفردية وتقييماته وبياناته المطبقة على منهجية موثّقة، ولا تمثل آراء Gartner أو شركاتها التابعة ولا تشكّل أي تخويل منها

MITRE | ATT&CK®

تم تأكيد جودة الاكتشاف من خلال تقييم MITRE ATT&CK

إدراك أهمية تحليل التكتيكات والتقنيات والإجراءات في التحقيق في الحوادث المعقدة ودور MITRE ATT&CK في سوق الأمن اليوم:

- شارك Kaspersky EDR في جولة التقييم الثانية لتهديد APT29 من MITRE وأظهر مستوى عاليًا من الأداء في اكتشاف تقنيات ATT & CK الأساسية من نطاق الجولة الثانية المطبقة في المراحل الحاسمة من الهجمات المستهدفة الحديثة
- يتم تعزيز اكتشافات Kaspersky EDR ببيانات من قاعدة معارف MITER ATT & CK، بهدف إجراء تحليل معمّق للتكتيكات والتقنيات والإجراءات الخاصة بالخصم.

اعرف المزيد عبر موقعنا الإلكتروني: kaspersky.com/MITRE

أخبار التهديدات الإلكترونية: securelist.com
أخبار أمن تكنولوجيا المعلومات: business.kaspersky.com
أخبار أمن تكنولوجيا المعلومات للشركات الصغيرة والمتوسطة الحجم: kaspersky.com/business
أخبار أمن تقنية المعلومات للمؤسسات الكبيرة: kaspersky.com/enterprise

www.kaspersky.com