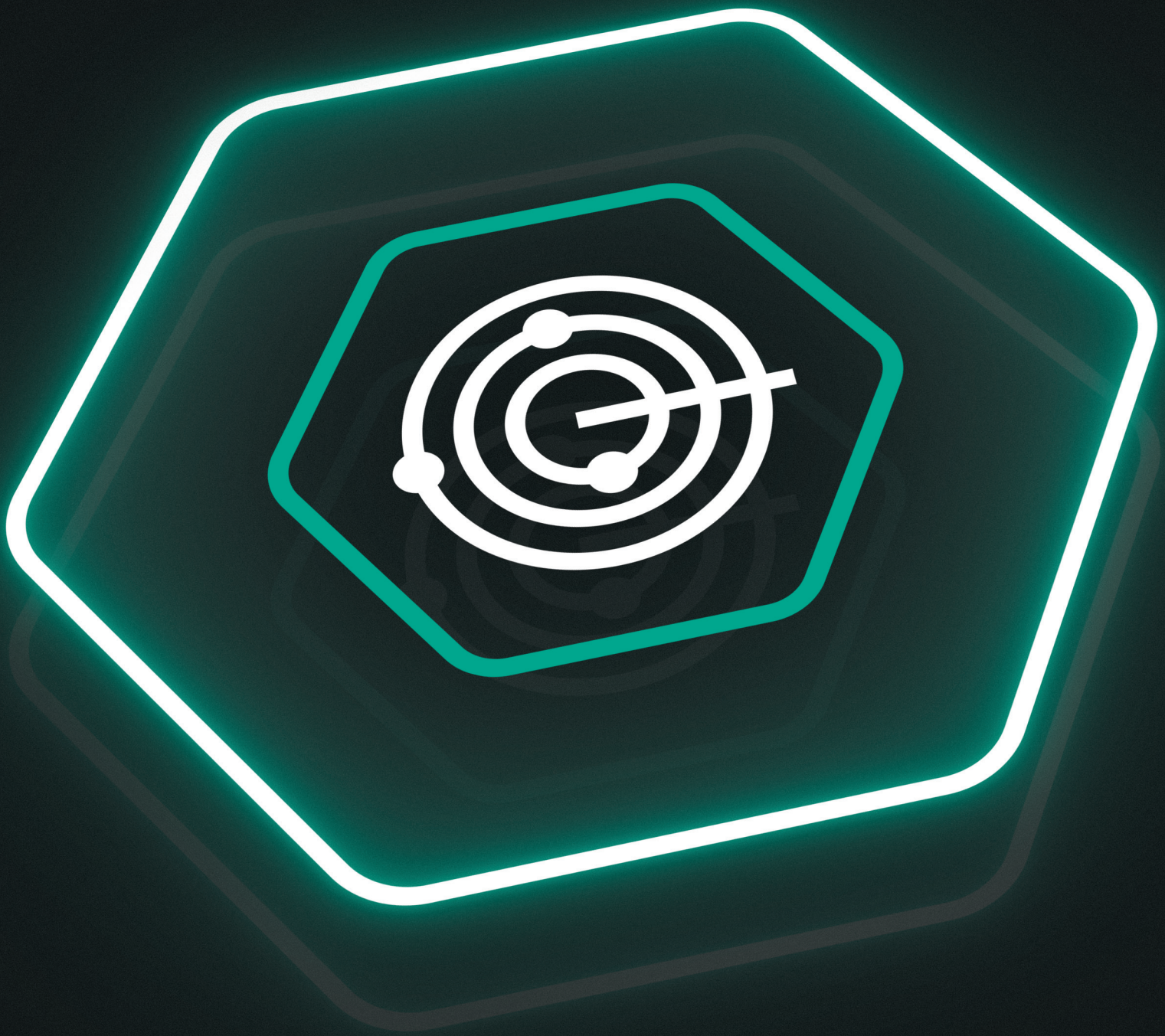


Kaspersky Anti Targeted Attack Platform

واجهوا المستقبل بأمان kaspersky

يتخصص مجرمو الإنترنت اليوم في تصميم أساليب فريدة ومبتكرة للاختراق وتهديد الأمن. مع استمرار تطور التهديدات وأصبحت أكثر تعقيدًا وتدميرًا، أصبح الاكتشاف السريع والاستجابة الأسرع والأنسب أمرًا بالغ الأهمية.

ومن الأهمية بمكان أن تستمر الشركات في إعادة التفكير في دفاعات أمن تكنولوجيا المعلومات الخاصة بها،

حتى يتسنى استباق ارتفاع معدلات التهديدات الإلكترونية، والحد من أي خسائر مالية يتم تكبدها.

حل موحّد من الأمن الإلكتروني لا نظير له

يفضل مجرمو الإنترنت المحترفون هذه الأيام اتباع نهج متعدد الأساليب. تجمع منصة **Kaspersky Anti Targeted Attack Platform** بين إمكانات اكتشاف التهديدات المتقدمة على مستوى الشبكة وإمكانات **EDR**، مع منح متخصصي أمن تكنولوجيا المعلومات جميع الأدوات التي يحتاجون إليها للتعامل مع الاكتشاف الفائق متعدد الأبعاد للتهديدات، وتطبيق التقنيات المتطورة والرائدة، وإجراء التحقيقات الفعالة، والبحث عن التهديدات بشكل استباقي وتقديم استجابة مركزية سريعة — وكل ذلك من خلال حل واحد.

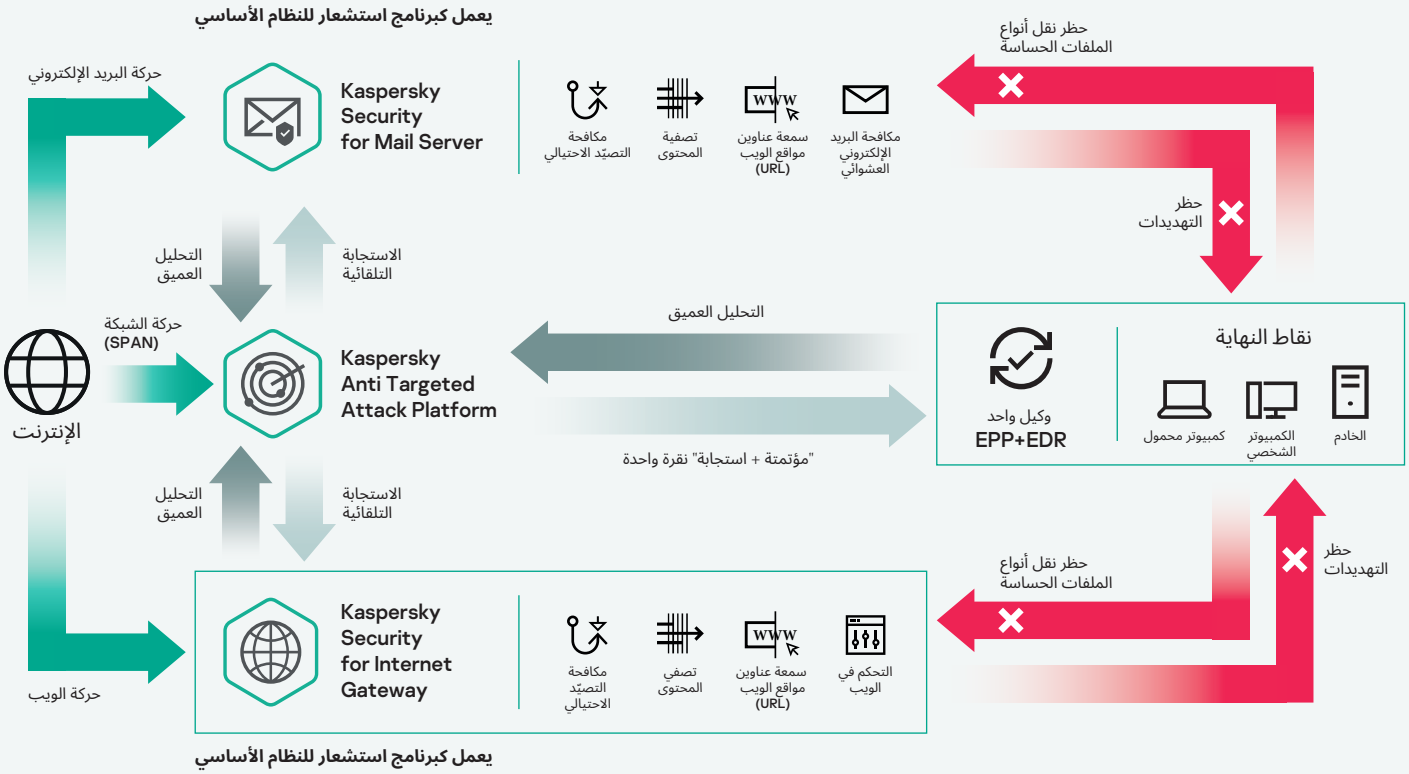
الهجمات الأكثر تعقيدًا تحت تركيزك ومراقبتك

تعمل المنصة (**Platform**) كحل متكامل لاكتشاف التهديدات والاستجابة لها بسرعة ودقة وتوفر حماية شاملة من التهديدات المستمرة المتقدمة والتي تتمتع بدعم معلومات التهديدات ومخططة لإطار **MITER ATT & CK**. جميع نقاط دخول التهديدات المحتملة – الشبكة والويب والبريد وأجهزة الكمبيوتر وأجهزة الكمبيوتر المحمولة والخوادم والأجهزة الافتراضية - تحت سيطرتك.

تم دمج نظام **Kaspersky Anti Targeted Attack Platform** بالكامل مع **Kaspersky Endpoint Security لقطاع الأعمال**، حيث يشارك وكيل واحد مع **Kaspersky EDR**. كما أنه يتكامل مع كل من **Kaspersky Security for Mail Server** و**Kaspersky Security for Internet Gateway**، اللذين يخدمان مستشعرات للنظام الأساسي، مما يوفر استجابة مؤتمتة للبريد الإلكتروني الأكثر تعقيدًا والتهديدات المنتقلة عبر الويب.

Kaspersky Anti Targeted Attack Platform:

- **يقلل** الوقت المستغرق للتعرف على التهديدات والاستجابة لها
- **يبسط** تحليل التهديدات والاستجابة للحوادث
- **يساعد** في القضاء على الثغرات الأمنية وتقليل "وقت الاستقرار" للهجوم
- **أتمتة** المهام اليدوية أثناء اكتشاف التهديدات والاستجابة لها
- **إتاحة** الوقت للعاملين في أمن تكنولوجيا المعلومات للقيام بمهام أخرى ذات أهمية بالغة
- **يدعم** الامتثال التنظيمي الكامل



حل أمن موثوق به يوفر خصوصية كاملة

يتم إجراء جميع تحليلات العناصر في الموقع، بدون تدفق بيانات صادرة، وتوفر Kaspersky Private Security Network تحديثات السمعة الواردة والفورية مع الحفاظ على العزل التام لبيانات الشركة.

نظام أساسي موحدة لتسريع الابتكار في التحول الرقمي من خلال:

- **استمرارية الأعمال التجارية المتكاملة.** نبني الأمن والامتثال في عمليات جديدة منذ البداية
- **رؤية كاملة** للبنية التحتية لتكنولوجيا المعلومات لشركتك
- **أقصى قدر من المرونة** يتيح النشر عبر كل من البيئة الفعلية والبيئة الافتراضية، إذا دعت الحاجة إلى الرؤية والتحكم
- **أتمتة مهام اكتشاف التهديدات والاستجابة لها**، وتحسين الفعالية من حيث التكلفة للأمان والاستجابة للحوادث وفِرق مركز عمليات الأمن
- **تكامل وثيق ومباشر** مع منتجات الأمان الحالية، وتعزيز مستويات الأمان الشاملة وحماية الاستثمار الأمني القديم

الميزات الرئيسية:

بنية برامج استشعار متعددة الطبقات – يتم تحقيق الرؤية الشاملة من خلال مجموعة برامج استشعارات الشبكة والويب والبريد الإلكتروني ووكلاء نقطة النهاية.

محركات اكتشاف التهديدات الشاملة – العمل مع البيانات من برامج استشعارات الشبكة (تحليل حركة مرور الشبكة) ووكلاء نقطة النهاية (إمكانيات EDR) للحصول على تقارير بيانات سريعة وعدد قليل من النتائج الإيجابية الزائفة.

آلية تحديد الوصول المتقدمة – توفر بيئة آمنة للتحليل العميق لنشاط التهديدات، وتقدم الدعم اللازم للتوزيع العشوائي لمكونات نظام التشغيل، وتسريع الوقت في الأجهزة الافتراضية، وتقنيات مكافحة التهرب، ومحاكاة نشاط المستخدم وتحديد النتائج إلى قاعدة معارف MITER ATT & CK - وكل ذلك يساهم في الكشف القائم على السلوك بكفاءة عالية.

التحليل الاستعادي- حتى في المواقف التي يتعذر فيها الوصول إلى نقاط النهاية المخترقة أو عندما يتم تشفير البيانات - من خلال البيانات المؤتمتة، وجمع العناصر وتقارير البيانات، والتخزين المركزي.

ثمة طريقتان لتفاعل معلومات التهديدات - مقارنة مؤتمتة ببيانات السمعة العالمية من Kaspersky Security Network والاستعلامات اليدوية للبحث عن التهديدات والتحقيق فيها من خلال بوابة Kaspersky Threat Intelligence Portal.

تقصي أثر التهديدات التلقائي في الوقت الفعلي – ترتبط الأحداث بمجموعة فريدة من مؤشرات الهجوم (IoAs) التي يستحدثها خبراء اكتشاف التهديدات لدى Kaspersky ويتم تحديدها إلى مصفوفة MITER ATT & CK، مما يوفر وصفًا واضحًا للأحداث وأمثلة وتوصيات للاستجابة.

تقصي أثر التهديدات الاستباقي باستخدام منشئ استعلام مرن وقوي – يمكن للمحللين إنشاء استعلامات معقدة للبحث عن السلوك غير النمطي والأنشطة المشبوهة والتهديدات الخاصة بالبنية التحتية لديك.

الخلاصة

الحماية الموثوقة للبيانات وأمن البنية الأساسية لتكنولوجيا المعلومات واستقرار عمليات الشركة والامتثال بقواعد السلامة تمثل المتطلبات الأساسية لتطوير الشركات اليوم بشكل مستدام.

تساعدك Kaspersky Anti Targeted Attack Platform بصفتك شركة متطورة في مجال أمن تكنولوجيا المعلومات على توفير وسائل دفاعية موثوقة لحماية البنية الأساسية لشركتك من التهديدات الشبيهة بالتهديدات المستمرة المتقدمة (APT) والهجمات المستهدفة، كما تدعم الامتثال التنظيمي دون الحاجة إلى أي موارد إضافية لأمن تكنولوجيا المعلومات. بها يتم تحديد الحوادث المعقدة والتحقيق فيها والاستجابة لها بسرعة، مما يرفع من كفاءة فريق أمن تكنولوجيا المعلومات أو فريق مراكز عمليات الأمن في شركتك وتخفيف العبء عنه عبر إعفائه من المهام اليدوية بفضل حل موحّد يعمل على زيادة الأتمتة ورفع مستوى جودة النتائج إلى أقصى حد.

اتضح أنه الحل الأكثر فعالية في القطاع الصناعي

أجرت SE Labs اختبارًا على نظام Kaspersky Anti Targeted Attack Platform ضد مجموعة من هجمات الاختراق، **ومنحتنا تصنيف AAA**.

في ICSA Labs' المستقلة: اختبار الدفاع ضد التهديدات المتقدمة (الربع الثالث من عام 2019)، قدم نظام Kaspersky Anti Targeted Attack Platform **معدلات اكتشاف بنسبة 100%، مع عدم وجود أي نتائج إيجابية زائفة**.

THE RADICATI GROUP, INC.

A TECHNOLOGY MARKET RESEARCH FIRM

تعترف Radicati Group بشركة Kaspersky بوصفها **تقوم بأفضل دور في الحماية من التهديدات المستعصية المستمرة (APT) - Market Quadrant 2020**.

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

وبصفتها واحدًا من 6 موردين في جميع أنحاء العالم والتي تم الاعتراف بها باعتبارها Gartner Peer Insights Customers' Choice لحلول EDR في عام 2020 - ثناء العميل النهائي لحل EDR الموسع - Kaspersky Anti Targeted Attack Platform مع Kaspersky EDR في جوهرها.

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

لقد شارك العنصر الأساسي في Kaspersky Anti Targeted Attack Platform - Kaspersky EDR - جولة التقييم الثانية لتهديد APT29 من MITRE، مما أظهر مستويات عالية من الأداء في اكتشاف تقنيات ATT & CK الرئيسية المطبقة في المراحل الحاسمة من الهجمات المستهدفة اليوم.

انقر فوق الرمز ربع وقوم بزيارة: kaspersky.com/MITRE

لمعرفة المزيد حول Kaspersky Anti Targeted Attack Platform، تفضل بزيارة:

kaspersky.com/enterprise-security/anti-targeted-attack-platform

Proven. Transparent. Independent.

نحن مُجرّبون. نحن مستقلون. نحن واضحون. نلتزم ببناء عالم آمن حيث نستفيد من التكنولوجيا في تحسين حياتنا. لهذا السبب، نعمل على توفير الأمان له لكي يتمتع كل فرد في كل مكان بالفرص اللا نهائية التي يوفرها. ارتقِ بمستوى الأمن الإلكتروني لديك لمستقبل أكثر أماناً.

اعرف المزيد عبر موقعنا الإلكتروني:
kaspersky.com/transparency

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