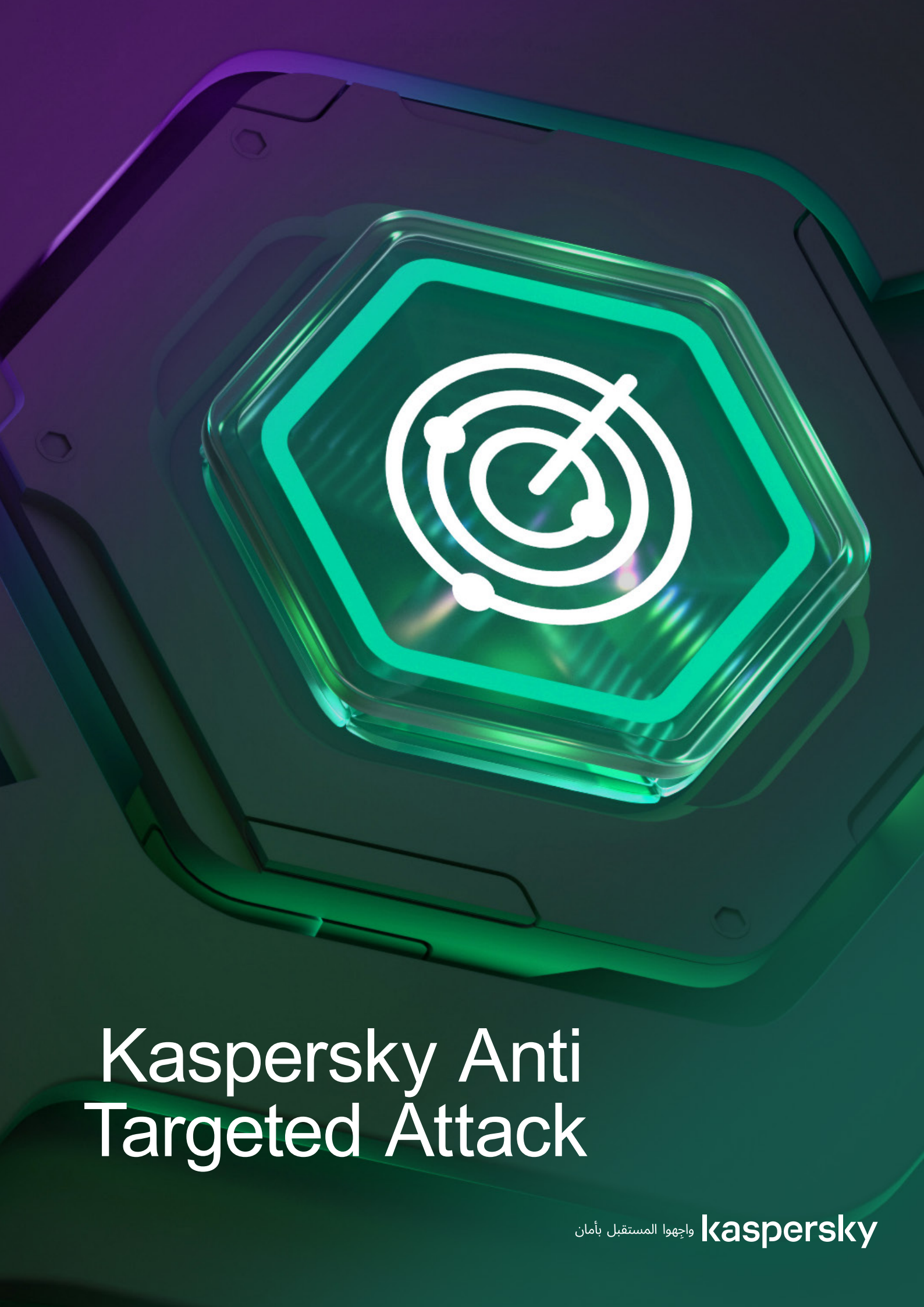


Kaspersky Anti Targeted Attack

واجِهوا المستقبل بأمان kaspersky

أمن إلكتروني لا يضاهى: مواكبة التهديدات المستمرة المتقدمة والتهديدات المتطورة

يتخصص مجرمو الإنترنت اليوم في تصميم أساليب فريدة ومبتكرة للاختراق وتهديد الأمان. ومع استمرار تطور التهديدات لتصبح أكثر تعقيداً وتدميراً، أصبح الاكتشاف السريع والاستجابة الأسرع والأنسب أمرًا بالغ الأهمية.

Kaspersky Anti Targeted Attack

يقلل الوقت المستغرق للتعرف على التهديدات والاستجابة لها

يُبسط تحليل التهديدات والاستجابة للحوادث

يساعد في القضاء على الثغرات الأمنية وتقليل "مدة بقاء" الهجوم

يؤتمت المهام اليدوية أثناء اكتشاف التهديدات والاستجابة لها

يتيح الوقت للعاملين في أمان تكنولوجيا المعلومات لأداء المهام الأخرى بالغة الأهمية

يدعم الامتثال التنظيمي

يساعدك حل Kaspersky Anti Targeted Attack (KATA) على بناء وسائل دفاعية موثوقة لحماية البنية التحتية لشركتك من التهديدات الشبيهة بالتهديدات المستمرة المتقدمة (APT) والهجمات الموجّهة ويدعم الامتثال التنظيمي دون الحاجة إلى أي موارد إضافية لأمان تكنولوجيا المعلومات. ويتم تحديد الحوادث المعقدة والتحقيق فيها والاستجابة لها بسرعة، مما يرفع من كفاءة فريق أمان تكنولوجيا المعلومات أو فريق مراكز عمليات الأمن في شركتك وتخفيف العبء عنه عبر إعفائه من المهام اليدوية بفضل حل موحّد يعمل على زيادة التشغيل التلقائي ورفع مستوى جودة النتائج إلى أقصى حد.

يوفر Kaspersky Anti Targeted Attack حماية شاملة لمكافحة التهديدات المستمرة المتقدمة والحماية من التهديدات الإلكترونية الأكثر تطوراً. ويمكنك الاختيار من بين وظائف اكتشاف الشبكة والاستجابة لها (NDR) ذات المستوى الأساسي أو المتقدم، ودمجها مع حل اكتشاف نقطة النهاية والاستجابة لها (EDR) وحتى سيناريوهات الاكتشاف والاستجابة الموسعة (XDR) الأصلية. والآن، أصبح لدى خبراء أمان تكنولوجيا المعلومات لديك جميع الأدوات التي يحتاجونها لتنفيذ عمليات الاكتشاف الفائقة للتهديدات متعددة الأبعاد، وتطبيق التقنيات الرائدة، وإجراء تحقيقات فعالة، واكتشاف التهديدات بشكل استباقي، وتقديم استجابة سريعة ومركزية.

خيارات مرنة

3 مستويات من الحماية ضد التهديدات المستمرة المتقدمة

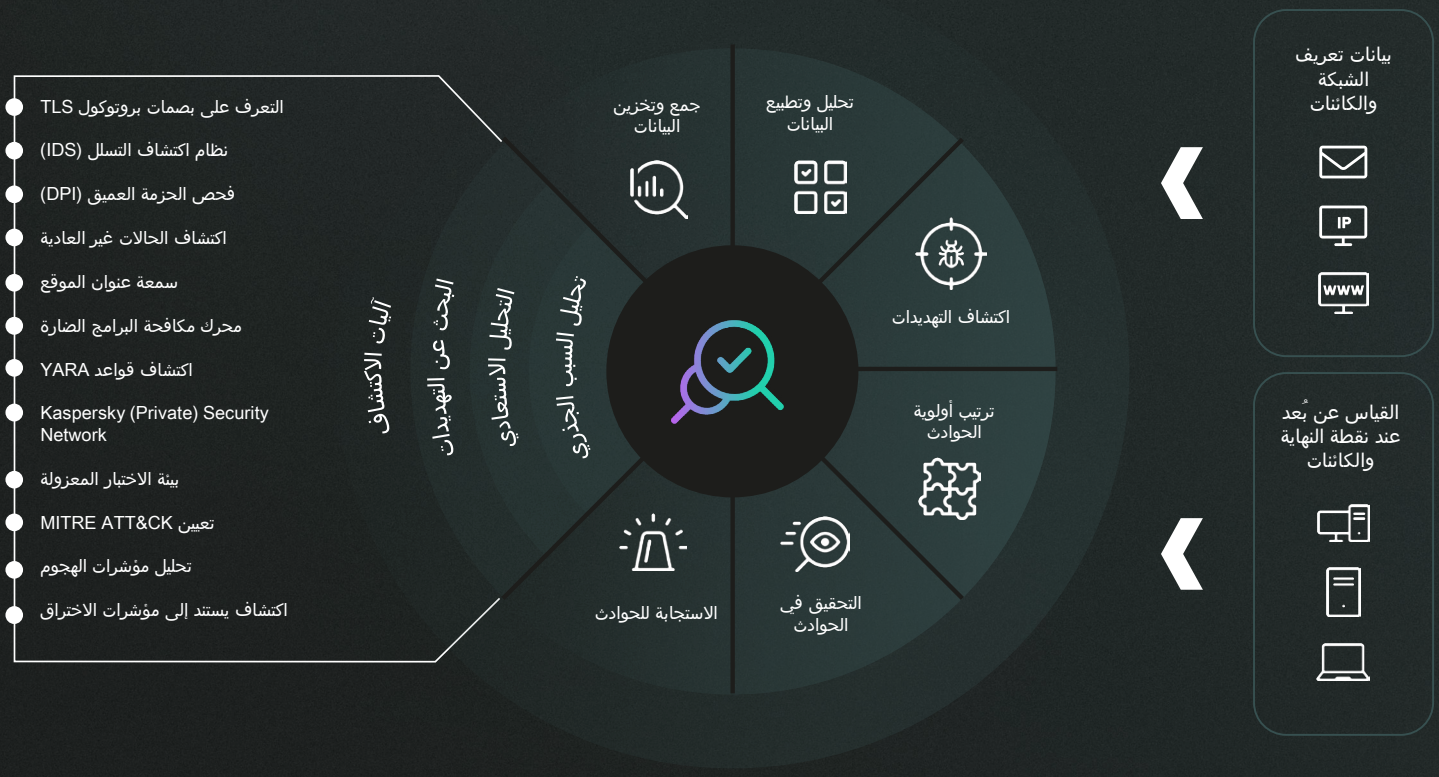
KATA ← KATA NDR Enhanced ← KATA Ultra

مقارنة

	KATA	KATA NDR Enhanced	KATA Ultra
وظائف اكتشاف الشبكة والاستجابة لها (NDR) الأساسية • مراقبة حركة شبكة الاتصال ومحركات الاكتشاف المتقدمة • التعرف على بصمات بروتوكول TLS • بروتوكول PCAP المتعلق بتنبيهات نظام اكتشاف التسلل (IDS) • تحليل سمعة عنوان الموقع • اكتشاف التسلل على أساس قواعد نظام اكتشاف التسلل (IDS) (الحركة بين الشبكة الداخلية والإنترنت) • الاستجابة الموجهة بواسطة الشبكة • الاستجابة التلقائية على مستوى البوابة وتكامل بروتوكول التكيف مع محتوى الإنترنت (ICAP) مع وضع الحظر	•	•	•
بيئة الاختبار المعزولة المتقدمة	•	•	•
الإثراء بالمعلومات عن طريق Kaspersky Threat Intelligence و MITRE ATT&CK	•	•	•
وظائف اكتشاف الشبكة والاستجابة لها (NDR) المحسّنة • فحص الحزمة العميق (DPI) لتحديد البروتوكول • اكتشاف التسلل على أساس قواعد نظام اكتشاف التسلل (IDS) (الحركة الداخلية بين الخوادم) • جدول جلسات الشبكة وتخطيط الشبكة ووحدة إدارة الأصول للحصول على رؤية كاملة للشبكة • تحليل القياس عن بُعد للشبكة ومراقبة نقطة النهاية (Windows وEPP Linux) • الحماية من مخاطر أمان الشبكة (الأجهزة غير المصرح بها وانتحال بروتوكول تحليل العنوان (ARP)، وما إلى ذلك) • تخزين حركة المرور الأصلية (التقاط الحزمة) والتحليل الاستعادي • الاستجابة التلقائية على أجهزة الشبكة عبر موصل واجهة برمجة التطبيقات (API) • اكتشاف الحالات غير العادية • اكتشاف تكنولوجيا المعلومات الخفية	•		•
قدرات Expert EDR	•		
وظائف Native XDR	•		

مستوى جديد من الأمان

يوفر Kaspersky Anti Targeted Attack حلاً متكاملاً للحماية من التهديدات المستمرة المتقدمة مدعومًا بمعلومات التهديدات والربط بإطار عمل MITRE ATT&CK. وتكون جميع نقاط دخول التهديدات المحتملة – الشبكة والويب والبريد وأجهزة الكمبيوتر وأجهزة الكمبيوتر المحمولة والخوادم والأجهزة الافتراضية - تحت سيطرتك.



تحليل حركة مرور الشبكة | مراقبة نشاط نقطة النهاية | مستودع مركزي للبيانات الأولية والنتائج النهائية | معلومات التهديدات العالمية | مجموعة أنشطة الاستجابة

التشغيل التلقائي لمهام اكتشاف التهديدات والاستجابة لها

تحسين كفاءة الإنفاق لفرق الأمان والاستجابة للحوادث ومركز عمليات الأمن

تكامل وثيق ومباشر

مع منتجات الأمان الحالية، وتعزيز مستويات الأمان الشاملة وحماية الاستثمار الأمني القديم

الرؤية الكاملة

رؤية كاملة للبنية التحتية لتكنولوجيا المعلومات في شركتك

أقصى قدر من المرونة

يتيح النشر عبر كل من البيئة الفعلية والبيئة الافتراضية، إذا دعت الحاجة إلى الرؤية والتحكم

إثراء تنبيهاتك باستخدام Kaspersky Threat Intelligence

استخدم معلومات شاملة جُمعت من أكثر من 100 مليون جهاز استشعار، ومستودعات ضخمة من الملفات الخبيثة والسليمة، وشبكة الويب المظلم، بالإضافة إلى أنشطة رصد التهديدات والاستجابة للحوادث المستمرة.

يمكنك الوصول إلى Threat Intelligence Portal مباشرةً من تنبيه نظام KATA: تحليل الملفات المشبوهة، والتحقق من الارتباطات بالبيانات الأخرى القابلة للرصد، وإضافة سياق عملي للتنفيذ.

لماذا Kaspersky

- انتشار عالمي وتقدير دولي
- كفاءة تقنية مؤكدة
- الشفافية والامتثال
- تجربة وخبرة عالمية المستوى
- تتمتع بشهرة كبيرة في مجال أمان تكنولوجيا المعلومات
- سجل حافل على مدار 28 عامًا من حماية العملاء لا مثيل له

Kaspersky Anti Targeted Attack

معرفة المزيد

#kaspersky
#bringonthefuture

me.kaspersky.com