Kaspersky Anti Targeted Attack Platform

این روزها، تبهکاران سایبری، سازوکارهای منحصربه‌فرد و خلاقانه‌ای را در نفوذ به سیستم‌ها و هک سازمان‌ها به کار می‌گیرند. همان‌طور که تهدیدات تکامل پیدا می‌کنند و روزبه‌روز پیچیده‌تر و مخرب‌تر می‌شوند، شناسایی سریع و اعمال واکنشی مؤثر، نقشی پررنگ پیدا می‌کند.

برای مقابله با تهدیدات فوق‌پیچیده امروزی، نیاز به تکامل رویکردهای دفاعی است تا بلکه از این طریق، خسارات ناشی از حملات احتمالی به حداقل برسد.

Kaspersky Anti Targeted Attack Platform:

- **کاهش** زمان موردنیاز برای شناسایی تهدیدات نوظهور و واکنش به آنها
- **تسهیل** تحلیل تهدیدات و واکنش به رخدادها
- **کمک** به حذف شکاف‌های امنیتی و کاهش مدت زمان بازیابی در نتیجه حمله
- **خودکارسازی** فرامین دستی در جریان تحلیل تهدید و واکنش به آنها
- **آزاد شدن** وقت کارکنان فناوری اطلاعات و در نتیجه تمرکز هر چه بیشتر آنها بر روی سایر امور کلیدی و بحرانی
- **پشتیبانی** کامل از الزامات و استانداردهای مطرح امنیتی

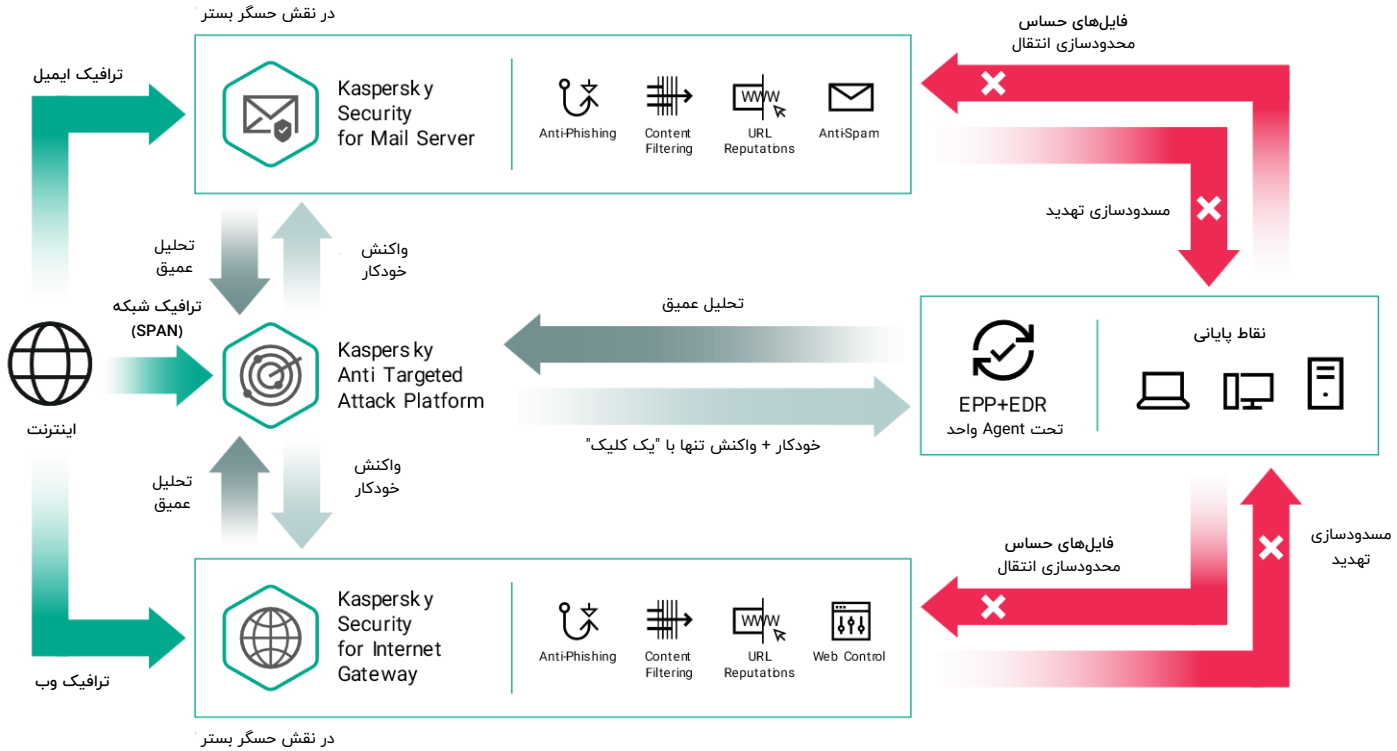
امنیت سایبری بی‌نظیر در راهکاری یکپارچه

در چند سال اخیر، مهاجمان حرفه‌ای، در جریان حملات هدفمند خود از تاکتیک‌ها و تکنیک‌های مختلفی برای پنهان ماندن از دید محصولات امنیت فناوری اطلاعات بهره گرفته‌اند.

Kaspersky Anti Targeted Attack Platform، فناوری‌های پیشرفته شناسایی تهدیدات در سطح شبکه را با قابلیت‌های EDR ترکیب می‌کند. همزمان، تمامی ابزارها و فناوری‌های موردنیاز برای کشف و شکار پیشگیرانه تهدیدات چندشکلی پیچیده، انجام تحقیقات مؤثر و واکنش سریع و متمرکز به آنها را فراهم می‌کند. همه این فناوری‌ها و قابلیت‌ها در راهکاری واحد در اختیار سازمان قرار می‌گیرد.

پیچیده‌ترین حملات تحت کنترل و تمرکز شما

این محصول، با رویکرد Extended Detection and Response، راهکاری مؤثر در محافظت در برابر تهدیدات ماندگار پیشرفته (APT) است. تمامی درگاه‌های بالقوه ورود تهدیدات – شبکه، وب، ایمیل، کامپیوترها، لپ‌تاپ‌ها، سرورها و ماشین‌های مجازی – همگی تحت رصد و کنترل خواهند بود. کاملاً با Kaspersky Endpoint Security for Business یکپارچه بوده و از یک Agent مشترک با Kaspersky EDR Expert استفاده می‌کند. همچنین قادر است از دو محصول امنیتی Kaspersky Security for Mail Server و Kaspersky Security for Internet Gateway به‌عنوان حسگرهای بستر بهره گرفته و واکنش‌های خودکاری را برای با مقابله با تهدیدات پیچیده ایمیلی و مبتنی بر وب اعمال کند.



یک راهکار امنیتی قابل اعتماد
با قابلیت جداسازی از اینترنت
انجام تمامی تجزیه‌وتحلیل‌ها در محل سازمان،
استعلام شهرت فایل‌ها و پروسه‌ها،
بدون جریان داده خروجی، با بهره‌گیری از
Kaspersky Private Security Network

یک راهکار متمرکز امنیتی برای تسریع نوآوری در تحول دیجیتال با فراهم نمودن:

- **تداوم یکپارچگی کسب‌وکار.** مهیا شدن امنیت و انطباق با الزامات امنیتی از پایه.
- **دید کامل** بر زیرساخت فناوری اطلاعات سازمان.
- **بالاترین انعطاف‌پذیری** به‌منظور فراهم نمودن امکان استقرار در محیط‌های فیزیکی و مجازی و به طور کلی هر کجا که نیاز به رصد و کنترل باشد.
- **خودکارسازی کشف تهدیدات و پاسخ به آنها،** بهینه‌سازی و صرفه‌جویی در منابع امنیتی و منابع انسانی فعال در حوزه امنیت سازمان.
- **ادغام دقیق با محصولات امنیتی موجود،** افزایش سطوح امنیتی و حفظ سرمایه‌گذاری‌های پیشین در خرید محصولات امنیتی.

قابلیت‌های اصلی

معماری حسگر چندلایه‌ای – فراهم شدن دیدی همه‌جانبه در نتیجه ترکیب و ادغام کنترل‌ها و حسگرهای تحت شبکه، وب و ایمیل و همچنین عوامل نقطه پایانی.

پویشگرهای گسترده کشف تهدید – بررسی داده‌های حسگرهای شبکه (تجزیه‌وتحلیل ترافیک شبکه) و عوامل نقطه پایانی (قابلیت‌های EDR) برای شناسایی سریع‌تر تهدیدات بالقوه و کاهش شناسایی‌های نادرست (False Positive).

سندباکس پیشرفته – یک محیط امن و قرنطینه‌شده برای تجزیه‌وتحلیل عمیق فعالیت فایل‌های مشکوک، مجهز به قابلیت‌های تشخیص تکنیک‌های ضدگریز، شبیه‌سازی فعالیت کاربر و نگاشت رخدادها بر طبق چارچوب MITER ATT&CK.

تجزیه‌وتحلیل گذشته‌نگر – حتی پس از آلوده شدن نقطه پایانی، غیرقابل‌دسترس شدن آن و یا بعد از رمزگذاری داده‌ها – در نتیجه استخراج خودکار داده‌ها و رخدادها و ذخیره‌سازی متمرکز آنها.

دو روش برای تعامل با اطلاعات تهدید – استعلام خودکار پیشینه جهانی فایل‌ها از Kaspersky Security Network و فراهم بودن امکان جستجوی دستی اطلاعات/نشانه‌های تهدید در سامانه Kaspersky Threat Intelligence Portal.

شکار خودکار و بلادرنگ تهدید – تطابق دادن رویدادها با مجموعه منحصربه‌فردی از شاخص‌های حمله (IoA) – ایجادشده توسط شکارچیان تهدید کسپرسکی – و ماتریس MITER ATT&CK، همراه با ارائه توصیف‌ها، مثال‌ها و توصیه‌های امنیتی.

کشف تهدید با ابزار گزارش‌گیری انعطاف‌پذیر و قدرتمند کسپرسکی – امکان انجام پرس‌وجوهای پیچیده برای جستجوی رفتارهای غیرمعمول، فعالیت‌های مشکوک و تهدیدهای خاص و هدفمند زیرساخت شما.

به‌طور خلاصه

حفاظت جامع از داده‌ها، امنیت زیرساخت فناوری اطلاعات، ثبات برای فرآیندهای تجاری و انطباق با الزامات بالادستی، پیش‌نیازهای توسعه پایدار هر شرکت امروزی است.

Kaspersky Anti Targeted Attack Platform شما را قادر می‌سازد تا به‌عنوان یک سازمان تکامل‌یافته در حوزه امنیت فناوری اطلاعات، یک سازوکار دفاعی مؤثر و پیشرفته داشته باشید. به‌نحوی که ضمن انطباق با الزامات و استانداردهای مطرح امنیتی، از زیرساخت‌های شما در برابر تهدیدات پیچیده APT و حملات هدفمند، بدون آن که نیاز به منابع امنیتی بیشتری داشته باشید محافظت می‌کند.

به لطف راهکاری متمرکز که استفاده از خودکارسازی و کیفیت استخراج و تحلیل رخدادها را به حداکثر می‌رساند، حملات فوق‌پیچیده هدفمند به سرعت شناسایی و بررسی شده و نسبت به آنها واکنش مؤثر نشان داده می‌شود. با Kaspersky Anti Targeted Attack Platform، کارایی واحد امنیت فناوری اطلاعات و تیم SOC سازمان، به سبب رهایی از وظایف دستی و هشدارهای بی‌اهمیت و کاذب، افزایش می‌یابد.

اطلاعات و جزییات بیشتر در:
shabakeh.net/products/kaspersky

شبکه گستر
امنیت شما | وظیفه ما

شرکت مهندسی شبکه گستر
نماینده رسمی فروش محصولات
شرکت کسپرسکی در ایران

تهران ۱۹۶۸۶ بلوار نلسون ماندلا
خیابان وحید دستگردی (ظفر)
شماره ۲۷۳ طبقه اول شرقی

تلفن / دورنگار: ۴۲۰۵۲ – ۰۲۱
رایانامه: info@shabakeh.net
تارنما: www.shabakeh.net