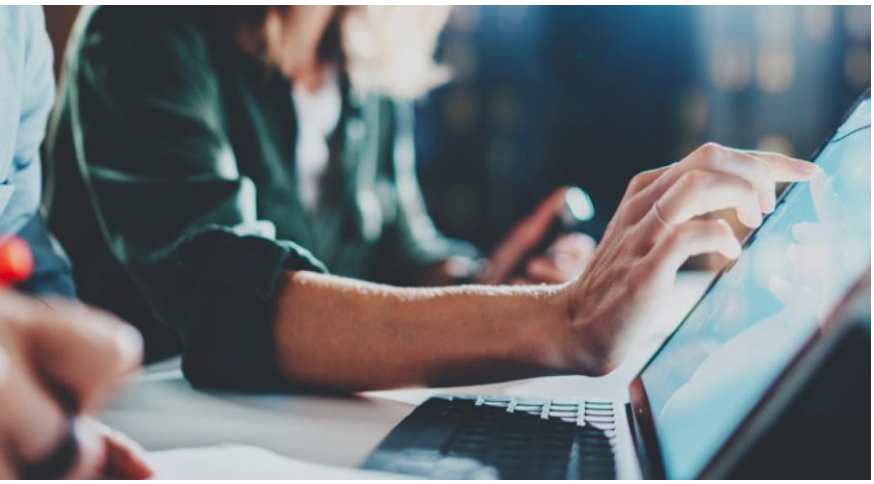
Trellix



Trellix Endpoint Protection Advanced

حفاظت پیشرفته در برابر حملات پیچیده امروزی

برای مقابله با تهدیداتی که سازمان شما با آن مواجه است، نیاز به راهکاری است که قادر به کنترل کامل چرخه دفاعی باشد. این به‌معنای مسلح نمودن متخصصان سازمان به قابلیت‌هایی است که با دقت بالاتر و تشخیص قوی‌تر، تهدیدات پیشرفته را شناسایی می‌کنند. راهکار دفاعی پیشرفته Trellix Endpoint Protection Advanced با بررسی و محدودسازی پروسه‌های مشکوک، با تهدیدات پیچیده و حملات تاکنون ناشناخته (Zero-day) مقابله می‌کند. در این راهکار، نرم‌افزار Trellix Endpoint Security با فناوری یکپارچه "یادگیری ماشین" و "محدودسازی پویای پروسه‌های مشکوک"، تهدیدات تاکنون ناشناخته را تقریباً بطور آنی شناسایی کرده و آنها را قبل از آلوده نمودن دستگاه‌های سازمان، دسته‌بندی و متوقف می‌کند. داده‌ها و گزارش‌های متعدد، شما را از رخدادها آگاه کرده و امکان تجسس و واکنش به رویدادها را تا مرحله مستحکم نمودن سیستم‌های دفاعی، فراهم می‌کند. با توجه به ساختار انعطاف‌پذیر راهکار، همراه با تغییر نیازهای سازمان، در هر زمان می‌توان به‌سادگی سیستم دفاعی جدیدی را به آن اضافه کرد.

دفاع خودکار و پیشرفته در برابر تهدیدات

تهدیدات پیشرفته را باید در همان مراحل ابتدایی اجرای حمله متوقف کرد. به همین دلیل Trellix Endpoint Protection Advanced شامل فناوری‌های Dynamic App Containment و Real Protect است. فناوری Dynamic App Containment با شناسایی رفتارهای مخرب برنامه‌های ناخواسته و پروسه‌های مشکوک، تهدیدات تاکنون ناشناخته را مهار و محدود ساخته و از آلوده شدن سیستم‌ها یا تأثیر بر روی کاربران جلوگیری می‌شود. Real Protect بر اساس فناوری یادگیری ماشین، تهدیدات را بررسی و دسته‌بندی کرده و یافته‌ها را برای اقدامات بعدی که می‌توانند به‌صورت خودکار انجام شوند، ضبط و نگهداری می‌کند.

ساخته شده برای کاهش پیچیدگی

پیچیدگی، دشمن اثربخشی است. در دنیای امروز فرصتی برای مدیریت چندین راهکار با رابط‌های کاربری و کنسول‌های متفاوت نیست. Trellix Endpoint Protection Advanced تنها با یک کنسول به نام Trellix ePolicy Orchestrator – به اختصار Trellix ePO – مدیریت می‌شود. با این کنسول قدرتمند قادر خواهید بود به سرعت بستر لازم را آماده کرده، توزیع نرم‌افزارها را سرعت بخشیده و دشواری‌ها و دغدغه‌های مدیریتی را کاهش دهید.

مزایای کلیدی

- متوقف ساختن تهدیدات تاکنون ناشناخته، باج‌افزارها و برنامه‌های بالقوه ناخواسته با بهره‌گیری از فناوری‌های یادگیری ماشین و محدودسازی پروسه‌های مشکوک
- سرعت بخشیدن به فرایند پاکسازی و حفظ بهره‌وری با تحلیل و واکنش خودکار
- حفاظت از سرویس Exchange با بررسی محتوا و پیشینه ایمیل و همچنین ایمن نگه داشتن صندوق پستی کاربران
- حفاظت از بستر SharePoint و یکپارچگی با این نرم‌افزار با هدف جلوگیری از تبدیل آن به مرکزی برای انتشار بدافزار و محتوای نامناسب
- مدیریت تمامی راه‌ها و امکانات ورودی و خروجی از جمله ابزارهای ذخیره‌سازی متصل به دستگاه

پویا، یکپارچه و متمرکز

Trellix Endpoint Protection Advanced بستری یکپارچه و پیوسته است که از چندین فناوری حفاظتی تشکیل شده است.

بخش ضدبدافزار نه تنها تحلیل کامل تهدیدات بدافزاری را فراهم می‌سازد بلکه در نتیجه یکپارچه شدن آن با سایر فناوری‌های امنیتی، به‌صورتی هوشمندتر با هر نوع تهدید نوظهور مقابله می‌کند.

با استفاده از یک لایه ارتباطی مشترک، سیستم حفاظتی نقاط پایانی می‌تواند از دیگر فناوری‌های امنیتی پیشرفته در خصوص پروسه‌های مشکوک که نخستین بار با آنها روبرو می‌شود، پرس‌وجو کرده تا آگاهی کامل‌تر و واکنش‌های صحیح‌تری را در برابر آنها نشان دهد.

کارآمد و بهینه

Trellix Endpoint Protection Advanced یک بستر مقیاس‌پذیر را به همراه فناوری‌های حفاظتی اساسی، بدون پیچیدگی و قربانی کردن کارایی، ارائه می‌کند که در نتیجه آن، بهره‌وری سازمان بهبود می‌یابد.

برای مثال، فعالیت سازمان در نتیجه مدیریت مرکزی از طریق Trellix ePO که تصویری کامل را از فرآیندهای توزیع و اعمال سیاست‌ها و همچنین وضعیت امنیتی دستگاه‌ها را در شبکه سازمان فراهم می‌کند، روان و آسان انجام می‌شود.

سازمان‌ها با چندین سیستم عامل نیز قادر خواهند بود تا بهره‌وری را از طریق سیاست‌های واحد برای سیستم‌های عامل Windows، Mac و Linux افزایش دهند.

با بهره‌گیری از راهکار Trellix Endpoint Protection Advanced انجام عملیات پویش با حداقل تأثیر بر روی حافظه، پردازشگر و منابع دیگر سیستم منجر به افزایش بهره‌وری سازمان می‌شود.

رابط آسان Trellix Endpoint Security بر روی دستگاه کاربران، آنها را قادر به رصد رویدادها و واکنش‌های صورت گرفته، می‌کند. Trellix Endpoint Protection Advanced مجهز به قابلیت‌های ضدتهدید، دیواره آتش، کنترل وب و کنترل بخش‌های سخت‌افزاری است.

در این راهکار محصولی نیز برای حفاظت از سرورهای ایمیل و صندوق‌های پست الکترونیک تحت Microsoft Exchange در برابر بدافزارها ارائه می‌شود.

امکانات موجود در راهکار

- Dynamic Application Containment: محدود کردن آلودگی با جلوگیری از اعمال تغییرات مخرب بر روی نقاط پایانی توسط هر پروسه مشکوک
- Real Protect: طبقه‌بندی رفتارها بر پایه "یادگیری ماشین" به‌منظور مسدود کردن تهدیدات تاکنون ناشناخته قبل از اجرا شدن
- Rollback Remediation: بازگردانی خودکار سیستم به حالت اولیه در نتیجه تغییرات اعمال‌شده توسط بدافزار و قرار دادن سیستم در وضعیت سلامت
- Threat Prevention: حفاظت جامع و چند لایه‌ای جهت شناسایی، مسدود و پاکسازی سریع بدافزار در بسترهای Windows، Mac و Linux
- Story Graph: به تصویر کشیدن جزییات رویداد در قالبی ساده
- Integrated Firewall: حفاظت از نقاط پایانی در برابر ارتباطات پرمخاطره
- Web Control: اطمینان از مرور امن وب با کنترل و پالایش سایت‌های فراخوان‌شده بر روی نقاط پایانی
- Security for Microsoft SharePoint: جلوگیری از به اشتراک گذاشته شدن فایل مخرب در نرم‌افزار SharePoint
- Security for Microsoft Exchange: جلوگیری از ورود ایمیل‌های دارای پیوست مخرب به سازمان
- Device Control: کنترل تجهیزات ورودی و خروجی دستگاه از جمله حافظه‌های ذخیره‌سازی
- ePolicy Orchestrator: ابزار مدیریتی جامع با مقیاس‌پذیری و انعطاف‌پذیری بالا و مدیریت خودکار تنظیمات امنیتی به‌منظور شناسایی و واکنش به مسائل امنیتی

شرکت مهندسی شبکه گستر
تهران بلوار نلسون ماندلا خیابان دستگردی (ظفر) شماره ۲۷۳
www.shabakeh.net info@shabakeh.net ۰۲۱ – ۴۲۰۵۲
شبکه گستر
امنیت شما | وظیفه ما