Trellix

Trellix Complete Endpoint Protection

بدافزارهای روز صفر و ناشناخته را کشف کرده، اولین آلودگی را محدود نموده و با تهدیدات پیچیده، پیشرفته و نوظهور به‌نحوی مؤثر مقابله کنید.

مقابله مؤثر با حملات و تهدیدات سایبری فوق‌پیشرفته که هر روز نیز بر توان آنها افزوده می‌شود مستلزم بکارگیری نسل جدیدی از راهکارهای حفاظت از نقاط پایانی است. در طی سال‌های اخیر، حرفه‌ای‌تر شدن بدافزارها و حملات سایبری از یک سو و افزایش خطرات آسیب‌پذیری‌های ناشناخته از سویی دیگر، بسیاری از سازمان‌ها را ناگزیر به استفاده از چندین راهکار غیرمتمرکز و حتی در برخی موارد ناهمگون کرده است. علاوه بر پیچیدگی فراوان، به دلیل یکپارچه نبودن این راهکارها، گزارش‌گیری و واکنش به‌موقع به رخدادهای امنیتی نیز در بسیاری موارد دشوار و غیرمؤثر است.

ترلیکس برای حل این دغدغه، راهکار Complete Endpoint Protection را ارائه کرده است. این راهکار علاوه بر مجهز بودن به محصولات و ابزارهای حفاظتی و مدیریتی قدرتمند، همزمان با انجام بررسی‌ها و انواع تحلیل‌ها و پردازش‌های ایستا و پویا، جهت تأمین حفاظت آنی، اطلاعات مربوط به تهدیدات را با تمامی نقاط پایانی و محصولات ثالث سازگار به اشتراک می‌گذارد.

دفاع در برابر هر کد مخرب

Trellix Complete Endpoint Protection با تحلیل‌های ایستا و پویا، بررسی پیشینه و پویش‌های رفتارشناسانه، بهره‌جوهای بالقوه را کشف کرده و سازمان را در برابر تهدیدات نوظهور ایمن می‌سازد. در این راهکار، با بهره‌گیری از Trellix Threat Intelligence Exchange، تهدیدات جدید مسدود شده و با به‌روز شدن آنی پیشینه و سابقه پروسه، از حملات آتی جلوگیری می‌شود. Complete Endpoint Protection با شناسایی شباهت‌های رفتار پروسه‌های جدید با پروسه‌های مخرب شناسایی‌شده، بکارگیری مدل‌های فناوری Real Protect و استفاده از فناوری‌های رایانش ابری ترلیکس بدافزارهای روز صفر (Zero-day) را خنثی می‌کند. در عمل، این روش طبقه‌بندی رفتاری منجر به شناسایی آن دسته از تهدیداتی می‌شود که به دلیل مکانیزم‌های پیشرفته استفاده‌شده در آنها از سد سایر نرم‌افزارهای دفاعی عبور می‌کنند. آمار جامع ارائه‌شده در کنسول مدیریتی بی‌نظیر Trellix ePolicy Orchestrator – به اختصار Trellix ePO –، کشف تهدیدات روز صفر و اجرای واکنش‌های به‌موقع را آسان می‌سازد. فناوری‌ها و روش‌های استفاده‌شده در راهکار Trellix Complete Endpoint Protection، ضمن فراهم نمودن بالاترین سطح حفاظت، عملاً با خنثی‌سازی حملات سایبری و بدافزارهای پیشرفته سبب افزایش کارایی کارکنان می‌شوند.

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
- Behavior Monitoring: رصد رفتار در سطح پروسه در حین تحلیل تکنیک‌ها و روال‌های حمله و اولویت‌بندی هشدارها با بازپخش رویدادها
- Rollback Remediation: بازگردانی خودکار سیستم به حالت اولیه در نتیجه تغییرات اعمال‌شده توسط بدافزار و قرار دادن سیستم در وضعیت سلامت
- Threat Intelligence Exchange: تبادل اطلاعات درباره تهدیدات و فراهم نمودن دیدی گسترده و کنترلی جامع
- Data Exchange Layer: گسترش امنیت با برقراری ارتباط میان محصولات ترلیکس و محصولات شرکت‌های ثالث و یکپارچه‌سازی آنها به‌نحوی آسان

واکنش سریع‌تر به رخدادهای امنیتی

با کاهش تعداد رخدادهای امنیتی، محدود کردن خودکار تهدیدات بیشتر، به‌اشتراک‌گذاری اطلاعات و بهینه کردن هشدارهای فوق فعال – برای اعمال واکنش‌های خودکار بر اساس سیاست سازمان –، بر آن چیزی که از همه چیز مهمتر است تمرکز کنید.

در Trellix Complete Endpoint Protection، با گردش‌کارهای آسان، به‌سهولت می‌توان تهدیدات را بررسی کرده، ظرفیت‌های امنیتی را توسعه داده و در عین حال، به‌بهترین نحو از سیستم‌های سازمان محافظت کرد.

علاوه بر اجزای یکپارچه این راهکار، محصولات امنیتی ثالث نیز می‌توانند اطلاعات و رویدادهای مربوط به تهدیدات را از طریق Trellix Data Exchange Layer با یکدیگر به اشتراک بگذارند. ضمن اینکه Trellix Threat Intelligence Exchange با در هم آمیختن دانش تهدیدات جامع حاصل شده در کل اکوسیستم، در کنار فناوری ابری Trellix Global Threat Intelligence سازمان را در برابر هر تهدید نوظهور ایمن می‌کند.

عملیاتی کردن پروسه‌های امنیتی، افزایش مقیاس‌پذیری و سازگاری بالا

صرف‌نظر از تعداد دستگاه‌ها - از پنج تا ده‌ها هزار دستگاه -، اعمال سیاست‌ها، بررسی رویدادها و اجرای فرامین همگی تنها با چند کلیک در کنسول مدیریتی Trellix ePolicy Orchestrator به آسانی فراهم است. این کنسول مدیریتی قدرتمند، استقرار و توزیع محصولات امنیتی ترلیکس را تسهیل کرده و مدیران و راهبران شبکه را با سطح دسترسی‌های متنوع قادر می‌سازد تا در هر لحظه، وضعیت امنیتی دستگاه‌های در محدوده مدیریتی خود را تحت رصد داشته باشند. گزارش‌های جامع این کنسول مدیریتی نیز امکان ارزیابی بلادرنگ رویدادها را فراهم می‌کنند.

Trellix Complete Endpoint Protection با بهره‌گیری از فناوری خودکار یادگیری ماشین و مدل‌های طبقه‌بندی رفتاری و همچنین با به‌اشتراک‌گذاری اطلاعات تهدید با محصولات امنیتی، راهکاری یکپارچه و متحد را در برابر تهدیدات نوظهور ارائه می‌دهد.

با این راهکار، سازمان را از گزند حملات آتی ایمن ساخته و با تعریف فرامین و واکنش‌های از قبل تعیین‌شده با خاطری آسوده تهدیدات بالقوه را خنثی کنید.

امکانات موجود در راهکار

- Threat Prevention: حفاظت جامع و چند لایه‌ای به‌منظور 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 فراخوان شده 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 مخرب به سازمان
- Application Control: کنترل برنامه‌ها و جلوگیری از اجرای هر گونه برنامه خارج از فهرست سفید سازمان
- Endpoint Security Storage Protection: حفاظت از تجهیزات ذخیره‌سازی NAS و جلوگیری از تبدیل آنها به انباره‌ای از بدافزارها
- 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