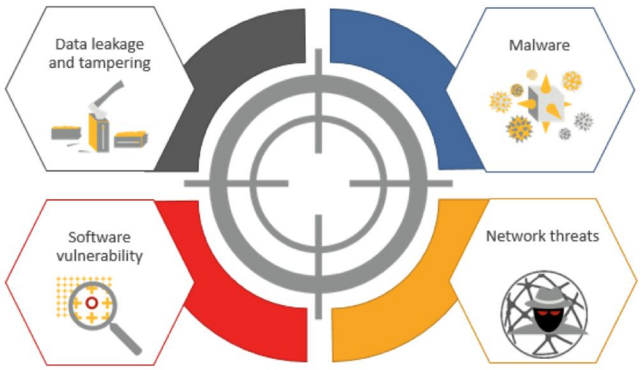
- مجهز به هوش مصنوعی بالا برای شناسایی تهدیدات ناشناخته
- مدیریت آسان و متمرکز
- مجهز به سندباکس و فناوری فریب برای به تله انداختن بدافزارها
- مجهز به فناوری تشخیص بدون امضاء مانند یادگیری ماشین، نظارت بر فعالیت برنامه و ...
- گزارش دهی جامع



در یک نگاه

محافظت از نقاط انتهایی در برابر کلیه حمله کنندگان با معماری Agent واحد

- مقابله با باج افزارها و سایر تهدیدات در حال وقوع با محافظت چند لایه، که ترکیبی از فن آوری های بدون امضا مانند یادگیری پیشرفته ماشین ، تجزیه و تحلیل رفتار و پیشگیری از سوء استفاده را با قابلیت های محافظت اثبات شده مانند جلوگیری از نفوذ ، تجزیه و تحلیل اعتبار و موارد دیگر است.
- از طریق محافظت قابل تنظیم ، برای ایجاد تصمیمات بهتر در زمینه سیاست ، به میدان دید وسیع در فایل های مشکوک دست پیدا کنید
- از تکنیک های فریبکاری برای آشکار کردن فایلهای مخرب پنهان و تعیین هدف آنها ، به منظور بهبود وضعیت امنیتی استفاده کنید
- محافظت از برنامه های معمول مورد استفاده در برابر سوء استفاده از آسیب پذیری و جدا کردن برنامه های مشکوک از فعالیت های مخرب

تحقق دفاع سایبری یکپارچه در مقیاس

- با ادغام در زیرساخت های امنیتی شبکه مانند درگاه های وب و ایمیل ، از جمله ادغام تجزیه و تحلیل محتوا برای دریافت اطلاعات جعبه ایمنی شبکه (sandbox) برای فایلهای مشکوک ، تهدیدات را در هر مکان شناسایی کرده و با SEP پاسخ دهید.
- ادغام با EDR برای بررسی حادثه و استفاده حداکثری پاسخ همان عامل SEP
- ادغام با زیرساخت های موجود فناوری اطلاعات به منظور خودکارسازی فرایندها با استفاده از APIهای آزاد

فعال کردن تجارت با عملکرد بالا ، راه حل سبک

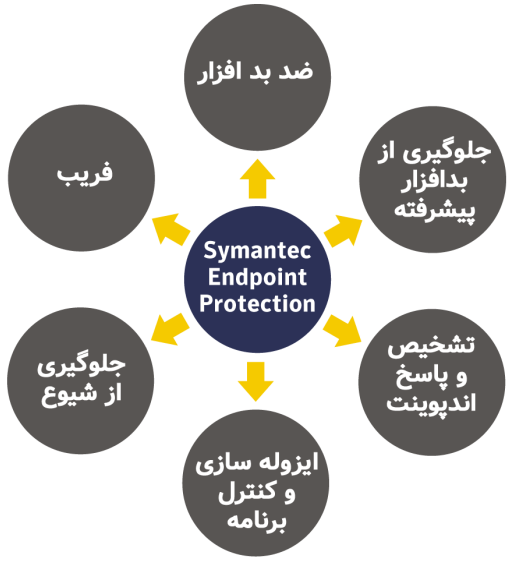
- بهینه سازی فرکانس به روزرسانی محتوا برای نقاط انتهایی با محدودیت پهنای باند شبکه بدون به خطر انداختن کارایی امنیتی
- افزایش عملکرد با یک agent سبک و مجموعه های تعریف ویروس، که به حداقل پهنای باند شبکه نیاز دارد
- سرعت تشخیص بالا با تکنیک های پیشرفته و همچنین جستجوی ابری دارای ثبت اختراع، در زمان واقعی که زمان اسکن سریع تری را ارائه می دهد

مقدمه

با طبیعت در حال تکامل مداوم محیط IT امروز ، مهاجمان از حملات پیچیده تری برای نفوذ به شبکه ها استفاده می کنند و نقطه پایان (اندپوینت-Endpoint)، آخرین خط دفاعی است. سازمانها بیشتر نگران آسیب و اختلال در فضای مجازی هستند زیرا حملات باج افزار در حال افزایش است و شیوع WannaCry و Petya گواه این امر است. علاوه بر این ، استفاده گسترده مهاجمان از حملات مخفیانه بدون فایل و حملات مخفی، به همراه "زندگی بدون زمین Living off the Land-LotL " (استفاده از ابزارهای رایج IT برای حمله) مواردی مانند محرمانه بودن ، یکپارچگی و در دسترس بودن دارایی های نقطه پایانی را تهدید می کند.

بنابراین تیم های امنیتی برای رسیدگی به حملات سایبری چه کاری می توانند انجام دهند؟

مدیریت محصولات و فناوری های چند نقطه ای طاقت فرسا است خصوصا، مدیریت امنیت در چندین منطقه جغرافیایی با سیستم عامل ها و پلتفرم های متنوع ، چالش های زیادی به همراه دارد. تیم های امنیتی با داشتن منابع و بودجه محدود ، فناوری هایی با مدیریت آسان می خواهند تا بتوانند برای بهبود امنیت کلی با یکدیگر ادغام شوند و نیازی به محصول دیگری نداشته باشند. (شکل ۱)



شکل۱ : سیمانتک امنیت کامل نقطه پایانی را ارائه می دهد.

Symantec Endpoint Protection (SEP) ، حفاظت برتر و چند لایه برای جلوگیری از تهدیدات، بدون در نظر گرفتن چگونگی حمله به Endpoint را ارائه می‌دهد SEP .با زیرساخت‌های امنیتی موجود سازمان ادغام می‌شود تا پاسخ های هماهنگ شده‌ای را که به سرعت تهدیدات را متوقف می‌سازد، ارائه دهد. عامل واحد و سبک وزنSEP ، عملکردی بالا، بدون به خطر انداختن بهره‌وری، ارائه می‌کند، بنابراین شما می‌توانید در کسب و کار خود تمرکز کنید.

SEP پرسنل امنیتی را قادر می سازد تا بسیاری از موارد استفاده امنیتی را که در چارچوب امنیتی در شکل ۲ آمده است ، اجرا کنند.

شکل ۲: (چارچوب امنیتی SEP)

محافظت از نقاط پایانی در برابر بردارحمله، با استفاده از یک معماری واحد Agent

جلوگیری

SEP بدون توجه به اینکه مهاجمان به زنجیره حمله چگونه حمله می کنند، از نقاط پایانی محافظت می کند (شکل ۳). این سطح از پیشگیری تنها با ترکیبی از فن آوری های پایه و فناوری های پیشرفته و جدید امکان پذیر است.

فناوری های بدون امضاء

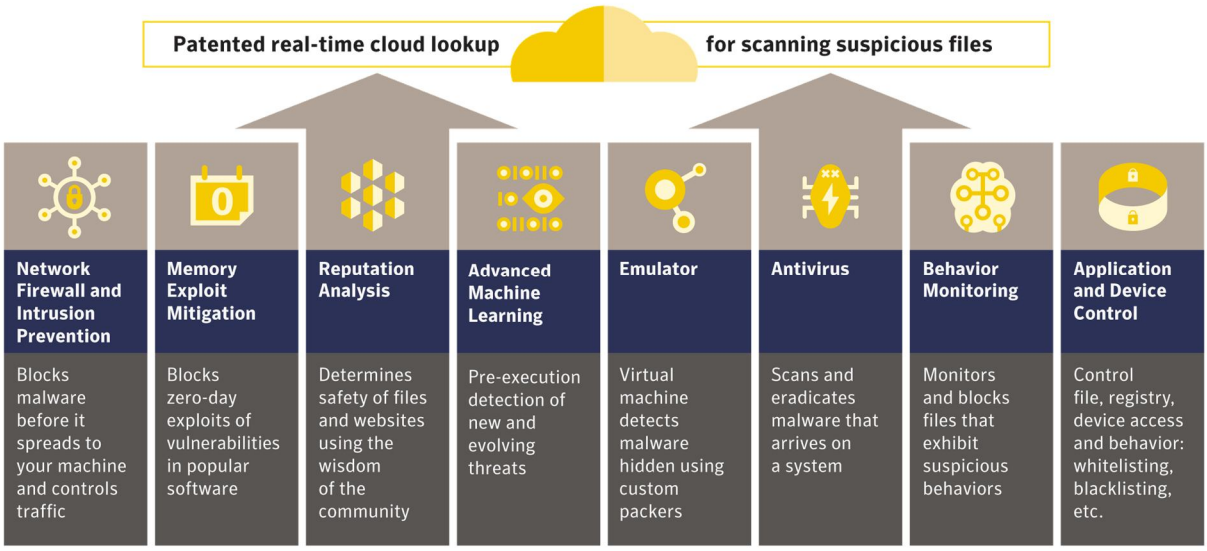
- یادگیری ماشین پیشرفته AML – تشخیص تهدیدات جدید و شکل گرفته قبل از اجرای آنها
- کاهش میزان بهره برداری از حافظه – بلوک کردن تهدیدات روز صفر در برابر آسیب پذیری های نرم افزارهای متداول
- نظارت بر رفتار – مانیتور و بلوک فایل هایی که رفتار مشکوک دارند.

قابلیت های پیشرفته

- شبکه هوشمند جهانی (GIN) – بزرگترین شبکه اطلاعاتی امنیت جهان، اطلاعات را از میلیون‌ها حسگر حمله به دست می‌آورد. این داده ها توسط بیش از یک هزار محقق تهدید ماهر بررسی می شوند تا دیدگاه منحصر بفرد را در مورد تهدیدات ارائه داده و محصولات پیشرفته ای برای مقابله با تهدیدات ارایه شود.
- تجزیه و تحلیل اعتبار – با استفاده از تکنیک های هوش مصنوعی در ابر که از GIN قدرت گرفته است، ایمنی پرونده ها و وب سایت ها را تعیین می شود.
- شبیه ساز – با استفاده از یک سندباکس سبک، بدافزارهای چند شکلی پنهان شده در بسته بندی‌های سفارشی را شناسایی می‌کند.
- ابر هوشمند تهدید – توانایی اسکن سریع با استفاده از تکنیک‌های پیشرفته مانند خطوط لوله گذاری، انتشار اعتماد و مرتب سازی queriesرا دارا می‌باشد و نیازی به دانلود همه تعاریف امضا برایEndpoint ، به منظور حفظ کارایی بالا را ندارد. تنها جدیدترین اطلاعات تهدید بارگیری می‌شود و حجم فایل‌های تعریف امضا تا ۷۰ درصد کاهش می‌یابد که این امر به نوبه خود استفاده از پهنای باند را کاهش می‌دهد.
- نمایش کلاینت خارج از شبکه – رویدادهای مهم را از مشتریانی که دور از شبکه ارتباطی هستند، دریافت می‌کند.

یکپارچه سازی پیشرفته

- ادغام تجزیه و تحلیل محتوا – از sandboxing پویا و موتورهای اضافی برای تجزیه و تحلیل بیشتر فایل‌های مشکوک استفاده می‌شود.



شکل ۳- محافظت چند لایه ای SEP

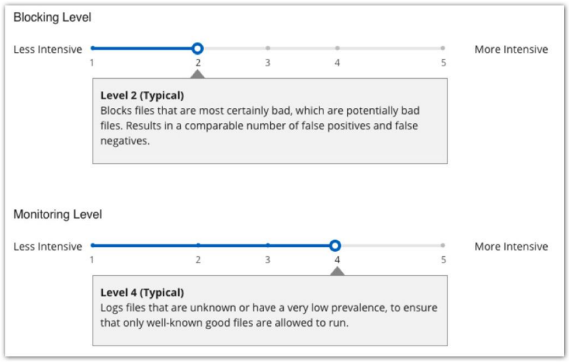
- ادغام احراز هویت چندگانه – از اعتبارسنجی سیمانتک ، حفاظت از ID ، PIV / CAC کارت‌های هوشمند برای احراز هویت در کنسول مدیریتی SEP استفاده می‌گردد.
- ادغام سرویس امنیت وب – ترافیک وب را از کاربران رومینگ به سرویس امنیتی وب سیمانتک با استفاده از یک پرونده PAC هدایت می‌کند.
- ادغام دروازه امنیتی وب – قابل برنامه‌ریزی بودن REST APIs، امکان ادغام با زیرساخت‌های امنیتی موجود از جمله دروازه امنیتی وب سیمانتک و هماهنگی پاسخ برای متوقف کردن گسترش تهدید را فراهم می‌سازد.

ویژگی های پایه

- آنتی ویروس و فایروال – بدافزارهایی که به سیستم وارد می‌شوند را اسکن و ردیابی کرده و نرم افزارهای مخرب را قبل از گسترش آن به دستگاه و کنترل ترافیک مسدود می‌کند.
- کنترل برنامه کاربردی و دستگاه – فایل، رجیستری، دسترسی و رفتار دستگاه را کنترل و همچنین لیست سفید و سیاه را ارائه می‌دهد.
- Power Eraser - ابزاری تهاجمی است که می تواند از راه دور برای رفع تهدیدهای مداوم پیشرفته و رفع بدافزارهای سخت گیرانه تحریک شود.
- یکپارچگی میزبان – اطمینان حاصل می‌کند که اندپوینت مورد محافظت قرار گرفته و با سیاست های اجرایی سازگار است. با بهره گیری از توانایی جداسازی یک سیستم مدیریت شده که مطابق با ملزومات شما نیست، تشخیص تغییرات غیرمجاز و ارزیابی خسارت ممکن می شود.
- قفل کردن سیستم – به برنامه‌های لیست سفید اجازه اجرا داده می شود و برنامه‌های لیست سیاه مسدود می شود.

علاوه بر این ، فقط SEP به تیم های امنیتی IT اجازه می دهد که سطح شناسایی و مسدود کردن را تنظیم کنند تا از بهینه سازی حفاظت و افزایش دید در پرونده های مشکوک برای هر محیط مشتری اطمینان حاصل شود(شکل ۴).

این امنیت قابل تنظیم با نام Intensive Protection (محافظت شدید)، با یک کنسول ابری جدید در دسترس است که به طور خودکار با کنسول SEP داخلی ادغام می شود وگردش کار آسانی را برای اضافه کردن فایلهای مشکوک به لیست سیاه و یا اضافه کردن موارد مثبت کاذب در لیست سفید ارایه می دهد.



شکل ۴: نظارت و انسداد قابل تنظیم از طریق Intensive Protection در دسترس است

معماری واحد agent سیمانتک، تیم های امنیتی IT را قادر می سازد فناوری امنیتی نوآورانه را با استقرار ساده، اضافه کنند. علاوه بر این ، SEP از بسیاری از محیط ها ، از جمله IPv6 ، پشتیبانی می کند.

کشف و پاسخ DETECTION AND RESPONSE (EDR)

Symantec Endpoint Detection and Response با استفاده از قابلیت های یکپارچه EDR در SEP، امکان بررسی و بازسازی حوادث را فراهم می کند.. هوش مصنوعی مبتنی بر ابر ، یادگیری دقیق ماشین ، تجزیه و تحلیل رفتاری و هوش تهدید ، مثبت کاذب را به حداقل می رساند و سطح بالایی از بهره وری را برای تیم های امنیتی تضمین می کند. تیم امنیتی می تواند EDR را در عرض یک ساعت مستقر کند تا حملات پیشرفته را فاش کند. قابلیت های EDR سیمانتک به پاسخ دهندگان حادثه این امکان را می دهد تا هنگام بررسی تهدیدها با استفاده از سندباکس محلی یا مبتنی بر ابر ، همه نقاط انتهایی تحت تأثیر را به سرعت جستجو و شناسایی کنند. علاوه بر این ، با ضبط مداوم فعالیت سیستم، امکان مشاهده کامل نقطه پایانی و پرس و جوی آن امکان پذیر می شود.

EDR و تجزیه و تحلیل حمله هدفمند

ادغام تجزیه و تحلیل هدفمند حمله (Targeted Attack Analytics-TTA) با EDR، چالش های امنیتی مهم را حل می کند. TAA تلفیقی از دورسنجی محلی و جهانی، هوش مصنوعی و تحقیقات حمله را برای افشای حملات ترکیب می‌کند، امری که بدون آن شناسایی موفقیت آمیز نمی‌شد.

با استفاده ازTAA و EDR، مشتریان از خدماتی همچون دریافت مداوم تحلیل‌های حملات جدید و مرسوم، آنالیز مفصل از حملات هکرها، ماشین‌های تحت آسیب و راهنمایی‌ها و توصیه‌های امنیتی، بهره مند خواهند شد.

Symantec EDR

- شناسایی و افشاء – زمان کشف تهدید را کاهش و به سرعت هدف را به نمایش می‌گذارد.
- بررسی و محتوی-افزایش بهره وری پاسخ گیرنده و رفع تهدید را تضمین می‌کند.
- حل مشکل- رفع اشکال سریع و ثابت و غیرقابل بازگشت را تضمین می کند.
- افزایش سرمایه گذاری های امنیتی – از مزایای ادغام و API های عمومی استفاده می‌کند.

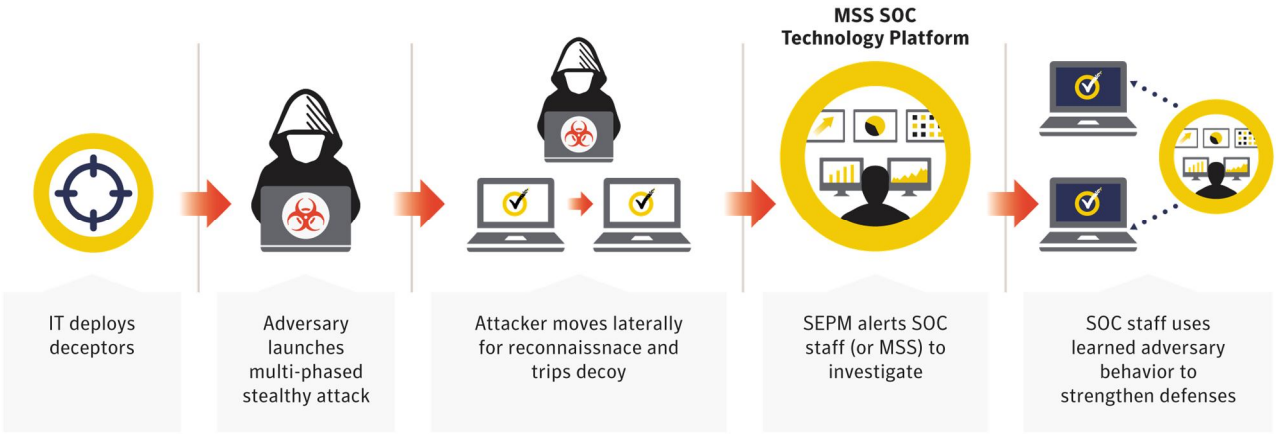
فریبکاری

SEP شامل توانایی تولید فریبنده ها (یعنی طعمه) برای افشای دشمنان مخفی و نشان دادن اهداف و تاکتیک های

مهاجم از طریق مشاهده زود هنگام است، به طوری که این اطلاعات می تواند برای افزایش موقعیت امنیتی شما مورد استفاده قرار گیرد. این ویژگی تشخیص دقیق و روشنی را در سریع‌ترین زمان ارائه می‌دهد. مشترکین SEP و مشتریان سرویس های امنیتی سیمانتک از پشتیبانی و پاسخگویی یک تیم خبره جهانی بصورت ۲۴*۷ در زمان واقعی بهره می‌گیرند. سیمانتک تنها تولید کننده پلتفرم محافظت از اندپوینت است که فناوری فریب را ارایه می کند.

مقاوم سازی

مقاوم سازی شامل چندین قابلیت افزودنی برای تکمیل پیشگیری SEP می‌باشد تا اثرات بی‌سابقه‌ای را در برابر نرم افزارهای مخرب و برنامه های مشکوک به ارمغان بیاورد. که شامل برنامه‌های پیشرفته حفاظتی است که در سریع‌ترین زمان با استفاده از همان عامل SEP سنجیده می‌شود. این قابلیت سطح حمله‌ها را کنترل و در حد پایین نگه می‌دارد تا برنامه‌ها بتوانند اجرا شده و کار حفاظتی خود را انجام



شکل ۵- نحوه کار فناوری فریبکاری

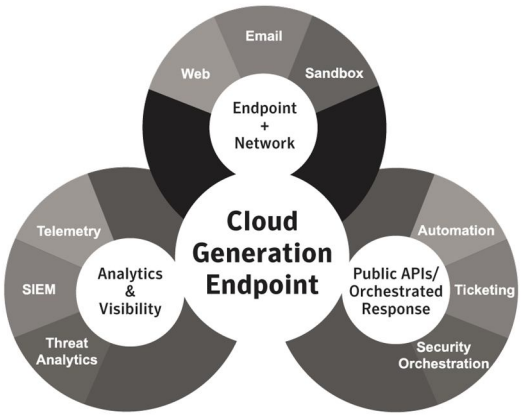
دهند. راه‌حل برنامه های پیشرفته حفاظتی برخی قابلیت‌ها را به اشتراک می‌گذارند. آنها برنامه جامع اکتشافی را برای یافتن برنامه‌های موجود Endpoint و کنترل ریسک و آسیب پذیری ارائه می‌دهند. این راه حل ها باعث افزایش بهره وری کارکنان از طریق پشتیبانی کامل از گردش کار کارمندان می شود.

فریبکاری SEP

- برای دستیابی به امنیت فعال، از فریب و طعمه برای شناسایی و به تاخیر انداختن حملات استفاده می کند.
- هدف مهاجم را برای بهبود وضعیت امنیتی تعیین می کند.
- ترفند فریب را در مقیاس کمتر برای ساده سازی گسترش و مدیریت ارائه می‌کند.

مقاوم سازی SEP

- امنیت برنامه جامع با به حداقل رساندن سطح حمله
- دید بی نظیر، با کشف و دسته بندی همه برنامه های نقطه پایانی
- سریعترین سرعت با استفاده از معماری عامل SEP



تحقق دفاع سایبری یکپارچه در مقیاس

اکثر سازمان‌های بزرگ از محیط های فناوری اطلاعات جهانی که به طور فزاینده پیچیده می‌شوند، پشتیبانی می‌کنند. با این حال، بسیاری از راه‌حل‌ها تنها کار خاصی را انجام می دهند. بنابراین ، سازمان ها به یک راه حل حفاظت از نقطه پایان(اندپوینت) احتیاج دارند که با تلفیق با سایر راه حل های امنیتی IT برای به اشتراک گذاشتن اطلاعات و دفاع از شبکه ، ارزش بیشتر و حفاظت کلی بهتری را فراهم کند.

SEP یک محصول پایه‌ای است که یکپارچگی را تسهیل می‌کند، به طوری که تیم های امنیتی IT می توانند تهدیدات را در هر نقطه از شبکه خود شناسایی کرده و با واکنش های هماهنگ با این تهدیدات مقابله کنند.

SEP در کنار راه حل های سیمانتک (به عنوان مثال، به عنوان یک جزء کلیدی از پلت فرم یکپارچه دفاع سایبری) و با محصولات شخص ثالث (از طریق APIs منتشر شده) برای تقویت وضعیت امنیتی کار می کند.

پلتفرم یکپارچه پدافند سایبری سیمانتک، برای محافظت از کاربران، اطلاعات، پیام ها و وب، پلتفرم ابری و محلی را با استفاده از هوش بی‌نظیر تهدید یکپارچه می‌کند .هیچ محصول دیگری نمی‌تواند راه‌حل های یکپارچه ای به این صورت ارائه دهد که پاسخ را در اندپوینت (لیست سیاه و اصلاح) ایجاد و با شناسایی یک تهدید در دروازه شبکه (یعنی دروازه های امنیتی وب و ایمیل) آن را اجرا کند.

راه حل سبک با کارایی بالا، جهت افزایش بهره وری

بروزرسانی مکرر محتویات ، پهنای باند را گرفته، عملکرد را کاهش و بهره‌وری را به خطر می اندازد. بدین ترتیب بهینه سازی بروزرسانی محتویات و ارائه تشخیص بهتر تهدیدات، یک پیروزی محسوب می‌شود. این قابلیت ها بار تیم IT را برای برنامه‌ریزی بروزرسانی‌های مکرر امنیتی کاهش می‌دهد. و کاربران نهایی هیچ زحمتی در به روزرسانی های امنیتی که بر بهره وری تأثیر می گذارد ندارند.

SEP با عملکرد بهتر و نیاز به پهنای باند کمتر، از حفاظت بهتری برخوردار است.

سیمانتک به طور پیوسته در آزمون های عملکرد، از جمله آزمایش های Passmark Software's Enterprise Endpoint Security Performance Benchmark tests برای ویندوز ۷ و ویندوز ۱۰ ، رتبه‌های بالائی را کسب کرده است. با مراجعه به مرکز عملکرد سمانتک، می‌توانید از دیگر اعتبار سنجی‌های آزمون کیفیت سیمانتک اطلاعات کسب کنید :

symantec.com/products/performance-center

در مقایسه با آنتی ویروس های نوظهور ، SEP با ترکیب چندین قابلیت در یک عامل واحد و سبک، پیچیدگی نقطه پایانی را کاهش داده است. برای رقابت با قابلیت های امنیتی سیمانتک، به چندین فروشنده نو ظهور ، راه حل های متعدد و مطمئناً چندین عامل نیاز خواهد بود.

درباره سیمانتک: شرکت سیمانتک (NASDAQ: SYMC)شرکت امنیتی پیشرو در زمینه امنیت سایبری، به سازمانها، دولتها و مردم کمک می کند تا مهمترین داده های خود را در هر کجا که زندگی می کنند، ایمن نگه دارند. سازمان ها در سراسر جهان به سیمانتک برای یافتن

Client Workstation and Server System Requirements*

Windows® Operating Systems

- Windows Vista (32-bit, 64-bit)
- Windows 7 (32-bit, 64-bit; RTM and SP1)
- Windows Embedded 7 Standard, POSReady, and Enterprise (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows Embedded 8 Standard (32-bit and 64-bit)
- Windows 8.1 (32-bit, 64-bit), including Windows To Go
- Windows 8.1 update for April 2014 (32-bit, 64-bit)
- Windows 8.1 update for August 2014 (32-bit, 64-bit)
- Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (32-bit, 64-bit)
- Windows 10 (32-bit, 64-bit)
- Windows 10 November Update (version 1511) (32-bit, 64-bit)
- Windows 10 Anniversary Update (version 1607) (32-bit, 64-bit)
- Windows 10 Creators Update (version 1703) (32-bit, 64-bit)
- Windows 10 Fall Creators Update (version 1709) (32-bit, 64-bit)
- Windows 10 April 2018 Update (version 1803) (32-bit, 64-bit)
- Windows Server 2008 (32-bit, 64-bit; R2, SP1, and SP2)
- Windows Small Business Server 2008 (64-bit)
- Windows Essential Business Server 2008 (64-bit)
- Windows Small Business Server 2011 (64-bit)
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2012 R2 update for April 2014
- Windows Server 2012 R2 update for August 2014
- Windows Server 2016

Windows Hardware Requirements

- 32-bit processor: 2 GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended)
- 64-bit processor: 2 GHz Pentium 4 with x86-64 support or equivalent minimum
- 1 GB of RAM (2 GB recommended)
- 530 MB of free space on the hard disk

Macintosh® Operating Systems

- Mac OS X 10.10, 10.11, macOS 10.12, 10.13

Mac Hardware Requirements

- 64-bit Intel Core 2 Duo or later
- 2 GB of RAM
- 500 MB of free space on the hard disk

Virtual Environments

- Microsoft Azure
- Amazon WorkSpaces
- VMware WS 5.0, GSX 3.2 or later, ESX 2.5 or later
- VMware ESXi 4.1 – 5.5
- VMware ESX 6.0
- Microsoft Virtual Server 2005
- Microsoft Windows Server 2008, 2012, and 2012 R2 Hyper-V
- Citrix XenServer 5.6 or later
- Virtual Box by Oracle

Linux Operating System (32-bit and 64-bit versions)

- Amazon Linux
- CentOS 6U3 - 6U9, 7 - 7U4; 32-bit and 64-bit; 32-bit and 64-bit
- Debian 6.0.5 Squeeze, Debian 8 Jessie; 32-bit and 64-bit
- Fedora 16, 17; 32-bit and 64-bit
- Oracle Linux (OEL) 6U2, 6U4, 6U5, 7, 7.1, 7.2, 7.3
- Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U4
- SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12, 12 SP1 - 12 SP3, 64-bit
- SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12 SP3, 64-bit
- Ubuntu 12.04, 14.04, 16.04; 32-bit and 64-bit

Linux Hardware Requirements

- Intel Pentium 4 (2 GHz CPU or higher)
- 1 GB of RAM
- 7 GB of free space on the hard disk

Manager System Requirements

Windows® Operating Systems

- Windows Server 2008 (64 bit)
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Web Browser

- Microsoft Internet Explorer 11
- Mozilla Firefox 5.x through 60
- Google Chrome 66
- Microsoft Edge

Hardware

- Intel Pentium Dual-Core or equivalent minimum
- 2 GB of RAM (8 GB or more available)
- 40 GB available minimum free hard disk space (200 GB recommended) for the management server and database

Database

Embedded database included or choose from the following:

- SQL Server 2008, SP4
- SQL Server 2008 R2, SP3
- SQL Server 2012, RTM – SP3
- SQL Server 2014, RTM – SP2
- SQL Server 2016, RTM, SP1
- SQL Server 2017

Symantec Endpoint Protection client must run one of the following Windows desktop operating systems to run Symantec Endpoint Protection Hardening:

- Windows 7 (RTM and SP1), Professional, Enterprise
- Windows 8, Professional, Enterprise
- Windows 8.1 (update for April 2014 and August 2014; Windows To Go), Professional, Enterprise
- Windows 10 (RTM), Professional, Enterprise
- Windows 10 November Update (version 1511), Professional, Enterprise
- Windows 10 Anniversary Update (version 1607), Professional, Enterprise
- Windows 10 Creators Update (version 1703), Professional, Enterprise
- Windows 10 Fall Creators Update (version 1709), Professional, Enterprise
- Windows 10 April 2018 Update (version 1803), Professional, Enterprise(Version 14.2 only)

Version 14.0.1.x clients only support 64-bit operating systems. Version 14.2 and later clients support both 32-bit and 64-bit operating systems.

راه حل های استراتژیک و یکپارچه برای دفاع در برابر حملات پیچیده در نقاط انتهایی ، ابر و زیرساخت ها چشم دوخته اند. به همین ترتیب، یک اجتماع جهانی بالغ بر ۵۰ میلیون نفر و خانواده ها به مجموعه محصولات Norton و LifeLockاعتماد کرده‌اند تا از زندگی و خانه و تمامی دستگاه های دیجیتال خود محافظت کنند. سیمانتک یکی از بزرگترین شبکه های اطلاعاتی غیرنظامی شبکه های سایبری را در اختیار دارد و می تواند در برابر تهدیدات پیشرفته تر محافظت به عمل آورد.

تهران، خیابان شهید بهشتی ، خیابان پاکستان ، کوچه چهارم ، پلاک ۱۱ ، طبقه چهارم ، واحد ۷
تلفن: ۸۸۸۰۴۹۶۱ | دورنگار: ۸۹۷۸۳۷۳۷ | کدپستی : ۱۵۳۱۶۴۵۹۱۸
www.arka.ir info@arka.ir
arka رایان سامانه آرکا