Symantec Endpoint Security

حفاظت تطبیقی برای سفارشی سازی خودکار و به حداکثر رساندن امنیت

مقدمه

شرکت‌ها در سراسر جهان سرمایه‌گذاری زیادی روی امنیت نقطه پایانی برای محافظت از دارایی‌های ارزشمند خود انجام می‌دهند. با وجود زمان و هزینه صرف شده، امروز بیش از هر زمان دیگری تخلفات رخ می دهد. چرا اینطور است؟

خوب، برخی از راه حل های امنیتی سطوح حفاظتی پایین تری را برای به حداقل رساندن موارد مثبت کاذب ارائه می دهند. اشتباهات پیکربندی و تنظیمات ضعیف را اضافه کنید، و به راحتی می توانید ببینید که چرا نقاط پایانی در معرض خطر قرار می گیرند.

پیشگیری مهم است زیرا تهدیدات سایبری جهانی تهاجمی تر از همیشه هستند و می توانند تأثیر خیره کننده ای بر یک تجارت داشته باشند. جلوگیری از حملات در اسرع وقت بسیار مهم است، زیرا پنجره تشخیص و واکنش به حمله مدرن بسیار کوتاه است. سرمایه گذاری در واکنش به حادثه نیز برای ایجاد یک وضعیت امنیتی سخت برای جلوگیری از حملات آینده بسیار مهم است. با سیمانتک، می توانید به مصالحه پایان دهید. وقتی می توانید هر دو را داشته باشید، چرا بین بهترین امنیت و بیشترین سادگی انتخاب کنید؟

پس جواب چیست؟ راه حل مناسب نیاز به به حداکثر رساندن حفاظت نقطه پایانی و اثربخشی تشخیص متعادل در همه دستگاه ها، سیستم عامل ها و کل زنجیره حمله دارد.

Symantec Endpoint Security Completeپیکربندی حفاظتی را خودکار می کند تا حفاظت سفارشی را به طور خاص به سازمان شما ارائه دهد و در عین حال در زمان، هزینه و تلاش شما صرفه جویی می کند.

شکل1 Symantec Endpoint Security Complete

ویژگی های کلیدی برای

Symantec Endpoint Security Complete

- حفاظت از تمام نقاط پایانی: لپ تاپ، رایانه های رومیزی، رایانه لوحی، دستگاه های تلفن همراه و سرورها
- عامل واحد برای کاهش سطح حمله، پیشگیری از حمله، پیشگیری از نقض، و تشخیص و پاسخ نقطه پایانی(EDR)
- تنها کنسول با قابلیت مشاهده تهدید در زمان واقعی
- استقرار انعطاف‌پذیر: مدل‌های داخلی، مدیریت‌شده ابری و مدل‌های ترکیبی
- حفاظت تطبیقی
- امنیت اکتیو دایرکتوری
- کنترل برنامه پیشرفته
- مدیریت امنیت هدایت شده با هوش مصنوعی.(AI)
- تجزیه و تحلیل حملات هدفمند و شکارچی تهدید
- شبکه جهانی اطلاعات: اطلاعات تهدید در زمان واقعی، تجزیه و تحلیل تهدید، طبقه بندی محتوا، و داده های مسدود کننده تهدید جامع را ارائه می دهد.
- ادغام با برنامه های شخص ثالث از جمله Microsoft Graph، Open C2و سایر راه حل های Symantec از طریق Symantec ICDx

بررسی اجمالی راه حل

Symantec Endpoint Security Complete جامع ترین و یکپارچه ترین امنیت نقطه پایانی را در جهان ارائه می دهد. پلتفرم Symantecتک عاملی به عنوان یک راه حل داخلی، ترکیبی یا مبتنی بر ابر، از تمام نقاط پایانی سنتی و موبایل محافظت می کند، دفاعی درهم تنیده را در سطح دستگاه، برنامه و شبکه ارائه می دهد و از هوش مصنوعی (AI) برای بهینه سازی تصمیمات امنیتی استفاده می کند. . یک سیستم مدیریت یکپارچه مبتنی بر ابر، حفاظت، شناسایی و پاسخ به تمام تهدیدات پیشرفته را که نقاط پایانی شما را هدف قرار می دهند، ساده می کند.

ایمنی نقطه پایانی بی بدیل برای سازمان مشتری

Symantec Endpoint Security یک رویکرد حفاظت تطبیقی نوآورانه ارائه می‌کند تا به سازمان‌ها کمک کند تا جابجایی راهکارها(shift left) حرکت کنند و بر افزایش حفاظت در کل زنجیره حمله تمرکز کنند.با تأکید بر پیشگیری برای مهار سریع Adaptive Protection پیکربندی امنیتی را خودکار می کند تا به طور خاص محافظت سفارشی شده را برای هر سازمان بدون زحمت ارائه دهد.

کاهش سطح حمله فعال و پیشگیری از حمله نوآورانه ، قوی‌ترین دفاع را در برابر سخت‌ترین تهدیدهایی که به بدافزارهای مخفی، سرقت مدارک، روش‌های حمله بدون فایل و «living off the lan» متکی هستند، ارائه می‌کنند. سیمانتک همچنین از نقض های شدید قبل از رخ دادن نفوذ جلوگیری می کند.

کاهش سطح حمله

سیمانتک دفاع پیشگیرانه نقطه پایانی را با قابلیت‌های کاهش سطح قبل از حمله بر اساس کنترل‌های خط‌مشی و فناوری‌های پیشرفته ارائه می‌کند.این قابلیت به‌طور مداوم آسیب‌پذیری‌ها و پیکربندی‌های نادرست را در میان برنامه‌ها، اکتیو دایرکتوری و دستگاه‌ها اسکن می‌کند. با استفاده دفاع کاهش سطح حمله در محل، بسیاری از تاکتیک‌ها و تکنیک‌های مهاجم از کار می افتد.

ارزیابی نقض به طور مداوم بررسی می شود

- ارزیابی نقض برای اکتیو دایرکتوری برای پیکربندی نادرست دامنه، آسیب‌پذیری‌ها و تداوم آن با استفاده از شبیه‌سازی حمله برای شناسایی خطرات
- Device Control خط‌مشی‌هایی را برای انواع مختلف دستگاه‌هایی که به رایانه‌های مشتری متصل می‌شوند، مانند دستگاه‌هایUSB ، مادون قرمز و FireWire تعیین می‌کند تا خطر تهدیدات و نفوذ را کاهش دهد.
- Application Control: ریسک برنامه‌ها و آسیب‌پذیری‌های آن‌ها را ارزیابی می‌کند و فقط به برنامه‌های شناخته شده خوب اجازه اجرا می‌دهد

پیشگیری از حمله

- پیشگیری از حملات چند لایه Symantec بلافاصله و به طور موثر در برابر بردارها و روش های حمله مبتنی بر فایل و بدون فایل محافظت می کند. یادگیری ماشینی و هوش مصنوعی آن از دستگاه های پیشرفته و طرح های تشخیص مبتنی بر ابر برای شناسایی تهدیدات در حال تحول در انواع دستگاه ها، سیستم عامل ها و برنامه های کاربردی استفاده می کند. حملات در زمان واقعی مسدود می شوند، بنابراین نقاط پایانی یکپارچگی را حفظ می کنند و از تأثیرات منفی اجتناب می شود.
- پیشگیری از بدافزار ترکیبی از تشخیص قبل از اجرا و مسدود کردن تهدیدهای جدید و در حال تکامل (یادگیری ماشین پیشرفته، sandboxing برای شناسایی بدافزار پنهان در بسته‌بندی‌های سفارشی، و نظارت و مسدود کردن رفتار فایل‌های مشکوک) و روش‌های مبتنی بر امضا (تجزیه و تحلیل اعتبار فایل و وب‌سایت و اسکن بدافزار).
- ماژول Exploit Prevention سوء استفاده‌های روز صفر مبتنی بر حافظه را در آسیب‌پذیری نرم‌افزارهای محبوب مسدود می‌کند.
- Intensive Protection به طور جداگانه تنظیم دقیق سطح شناسایی و مسدود کردن را برای بهینه سازی حفاظت و به دست آوردن دید بهتر در فایل های مشکوک فعال می کند.
- امنیت اتصال شبکه‌های Wi-Fi را شناسایی می‌کند، از فناوری اعتبار نقطه اتصال همراه استفاده می‌کند و یک VPN مبتنی بر سیاست را برای محافظت از اتصالات شبکه و پشتیبانی از انطباق ارائه می‌کند.

پیشگیری از نقض

- رویکرد پیشگیری سیمانتک مستلزم مهار مهاجمان در اسرع وقت - در نقطه پایانی - قبل از اینکه فرصتی برای ادامه در شبکه داشته باشند. فن‌آوری‌های مختلف فریب و جلوگیری از نفوذ مبتنی بر هوش مصنوعی با هم کار می‌کنند تا پایداری شبکه را قبل و بلافاصله پس از به خطر انداختن نقطه پایانی خنثی کنند - قبل از اینکه یک نقض کامل رخ دهد.
- Intrusion Prevention و Firewall حملات شناخته شده بدافزار مبتنی بر شبکه و مرورگر را با استفاده از قوانین و خط مشی ها مسدود می کند و از تنظیم فرمان و کنترل با فهرست سیاه آدرس IP دامنه خودکار جلوگیری می کند.
- فریب از فریب ها و طعمه ها (فایل های جعلی، اعتبارنامه ها، اشتراک های شبکه، ورودی های حافظه پنهان، درخواست های وب و نقاط پایانی) برای افشای، تعیین قصد و تاکتیک های مهاجم و به تاخیر انداختن مهاجمان از طریق مشاهده اولیه استفاده می کند.

پیشگیری از نقض (ادامه)

- Active Directory Security از سطح حمله اولیه برای جابجایی جانبی و سرقت اعتبار دامنه با کنترل درک مهاجم از منابع اکتیو دایرکتوری از نقطه پایانی با استفاده از مبهم سازی نامحدود (به معنای دارایی جعلی و ایجاد اعتبار) دفاع می کند. با مبهم سازی، مهاجم هنگام تعامل با دارایی های جعلی یا تلاش برای استفاده از اعتبارنامه های مدیریت دامنه بر اساس ادراک اکتیو دایرکتوری، خود را تسلیم می کند.
- سیاست‌های مدیریت خودکار، مبتنی بر هوش مصنوعی ویادگیری ماشین پیشرفته، به‌طور منحصربه‌فردی شاخص‌های سازش و ناهنجاری‌های تاریخی را برای تطبیق مستمر آستانه‌ها یا قوانین خط‌مشی نقطه پایانی ترکیب می‌کند و آنها را به روز نگه می‌دارد و با نمایه ریسک فعلی سازمان شما همسو می‌کند.

پاسخ پس از نقض و اصلاح

سیمانتک فناوری‌های تشخیص و پاسخ نقطه پایانی (EDR) و تحلیلگر مرکز عملیات امنیتی (SOC) را با هم ترکیب می‌کند و ابزارهای لازم برای بستن سریع حوادث نقطه پایانی و به حداقل رساندن تأثیرات حمله را در اختیار مشتری قرار می‌دهد. قابلیت‌های EDR یکپارچه، در معماری تک عاملی که هر دو نقطه پایانی سنتی و مدرن را پوشش می‌دهد، حملات پیشرفته را دقیقاً شناسایی می‌کند، تجزیه و تحلیل‌های بی‌درنگ ارائه می‌کند و شما را قادر می‌سازد تا به طور فعال تهدیدها را شکار کنید و تحقیقات قانونی و اصلاح را دنبال کنید.

- رفتار قانونی امکان ثبت و تجزیه و تحلیل رفتار نقطه پایانی را برای شناسایی تکنیک‌های حمله پیشرفته که ممکن است از برنامه‌های کاربردی قانونی برای اهداف مخرب استفاده کنند، فراهم می‌کند. این داده ها با چارچوب MITER ATT&CK غنی شده است تا به راهنمایی پاسخ دهندگان حوادث در طول تحقیقات کمک کند.
- ابزارهای Advanced Threat Hunting در Symantec EDR ارائه شده‌اند که شامل کتابخانه های داخلی است که بهترین شیوه‌های تشخیص تهدید و رفتار غیرعادی را در بر می‌گیرد. پاسخ‌دهنده‌های رویداد می‌توانند در سراسر شرکت به دنبال IOC (هرگونه شواهد دال بر نقض امنیت) باشند تا مستقیماً در نقطه پایانی پرس‌وجو کنند.
- Integrated Responseبا بازیابی فایل‌ها، حذف فایل‌ها، جداسازی نقاط پایانی و فهرست سیاه، اقدام مستقیمی روی نقطه پایانی انجام می‌دهد Symantec EDR .از ارسال خودکار فایل های مشکوک شناسایی شده به sandboxing برای تجزیه و تحلیل کامل بدافزار از جمله افشای بدافزارهایی که VMAآگاه هستند، پشتیبانی می کند.
- Threat Hunterحوادث با وفاداری بالا را شکار می کند و قدرت یادگیری ماشینی پیشرفته و تحلیلگران خبره SOC را برای کشف ابزارها، تاکتیک ها و رویه های مورد استفاده توسط مهاجمان ترکیب می کند. این تضمین می کند که حملات حیاتی به سرعت با زمینه مربوطه شناسایی می شوند.

علاوه بر این، دسترسی بصری به داده‌های امنیتی جهانی سیمانتک را برای تقویت تلاش‌های تیم شما برای شکار تهدید ارائه می‌کند.

- Rapid Response زمان رفع تهدیدات و پاسخگویی به مهاجمان را در زمان واقعی به حداقل می رساند. ابزارها و کتابخانه های داخلی حاوی تهدیدهایی با جداسازی مهاجمان هستند و دسترسی تعاملی به نقاط پایانی را فراهم می‌کنند.

به راحتی محیط پویای نقطه پایانی خود را ایمن کنید

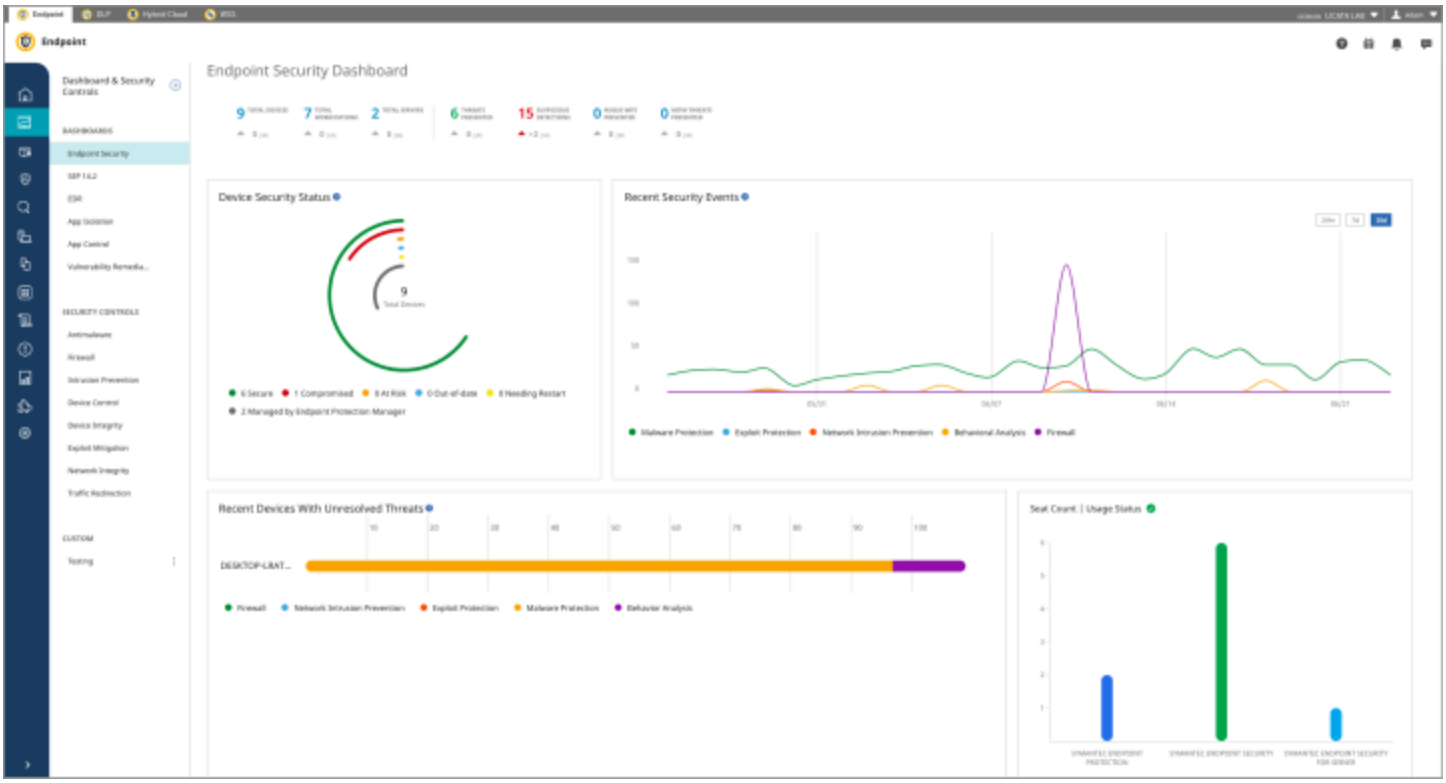
پشته تک عاملی ردپای امنیتی نقطه پایانی را کاهش می‌دهد و در عین حال بهترین فناوری‌های پیشگیری، شناسایی و پاسخ را یکپارچه و هماهنگ می‌کند. همه چیز را از یک سیستم مدیریت مبتنی بر ابر (مدیر یکپارچه دفاع سایبری) مدیریت کرده، زمان، منابع و تلاش مورد نیاز برای پیکربندی، گسترش، مدیریت و حفظ وضعیت امنیتی را به حداقل می رساند. همه چیزهای مورد نیاز با یک یا دو کلیک قابل دسترسی است، بهره‌وری سرپرست را بهبود می‌بخشد و زمان پاسخ‌دهی را سرعت می‌بخشد تا به سرعت رویدادهای امنیتی بسته شود.

- مدیریت امنیتی هدایت‌شده: با هوش مصنوعی سیاست‌ها را با دقت بیشتری به‌روزرسانی می‌کند و پیکربندی‌های نادرست کمتری بوجود می آید.
- مدیریت امنیت خودمختار به طور مداوم از رفتارهای مدیر و کاربر یاد می‌گیرد تا ارزیابی‌های تهدید را بهبود بخشد، پاسخ‌ها را تنظیم کند و وضعیت امنیتی کلی شما را تقویت کند.

کاهش پیچیدگی با Symantec و ادغام شخص ثالث

Symantec Endpoint Security یک راه حل اساسی است که یکپارچه سازی را تسهیل می کند تا تیم های امنیتی فناوری اطلاعات بتوانند تهدیدها را در هر نقطه از شبکه خود شناسایی کرده و با یک پاسخ هماهنگ به این تهدیدات بپردازند Symantec Endpoint Security .در کنار راه حل های دیگر Symantec و با محصولات شخص ثالث از طریق برنامه های اختصاصی وAPI های منتشر شده برای تقویت وضعیت امنیتی شما کار می کند. هیچ فروشنده دیگری راه حل یکپارچه ای ارائه نمی دهد که پاسخی را در نقطه پایانی (لیست های سیاه و اصلاح) که توسط شناسایی تهدید در دروازه های امنیتی وب و ایمیل ایجاد می شود، هماهنگ کند.

شکل 2 : رابط کاربری نقطه پایانی

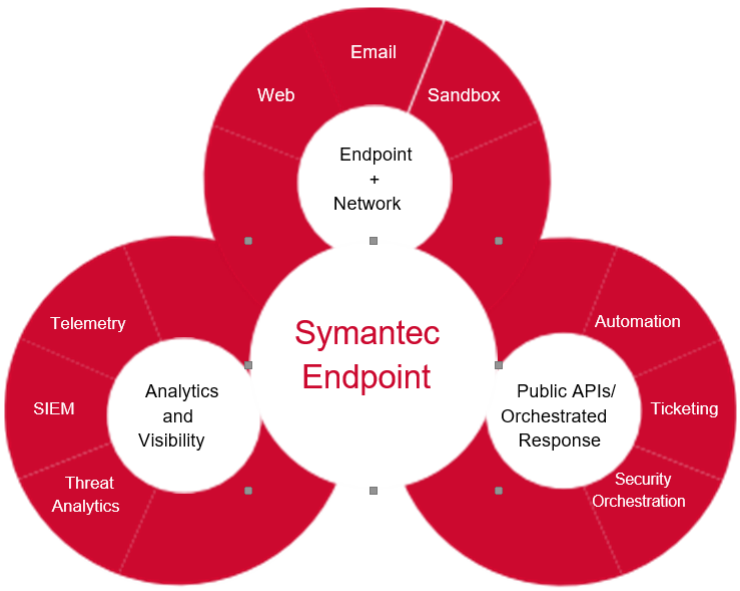


کاهش پیچیدگی با Symantec و ادغام شخص ثالث (ادامه)

ادغام های خاص عبارتند از:

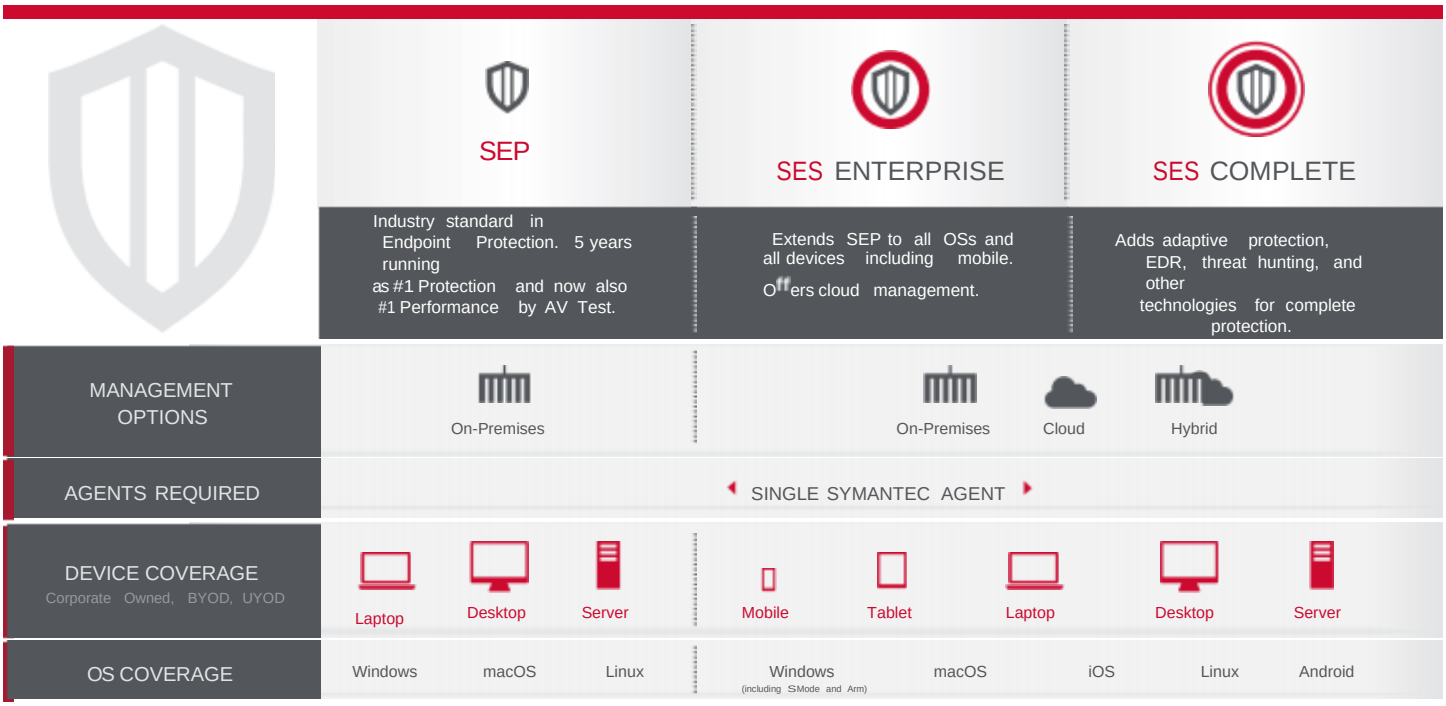
- Symantec Web Security Service: ترافیک وب را از کاربران رومینگ Symantec Endpoint Security به Symantec Web Security Serviceو Symantec CASB با استفاده از یک فایل PAC هدایت می کند.
- اعتبار سنجی و محافظت از شناسه :Symantec احراز هویت چند عاملی از جمله کارت های هوشمند PIV/CAC به کنسول های مدیریتی مبتنی بر CloudS و Symantec Endpoint Security.
- تجزیه و تحلیل محتوای : Symantec از پویایی در سندباکس اولیه و موتورهای تهدید اضافه شده برای تجزیه و تحلیل بیشتر فایل های مشکوک ارسال شده از Symantec Endpoint Security استفاده می کند.

شکل 3 : Symantec Endpoint Security



شکل 4: گزینه های لایسنس

امکانات



فن آوری های محافظت