SEQRITE

End Point Security Vs Trend Micro

سکورایت اندپوینت سکیوریتی کوییک هیل و ترندمیکرو انترپرایس سکیوریتی

Fanoos ICT Co
Quick Heal Distributer in Iran

Document: Seqrite EPS 7 vs Trend Micro Enterprise Security & Data Protection (Feature Comparison)

Date: 12 August 2016

ویژگی	Seqrite EPS 7	Trend Micro Enterprise Security & Data Protection

محافظت هسته

Antivirus, Antimalware	✓	✓

ارائه محافظت بلادرنگ در برابر انواع تهدیدات ناشی از انتقال فایل، دانلود اینترنتی، پیوست های ایمیل، فایل‌های آرشیوی و غیره.

Email Protection	✓	✓

ایمیل های آلوده و مخرب را پیش از ورود به صندوق پستی (Inbox) شما مسدود می کند.

Behaviour Detection System	✓	✓

نظارت بر فعالیت و جلوگیری از رفتار مشکوک.

Spam Protection	✓	✓

ایمیل‌های انبوه تبلیغاتی و ناخواسته را فیلتر کرده، می توان لیست سفید و لیست سیاه از آدرس های ایمیل ایجاد کرد.

Auto run Protection	✓	✓

از سیستم در برابر برنامه های مخرب که به صورت خودکار در زمان اتصال ابزارهای خارجی ذخیره سازی مانند (CD/DVD/USB) اجرا می شوند محافظت می کند.

Safe Mode Protection	✓	✗

از دسترسی به سیستم در حالت Safe Mode ویندوز جلوگیری می کند.

Self-Protection	✓	✓

از فایل ها / مدخل های رجیستری آنتی ویروس در برابر دستکاری و یا قطع اجرای آنها جلوگیری می کند.

Removal of Conflicting Software	✓	✓

آنتی ویروس / راهکار محافظ اندپوینت شرکت های دیگر را پیش از نصب کلاینت EPS حذف می کند.

اسکن آسیب پذیری و مدیریت وصله

Vulnerability Scan

برای شناسایی نقاط آسیب پذیر کلایتها را اسکن کرده و آسیب پذیری های موجود در انواع برنامه ها را شناسایی می کند. خلاصه ای از سطوح بالا، متوسط و پایین خطرات را ارائه می دهد.

Patch Management

بررسی و نصب خودکار وصله های مورد نیاز برنامه های مایکروسافت مانند آفیس، سیستم عامل ویندوز، اینترنت اکسپلورر و غیره. خلاصه ای از آپدیت های حیاتی، مهم و متوسط موردنیاز کلاینت ها را ارائه می‌دهد.

محافظت از شبکه

Firewall

بر اساس قوانین و رول های از قبل تعیین شده، اتصالات ورودی و خروجی را مانیتور، نظارت و کنترل می‌کند.

IDS/IPS

ترافیک های شبکه‌ی مخرب را شناسایی از نفوذهای غیرمجاز که از نقاط آسیب پذیر سوء استفاده می کنند جلوگیری می کند.

Port Scan Attack Detection

تلاش برای دسترسی به سیستم از طریق پورت های باز را شناسایی می کند.

DDOS Attack Detection

حملات توزیع شده اخلال در خدمت (Distributed Denial of Service) در شبکه را شناسایی می کند.

Source of Infection

منبع ورود آلودگی را نشان می‌دهد.

مدیریت دارایی

Asset Management (*)	✓	✗
اطلاعات جامعی درباره پیکربندی سیستم، اطلاعات سخت افزاری سیستمی و نرم افزارهای نصب شده بر روی کلاینت ها ارائه می دهد. هرگونه تغییرات سخت افزاری و نرم افزاری بر روی کلاینت ها ردیابی می کند. مثلا RAM تغییر یافت، Skype نصب شد / حذف شد.		
i. اطلاعات سیستمی	✓	✗
ii. ردیابی تغییرات سخت افزاری بر روی کلاینت ها	✓	✗
iii. ردیابی تغییرات نرم افزاری بر روی کلاینت ها	✓	✗

امنیت وب

Browsing Protection	✓	✓
وب سایت های مخرب را مسدود کرده و در نتیجه محیطی امن برای وبگردی ارائه می دهد.		
Phishing Protection	✓	✓
سایت های جعلی (فیشینگ) و کلاهبردار که درصدد سرقت اطلاعات محرمانه کاربران مانند اطلاعات حساب کاربری، کارتهای بانکی و غیره هستند را مسدود می کند.		
Browser Sandbox	✓	✓
یک محیط مجازی برای دسترسی به وب سایت های ارائه می دهد. زمانی که یک وب سایت در مرورگر سندباکس اجرا می‌شود، همه فایلهای دانلود شده مانند کوکی ها، فایلها موقت اینترنتی از دسترسی به سیستم مجزا (ایزوله) شده و از آلوده شدن سیستم جلوگیری می کند.		
Safe Banking	✓	✗
یک محیط امن و ایزوله برای انجام امور بانکی و تراکنش های آنلاین ارائه می دهد. با مسدود کردن دسترسی به درگاههای نا امن پرداخت و برنام های های سرقت داده مانند کلیدنگارها، از فعالیتهای کلاهبردارانه جلوگیری می‌کند.		
Web Filtering	✓	✓
برای افزایش بهره وری کارمندان، ادمین می تواند دسترسی به یک وب سایت خاص و یا گروه خاصی از وب‌سایت‌ها مانند شبکه های اجتماعی، بازی و غیره را مسدود یا محدود نماید.		

کنترل ابزار پیشرفته

اعمال کنترل بر روی دستگاهها و ابزارهای غیرمجاز در شبکه را ممکن می سازد. مثل ابزار ذخیره سازی USB، موبایل‌ها، وب‌کم‌ها، کارت‌خوان های حافظه، چاپگرها، اسکنرها و غیره.

i. USB Storage Device	✓	✓
ii. CD/DVD	✓	✓
iii. Internal Card Reader (SD Cards, Memory Cards)	✓	✓
iv. Floppy Drive	✓	✓
v. Wi-Fi	✓	✓
vi. Bluetooth	✓	✓
vii. Firewire Bus	✓	✗
viii. Serial Port	✓	✗
ix. SATA Controller	✓	✗
x. Thunderbolt	✓	✗
xi. PCMCIA	✓	✓
xii. Card Reader Device (MTD/SCSI)	✓	✗
xiii. Windows Portable Device (Digicams, Smartphones)	✓	✓
xiv. iPhone/iPad/iPod	✓	✓
xv. Blackberry	✓	✓
xvi. Scanner & Imaging Devices	✓	✓
xvii. Webcam	✓	✗
xviii. Local Printers	✓	✓
xix. Teensy Board	✓	✗
xx. Network Share	✓	✓
Temporary USB Storage Access	✓	✗

مدیر شبکه می تواند به کاربران خاص برای یک زمان مشخص، دسترسی موقت به حافظه های USB بدهد.

پیشگیری از نشت اطلاعات

DLP	✓	✓

بسته DLP از سرقت داده ها و یا نشت اطلاعات محرمانه جلوگیری کرده، و با مانیتورینگ و نظارت بر انواع کانال های انتقال داده، از نشت اطلاعات سازمانی به خارج از شبکه پیشگیری می کند.

– DLP برای جلوگیری از نشت اطلاعات بر کانال های انتقال داده زیر نظارت می کند:

Disable Print Screen	✓	✓

تصویربرداری از صفحه نمایش توسط کاربر یا برنامه را مسدود می کند.

Removable Device	✓	✓

بر انتقال اطلاعات به ابزارهای جداشدنی مانند فلش ها، CD/DVD ها نظارت می کند.

Network Share	✓	✓

بر انتقال اطلاعات به مکان های مختلف در شبکه نظارت می کند.

Clipboard	✓	✓

بر کپی اطلاعات به حافظه موقت سیستم نظارت می کند.

DLP انتقال اطلاعات از طریق برنامه های مختلف مانند پیامرسانی های فوری، برنامه های به اشتراک گذاری فایل / خدمات ابری، شبکه های اجتماعی، مرورگرهای وب، برنامه های کلاینتی ایمیل و غیره را مانیتور می‌کند.

Instant Messengers	✓	✓
File Sharing/Cloud Services	✓	✓
Social Media	✓	✗
Web Browsers	✓	✗
Email Clients	✓	✓

DLP انواع داده های زیر مانیتور می کند:

File Types

انتقال اطلاعات فایل های مختلف مانند فایل های آفیس، فایل های گرافیکی، فایل های برنامه نویسی و غیره را مانیتور یا مسدود می کند.

Confidential Data

انتقال اطلاعات از طریق فایل های حاوی اطلاعات محرمانه مانند شماره کارت اعتباری / بانکی، اطلاعات شخصی مانند شماره ملی، شماره تلفن، شماره بیمه و غیره را مانیتور یا مسدود می کند.

User Defined Dictionaries

انتقال اطلاعات از طریق فایل های حاوی کلمات و یا عبارات کلیدی مشخص شده توسط ادمین را مانیتور یا مسدود می کند.

Data-At-Rest Scan

اطلاعات محرمانه ساکن در درایوهای محلی، پوشه ها و دستگاه های قابل حمل متصل به کلاینت ها را شناسایی می‌کند.

نظارت بر فعالیت فایل

File Activity Monitor

بر فعالیت های فایل مانند کپی، تغییر نام و حذف فایل ها بر روی درایوهای محلی، درایوهای قابل حمل و درایوهای شبکه نظارت می کند.

مدیران شبکه به راحتی می توانند هرگونه تغییر در فایل ها در شبکه را ردیابی و ممیزی کنند.

کنترل برنامه

Application Control	✓	✓

استفاده از برنامه های غیر مجاز را در شبکه مسدود می کند. ادمین می تواند دسترسی به دسته بندی های از پیش تعریف شده نرم افزارها مانند برنامه به اشتراک گذاری فایل، بازی و غیره و یا هر فایل اجرایی یا برنامه ی جدید که توسط ادمین معرفی می شود را مجاز یا مسدود نماید. تغییرنام، تغییر مسیر تاثیری در اجرای سیاست های ادمین ندارد.

بهینه سازی

Tuneup	✓	✓

موجب می شود تا عملکرد سیستم بهبود یابد.

Disk Clean-up	✓	✓

با حذف فایل های زائد، فایل های موقتی، فایل های کش اینترنتی و غیره، فضای آزاد دیسک را افزایش می‌دهد.

Registry Clean-up	✓	✓

مدخل های نامعتبر و منسوخ رجیستری که به علت حذف نامناسب برنامه ها به وجود آمدند، را حذف و کارایی سیستم را بهبود می بخشد.

Defragmentation	✓	✗

یکپارچه ساز، قطعات و فرگمنت های پراکنده را به هم متصل کرده و عملکرد سیستم را بهبود می بخشد. داده ها بر روی هارد دیسک در بخش های کوچک در مکان های مختلف توزع شده اند. با افزایش استفاده از سیستم، قطعات فایلها افزایش می یابند، بنابراین زمان دسترسی به فایلها افزایش یافته و سرعت سیستم کاهش می یابد.

استقرار کلاینت

روش های متعدد نصب و استقرار بر روی کلاینتهای EPS پشتیبانی می شود.

Active Directory

با هماهنگ سازی با اکتیو دایرکتری، در شبکه مبتنی بر دامنه، محافظ اندپوینت می تواند بلافاصله بر روی همه کلاینت ها به صورت خودکار نصب شود.

شبکه دامنه به صورت دوره ای اتصال کلاینت جدید به شبکه را بررسی کرده، و در صورت شناسایی، آنتی ویروس به طور خودکار در کلاینت های جدید نصب می شوند.

Remote Install/Uninstall

امکان نصب از راه دور کلاینت ها با مشخص کردن نام میزبان، یا آدرس IP، یا یک رنجی از IP وجود دارد.

Notify Install

یک ایمیل اطلاع رسانی با لینک نصب (از سرور داخل شبکه) و دستورالعمل استقرار کلاینت ارسال می‌کند.

Client Packager

ساخت بسته نصب خودکار کلاینتی که می تواند از طریق ابزارهای حافظه مانند فلش ها، اشتراک گذاری فایل در شبکه، برنامه های کاربردی، CD/DVD و غیره توزیع و استفاده شود.

Login Script

اسکریپت لاگین به کلاینت ها در شبکه مبتنی بر دامنه اختصاص می یابد تا به محض ورود کاربران به شبکه، محافظ اندپوینت بر روی آنها نصب شود.

Disk Image

می توان با استفاده از ابزارهای ساخت تصویر (ایمیج)، از کلاینت حاوی سکورایت EPS تصویر تهیه کرده و فرایند نصب را در آن سیستم و یا سیستم های مشابه تسهیل کرد.

ثبت و اطلاع رسانی گزارش ها

ادمین می تواند در زمان دلخواه به گزارش ها و وقایع ثبت شده توسط ماژول های مختلف امنیتی دسترسی یافته و یا در دوره های زمانی تعیین شده به او ایمیل شود. می توان گزارش ها را مشاهده، چاپ و یا از آنها با فرمت csv. یا pdf. خروجی گرفت. اعلان های حوادث مختلف مانند شیوع ویروس، شناسایی حمله اسکن پورت، نقض سیاست کنترل ابزار و غیره می توانند به چندین آدرس ایمیل یا شماره موبایل ارسال شوند.

Export Reports (csv/pdf)	✓	✓
Scheduled Reports	✓	✓
SMS Notifications/Alerts	✓	✗
Email Alerts	✓	✓
News Alerts	✓	✗

مدیریت

Dashboard	✓	✓

داشبورد یک رابط گرافیکی مبتنی بر وب است که وضعیت فعلی کلاینت ها را نمایش داده و یک دید کلی از همه ماژول های امنیتی ارائه می دهد.

Management Console	✓	✓

یک کنسول مدیریت مبتنی بر وب که از هر مکانی در شبکه قابل دسترس است.

Cloud Management Platform	✓	✓

ابر Seqrite یک پلتفرم مدیریت مبتنی بر ابر می باشد که چندین EPS نصب شده در مکان های جغرافیایی مختلف را به صورت متمرکز مدیریت می کند.

Groups & Policies	✓	✓

می توان برای واحدهای مختلف یک سازمان، گروه ها و زیر گروه های متعدد ایجاد کرد. می‌توان با توجه به نیاز هر گروه سیاست‌های ویژه ای تعیین کرد.

بروزرسانی

Update Manager	✓	✓

اندپوینت سکوریتی EPS در یک محل مرکزی بروزرسانی ها را به صورت خودکار دانلود کرده و سپس توسط کلاینت ها دریافت می‌شود.

Multiple Update Manager	✓	✓

پلتفرم رومینگ

Cloud Platform to manage Roaming Clients	✓	✗

پلتفرم رومینگ یک رهکار مبتنی بر ابر می باشد که مدیر را قادر می سازد کلاینت هایی که به خارج از شبکه محلی منتقل شدند را مدیریت کند. با پلتفرم رومینگ، مدیر می تواند سیاست های خود را از راه دور اعمال و وضعیت کلاینت رومینگ (خارج از شبکه محلی) را مشاهده نماید.

سازگاری

Windows	✓	✓
MAC	✓	✓
Linux	✓	✓

شرکت فناوری ارتباطات و اطلاعات فانوس

نماینده رسمی شرکت تکنولوژی های کوییک هیل در ایران

تلفن: ۷۷۸۸۵۶۶۵ و ۷۷۱۴۲۵۲۶ (۰۲۱)

دورنگار: ۴۳۸۵۸۵۸۰ (۰۲۱)

پیامک: ۳۰۰۰۴۶۲۵

ایمیل: info@qhi.ir

وب سایت: www.quickheal.co.ir

Fanoos ICT Co.

Quick Heal Technologies Ltd. Authorized Distributor in Iran

Tel: +98 (21) 77 88 5665, 77 14 25 26

Email: info@qhi.ir

Official Blog: blogs.quickheal.co.ir

SEQRITE™ Enterprise Security Solutions by Quick Heal

Quick Heal®

Fanoos ICT Co Quick Heal Distributer in Iran