راهکار جامع امنیت سازمانی

ویژه شرکت‌ها و سازمان‌های متوسط و بزرگ

تکنولوژی های کوییک هیل

با تاکید بر امنیت سازمانی مبتنی بر

Seqrite

ENDPOINT SECURITY 7

Fanoos ICT Co
Brilliant Vision

Quick Heal
Security Simplified

SEQRITE
Enterprise Security Solutions by Quick Heal

معرفی

محصولات جامع امنیتی

- **امنیت شخصی:**
  - کامپیوتر، لپ تاپ
  - موبایل و تبلت.
- **امنیت سازمانی:**
  - اندپوینت سکیوریتی (EPS)
  - سامانه یکپارچه مدیریت تهدیدات (UTM)
  - مدیریت ابری دستگاههای همراه (MDM)
  - مدیریت ابری (Seqrite Cloud)
  - مانیتورینگ جامع حملات شبکه

پشتیبانی فنی

- پشتیبانی جامع به صورت تلفنی، ایمیل، تیکت، چت به همه مشترکان ارائه می گردد.
- پشتیبانی ۲۴*۷ توسط شرکت فانوس و شرکت کوییک هیل به صورت مستقیم به کاربر نهایی
- تنها آنتی ویروس دارای آپدیت سرور و هانی‌پات در ایران

آنتی ویروس اورجینال

- تولید آنتی ویروس و یا انجین برای برخی از شرکت‌های بزرگ در کشورهای نظیر آمریکا (مانند گاردین Guardian و ۳۴۷ آمریکا که در بخش امنیت شبکه و اندپوینت سکیوریتی فعال می‌باشد).
- برای استفاده از تجربیات و منابع انسانی آموزش‌دیده کوییک‌هیل، واحد توسعه آنتی‌ویروس شرکت سیمانتک در همان شهر پونای هند مستقر می‌باشد.

همکاران تجاری کوییک‌هیل در ایران

- شرکت رایتل، صبانت
- شرکت مخابرات استانهای مختلف (مازندران، سمنان، زنجان، کرمانشاه، لرستان و...)،

تکنولوژی های انحصاری

- ۳ ثبت اختراع تقدیر شده جهانی
- DNA Scan الگو گرفته از علم ژنتیک
- PC2Mobile
- انجین انحصاری
- سرمایه‌گذاری بزرگترین شرکت سرمایه گذار جهان Sequoia Capital (اپل، گوگل، اوراکل، سیسکو، یاهو، انویدیا، WhatsApp و...)

نماینده رسمی در ایران

- شرکت فناوری ارتباطات و اطلاعات فانوس نمایندگی شرکت در ایران از سال ۱۳۸۶
  - سازمانهای امنیتی ایرانی مانند پژوهشگاه هوا فضای کشور
  - شرکت های زیر مجموعه وزارت نیرو
  - سازمانهای دولتی
  - شهرداری ها
  - شرکت های بزرگ خصوصی

کوییک هیل با بیش از ۲۳ سال سابقه در حوزه امنیت فناوری اطلاعات در قطب نرم‌افزاری جهان در پونای هند می‌باشد.

- ۳۱ شعبه در هند
- شعبه در آمریکا، ژاپن، امارات و کنیا
- نمایندگی رسمی در ۷۰ کشور جهان

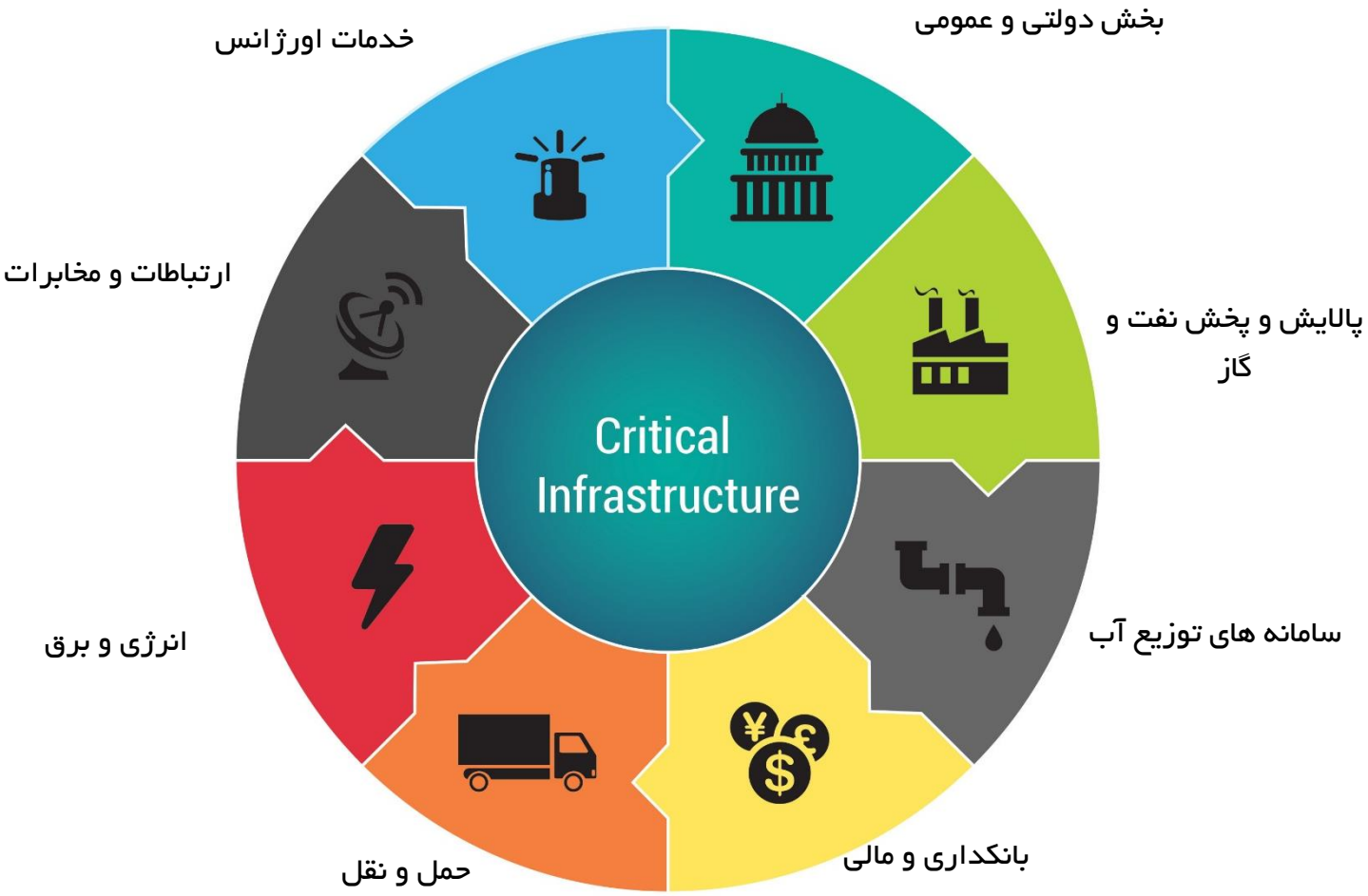
کاربران فعال بیش از ۸۵ میلیون

تائیدیه های کوییک هیل و فانوس در ایران:

- نمایندگی رسمی و مستقیم در ایران
- سازمان نظام صنفی رایانه ای کشور
- مرکز فناوری اطلاعات و رسانه های دیجیتال وزارت فرهنگ و ارشاد اسلامی
- سفارت جمهوری اسلامی ایران در هند
- تائیدیه حراست وزارت نیرو
- ایران کد
- شرکت مادرتخصصی آب کشور
- تائیدیه حراست مخابرات برخی استانها
- وزارت تعاون
- شورای عالی انفورماتیک
- مرکز توسعه تجارت الکترونیکی وزارت صنعت، معدن و تجارت
- مورد تایید بسیاری از سازمانهای دولتی

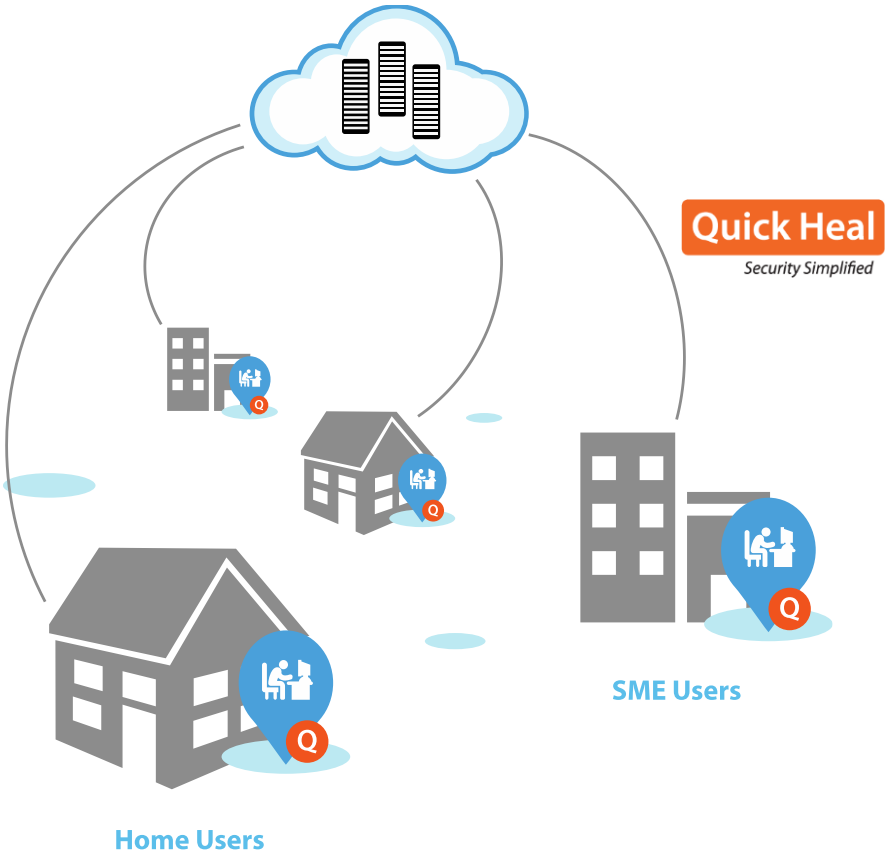
برخی از مشتریان جهانی:

- سازمان انرژی اتمی هند
- شرکت های بزرگ جهانی مانند تویوتا
- سازمانها و دانشگاه های بزرگ جهانی مانند وزارت آموزش و پرورش انگلستان
- سازمانهای دفاعی بزرگ مانند نیروی دریایی هند
- دانشگاه تگزاس آمریکا
- بانک مرکزی هند


بخش دولتی و عمومی
خدمات اورژانس
پالایش و پخش نفت و گاز
ارتباطات و مخابرات
Critical Infrastructure
سامانه های توزیع آب
انرژی و برق
بانکداری و مالی
حمل و نقل

محصولات خانگی

Retail / SMB



Retail / SMB

- جلوگیری از سرقت اطلاعات شخصی
- محافظت از برنامه ها و USB های غیرمجاز (فلش، هارد اکسترنال ...)
- اسکن خودکار فلش بلافاصله بعد از اتصال
- حذف کامل فایلهای خصوصی بدون امکان بازیابی
- بروزرسانی خودکار، سریع و کم حجم آنتی‌ویروس
- سرعت بالای اسکن
- محافظت در برابر همه انواع ویروس‌ها، ایمیل‌ها، وب‌سایت‌های آلوده، حملات اینترنتی
- عدم تاثیر در کاهش سرعت سیستم
- شناسایی ویروسهای منتشر شده در ایران
- امکان استثنا کردن فایلهای خاص از ویروسیابی
- کاهش مصرف پهنای باند ناشی از ویروس ها و همچنین استفاده از آنتی ویروس های کرک شده
- پشتیبانی رایگان تلفنی، وب، ایمیل، تیکت و ریموت
- و...

محصولات موبایل Mobile / Tablet

Quick Heal
Security Simplified

Fonetastic

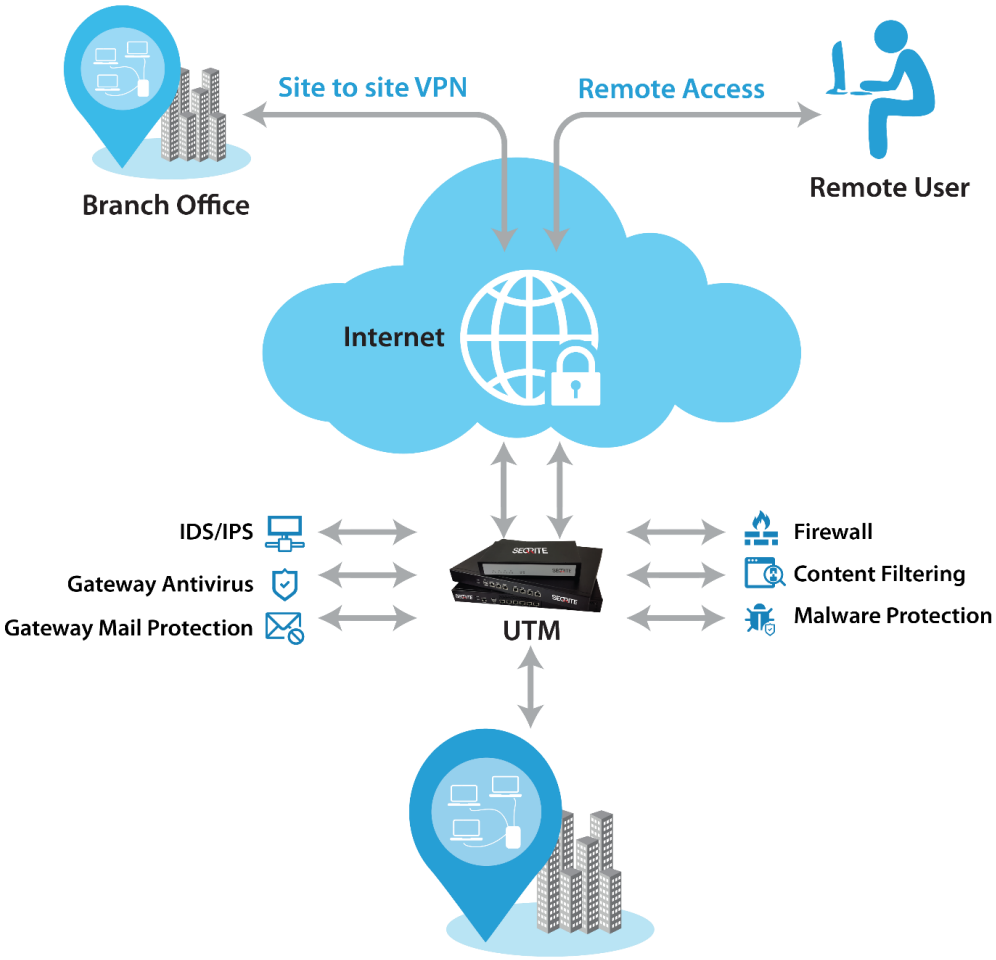
Quick Heal
Gadget Securance

Mobile

- عدم تاثیر در کاهش سرعت موبایل
- بروزرسانی خودکار، سریع و کم حجم
- محافظت در برابر همه انواع ویروس‌ها، برنامه های مخرب، وب‌سایت‌های آلوده، حملات اینترنتی
- اسکن کامل حافظه اصلی و حافظه جانبی از ویروس‌ها، و دیگر بدافزارها
- محافظت از سایتهای کلاهبردار و آلوده
- محافظت از سرقت اطلاعات شخصی
- مدیریت خانواده
- مسدود کردن تماس‌های صوتی مزاحم
- مسدود کردن پیامک‌های مزاحم
- امکان مدیریت مصرف پهنای باند
- ویژگی ضدسرقت
- قفل کردن موبایل از راه دور
- حذف از راه دور اطلاعات شخصی
- قفل کردن خودکار موبایل در زمان تغییر سیمکارت
- پیامک شماره سیمکارت جدید، به محض تغییر سیمکارت
- ارسال تصویر سارق موبایل
- رهگیری موبایل (با استفاده از GPS)
- گزارش استفاده از منابع سیستمی و شبکه ای و بهبود کارایی موبایل
- پشتیبان گیری بر روی فضای امن ابری

سامانه یکپارچه مدیریت تهدیدات

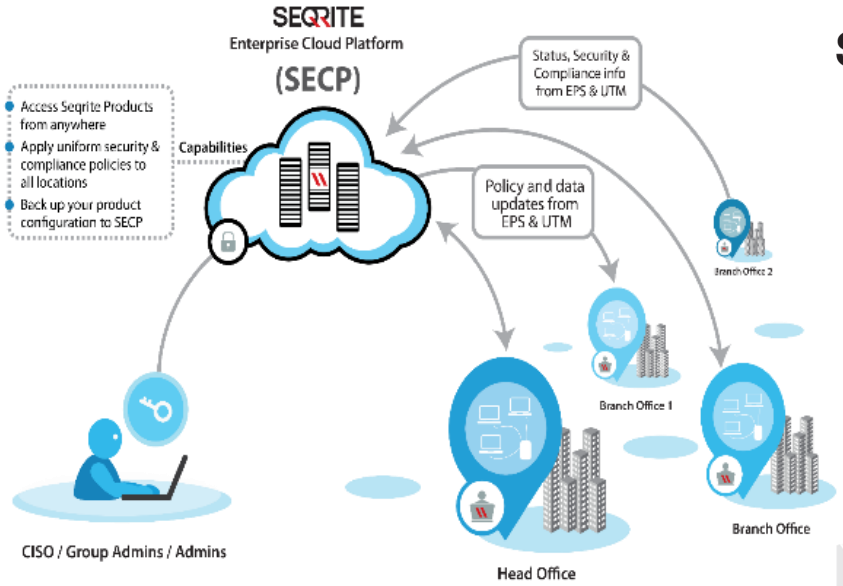
Unified Threat Management



Terminator (UTM)

- فایروال، IDS / IPS، آنتی‌ویروس، محافظ ایمیل، آنتی فیشینگ قدرتمند کوییک هیل در سطح گیتوی شبکه
- ارتباط امن بین شعبات مختلف و یا لپ تاپ به شبکه از بستر اینترنت (VPN)
- Bandwidth Management تعریف، کنترل و مدیریت پهنای باند، حجم، سرعت، و زمان دسترسی کاربران
- Content Filtering + Web Security مدیریت محتویات مختلف و نوع سایتها
- Load Balancing: افزایش سرعت و رفع قطعی اینترنت و کار با ترکیب دو اتصال ISP به صورت همزمان
- Policy Based Routing تعیین جریان ترافیکی درون شبکه سازمان، اولویت‌بندی و سفارشی‌سازی سیاست‌ها
- Application Access & Control کنترل بیش از ۱۵۰۰ برنامه در داخل شبکه
- جلوگیری از اتلاف وقت کارمندان و افزایش بهره وری با مانیتورینگ و ثبت و اعمال محدودیت بر روی کاربران
- افزایش امنیت و جلوگیری از نفوذ هکرها و شرکت های رقیب به اطلاعات سازمان
- جلوگیری از اتلاف پهنای باند و افزایش سرعت اینترنت و فعالیت های کاری مرتبط
- گزارش گیری کامل از دسترسی به سایتهای گوناگون بر حسب کاربر و زمان و جلوگیری از بروز مشکلات حقوقی و امنیتی

سامانه مدیریت ابری Cloud

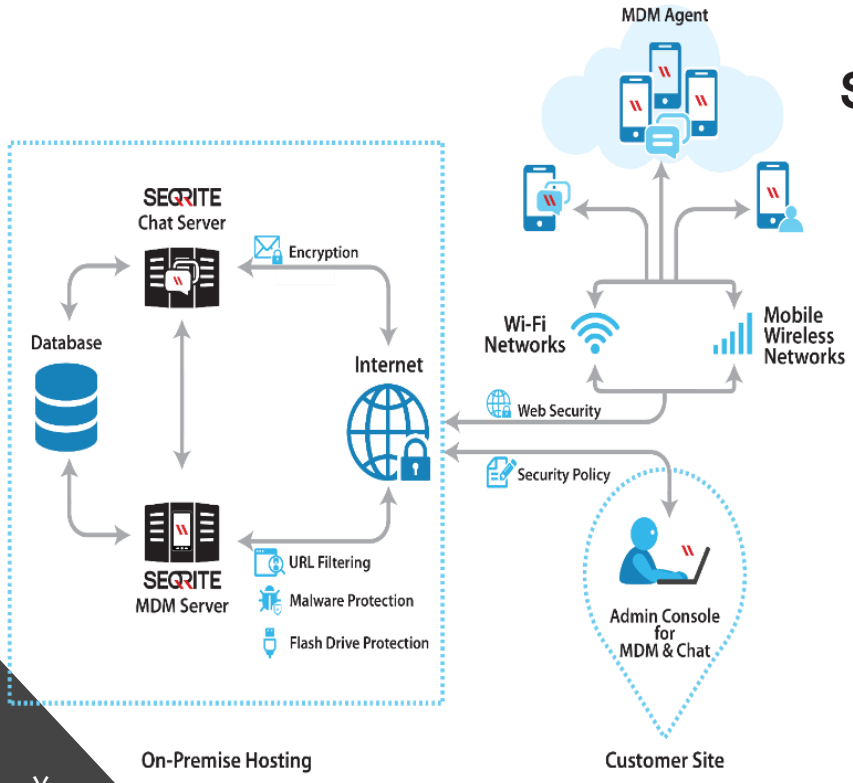


SEQRITE

Cloud

- کنسول مدیریت یکپارچه برای مانیتورینگ و مدیریت اندپوینت سکیوریتی ها و UTMهای توزیع شده
- داشبورد قدرتمند ابری
- سیاست گذاری امنیتی
- مدیریت چند سطحی
- دسترسی همیشه و همه جا به مدیریت ابری Seqrite Endpoint Security و TERMINATOR
- اعمال سیاست های متمرکز سازمان
- پشتیبان گیری از تنظیمات EPS و UTM

سامانه مدیریت یکپارچه دستگاههای همراه Mobile Device Management



SEQRITE

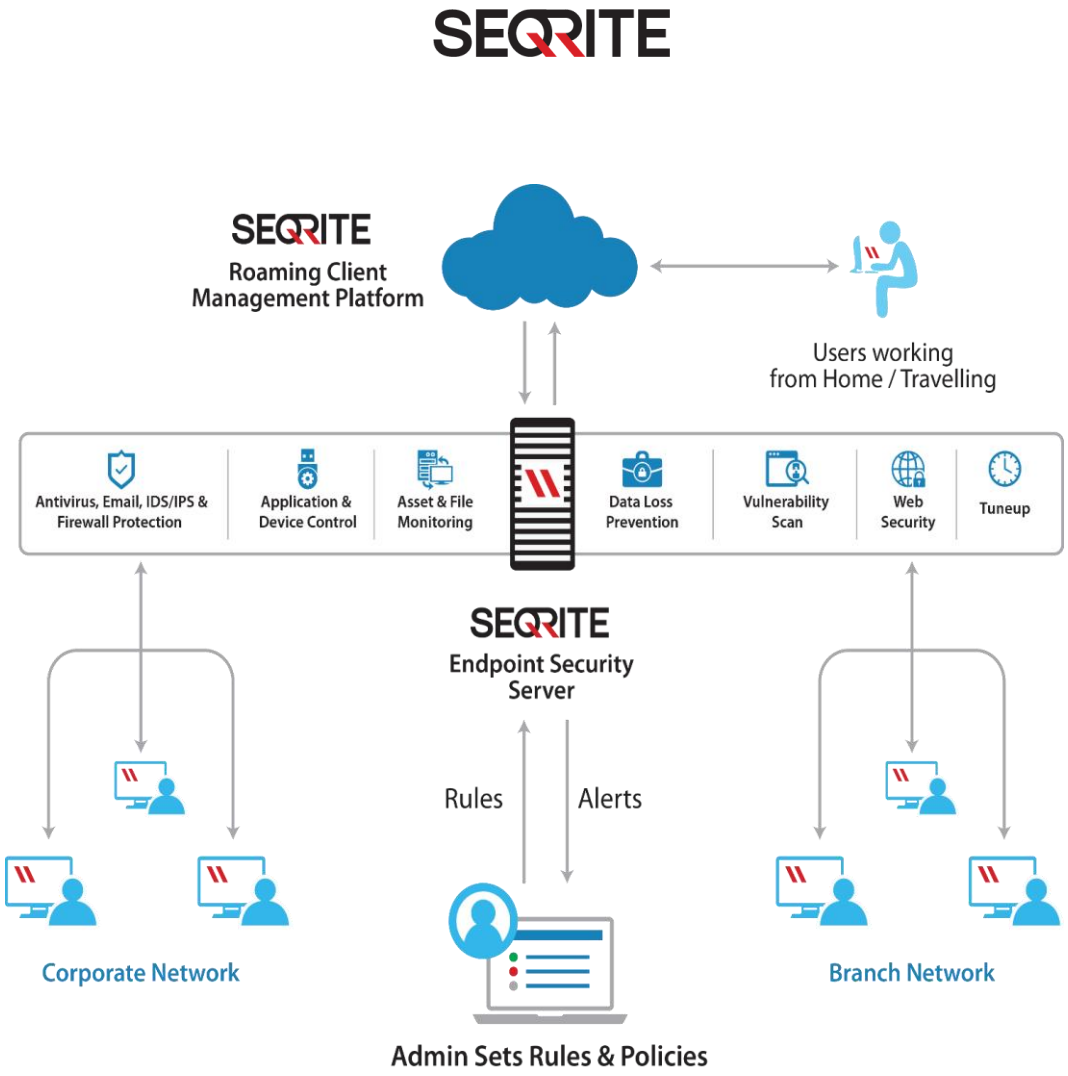
MDM

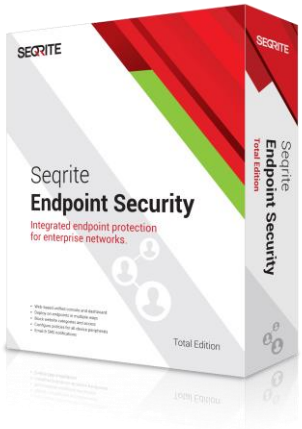
- امکان مدیریت و امن سازی موبایل کارمندان در محیط سازمانی
- کنسول مدیریتی یکپارچه مبتنی بر ابر
- کنترل برنامه
- گزارش گیری سفارشی
- مانیتورینگ و کنترل داده، SMS، تماس
- مدیریت جامع امنیتی مانند، محافظ وب، فیلترینگ وب، ضد سرقت، مکان‌یابی
- نصب، حذف و اعمال سیاستها به صورت متمرکز، خودکار و آسان

امنیت سازمانی با اندپوینت سکیوریتی Endpoint Security

Endpoint Security

- نصب، آرایش و بکارگیری آسان
- گروه بندی و سیاستگذاری کلایتها
- تولید آنلاین گزارشات آماری
- پشتیبانی همزمان از کلایتهای ویندوز، لینوکس و MAC
- سازگار با انواع پیکربندی شبکه
- آنالیز هوشمند پکت‌ها IDS/IPS
- برنامه ریزی متمرکز اسکن
- مدیریت کلایتها خارج از شبکه
- کنترل برنامه ها
- کنترل ۲۵ نوع مختلف دیوایس
- بروز رسانی مستقیم ازآپدیت سرور اصلی کوییک هیل
- محافظت از Safe Mode
- مدیریت تحت وب و متمرکز
- اسکن آسیب پذیری
- DLP جلوگیری از نشت اطلاعات سازمانی
- ثبت فعالیت فایلهای محرمانه سازمانی
- مدیریت دارایی
- مدیریت وصله
- امکان راه‌اندازی هانی پات در بستر شبکه داخلی سازمان
- و...





پشتیبانی از:

ویندوز مک لینوکس

DNAScan رفتارشناسی پیشرفته مبتنی بر ژنتیک انسانی

با فناوری بسیار پیشرفته از کاربران در برابر تهدیدهای پیچیده و ناشناخته امنیتی محافظت می کند.
ساختار باینری فایلها (استاتیک) و رفتارهای داینامیک همه پروسس های جدید سیستم را مانیتور کرده و پروسس مخرب را شناسایی آن را متوقف و همه تغییرات خرابکارانه بدافزار را به قبل برمی گرداند.

مزایا:

- محافظت از سیستم شما در برابر حملات روز–صفر
- محافظت از سیستم شما در برابر حملات هدفمند
- محافظت در برابر روتکیت های ناشناخته
- محافظت در برابر باج افزارهای ناشناخته
- شناسایی فعالیت های انواع بدافزارها مانند کلیدنگارها، تروجان ها و بات نت ها

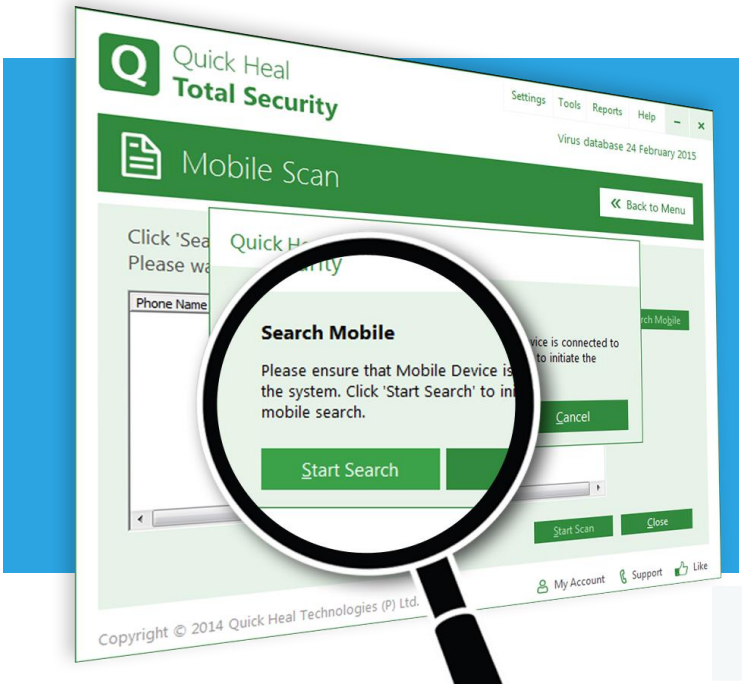
بانکداری امن Safe Banking

یک محیط مجازی کاملا امن برای محافظت تراکنشهای بانکی آنلاین، خرید و پرداخت اینترنتی در برابر همه انواع تهدیدات می سازد.

مزایا:

- وب سایت های آلوده و یا جعلی را مسدود می‌کند.
- حصول اطمینان از اینکه کاربران از سایتهای بانکداری و یا فروشگاهی امن استفاده می کنند.
- برنامه های سارق اطلاعات را مسدود می کند.
- از تغییر مسیر به وب سایت های آلوده جلوگیری می‌کند.

اسکن انحصاری موبایل PC2Mobile Scan



ویژگی انحصاری ویروسیابی گوشی‌های موبایل، PDAها، تلفن‌های هوشمند از طریق اتصال آنها با بلوتوث یا کابل به کامپیوتر و پاکسازی همزمان از وجود ویروس‌های خاص موبایل و کامپیوتری

مزایا:

- دستگاهها را از وجود ویروس و بدافزار پاکسازی می‌کند.
- از همه مدل های سیستم عامل اندروید، iOS و ویندوز پشتیبانی می کند.

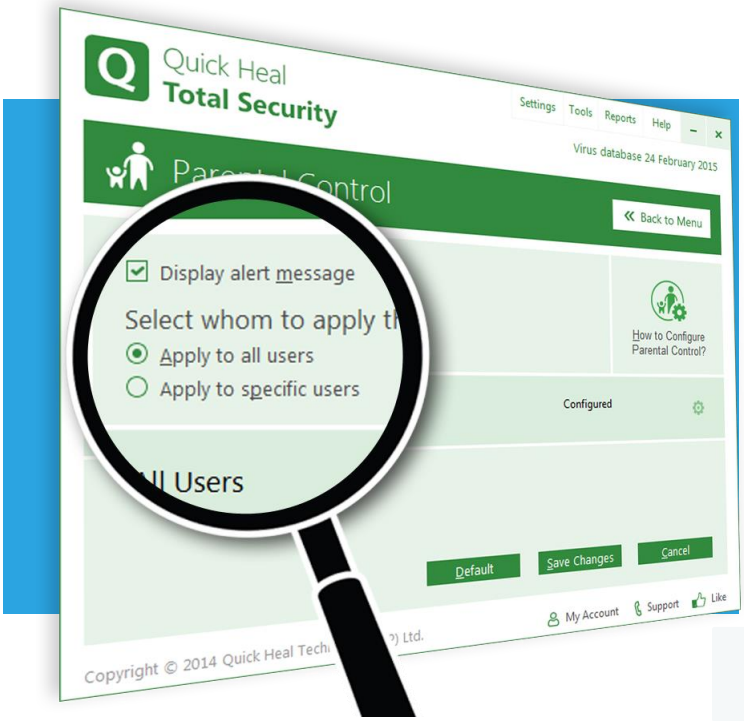
امنیت وب Web Security

فناوری مبتنی-بر-ابر، امنیت پیشگیرانه برای مقابله با تهدیدات امنیتی مبتنی بر وب فراهم و به صورت خودکار دسترسی به سایت های کلاهبردارانه و آلوده را مسدود می سازد.

مزایا:

- آنتی-فیشینگ، وب سایت هایی که اطلاعات کاربران را می ربایند، مسدود می کند.
- وب سایت هایی که می توانند به سیستم کاربران ویروس وارد کنند را مسدود می کند.
- سندباکس با ایجاد یک محیط مجازی بر روی سیستم، با اسکن و پاکسازی کلیه فایل‌های دانلود شده از انتشار تهدید به بیرون ممانعت و امکان دسترسی هکرها و بدافزارها به اطلاعات مهم مثل خرید اینترنتی با استفاده از پنل بانکی شاپرک، رمزهای عبور، اطلاعات کارت‌های بانکی و اطلاعات شخصی را مسدود می‌نماید.

کنترل خانواده Parental Control



به والدین امکان زمانبندی، مانیتورینگ و کنترل دسترسی فرزندان به اینترنت را می دهد.

مزایا:

- قفل کردن سایت های نامناسب برای فرزندان
- افزایش بهره وری اینترنت برای کودکان
- محافظت از فرزندان در برابر مجرمان آنلاین

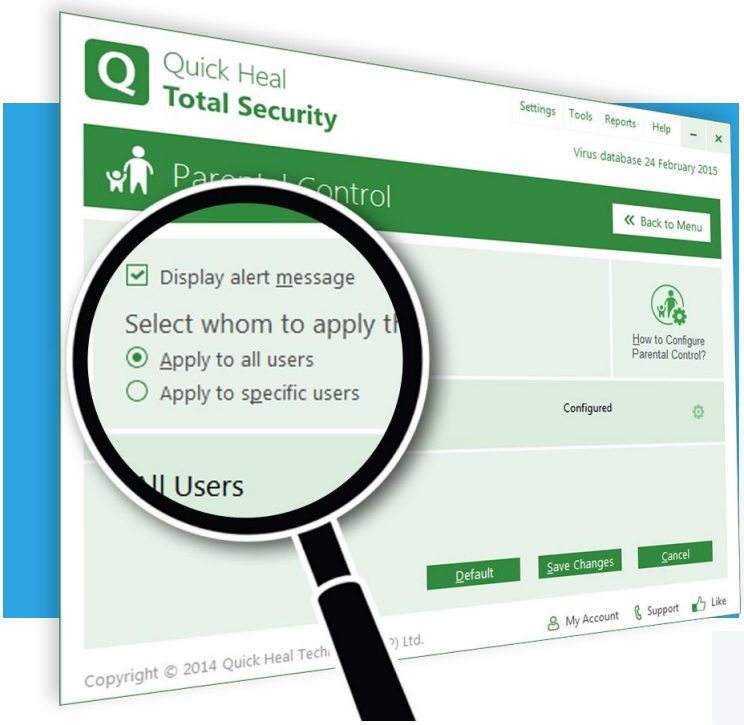
ردیابی لپ تاپ‌های گمشده Laptop Tracker

ویژگی منحصربفردی که کوییک‌هیل را برای نوت‌بوک‌ها و رایانه‌های کیفی تبدیل به یک بیمه‌نامه سرقت می‌کند.

مزایا:

- یافتن لپ‌تاپ های مسروقه همانند یک GPS مجازی برای لپ‌تاپ ها
- اعلام مکان و زمان اتصال به اینترنت به صاحب لپ‌تاپ

کنترل خانواده Parental Control



به والدین امکان زمانبندی، مانیتورینگ و کنترل دسترسی فرزندان به اینترنت را می دهد.

مزایا:

- قفل کردن سایت های نامناسب برای فرزندان
- افزایش بهره وری اینترنت برای کودکان
- محافظت از فرزندان در برابر مجرمان آنلاین

ویژگی های تکمیلی Additional features

Data Theft Protection
محافظت در برابر سرقت اطلاعات

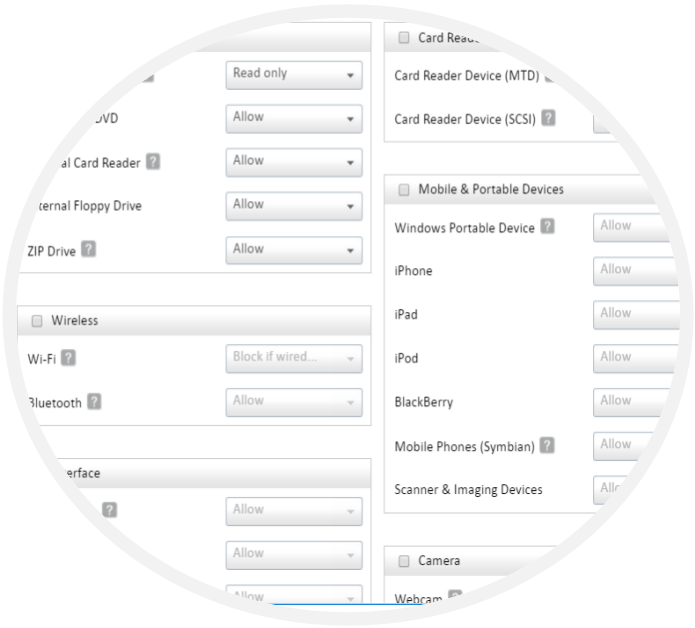
Privacy Protection
محافظت از حریم خصوصی

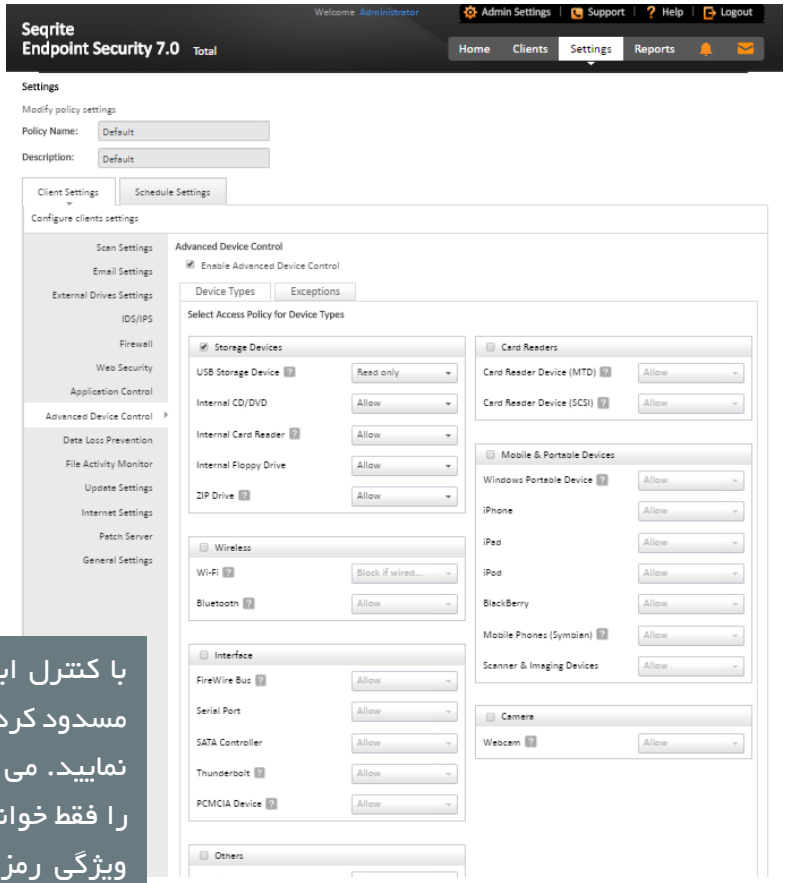
Email Security
امنیت ایمیل

Flash Drive Protection
محافظت از درایوهای فلش

محافظت کامل از همه تجهیزات شبکه و کنترل نشت اطلاعات

کنترل ابزار پیشرفته Advanced Device Control



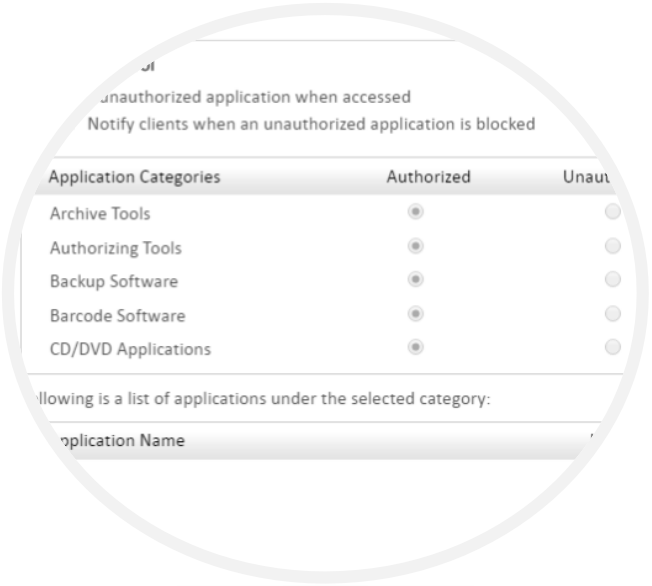


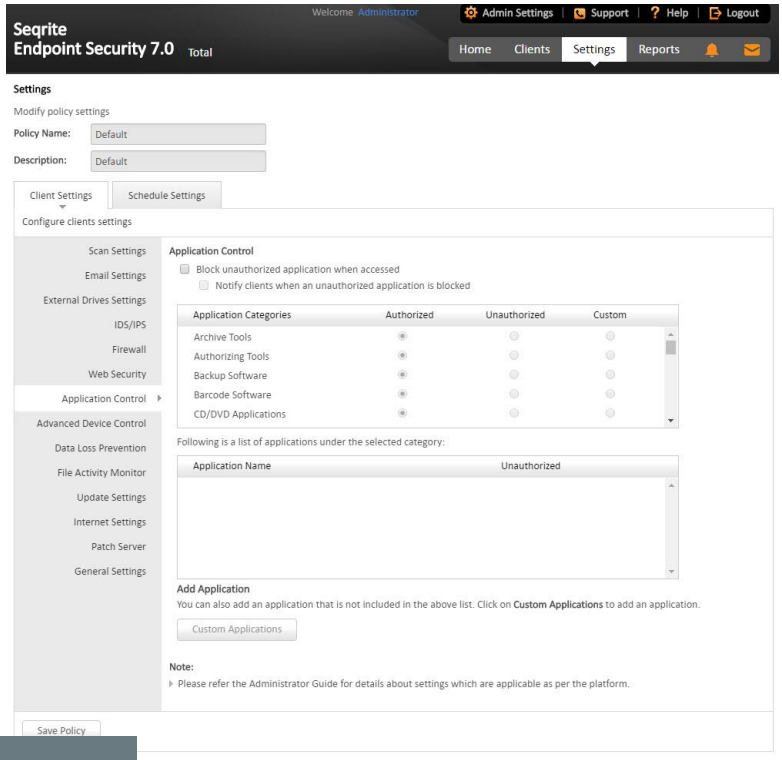
با کنترل ابزار پیشرفته می توانید دسترسی ها (مانند فقط خواندنی، مسدود کردن کامل و...) برای انواع مختلف دستگاه های جانبی پیکربندی نمایید. می توانید دسترسی به انواع ابزارهایی که در صفحه بعد آمده را فقط خواندنی و یا کاملا مسدود نمایید.

ویژگی رمزنگاری ابزار ادمین را قادر می سازد تا اجازه استفاده از ابزارهای ذخیره سازی را فقط در داخل سازمان بدهد.

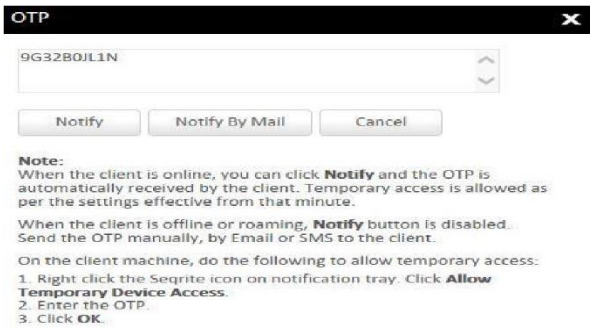
Cameras, other wireless devices, card readers,...

کنترل برنامه Application Control



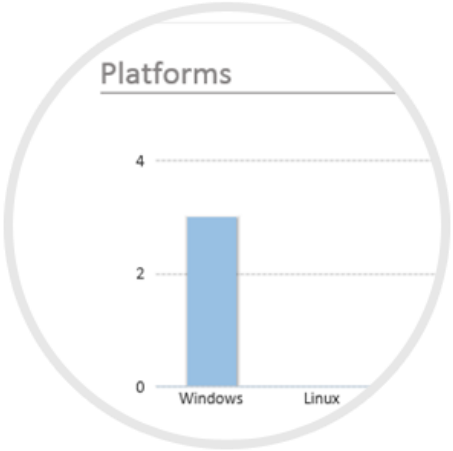


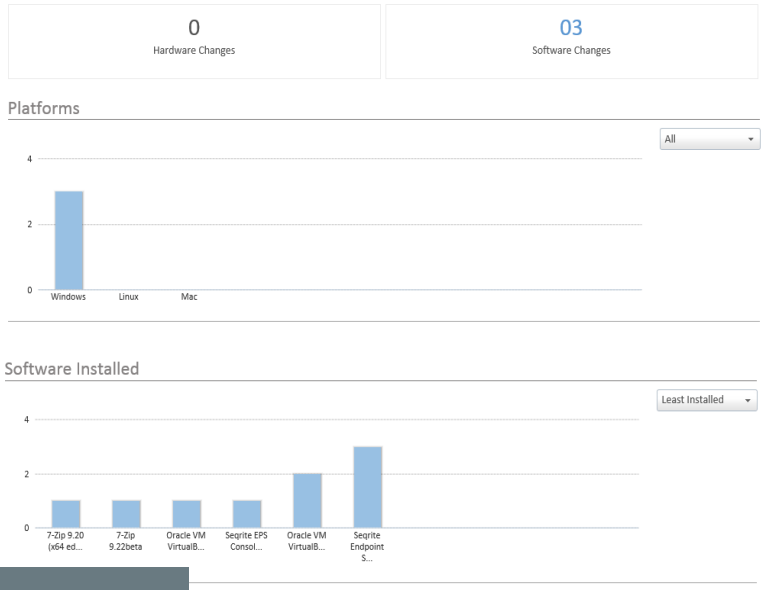
ادمین می تواند امکان اجرا و استفاده از برنامه‌ای خاص یا یک دسته از پیش تعریف شده نرم افزارها مانند اشتراک گذاری فایل، بازی و یا هر فایل اجرایی یا برنامه ی جدید که توسط ادمین معرفی می شود را در سراسر شبکه مجاز یا مسدود نماید. تغییرنام، تغییر مسیر تاثیری در اجرای سیاست های ادمین ندارد. مثل مسدود کردن برنامه های دانلود اینترنتی) مانند IDM یا تلگرام یا Babylon برای گروهی از کاربران همچنین امکان اعطای مجوز موقت استفاده از دیوایس های مسدود شده در مواقع ضروری برای کاربر خاص وجود دارد.



مدیریت دارایی

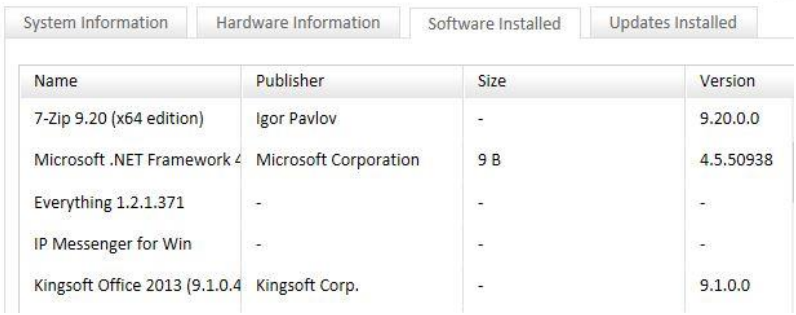
Asset Management

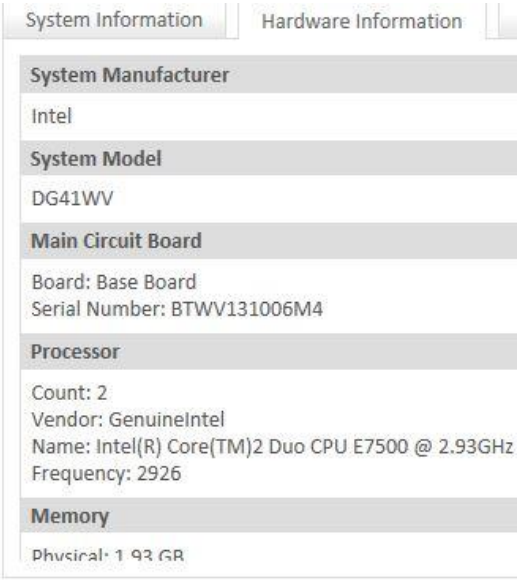




اطلاعات جامعی درباره پیکربندی سیستم، اطلاعات سخت افزاری سیستمی و نرم افزارهای نصب شده بر روی کلاینت ها ارائه می دهد. هرگونه تغییرات سخت افزاری و نرم افزاری بر روی کلاینت ها ردیابی می کند .

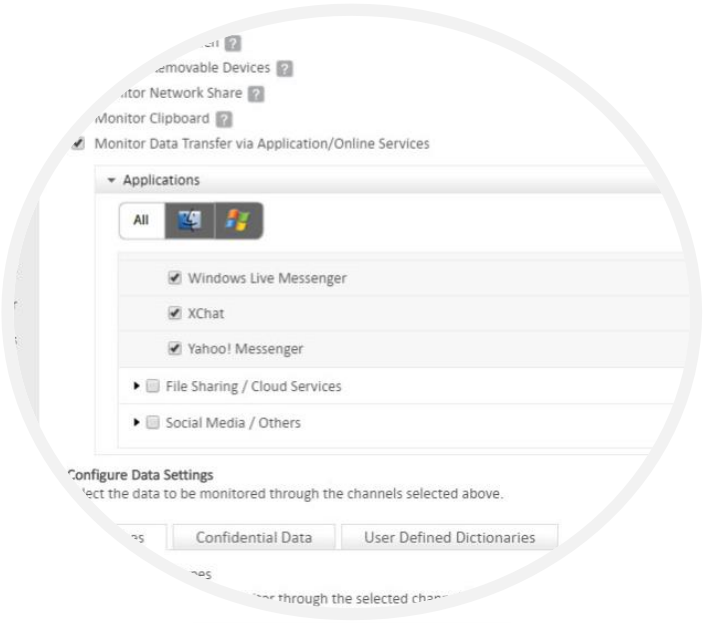
(مانند نصب برنامه Skype، یا ارتقای RAM از ۲ GB به ۴ GB و...)

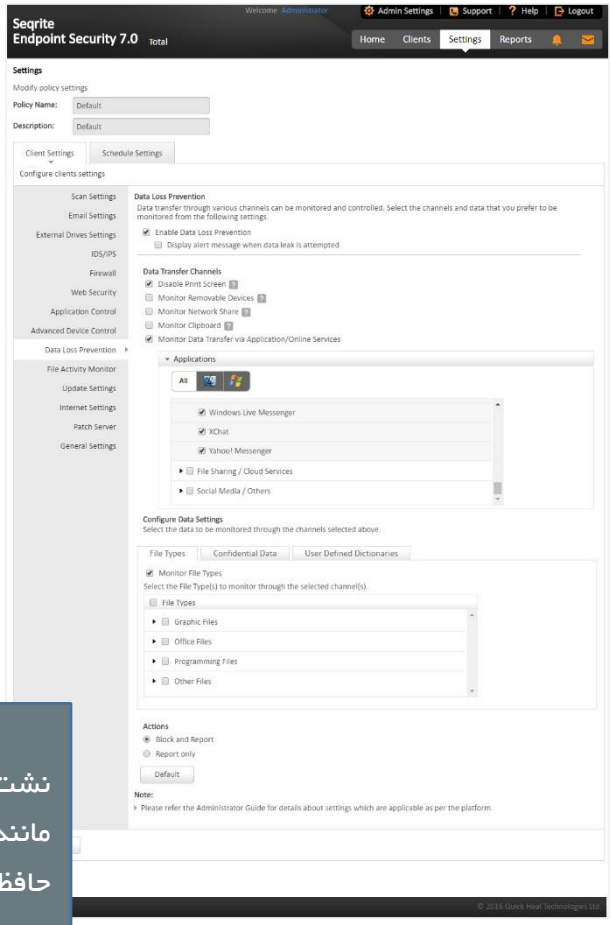




محافظت از نشت اطلاعات

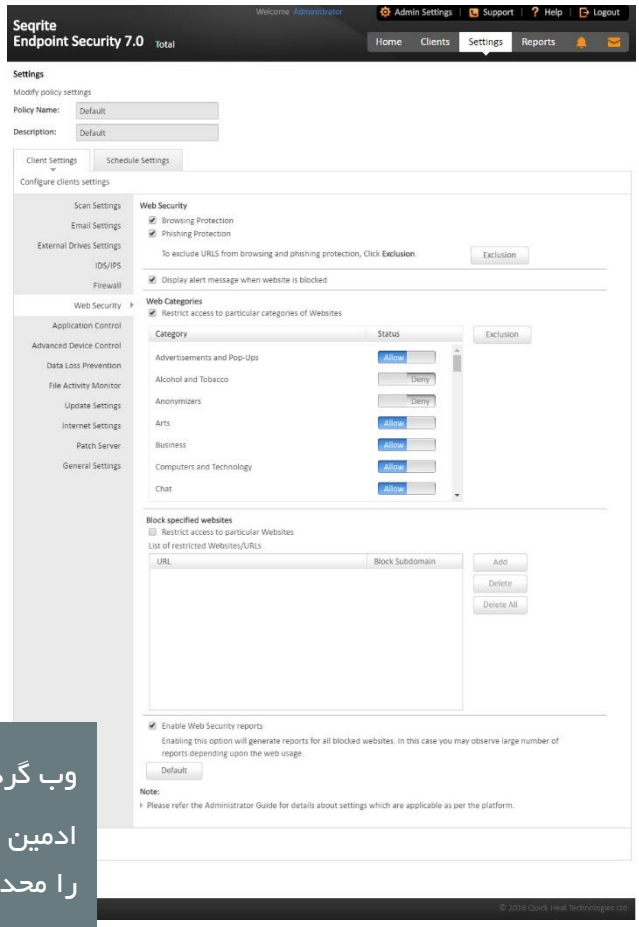
Data Loss Prevention





نشت اطلاعات حساس سازمانی به بیرون از طریق کانال های انتقال داده مانند: ابزارها و درایوهای جدا شدنی، اشتراک گذاری ها در شبکه، حافظه موقت کلیپ بورد، Print screen، برنامه های کاربردی و سرویسهای آنلاین (مانند مرورگرهای وب، برنامه های ایمیل و غیره) را مسدود می کند.

فیلترینگ وب سایت Web Content Filtering

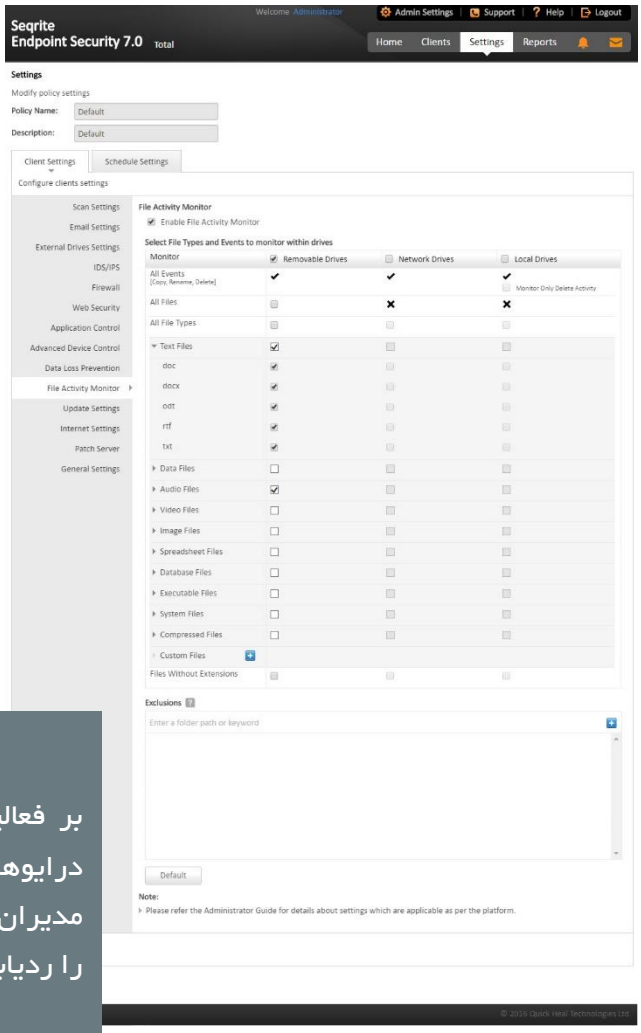


وب گردی کارمندان را مانیتور و فیلتر، بهره وری را افزایش می‌دهد.

ادمین می تواند، دسترسی به یک سایت خاص یا دسته ای وب سایت‌ها را محدود یا مسدود کند. مانند وب سایت های بازی، خبری، سرگرمی

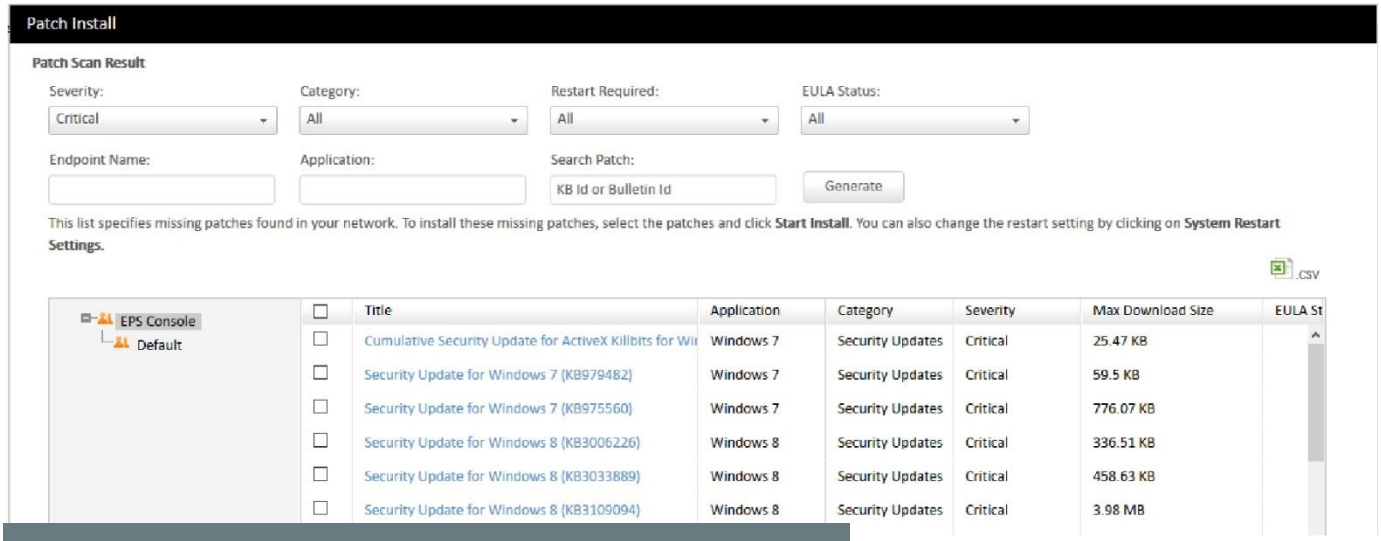
حصول اطمینان از اینکه کارمندان از شبکه ی سازمان برای دسترسی به محتویات نامناسب استفاده نمی کنند.

مانیتور فعالیت فایل File Activity Monitor



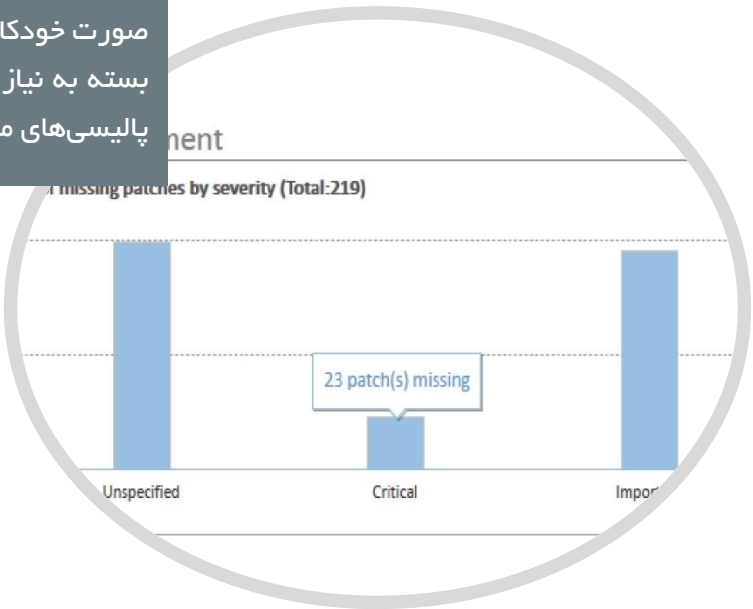
بر فعالیت های فایل مانند کپی، تغییر نام و حذف فایل ها بر روی درایوهای محلی، درایوهای قابل حمل و درایوهای شبکه نظارت می کند. مدیران شبکه به راحتی می توانند هرگونه تغییر در فایل ها در شبکه را ردیابی و ممیزی کنند.

مدیریت وصله Patch Management



مدیریت وصله، به صورت متمرکز حفره های موجود در پلتفرم سیستم عامل های ویندوز و سایر برنامه‌های کاربردی مایکروسافت را بر روی همه کلاینتهای شبکه بررسی و در صورت نیاز وصله های ضروری را به صورت خودکار نصب می کند.

بسته به نیاز سازمان، می توان مدیریت وصله ها را بر روی گروه ها و پالیسی‌های مجزا پیکربندی و اعمال کرد.



مقایسه محصولات سکورایت اندپوینت سکیوریتی

Enterprise Suite	Total	Business	SME	Features
✓	✓	✓	✓	Antivirus
✓	✓	✓	✓	Email Protection
✓	✓	✓	✓	IDS/IPS Protection
✓	✓	✓	✓	Firewall Protection
✓	✓	✓	✓	Phishing Protection
✓	✓	✓	✓	Browsing Protection
✓	✓	✓	✓	SMS Notification
✓	✓	✓	✓	Vulnerability Scan
✓	✓	✓		Asset Management
✓	✓	✓		Spam Protection
✓	✓	✓		Web Filtering
✓	✓			Advanced Device Control
✓	✓			Application Control
✓	✓			Tuneup
✓	✓			File Activity Monitor
✓	✓			Patch Management
✓				Data Loss Prevention

راهکار اختصاصی برای مقابله با باج افزارها Anti-Ransomware

اولین و تنها شرکت امنیتی که با انواع جدید و ناشناخته این نوع از بدافزارهای خطرناک به صورت پیشگیرانه محافظت می کند، ماژول ویژه برای مقابله با رشد فزاینده باج افزارها (Ransomware) توسعه داده است.


بازدید از سایت آلوده
کلیک بر روی لینک مخرب
باز کردن پیوست آلوده ایمیل
استفاده از فلش مموری های آلوده
ازطریق آسیب پذیری ترمیم نشده امنیتی
گسترش باج افزار
در سال ۲۰۱۴، یک باج افزار به نام CryptoWall بیش از ۶۰۰ میلیون کامپیوتر را آلوده و ۵ میلیارد فایل را به گروگان گرفت.
مجرمان بیش ز ۱ میلیون دلار از قربانیان اخاذی کردند.
آزمایشگاه کوییک هیل
۲۸ خانواده جدید باج افزار را در سال ۲۰۱۵ شناسایی کرد.
2015
آلودگی های باج افزار از سه ماه نخست تا سه ماه چهارم بیش از ٪۳۰۰ رشد داشته است.
٪۵۰ قربانیان باج افزارها از ترس از دست دادن اطلاعات مهم خود، باج را می پردازند.
مابقی به احتمال زیاد اگر بد افزارها فایلهای آنها را به گروگان بگیرد، وجه را می پردازند.
ضد-باج افزار کوییک هیل چه کمکی می کند؟
ماژول ضد باج افزار کوییک هیل با با یک متد شناسایی فعال، از رمزنگاری داده ها توسط باج افزار جلوگیری می کند.
"کاربر محترم! لطفا جهت بررسی اطلاعات حساب خود پیوست را دانلود کنید..."
یک ایمیل جدید از بانک !
کاربر با احساس فوری بودن نامه فایل پیوست را دانلود می کند.
خواندن ایمیل توسط کاربر
دریافت ایمیل توسط کاربر
هکر یک ایمیل بارگذار باج افزار به قربانی مورد هدف ارسال می کند.
فایل پیوست دانلود می شود. قطعات باج افزار شروع به نصب می کنند.
کوییک هیل شروع به اسکن فایل های مخرب، و اجرای آنالیز رفتار بر روی آن می کند.
باج افزار شناسایی شد!
ضد باج افزار در مورد آلوده بودن فایل به کاربر هشدار می دهد و توصیه به حذف آن می کند.
کوییک هیل با موفقیت مسدودکرد بیش از
٤٠٠ هزار حملات باج افزار
در طی دوره ۲ ماهه
(Jan - Feb, 2016)

چرا ماژول ضد-باج افزار کوییک هیل از دیگر ابزارهای ضدباج افزار موثر تر و پیشرفته تر است؟

ضد-باج افزار کوییک هیل ...

- نظارت فعالانه بر سیستم برای پیشگیری از باج افزارهای جدید

اسکن همه فایل های دانلود شده که هر یک از اجزای آنها پتانسیل تبدیل شدن به یک حمله باج افزار را دارند.

- اجرا بر روی موتور شناسایی مبتنی بر رفتار

تجزیه و تحلیل بلادرنگ چگونگی عملکرد یک برنامه، به طوری که می توان آن را قبل از هر گونه آسیب متوقف کرد.

- نگهداری یک نسخه پشتیبان از فایل های کاربر

پشتیبان گیری فعال مانع از دست دادن داده ها حتی در صورت رمزنگاری برخی از فایل ها توسط باج افزار می شود.

- تولید گزارش از تمام فایل های رمز شده

به کاربران در حفظ اطلاعات رهگیری فایل های رمزگذاری شده، کمک می کند.

- نمایش پاپ آپ اطلاع رسانی در هنگام شناسایی یک باج افزار

هشدار فوری به کاربران برای اقدام صحیح

- جلوگیری از گسترش آلودگی باج افزارها

آلودگی باج افزارهای شناسایی شده را ایزوله کرده و از گسترش آنها و انجام هر گونه آسیب جلوگیری می کند.

Quick Heal Technologies Ltd.

شرکت فناوری ارتباطات و اطلاعات فانوس

تاریخ تاسیس: ۱۳۸۲

اطلاعات تماس دفتر تهران:

(۰۲۱) ۷۷ ۱۴ ۲۵ ۲۶ و ۷۷ ۸۸ ۵۶ ۶۵

(۰۲۱) ۴۳ ۸۵ ۸۵ ۸۰

اطلاعات تماس دفتر مازندران:

(۰۱۱) ۴۲۰ ۴۹ ۳۰۰ و ۴۲۰ ۴۹ ۳۳۳ و ۷۲۲ ۴۲

(۰۱۱) ۴۲۰ ۳۸ ۱۷۹

www.quickheal.co.ir

info@qhi.ir | info@fanoos.ir

3000 46 25

@fanoosict