ENDPOINT PROTECTOR | by CoSoSys

جلوگیری از نشت اطلاعات و مدیریت دستگاه های موبایل

مناسب برای شبکه در هر اندازه و در هر صنعتی

برای Winodws، Mac و Linux

محافظت از تمامی شبکه

ENDPOINT PROTECTOR | by CoSoSys

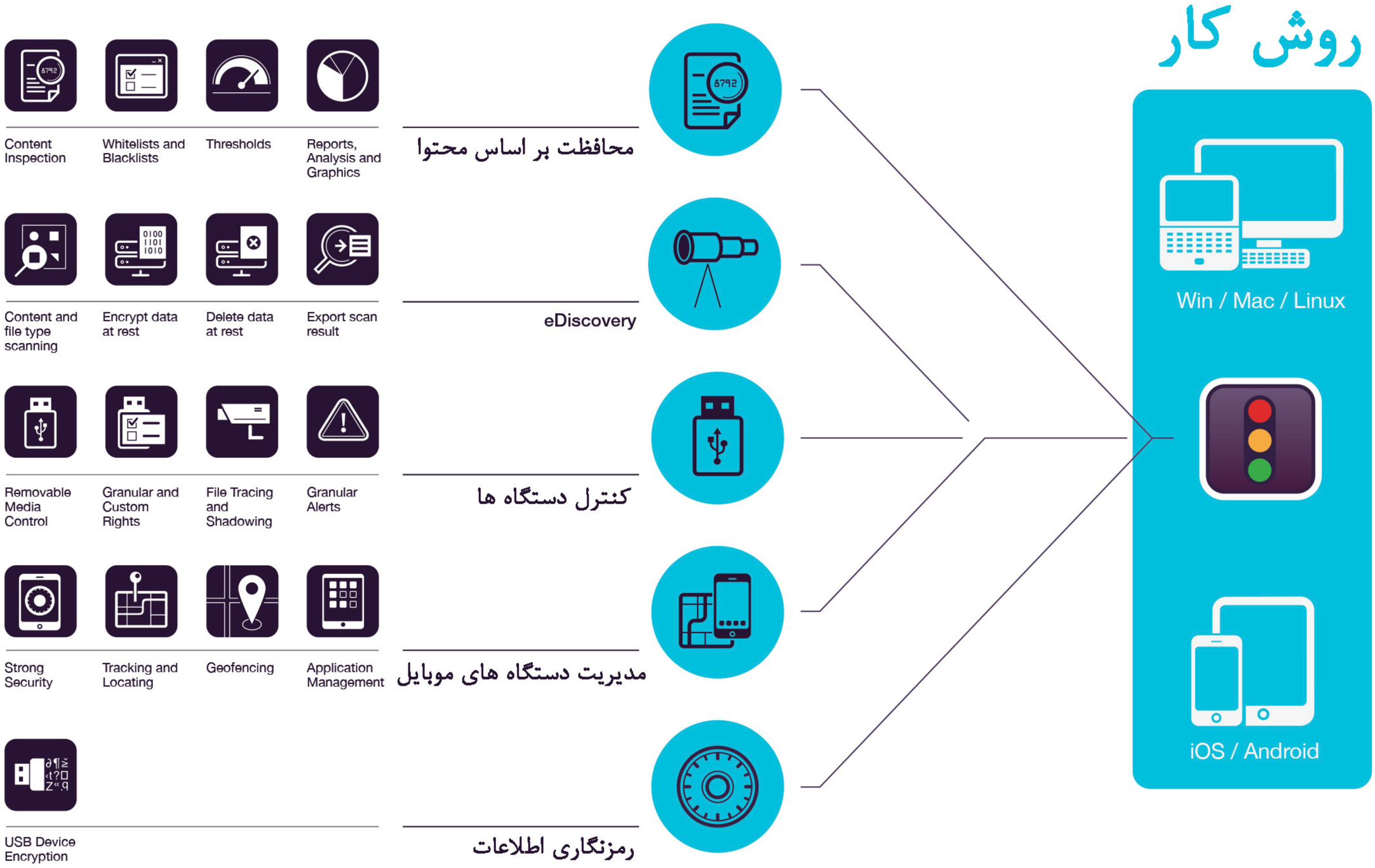
راهکاری حرفه ای برای امنیت اطلاعات، در برابر خطرات دستگاه های ذخیره سازی خارجی، سرویس های ابری و دستگاه های موبایل

در جهانی که دستگاه های قابل حمل، شیوه زندگی و ابعاد زندگی ما را تغییر داده اند، Endpoint Protector برای محافظت از اطلاعات محرمانه در برابر تهدیدات داخلی طراحی شده است، در حالی که بهره وری را حفظ نموده و کار را راحت، امن و لذت بخش تر نماید.

روش های مبتنی بر لیست سیاه و سفید، انعطاف پذیری در ایجاد سیاست ایجاد می نمایند. سازمان ها می توانند استفاده از دستگاه های قابل حمل خاص و انتقال داده ها به برنامه های کاربردی اشتراک گذاری مبتنی بر ابر و سایر سرویس های آنلاین را منع کنند، اما اجازه انتقال به URL های خاص و نام دامنه برای برخی از کامپیوتر ها / کاربران / گروه ها، را صادر نموده تا از وقفه در کار سازمان اجتناب نماید.

Endpoint Protector به صورت سخت افزار و یا دستگاه مجازی ارائه می شود، می تواند در عرض چند دقیقه تنظیم شود. علاوه بر این، رابط مدیریتی آن اجازه می دهد تا مدیریت سیاست ها و چک کردن گزارش از هر دستگاه، از دسکتاپ تا تبلت امکان پذیر باشد. Endpoint Protector به طور چشمگیری خطرات ناشی از تهدید داخلی را کاهش می دهد که می تواند منجر به نشت، ربودن و یا در معرض خطر قرار گرفتن اطلاعات شود. علاوه بر این، هماهنگی با قوانین و مقررات مختلف نیز برآورده شده است.

روش کار



محافظت بر اساس محتوا
برای Windows، macOS و Linux

نظارت و کنترل داده ها در حال حرکت، تصمیم گیری در مورد فایل هایی که می توانند یا نمی توانند شرکت را از طریق نقاط خروجی مختلف ترک کنند. فیلترها را می توان بر اساس نوع فایل، برنامه، محتوای سفارشی و یا از پیش تعریف شده، Regex و موارد دیگر تنظیم کرد.

eDiscovery
برای Windows، macOS و Linux

اسکن داده ها در نقطه های پایانی در شبکه و انجام اقدامات ضروری مانند رمزگذاری یا حذف فایل در مواردی که داده های محرمانه بر روی رایانه های غیر مجاز شناسایی می شوند.

کنترل دستگاه ها
برای Windows، macOS و Linux

نظارت و کنترل دستگاه ها و پورت های USB. امکان تعریف انواع دسترسی بر اساس نوع دستگاه، کاربر، گروه، کامپیوتر و ...

مدیریت دستگاه های موبایل
برای iOS، Android و macOS

سطح امنیت روی گوشی های هوشمند و تبلت ها را مدیریت، کنترل و تنظیم کنید. امکان ارسال تنظیمات امنیتی، تنظیمات شبکه، تنظیمات برنامه ها و ...

رمزنگاری اطلاعات
برای Windows و macOS

به طور خودکار، اطلاعات روی دستگاه های ذخیره سازی خارجی را با استفاده از الگوریتم AES 256 رمز گذاری کنید. امکان استفاده در پلتفرم های مختلف، بسیار آسان و کاربردی.

محافظت بر اساس محتوا

برای Windows، macOS و Linux

ایمیل مشتریان: Lotus Notes / Thunderbird / Outlook • مرورگرهای وب: IE / Firefox / Chrome / Safari • پیام رسان: Yahoo messenger / Microsoft Communicator / Skype • خدمات ابر و به اشتراک گذاری فایل: Dropbox / Kazaa / BitTorrent / SkyDrive / iCloud • دیگر برنامه ها Windows DVD / Samsung Kies / Applic iTunes Maker / Total Commander / Team Viewer • دیگران

فیلتر محتوای از پیش تعریف شده
فیلترها را می توان بر اساس محتوای از پیش تعریف شده ای مانند شماره کارت های اعتباری و غیره تعریف نمود.

فیلتر محتوای سفارشی
فیلترها را می توان بر اساس محتوای سفارشی مانند کلمات کلیدی و عبارات ایجاد کرد. دیکشنری های مختلف از کلمات و عبارات را می توان ایجاد کرد.

فیلتر عبارات با قاعده
فیلترهای پیشرفته سفارشی را می توان برای پیدا کردن یک توالی خاص در داده های منتقل شده در سراسر شبکه محافظت شده استفاده نمود.

فیلتر بر اساس نوع فایل
فیلترهای نوع فایل را می توان برای جلوگیری خروج اسناد خاص براساس فرمت آنان استفاده کرد، حتی اگر به صورت دستی توسط کاربران تغییر داده شود.

لیست سفید فایل ها
در حالی که تمام تلاش های دیگر انتقال فایل ها مسدود شده است، لیست سفید می تواند ایجاد شود تا از افزونگی جلوگیری شود و بهره وری افزایش یابد.

لیست سفید دامنه ها و URL ها
پیاده سازی سیاست های شرکت، اما به کارکنان اجازه می دهد که انعطاف پذیری لازم را جهت انجام کارهای خود داشته باشند. پورتال شرکت یا آدرس های ایمیل را درون لیست سفید قرار دهید.

مسدود نمودن Print Screen
لغو قابلیت ضبط صفحه نمایش و اطمینان از عدم خروج اطلاعات ارزشمند نمایش داده شده روی صفحه نمایش، از شبکه محافظت شده.

نظارت بر Clipboard
از بین بردن نشت اطلاعات حساس از طریق کپی و چسباندن / برش و چسباندن، افزایش امنیت اطلاعات بیشتر.

گزارش ها و تحلیل ها
نظارت بر فعالیت های مربوط به انتقال فایل ها با ابزار گزارشگیری و تحلیل قدرتمند. گزارش ها و وقایع همچنین می توانند به راه حل SIEM صادر شوند.

داشبورد و گرافیک
برای یک مرور کلی بصری در مورد رویدادهای مهم و آمارها، گرافیک و نمودارها در دسترس هستند

Active Directory
از AD یا ابزارهای مشابه استفاده کنید، و در سازمان های بزرگتر پیاده سازی را ساده تر کنید. وارد کردن و همگام سازی تمام گروه ها و کاربران.

آستانه های مختلف برای فیلتر ها
تعریف کنید انتقال چه تعداد فایل مجاز است. این تعاریف هم بر روی یکایک آنها قابل تعریف است و هم به صورت مجموع تعداد تخلف های صورت

رهگیری فایل
ضبط انتقال فایل ها و یا تلاش های صورت گرفته برای انتقال از طریق برنامه های کاربردی مختلف آنلاین و سرویس های ابر، یک دید کلی از اقدامات کاربران را ارائه می کند.

نمونه برداری فایل
یک نسخه از فایل هایی که به دستگاه های کنترل شده یا از طریق ایمیل، فضای ذخیره سازی ابری یا سایر برنامه ها منتقل شده اند، ذخیره می کند.

گذرواژه موقت آفلاین
به طور موقت اجازه انتقال به رایانه های قطع شده از شبکه را می دهد. اطمینان از امنیت و بهره وری.

ایجاد ایمیل های هشدار
ایمیل های از پیش تعریف شده و سفارشی می تواند برای ارائه اطلاعات در مورد مهم ترین رویدادهای مربوط به انتقال فایل های محرمانه تنظیم شود.

DLP برای پرینترها
اعمال سیاست ها برای چاپگرهای محلی و شبکه برای جلوگیری از چاپ اسناد محرمانه و جلوگیری از سرقت و از دست دادن اطلاعات.

سیاست های محافظت آگاه HIPAA
اسکن عمیق اسناد قبل از انتقال برای PHIinfo، داروهای مورد تایید FDA و کدهای ICD-9 و غیره ساخته شده است.

DLP برای Thin Client ها
حفاظت از داده ها در سرورهای ترمینال و جلوگیری از از دست رفتن اطلاعات در محیط های Thin Client مثل هر نوع دیگر از شبکه.

ویژگی های بیشتر

بسیاری از ویژگی های دیگر نیز در دسترس هستند.

info@endpointprotector.com

eDiscovery
برای macOS، Windows و Linux

نـوع فایـل: فایـل هـای گرافیکـی / فایـل هـای اداری / فایـل هـا بایگانـی / فایـل هـای برنامـه نویسـی / فایـل هـای رسـانه ای، و غیـره • محتویـات از پیـش تعریـف شـده: کارت هـای اعتبـاری / اطلاعـات شناسـایی شـخصی / آدرس / SSN / شناسـه / گذرنامـه / شـماره تلفـن / شناسـه مالیـات / شـماره تامیـن اجتماعـی و غیـره • محتـوای قابـل تعریـف / نـام فایـل / عبـارات منظـم / HIPAA

اسکن بر اساس محتوا و نوع فایل
ایجـاد سیاسـت هـای سفارشـی eDiscovery بـرای تعییـن نوع محتوایـی کـه بـرای سـازمان شـما حسـاس اسـت بسـته بـه نـوع فایـل، محتـوای پیـش فـرض، محتـوای سفارشـی، نـام فایـل، محتـوای محافظـت شـده بـا Regex یـا HIPAA تعییـن مـی شـود. شـروع بـه اسـکن کـردن اطلاعـات حسـاس بـا توجه به محتوای انتخاب شده.

رمزگذاری داده ها
هنگامـی کـه داده هـای محرمانـه یافـت مـی شـود، گزینـه ای بـرای رمزگـذاری آن بـا راهـکار رمزنـگاری قـوی AES 256 در دسـترس اسـت تـا از دسترسـی کارمنـدان غیرمجـاز جلوگیـری شود و امکان نشت داده ها را متوقف کند.

پاک کردن داده ها
محافظـت از اطلاعـات و اطمینـان از انطبـاق بـا مقـررات صنعـت بـا حـذف اطلاعـات حسـاس بلافاصلـه بعـد از شناسـایی آن اگـر خط مشی شرکت را نقض می کند.

صادر نمودن نتایج اسکن
نتایج اسکن برای صادر کردن در فایل های اکسل، PDF یا CSV در دسـترس هسـتند و مـی تواننـد بعنـوان گـزارش بـرای مدیریـت یـا اسـناد ممیـزی اسـتفاده شـوند. نتایـج اسـکن، جزئیـات مربـوط بـه اینکـه اطلاعـات حسـاس در چـه رایانـه یافـت شـد، چـه اطلاعـات حساسـی، مسـیر، زمـان کشـف، اگـر فایـل رمزگـذاری شـده، حـذف شـده و یـا گـزارش شـده باشـد و سـایر اطلاعات ارزشمند را ارائه می دهد.

لیست سیاه بر اساس نوع فایل
لیسـت سـیاه نـوع فایـل را مـی تـوان بـرای شناسـایی اسـناد خـاص ذخیـره شـده در نقـاط انتهایـی شـبکه اسـتفاده کـرد: فایـل هـای گرافیکـی، فایـل هـای اداری، فایـل هـای بایگانـی، فایل های برنامه نویسی و بسیاری دیگر.

لیست سیاه محتوا از پیش تعریف شده
اطلاعـات موجـود بـر روی لیسـت سـیاه فهرسـت محتـوا ماننـد شـماره کارت اعتبـاری، شـماره هـای امنیـت اجتماعـی، اطلاعـات شـخصی و سـایر اطلاعـات را اضافـه کنیـد و کشـف کنیـد کـه در آنهـا کجـا ذخیـره شـده انـد و اگـر خـط مشـی شـرکت را نقـض مـی کنـد. ایـن لیسـت سـیاه مـی توانـد بـه اطمینـان از انطبـاق با مقررات مانند HIPAA، PCI DSS و دیگران کمک کند.

لیست سیاه محتوای سفارشی
یـک لیسـت سـیاه براسـاس محتـوای سفارشـی ماننـد کلمـات کلیـدی و عبـارات ایجـاد کنیـد. واژه نامـه هـا مـی تواننـد از طریـق تایـپ کـردن، Copy / Paste و یـا Import کـردن ایجاد شوند.

لیست سیاه بر اساس نام فایل
جسـتجو بـرای فایلـی خـاص بـر اسـاس نـام آن و ردیابـی مـکان آن. نتایـج در نتایـج اسـکن eDiscovery نمایـش داده مـی شـوند با لیسـت فایـل هـای یافـت شـده و اقداماتـی ماننـد حـذف، رمزگذاری یا رمزگشایی قابل انجام می باشد.

لیست سیاه عبارات با قاعده
لیسـت سـیاه سفارشـی را مـی تـوان بـرای پیـدا کـردن قاعـده ای خاصـی در داده هـای ذخیـره شـده در شـبکه محافظـت شـده ایجاد کرد.

داده های محافظت شده HIPAA
اجازه می دهد تا اسکن در نقاط پایانی برای اطلاعات PHI، داروهای مـورد تاییـد FDA، کدهـای ICD-10 و ICD-9 ، و غیـره انجـام پذیـرد. مطابقـت با قوانین HIPAA و تشـخیص مکانـی که اطلاعات بهداشـتی قانونـی محفـوظ مـی باشـد و در صـورت لـزوم انجـام اقدامات لازم برای محافظت از اطلاعات.

آستانه ها
بـا اسـتفاده از تعریـف آسـتانه هـا، از اسـکن بیـش از حـد اجتنـاب کنیـد. شـما مـی توانیـد تعییـن کنیـد بـا توجـه بـه تعـداد مشـخصی از تخلفـات بازرسـی بایـد متوقـف شـود و یـا بـا توجـه به حداقل اندازه فایل چه فایلی باید اسکن شود.

لیست سفید فایل های MIME
حـذف فایـل هـای MIME از اسـکن کـردن، اضافـه کـردن آنها به لیسـت سـفید، بـرای جلوگیـری از افزونگـی و افزایـش بهـره وری. به راحتی سیاست های eDiscovery را مدیریت کنید.

لیست سفید فایل های مجاز
آپلـود فایـل هـا در لیسـت سـفید بـه عنـوان اسـتثنا از سیاسـت هـای اسـکن کـه در eDiscovery تعییـن شـده اسـت. صـرف نظـر از ایـن کـه سیاسـت بـر اسـاس نـوع فایـل، محتـوای پیـش فـرض ، محتـوای سفارشـی و غیـره تعریـف شـده باشـد، فایـل هایـی کـه در لیسـت سـفید اضافـه شـده انـد از اسـکن حـذف می شوند.

ویژگی های بیشتر
بسیاری از ویژگی های دیگر نیز در دسترس هستند.
info@endpointprotector.com

کنترل دستگاه

برای Windows، macOS و Linux

درایوهای USB / چاپگرها / دستگاه های بلوتوث / پخش کننده های MP3/ هارد دیسک اکسترنال / Teensy Board / دوربین های دیجیتال / وب کم / تاندربولت / PDA / مسیرهای به اشتراک گذاری شبکه / iPod / iPhone / FireWire / درایورهای ZIP / پورت سریال / دستگاه های ذخیره سازی PCMCIA / دستگاه های بیومتریک / غیره

تنظیم حقوق در سطح جهانی
به طور پیش فرض، حقوق تعریف شده در این سطح از طریق شبکه به همه دستگاه ها اعمال می شود. با این حال، ماژول گزینه های بسیار زیادی دارد.

تنظیم حقوق بر اساس گروه
حقوق دستگاه می تواند به صورت جزئی بر اساس گروه ها تنظیم شود و اجازه دسترسی متفاوت به بخش های مختلف را می دهد.

تنظیم حقوق بر اساس کامپیوترها
حقوق دستگاه را می توان بر اساس کامپیوترها ایجاد کرد. هنگامی که رایانه ها نقش منحصر به فردی در سازمان ایفا می کنند مفید است.

تنظیم حقوق بر اساس کاربران
بر اساس نقش ها و وظایف آنها، هر کاربر می تواند حقوق دسترسی به دستگاه های مختلف را با توجه به سیاست های شرکت دریافت کند.

تنظیم حقوق بر اساس دستگاه
جزئیات دقیق حقوق می تواند بر اساس شناسه فروشنده، شناسه محصول و شماره سریال دستگاه باشد.

کلاس های سفارشی
حقوق را می توان بر اساس کلاس های دستگاه ایجاد کرد که مدیریت محصولات یک شرکت را ساده تر می کند.

دستگاه های مورد اطمینان
برای دستگاه های رمز شده، دسترسی های مختلف دسترسی می تواند بر اساس سطح رمزگذاری (نرم افزار، سخت افزار، و غیره) تعریف شود.

رهگیری فایل ها
ضبط همه انتقال فایل ها یا تلاش های انجام شده برای دستگاه های مختلف ذخیره سازی USB، ارائه یک دید کلی از اقدامات کاربران را فراهم می آورد.

نمونه برداری فایل ها
یک نسخه از فایل هایی که به دستگاه های کنترل شده منتقل شده اند را ذخیره می نماید و بعدا می توانند برای اهداف حسابرسی مورد استفاده قرار گیرند.

گذرواژه موقت آفلاین
به طور موقت اجازه دسترسی دستگاه به کامپیوتر قطع شده از شبکه را می دهد. اطمینان از امنیت و بهره وری.

ایجاد ایمیل های هشدار
ایمیل های از پیش تنظیم شده و هشدارهای سفارشی را می توان برای ارائه اطلاعات در مورد مهم ترین وقایع مربوط به استفاده از دستگاه ها تنظیم کرد.

داشبورد و نمودارها
برای یک مرور کلی بصری در مورد رویدادهای مهم و آمارها، گرافیک و نمودارها در دسترس هستند.

گزارش ها و تحلیل ها
نظارت بر فعالیت های مربوط به استفاده از دستگاه ها با ابزار گزارشگیری و تحلیل قدرتمند. گزارش ها و وقایع نیز می توانند صادر شوند.

ویژگی های بیشتر
بسیاری از ویژگی های دیگر نیز در دسترس هستند.
info@endpointprotector.com

رمزنگاری

برای Windows و macOS

رمزنگاری USB
مجاز کردن فقط دستگاه های USB رمزگذاری شده و اطمینان از اینکه همه داده های کپی شده در دستگاه های ذخیره سازی قابل جابجایی، به صورت خودکار محافظت می شوند.

مکانیسم های امنیتی قوی
رمزگذاری AES 256-bit، حفاظت از رمز عبور و تکنیک های ضد جعل را برای اطمینان از صحت برنامه کاربردی انجام می دهد.

گذرواژه اصلی
ایجاد یک رمزعبور اصلی، تداوم در شرایط مختلف مانند بازنشانی رمز عبور کاربر را فراهم می کند.

ویژگی های بیشتر
رمزنگاری همچنین برای محیط های ذخیره سازی ابری، فولدرهای محلی، CD و DVD قابل اجرا می باشد.
info@endpointprotector.com

مدیریت دستگاه های موبایل

برای Android، iOS و macOS

نصب از راه دور برای iOS و Android
دستگاه ها می توانند از راه دور از طریق پیامک، ایمیل، لینک URL یا کد QR ثبت نام کنند. بهترین راه برای شبکه خود را انتخاب کنید.

ثبت نام به صورت انبوه
برای یک فرآیند استقرار کارآمد، می توان تا ۵۰۰ گوشی و تبلت را در یک زمان ثبت نام کرد.

قفل از راه دور
از راه دور قفل فوری دستگاه تلفن همراه در صورت بروز هر گونه حادثه مرتبط فعال کنید. از نشت داده ها به علت گم شدن دستگاه ها اجتناب کنید.

رهگیری و تعیین محل
بر دستگاه های تلفن همراه شرکت نظارت کنید و در همه زمان ها از موقعیت داده های حساس شرکت مطلع باشید.

غیرفعال کردن قابلیت های داخلی
کنترل مجوز برای ویژگی های داخلی مانند دوربین، اجتناب از نقض داده ها و از دست دادن اطلاعات حساس.

پخش صدا برای پیدا کردن دستگاه های گمشده
مکان یابی یک دستگاه تلفن همراه گمشده با راه اندازی یک زنگ با صدای بلند تا زمانی که یافت شود (فقط برای اندروید پشتیبانی می شود).

مدیریت برنامه های دستگاه های موبایل
با توجه به سیاست های امنیتی سازمان، برنامه ها را مدیریت کنید. فورا برنامه های رایگان و پرداختی را برای تلفن های همراه ثبت نام شده ارسال کنید.

ارسال تنظیمات شبکه
تنظیمات شبکه مانند تنظیمات ایمیل، Wi-Fi و VPN را ارسال کنید یا آنها را غیرفعال کنید، از جمله بلوتوث، حالت زنگ و غیره را تنظیم کنید.

هشدارها
هشدارهای از پیش تعریف شده در دسترس هستند، همچنین گزینه ای برای تنظیم هشدارهای سفارشی سیستم نیز موجود می باشد.

گزارش ها و تجریه و تحلیل
نظارت بر فعالیت های کاربران، مربوط به استفاده از دستگاه با ابزار قدرتمند گزارشگری و تجزیه و تحلیل. گزارش ها و وقایع نیز می توانند صادر شوند.

حالت Kiosk با Samsung Knox
قفل کردن یا قرار دادن دستگاه تلفن همراه در برنامه های خاص. از راه دور موارد امنیتی بر روی تلفن همراه اجرا می شوند و آنها را به دستگاه های اختصاصی تبدیل می کند.

مدیریت macOS
برای گسترش ویژگی های DLP، مکینتاش نیز می تواند در ماژول MDM ثبت شود و از گزینه های مدیریت اضافی استفاده کند.

اعمال رمز عبور
با اجرای سیاست های رمز عبور قوی، حفاظت پیشگیرانه از اطلاعات مهم ذخیره شده شرکت در دستگاه های تلفن همراه را اجرا نمایید.

پاک کردن از راه دور
برای شرایط بحرانی که تنها راه جلوگیری از نشت داده ها پاک کردن دستگاه است، این امر به راحتی می تواند از راه دور انجام شود.

سیاست مبتنی بر موقعیت
یک محدوده را در یک منطقه جغرافیایی تعیین کنید، کنترل بیشتری بر سیاست های MDM که در این منطقه خاص اعمال می شود داشته باشید.

محدودیت های iOS
اطمینان حاصل کنید که فقط استفاده از کسب و کار امکان پذیر است. در صورت عدم پذیرش با سیاست های شرکت، iCloud، Safari، App Store و غیره را غیرفعال کنید.

اعمال Vcard بر روی Android
مخاطبین را برای دستگاه های تلفن همراه اندروید اضافه کنید و آنها را اعمال کنید و مطمئن شوید که نیروی کار همراه شما به سرعت می تواند با افراد مناسب ارتباط برقرار کند.

نظارت بر برنامه ها
می دانید کارکنان شما چه برنامه هایی را بر روی دستگاه های تلفن همراه خود دانلود می کنند، قرار دادن یک مرز دائمی بین کار و اوقات فراغت.

مدیریت دارایی
به دست آوردن بینش در دستگاه تلفن همراه در مورد نام ، نوع، مدل، ظرفیت، نسخه های سیستم عامل، اپراتور، IMEI، MAC و غیره

ایجاد ایمیل های هشدار
ایمیل های هشدار را می توان برای ارائه اطلاعات در مورد مهم ترین وقایع مربوط به استفاده از دستگاه های تلفن همراه تنظیم کرد.

داشبورد و نمودارها
برای یک مرور کلی بصری در مورد رویدادهای مهم و آمارها، گرافیک و نمودارها در دسترس هستند.

ویژگی های بیشتر
بسیاری از ویژگی های دیگر نیز در دسترس هستند.
info@endpointprotector.com

۱۰۰٪ قابل انعطاف برای نصب

مناسب برای هر نوع شبکه، این محصول امکان استفاده برای سازمان بزرگ، تجارت های متوسط و کوچک و حتی کاربران خانگی را نیز دارد. با معماری کاربر/سرور و کنسول مدیریتی تحت وب، نصب در شبکه و مدیریت کاربران بسیار راحت انجام می شود. علاوه بر این، امکان تهیه به صورت فیزیکی، مجازی، سرویس ابری Amazon، نسخه ابری و نسخه Stand-alone، این اختیار را به کاربر می دهد تا با خیال آسوده، بهترین نسخه را برای شبکه خود انتخاب کند.

Endpoint Protector

محافظت بر اساس محتوا، کنترل دستگاه ها، eDiscovery و رمز گذاری بر روی سیستم های مختلف و مدیریت دستگاه های موبایل و برنامه های آنها

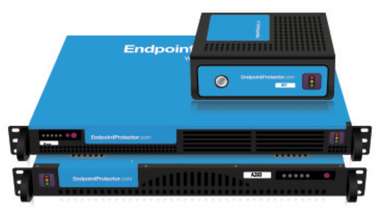
My Endpoint Protector

محافظت از محتوا، کنترل دستگاه ها و رمز گذاری بر روی سیستم های Windows و Mac و همچنین مدیریت دستگاه های موبایل و برنامه های آنها

Cloud Solution

Amazon Instance

Virtual Appliance



Hardware Appliance

ماژول ها





●	●	●	●	Windows XP / Windows Vista	(32/64 bit)	Windows
●	●	●	●	Windows 7 / 8 / 10	(32/64 bit)	
●	●	●	●	Windows Server 2003 - 2016	(32/64 bit)	
●	●	●	●	macOS 10.6	Snow Leopard	macOS
●	●	●	●	macOS 10.7	Lion	
●	●	●	●	macOS 10.8	Mountain Lion	
●	●	●	●	macOS 10.9	Mavericks	
●	●	●	●	macOS 10.10	Yosemite	
●	●	●	●	macOS 10.11	El Capitan	
●	●	●	●	macOS 10.12	Sierra	
n/a	●	●	●	Ubuntu		Linux
n/a	●	●	●	OpenSUSE		
n/a	●	●	●	CentOS / RedHat		
●				iOS 4, iOS 5, iOS 6, iOS 7, iOS 8, iOS 9, iOS 10		iOS
●				Jelly Bean (4.1+), KitKat (4.4+), Lollipop (5.0+), Marshmallow (6.0+), Nougat (7.0+)		Android

www.**ertebateamn**.com

www.**endpointprotector**.com

شماره تماس: ۸۸۵۳۲۹۳۲ ۰۲۱ | ۸۸۷۴۷۳۷۹ ۰۲۱
info@ertebateamn.com | www.ertebateamn.com

Official Partner

ارتباط امن
Ertebate Amn

COSOSYS