

جلوگیری از نشت اطلاعات

ارشیبظ امدت
Ertebare Amn



eset TECHNOLOGY ALLIANCE

راه کار امنیتی Safetico راه حل کامل DLP (پیشگیری از نشت اطلاعات) را ارائه می دهد که طیف گسترده ای از تهدیدات امنیتی که از یک منبع مشترک - که عامل انسانی است - را شامل می شود. Safetico از نشت داده های برنامه ریزی شده یا تصادفی، اقدامات مخرب عمدی، مسائل بهره وری، خطرات BYOD و موارد دیگر حفاظت می کند.

فلسفه امنیتی Safetico بر اساس سه پایه است: کامل بودن، انعطاف پذیری و سهولت استفاده.

DLP شرکت Safetico به طور کامل گزارش فعالیت های کاربران را به مدیریت سیستم ارائه می دهد و سیاست های امنیتی شرکت را به اجرا در می آورد.

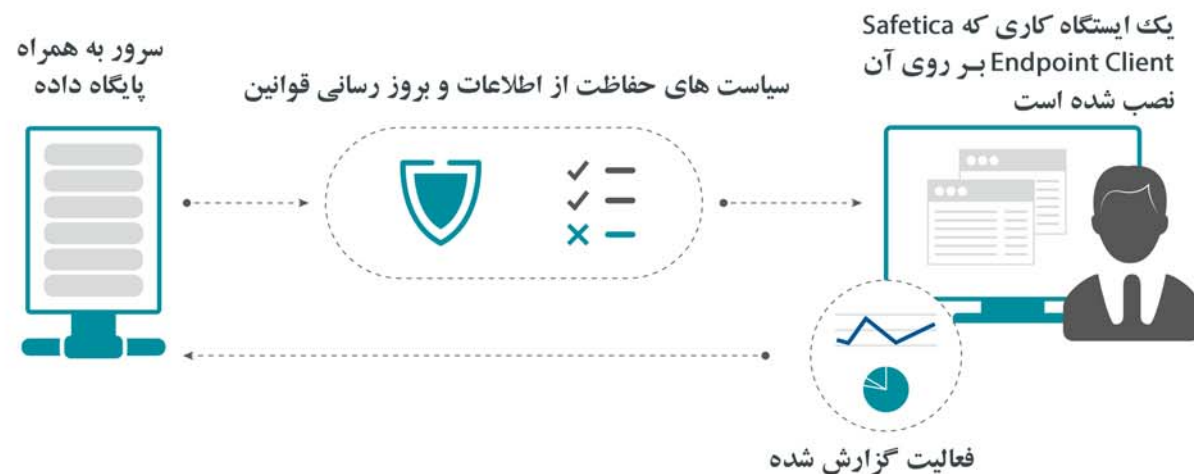
Safetico یک مجموعه کامل از ابزارهای امنیتی را در یک بسته نرم افزاری واحد ارائه می دهد که در غیر این صورت نیاز به چندین راه حل امنیتی از تولید کنندگان مختلف خواهد بود.

ویژگی های کلیدی

راهکار کامل جلوگیری از نشت اطلاعات	Safetico با پوشش تمامی کانال های اصلی نشت داده، DLP نقطه پایانی را با قابلیت های DLP شبکه فراهم می کند.
زمان کوتاه تا استفاده	روش انعطاف پذیر برای مسدود کردن کانال های نشت داده به Safetico سریع ترین زمان استقرار را در کلاس محصولات DLP می دهد.
مقاومت بالا در برابر تهاجم	حفاظت مداوم را حتی در زمانی که کاربران با دسترسی مدیر سیستم هستند، به ارمغان می آورد.
عملکردهای تخصصی برای جلوگیری از نشت اطلاعات	Safetico از اطلاعات در برابرعکس گرفتن از صفحه نمایش، سرقت Clip Board، چاپ مجازی، تبدیل فایل، آرشو شدن و توابع رمزگذاری محافظت می کند.
رویکرد محتاطانه	حفاظت داده Safetico توسط پروتکل ها یا برنامه های خاص محدود نمی شود.
قوانین حفاظت از داده واضح	مدیران به سادگی مکان هایی که اطلاعات محرمانه نباید از آنها خارج شوند را انتخاب می کنند. سپس Safetico امنیت را فراهم می کند.
محاسبه دقیق زمان استفاده	"باز شده" به معنای استفاده فعال نیست. گزارش های فعالیت Safetico نشان می دهد که کاربران به طور دقیق چه مدت زمانی در وب سایت های بازدید شده یا در برنامه های کاربردی فعال بودند.
بررسی و هشدار خودکار	Safetico مهم ترین جزئیات ثبت شده را انتخاب می کند و یک گزارش خلاصه را برای گیرندگان تعیین شده ارسال می کند. جزئیات کامل در صورت لزوم نیز در دسترس هستند.

نحوه فعالیت

ایستگاه های کاری محل وقوع اتفاقات است. کاربران با داده های حیاتی سازمان کار می کنند، به اینترنت دسترسی دارند، ایمیل های خود را می خوانند، اسناد را برای چاپگر ارسال می کنند و رسانه های قابل حمل خود را متصل می کنند. Safetico یک عامل (Safetico Endpoint Client) را در نقطه های مورد نظر نصب می کند و با استفاده از سرور (Safetico Management Service) ارتباط منظمی برقرار می کند. این سرور یک پایگاه داده از فعالیت های ایستگاه کاری ایجاد می کند و سیاست های جدید حفاظت از داده ها را به هر ایستگاه کاری ارسال می کند.



ویژگی های کلیدی

جלוگیری کامل از نشت اطلاعات	Safetica با پوشش همه کانال های اصلی نشت داده، DLP نقطه پایانی را با قابلیت های DLP شبکه فراهم می کند.
موارد برتر و سوابق فعالیت و عملکرد کاربران	در صورت تغییر ناگهانی در روند فعالیت کارمند، به مدیران شرکت هشدار می دهد و در طول زمان تغییرات عملکرد دپارتمان های مختلف را نشان می دهد.
گزارش فعالیت	وقایع امنیتی را از چند جهت مختلف بررسی می کند و بر تمامی فعالیت های کاربران برای نشانه هایی از خطر بالقوه، حتی قبل از سرقت واقعی داده ها نظارت دارد.
جلوگیری از نشت اطلاعات در ایمیل	اطمینان از عدم وجود اطلاعات طبقه بندی شده در صندوق پستی اشتباه. سوابق فایل های حساس ارسال شده را برای گزارش های بعدی ذخیره می کند.
کنترل برنامه ها بر اساس زمان	انتخاب برنامه های کاری و جلوگیری از اجرای باقی برنامه ها در مجموعه. برنامه ها را می توان برای یک بازه زمانی مشخص در دسترس قرار داد.
کنترل وب	به راحتی AUP شرکت (سیاست استفاده قابل قبول) را با دسته بندی های دقیق از پیش تعریف شده و فیلتر کلمات کلیدی به اجرا در می آورد.
نظارت بر چاپگرها	محدود کردن مواردی که می توانند چاپ شوند و همچنین ایجاد سهمیه بندی برای کاربران و دپارتمان ها در استفاده از چاپگرها.
کنترل دستگاه ها	از اتصال دستگاه های غیر مجاز در محل کار توسط کارکنان جلوگیری کند. پورت های مختلف می تواند برای دستگاه های خاص فعال شود یا برای همه مسدود شود.
مدیریت رمز گذاری	Safetica رمز گذاری کامل دیسک یا تمامی پارتیشن ها را ارائه می دهد و درایو های مجازی محلی یا تحت شبکه را برای ذخیره سازی امن فایل ها ایجاد می کند. Safetica علاوه بر رمز عبور و روش های دسترسی مبتنی بر کلید، دیسک های مسافرتی امن را نیز فراهم می کند و از قابلیت "رمز گذاری در هنگام کپی کردن" برای خروج داده ها از منطقه امن استفاده می کند.
حالت تست و بررسی	کمک می کند شرکت ها و سازمان ها حفاظت از داده ها را با تست کامل برای همه شرایط "چه می شود اگر" بدون توقف روند کسب و کار، انجام دهند.
مدیریت متمرکز	کنسول مدیریت متمرکز Safetica مدیریت یکپارچه امنیت و گزارش گیری را فراهم می کند.
طبقه بندی اطلاعات در حرکت	اطلاعات جدید را بلافاصله پس از ایجاد یا دریافت یک فایل محرمانه، حفاظت می کند.
بررسی SSL/HTTPS	بررسی و محافظت از خطوط ارتباطی امن از جمله وب سایت ها با استفاده از پروتکل HTTPS، برنامه های کاربردی پیام رسان با اتصالات امن و ارسال ایمن ایمیل.
هزینه پایین خرید	مشتریان را از نیاز به خرید محصولات امنیتی اضافی آزاد می کند. Agent های نصب شده روی سیستم ها، ویژگی های پیشگیری از نشت اطلاعات را برای شبکه شرکت نیز فراهم می کنند.
انعطاف در استفاده	Safetica هر برنامه کاربردی، پروتکل پیام رسان یا سرویس ایمیل تحت وب را با توجه به رویکرد جهانی منحصر به فردش پوشش می دهد.



TECHNOLOGY ALLIANCE

فناوری های ESET با هدف محافظت بیشتر از کسب و کارها، طیف وسیعی از راه حل های امنیتی IT را به ارمغان آورده است. ESET ارائه ترکیبی از تکنولوژی اثبات شده و قابل اطمینان با سایر محصولات امنیتی منحصر به فرد، گزینه های برتری را برای حفاظت از محیط کاری در دنیای سایبری همیشه در حال تغییر ارائه کرده است.



پوشش رویداد های نقاط پایانی

گزارش دهی و جلوگیری از فعالیت

جلوگیری از نشت اطلاعات

- همه هارد درایوها، USB، FireWire، کارت SD / MMC / CF، درایو SCSI
- انتقال فایل تحت شبکه (نا امن و امن)
- ایمیل (پروتکل SMTP، POP، IMAP، Microsoft Outlook / MAPI)
- SSL / HTTPS (تمام مرورگرها و برنامه های کاربردی با مدیریت گواهی استاندارد)
- کپی / ذخیره، Clip Board، کشیدن و رها کردن فایل
- چاپگرهای مجازی، محلی و شبکه
- بلوتوث، پورت IR / COM / Parallel
- دستگاه های خواندن و ضبط CD / DVD / BluRay
- دسترسی برنامه ها به فایل های مختلف را کنترل می کند

- همه عملیات انجام شده روی فایل ها
- روندهای بلند مدت، نوسانات کوتاه مدت فعالیت
- وب سایت ها (همه مرورگرهای پشتیبانی شده شامل ترافیک HTTPS) - زمان فعال و غیر فعال
- ایمیل ها و سرویس های تحت وب (تقریباً تمام ارائه دهندگان)
- کلمات کلیدی مورد جستجو (اکثر موتورهای جستجو پشتیبانی می شوند، جستجوی ویندوز پشتیبانی می شود)
- سرویس های پیام رسان (مستقل از برنامه - تمامی پروتکل ها پشتیبانی می شوند)
- میزان استفاده از برنامه های فعال و غیر فعال
- چاپگرهای مجازی، محلی و شبکه
- فعالیت صفحه (نظارت هوشمند)
- صفحه کلید

موارد استفاده

امنیت اطلاعات کلیدی کسب و کار

مدیریت دستگاه های قابل حمل

رمز گذاری اطلاعات

رسیدن به قوانین سازمانی

کنترل عملکرد

معماری راهکار

سیستم ها و رایانه های مجهز به عامل Safetica



1

اقدامات ثبت و ضبط شده و قوانین با استفاده از یک برنامه عامل کوچک اجرا می شود (به صورت اختیاری از کاربر مخفی می شود).

سرویس مدیریت داده Safetica و پایگاه SQL



2

داده ها به طور خودکار از رایانه های شبکه به سرور منتقل می شوند، اطلاعات لپتاپ ها در هنگام اتصال به شبکه نیز منتقل خواهد شد. تنظیمات مدیریتی در جهت معکوس همگام سازی می شود.

کنسول مدیریت Safetica به همراه تنظیمات و خروجی ها



3

تمام داده ها را می توان از کنسول مدیریتی مشاهده نمود. همه تنظیمات را می توان در همین کنسول تعریف کرد.

سرویس مدیریت Safetica در شعبات دیگر



4

Safetica مدیریت شعبه های متعدد را از یک کنسول مدیریت واحد، پشتیبانی می کند.

هنگامی که مناطق امن برای تمام داده های محافظت شده ایجاد شده است، Safetica به صورت بی صدا، هر گونه تعامل با این فایل ها را بررسی می کند و در صورت ممنوع بودن یک عمل، آن را مسدود می کند یا سایر اقدامات انتخاب شده را انجام می دهد. این اقدامات تعریف شده توسط شرکت می تواند شامل اطلاع رسانی به مدیر امنیت برای هر رویداد و رمز گذاری داده ها باشد. داده ها بر روی لپ تاپ ها و دیسک های قابل حمل حتی در خارج از محیط شرکت محافظت می شوند.

Safetica کنترل نهایی را برای آنکه چه کسی به کامپیوترهای شرکت چه دستگاهی وصل می کند را برای مدیریت فراهم می کند، کانال دیگری را برای نشت داده ها حذف می کند و به طور چشمگیری تعداد مداخلات در خدمت رسانی را کاهش می دهد.

Safetica نرم افزار کامل رمز گذاری دیسک را ارائه می دهد، می تواند یک سیستم ذخیره سازی فایل رمز گذاری شده ایمن فراهم کند، کلید های متصل شده را مدیریت کند و از ذخیره اطلاعات در مکان های ناامن جلوگیری کند.

با Safetica Endpoint Client موجود روی سیستم ها و مدیریت قوانین در کنسول مدیریتی Safetica، شما قادر به رعایت قوانین حریم خصوصی و کنترل استفاده از اطلاعات حساس هستید.

حتی بدون استفاده مستقیم از رابط کاربری کنسول مدیریتی، مدیران می توانند گزارش های خلاصه ای را به طور منظم در مورد کاربران یا گروه های مختلف دریافت کنند.

پیش نیاز های سیستم

مشخصات سیستم کاربر

- پردازنده دو هسته ای ۲.۴ گیگاهرتزی
- ۲ گیگابایت حافظه RAM
- ۱۰ گیگابایت فضای آزاد دیسک
- ۷ MS Windows و بالاتر، ۳۲ بیتی و ۶۴ بیتی

مشخصات سرور

- پردازنده دو هسته ای ۲ گیگاهرتزی (چهار هسته ای توصیه می شود)
 - ۴ گیگابایت حافظه RAM
 - ۲۰ گیگابایت فضای آزاد دیسک
 - پشتیبانی از Active Directory
 - ۲۰۰۸ R۲ MS Windows Server و بالاتر، ۳۲ بیتی و ۶۴ بیتی
 - نیاز به اتصال سرور با ۲۰۰۸ R۲ MS SQL
- مشخصات پایگاه داده

- حداقل ۱۰۰ گیگابایت فضای آزاد دیسک
- ۲۰۰۸ R۲ MS SQL و بالاتر (MS SQL Express ۲۰۱۲ و بالاتر توصیه می شود)
- MS SQL Express ۲۰۱۲ به صورت اختیاری در مراحل نصب قرار دارد



ارشیبظ امت

Ertebate Amn

eset@ertebateamn.com

sales@ertebateamn.com



۸۶۰۸۳۶۴۱

۸۶۰۸۴۷۱۹



TECHNOLOGY ALLIANCE