محافظت اطلاعات در شبکه توسط McAfee Data Protection Lost

McAfee Total Protection for Data Loss Prevention

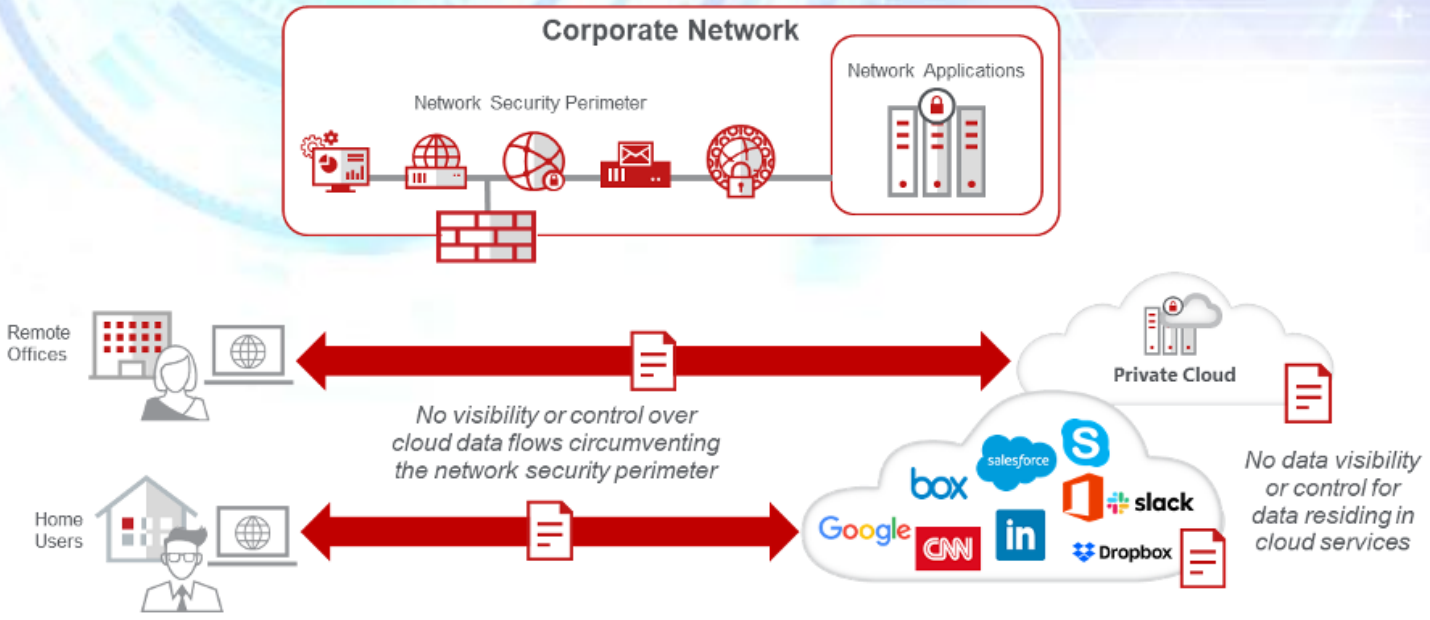
محافظت از نشت اطلاعات. ایستادگی در برابر تهدیدات. سهولت در مدیریت.

از آنجایی که سازمان ها و شرکت‌ها، درخواست های بسیاری برای استفاده امن از داده ها دارند، لذا بکارگیری راه حل های حفاظتی اجتناب ناپذیر است. راه کارهای ارائه شده در برخی از محصولات برای جلوگیری از نشت اطلاعات (DLP) نیاز به تلاش و هزینه های قابل توجهی دارد. این محصولات شناسایی اطلاعات حفاظت شده را به تیم IT می سپارند. آیا می توان از IT انتظار داشت راجع به اطلاعات همه بخش های سازمان و نحوه مدیریت آنها آگاهی کامل داشته باشد ؟ البته که نه. شناسایی همه اطلاعات حساس، تفسیر قواعد حاکم بر آنها و تبدیل آنها به policy های مؤثر توسط بخش IT غیر ممکن است. در مواجهه با این معضل، تعداد قابل توجهی از شرکت ها به راه حل هایی روی آوردند که بصورت تخصصی از داده ها حفاظت نمی کنند و تنها دید کمی از خطرهای مرتبط با اطلاعاتشان را به آنها می دهد. درحالیکه محصول DLPمکافی به طور موثر از اطلاعات شما در هرجایی محافظت می کند. این محصول در عرض تنها چند دقیقه (نه ماهها) تجزیه و تحلیل داده های بخش‌های مختلف را انجام می‌دهد.

ایجاد یک پایگاه داده برای حفاظت کامل از اطلاعات

McAfee Total Protection for DLP با حفاظت از اطلاعات حساس - در شبکه، در سیستم های ذخیره سازی، و یا در کلاینت‌ها- و در عین حال با صرفه جویی از وقت و هزینه و با بکارگیری، مدیریت و گزارش متمرکز، از مالکیت اطلاعات محافظت و رضایتمندی مشتری را تضمین می کند. همچنین این روش با سایر راه حل‌ها در مجموعه پروژه حفاظت از داده مانند امنیت ایمیل، امنیت وب، و رمزگذاری ادغام گردیده است تا از داده های ساکن، داده های در حال استفاده و داده های درحال انتقال نهایت حفاظت را داشته باشد.

«هنگامی که داده ها در خطر هستند ، سرعت مهم ترین معیار است» .نمیتوان به راه حل حفاظت از داده ها ماهها زمان داد تا بتواند قدرت تحلیل پیدا کند. هر دقیقه ای که داده بصورت محافظت نشده بماند بمنزله آنست که یک دقیقه دیگر اعتبار کسب‌وکار و امنیت اطلاعات مشتریان در معرض خطر است. برخی از راه حل ها نیاز به تمهیدات طولانی و پیچیده ای دارند که نیازمند مهارت های بسیار تخصصی جهت ساخت، توسعه و انجام تنظیمات می باشند. هزینه های بکارگیری سنگین می تواند قیمت خرید را دو برابر کرده و مدت زمانی که سیستم در ریسک است را افزایش دهد که می‌تواند خرابی بی حد و حسابی به بار آورد McAfee Total Protection for DLP این بن بست را می شکند. به محض اتصال به سیستم شروع به کار می کند. در عرض یک هفته، سیستم حجم زیادی از اطلاعات در مورد استفاده از داده ها را جمع آوری می نماید که به شما امکان می دهد تا اقدام به ایجاد policy های موثر نمایید که بلافاصله به نتیجه برسد.



چگونه از چیزی که سر در نمی آورید می توانید حفاظت کنید؟

در اکثر راه حل هایDLP ، اگر نتوان بدرستی توصیف کرد که داده ها از چه نوعی هستند و در کجا قرار دارند، نمیتوانند از آنها محافظت کنند.

آیا تا کنون قادر به دنبال کردن تغییراتی که دقیقه به دقیقه روی داده های درون سازمان شما رخ می دهد بوده اید ؟

حقیقتا هیچ دپارتمان IT نمی تواند این وظیفه را به تنهایی انجام دهد McAfee Total Protection برای پیشگیری از نشت اطلاعات به شما کمک می کند تا به سادگی داده هایی که در شبکه شما در جریان هستند را درک کرده و به شما و ذینفعان کسب و کارتان یک نقشه حقیقی از تمام اطلاعات حساس و ارزشمند ارائه می دهد . این راه حل باعث ایجاد بینش لازم جهت تنظیم policy هایی بمنظور محافظت از داده ها در حال و آینده خواهد شد.

معرفی ماژول‌های تخصصی McAfee Data Loss Prevention

McAfee DLP Manager

ابزارMcAfee DLP Manager ، کنترلر مرکزی در DLP و نقطه محوری مدیریت سازمان است که نظارت و مدیریت آن را از طریق سرور ®McAfee ePolicy Orchestrator® McAfee ePO™ انجام می دهد. سرور مک آفی EPO یک دید یکپارچه از وضعیت کلی ریسک‌های موجود در سازمان شما می دهد، و شما می توانید براحتی در مورد رویداد امنیتی خاصی ریز شده و علت را بیابید. همچنین هزینه عملیاتی کلی و مرتبط با مدیریت و نگهداری را کاهش می دهد، چرا که به شما اجازه می دهد در صورت نیاز به ارائه گزارش، به سرعت نمایی کلی از وضعیت امنیت اطلاعات را داشته باشید، policy را اعمال کنید و roleهای اجرایی تفویض نمایید . این اراهکار باعث می شود سهامداران سازمان با همکاری یکدیگر و بدون نیاز به بخش IT وقایع را مدیریت نمایند.

قوانین (Roles) از پیش تعیین شده به شما کمک می کند تا:

- سرعت راه اندازی سیستم برای اعضای کلیدی تیم در سازمان، از جمله مدیران، قسمت حقوقی، منابع انسانی، انطباق، عملیات و امنیت اطلاعات افزایش یابد
- تعریف role های اضافی تنها با چند کلیک ماوس.
- ادغام با اکتیو دایرکتوری مایکروسافت برای خدمات احراز هویت (authentication) متمرکز.

McAfee DLP Discover

فهمیدن اینکه اطلاعات حساس در کجا مستقر هستند اولین قدم در حفاظت از آن است. ابزار McAfee DLP Discover کشف این موضوع را به کمک یک فرایند سه مرحله ای (فهرست کردن، دسته بندی و بازسازی) ساده کرده است. بر خلاف سایر روش ها که از شما انتظار دارند بدانید دقیقا چه محتویاتی را می خواهید محافظت کنید و احتمالا این اطلاعات در کجا ذخیره شده اند، ابزار McAfee DLP Discover این وظیفه سنگین را به عهده می گیرد. به سرعت اطلاعات دسته بندی نشده را طبقه بندی می کند بطوری که تنها فایل های مرتبط بررسی و اصلاح می شوند .سه مرحله عبارتند از:

- فهرست: فهرستی از دارایی ها در سراسر سازمان ایجاد کرده و تنها به جهت افزایش سرعت بر روی ابرداده آنالیز انجام می دهد.
- طبقه بندی: محتویات را دسته بندی کرده و بر روی محتویات دسته بندی شده آنالیز انجام می دهد.
- بازسازی: داده های طبقه بندی شده را از لحاظ نقضpolicy ها بررسی میکند، بازسازی می کند و سپس اطلاعات را ثبت می کند.

به کمک توانایی جدید مک‌آفی در طبقه بندی اطلاعات در ابزار McAfee DLP Discover ، شما راهی سریع برای طبقه بندی و اسکن داده ها و همچنین اصلاح وظایف (task) دارید.

McAfee DLP Prevent

ابزار McAfee DLP Prevent بر روی اطلاعاتی که شبکه را از طریق email ، webmail، instant messaging (IM)، ویکی ها، بلاگ ها، پورتال ها و تکنولوژی Web 2.0 ترک میکنند policy اعمال می نماید

همچنین امنیت اطلاعاتی نظیر کد ملی، شماره کارت اعتباری و اطلاعات مالی که شما می دانید باید محافظت شوند و همچنین اطلاعاتی که از ارزش معنوی بالایی برخوردارند و شما می خواهید حفاظت شوند را تضمین مینماید.

ابزار McAfee DLP Prevent به شما اجازه می دهد تا به کمک اقدامات اصلاحی که شامل رمزگذاری، redirect، قرنطینه و حتی بلاک کردن می شود بتوانید برقراری قوانین بر اطلاعات حساس را تضمین و ریسک نشت اطلاعات کسب و کارتان را کاهش دهید .ابزار McAfee DLP Prevent با درگاههای شبکه بر اساس استانداردها بصورت یکپارچه عمل می کند:

بر روی اطلاعاتی که شبکه را از طریقemail ، webmail، instant messaging (IM)، ویکی ها، بلاگ ها، پورتال ها، HTTP/HTTPSو FTP ترک می کنند policy اعمال می نماید.عملکرد یکپارچه با پورت ایمیل از طریق SMTPدر حالی که ترافیک وب با استفاده از پروتکل "ICAP" کنترل میگردد.

قابلیت های حفاظتی پیشرفته

McAfee DLP Endpointحفاظت جامعی را از همه کانال‌های احتمالی نشت ارائه می‌کند، از جمله دستگاه‌های ذخیره‌سازی قابل جابجایی، ابر، ایمیل، پیام‌رسانی فوری، وب، چاپ، کلیپ‌بورد، ضبط صفحه، برنامه‌های اشتراک‌گذاری فایل و غیره.

مدیریت متمرکز

- توسط یک کنسول مدیریت بومی – MVISION ePO – Cloud برای مدیریت خط مشی ها و رویدادها به آسانی مدیریت می شود.
- این سیاست و موتورهای طبقه‌بندی و جریان‌های کاری اتفاق با ®McAfee مشترک است MVISION Cloud (CASB)و ®McAfeeشبکه.DLP
- چندین خط مشی و مجموعه قوانین قابل استفاده مجدد به شما این امکان را می دهد که چندین خط مشی DLP را در سراسر سازمان تعریف کنید و به شما در ایجاد خط مشی ها بر اساس دفتر، بخش، مقررات و موارد دیگر کمک می کند.
- جزئیات پیشرفته در مدیریت رویداد می‌توانند با هر ویژگی حادثه (به عنوان مثال، شماره سریال دستگاه، نام فایل شواهد و گروه‌ها) پرس و جو/فیلتر/مشاهده کنند.
- قابلیت نظارت و ممیزی متمرکز رویداد.
- بهبود کنترل دسترسی مبتنی بر نقش (همچنین به عنوان تفکیک وظایف شناخته می شود) برای مدیریت خط مشی، و همچنین بررسی رویداد.
- رابط میز راهنمایی با دسترسی آسان.

ویژگی های کلیدی McAfee DLP Endpoint عبارتند از :

- قابلیت تنظیم برچسب های Microsoft Azure Information Protection (AIP) برای داده های در حال جریان و شناسایی فایل های دارای برچسب.AIP
- ادغام با تجزیه و تحلیل رفتاری کاربر شخص ثالث (UEBA) با تهدیدهای خودی مقابله می کند. تجزیه و تحلیل های امنیتی را برای تشخیص رفتار غیرعادی و بسیار خطرناک کاربر و نهاد انجام می دهد.
- طبقه بندی دستی به کاربران امکان می دهد اسناد را به صورت دستی طبقه بندی کنند، آگاهی حفاظت از داده های کارکنان را افزایش می دهد و بار اداری را کاهش می دهد.
- اسکن و اصلاح توسط کاربر به کاربران امکان می دهد اسکن های کشف نقطه پایانی را اجرا کنند و اقدامات خود اصلاحی را انجام دهند.
- طبقه بندی انعطاف پذیر است و شامل فرهنگ لغت، عبارات منظم و الگوریتم های اعتبار سنجی، اسناد ثبت شده، و پشتیبانی از راه حل های طبقه بندی کاربر شخص ثالث است.
- فناوری برچسب‌گذاری منحصربه‌فرد اسناد را بر اساس منشأ آنها شناسایی می‌کند و به جلوگیری از تکرار، تغییر نام یا خروج اطلاعات حساس از برنامه‌های کاربردی وب، برنامه‌های کاربردی شبکه و اشتراک‌های شبکه کمک می‌کند.
- پشتیبانی از مجازی سازی پیشرفته از دسکتاپ های راه دور و راه حل های زیرساخت دسکتاپ مجازی (VDI) محافظت می کند.

اجرای انطباق و آموزش کاربر

با ناپدید شدن محیط شرکت، اجرای انطباق برای شرکت ها چالش برانگیزتر می شود McAfee DLP Endpoint .نه تنها می تواند به شما در نظارت بر رفتارهای روزمره کاربر کمک کند، بلکه می تواند با ارائه آموزش به کاربر از انطباق آن اطمینان حاصل کند McAfee DLP Endpoint .با کلیک یک دکمه گزارش های دقیقی را برای اثبات به حسابرسان، مدیریت ارشد و سایر موارد ارائه می دهد.

ذینفعان که تدابیر انطباق داخلی و مقرراتی وجود دارد. این خط‌مشی‌های قالب‌بندی‌شده برای مقررات و موارد استفاده ارائه می‌دهد، که این امر را برای شما آسان می‌کند که مطابقت داشته باشید. کاربران شما همچنین از طریق پنجره های اجرایی بر اساس خط مشی شرکت شما بازخورد بلادرنگ دریافت می کنند و این فرصت های آموزشی کوچک به شما کمک می کند فرهنگ امنیتی سازمانی قوی تری بسازید.

مزایای کلیدیDLP

■دستگاه به ابر: به راحتی خط‌مشی‌های DLP داخلی را به فضای ابری برای تشخیص از دست رفتن داده‌ها گسترش دهید.
■قابلیت‌های حفاظتی پیشرفته: از اثرانگشت، طبقه‌بندی و برچسب‌گذاری فایل برای ایمن کردن داده‌های حساس و بدون ساختار، مانند مالکیت معنوی و اسرار تجاری، استفاده کنید.

■مدیریت متمرکز: ادغام بومی با (MVISIONePO™) ®McAfee MVISION ePolicy Orchestrator به ساده‌سازی خط‌مشی و مدیریت رویداد ۲ کمک می‌کند.

■اجرای انطباق: با پرداختن به اقدامات روزمره کاربر، مانند ارسال ایمیل، پست ابری، دانلود در دستگاه های رسانه ای قابل جابجایی، و موارد دیگر، از انطباق اطمینان حاصل کنید.

■آموزش کاربر: بازخورد در زمان واقعی از طریق یک پنجره آموزشی به شکل گیری آگاهی و فرهنگ امنیتی شرکت کمک می کند