LianGroup

Mehrna Rayaneh Lian

فلکه دوم صادقیه، بلوار آیت الله کاشانی
خ نجف زاده فروتن، خ اعتمادیان، پلاک ۴۲، واحد ۲

۰۲۱ ۹۱۰۰۴۱۵۱

Symantec™

جلوگیری از نشت اطلاعات با استفاده از Symantec DLP

تضمین امنیت اطلاعات حساس سازمان و سازگاری آن‌ها با قوانین، کار آسانی نیست. به ویژه که هر روز، چالش‌های جدیدی در زمینه حفاظت از اطلاعات پیش روی ما قرار می‌گیرد. کارمندان شرکت، فایل‌های زیادی را از طریق سرویس‌های ذخیره سازی ابری به اشتراک می‌گذارند و از طریق تلفن همراه شخصی خود، به این اطلاعات دسترسی دارند. این موارد، امنیت اطلاعات سازمان را به خطر می‌اندازد و همان طور که گزارش‌ها نشان می‌دهند، تعداد حملات سایبری هدفمند، پیوسته در حال افزایش است. یکی از چالش‌های دنیای امنیت اطلاعات این است که مجرمان سایبری، همواره روش‌های جدیدی ابداع می‌کنند که می‌توانند اقدامات امنیتی صورت گرفته را شکست داده و پس از نفوذ به سیستم، داده‌های مهم شرکت را به سرقت ببرند. وقتی تمام این موارد را کنار هم می‌گذاریم، محافظت از اطلاعات در برابر از بین رفتن و سرقت، دشوارتر از قبل می‌شود.

شما برای حفاظت از اطلاعات سازمان خود در این محیط چالش برانگیز، چه تدبیری اندیشیده‌اید؟ یا بهتر است بپرسیم که یک استراتژی کامل و موفق باید چه ویژگی‌هایی داشته باشد که هم راهکاری در برابر حملات هدفمند و توسعه مرزهای امنیت داشته باشد و هم به نیازها و عادت‌های کاربر پاسخ مناسبی بدهد؟

محصول DLP سیمانتک، با یک راهکار جامع که امنیت اطلاعات فضای ابری و موبایل محور را شامل می‌شود، به این پرسش، پاسخ مناسبی می‌دهد. DLP Symantec به شما این امکان را می‌دهد که:

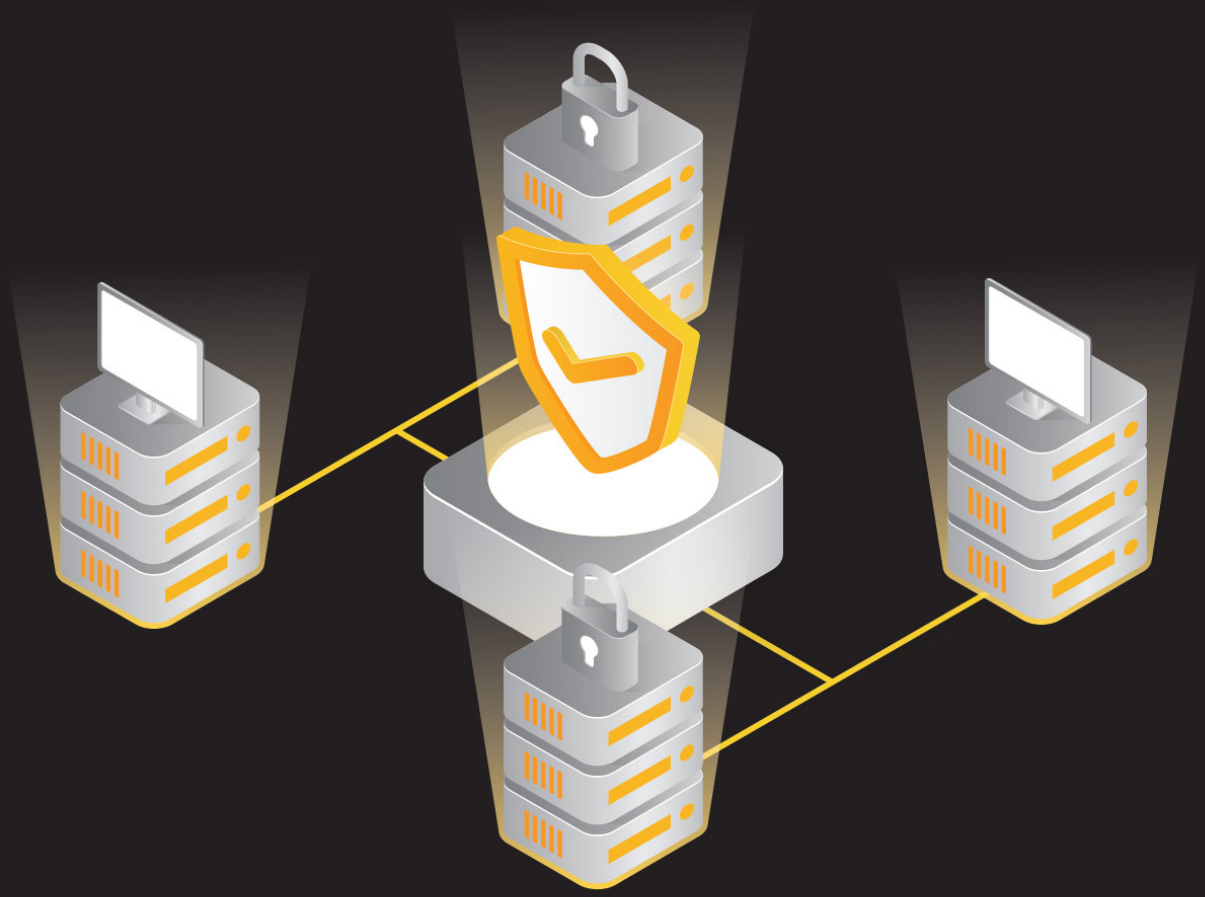
- محل ذخیره‌سازی داده‌ها را در تمام سیستم‌های ابری، موبایل، شبکه، اندپوینت و حافظه کشف کنید.
- چه کارمندان شما در شبکه آنلاین باشند و چه آفلاین، می‌توانید بر نحوه استفاده از داده‌ها نظارت کنید.
- بدون توجه به این که دیتا کجا ذخیره شده یا چطور استفاده می‌شود، از نشت یا سرقت آن جلوگیری کنید.

راهکار بی‌نظیر و تکنولوژی پیشرفته سیمانتک، قابلیت DLP را به دستگاه‌های موبایل و مبتنی بر فضای ابری اضافه می‌کند. Symantec DLP به شما امکان می‌دهد که امنیت شبکه خود را بالا برده و policy ها را فراتر از مرزهای شبکه خود پیاده سازی کنید. این محصول با متدولوژی‌های اثبات شده‌ی استقرار، ابزارهای مدیریت حادثه قدرتمند و پوشش جامع، به امنیت کانال‌های پر خطر شما کمک کرده و هزینه نهایی را تا کمترین حد ممکن، کاهش می‌دهد.

کشف کنید که در هر کدام از کانال‌ها، دیتا کجا قرار دارد: فضای ابری، ایمیل، وب، نقاط پایانی و حافظه

بر نحوه استفاده از داده‌ها نظارت کنید

در زمان واقعی، از داده‌ها در برابر افشا یا سرقت شدن محافظت کنید



داده‌های بیشتر با استفاده از سیستم شناسایی حساس به محتوا

DLP سیمانتک، تکنولوژی‌های پیشرفته را ترکیب می‌کند که این کار می‌تواند تمام اطلاعات حساس سازمان شما را، با دقت بسیار بالایی شناسایی کند؛ فرق نمی‌کند که این اطلاعات در سکون، حرکت و یا در حال استفاده باشند. فناوری‌های شناسایی DLP Symantec شامل موارد زیر می‌شود:

1 تطبیق دقیق داده‌ها (EDM)

که با استفاده از انگشت نگاری منابع اطلاعاتی ساختاریافته از جمله database، سرورهای دایرکتوری و دیگر فایل‌های ساختاریافته، محتوا را شناسایی می‌کنند.

تطبیق محتوای توصیف شده (DCM)

میزان مطابقت با کلمات کلیدی خاص، عبارات یا الگوهای منظم و خصوصیات فایل را بررسی می‌کند و با استفاده از این روش، محتوا را شناسایی می‌کند. DLP سیمانتک، بیش از ۳۰ شناساگر ارائه می‌دهد که هرکدام از آن‌ها، الگوریتم‌های از پیش تعیین شده‌ای هستند که الگو مطابق را با هوش داخلی ترکیب می‌کنند تا false positive را کاهش دهند. برای مثال، شناساگر داده «شماره کارت اعتباری»، الگوهای ۱۶ رقمی را شناسایی کرده و به آن‌ها با یک «Luhn check» اعتبار می‌دهد.

یادگیری ماشین وکتور (VML)

که از دارایی معنوی شرکت‌ها محافظت می‌کند. منظور از دارایی معنوی، آن دسته از دارایی‌های شرکت است که ممکن است نادر یا توصیف آن‌ها دشوار باشد؛ برای مثال، می‌توان به گزارش‌های مالی و کد منبع اشاره کرد. VML این دسته از محتوا را با استفاده از انجام تجزیه و تحلیل آماری بر روی داده‌های بدون ساختار و مقایسه آن با محتوا و داده‌های مشابه شناسایی می‌کند. برخلاف دیگر فناوری‌های شناسایی، نیازی به تعیین موقعیت، توصیف یا انگشت‌نگاری اطلاعات، توسط شما نیست.

تطبیق داده‌های ایندکس شده (IDM)

برای شناسایی اطلاعات محرمانه، شامل اطلاعات مایکروسافت آفیس؛ PDFها، فایل‌های باینری مانند JPEG، طرح‌های CAD و فایل‌های چند رسانه‌ای، از روش‌های انگشت‌نگاری استفاده می‌کند. همچنین IDM، محتوای مشتق شده را هم مانند متنی که از یک منبع اطلاعاتی به فایل دیگری کپی شده باشد، شناسایی می‌کند.

شناسایی نوع فایل

بیش از ۳۳۰ نوع فایل مختلف مانند ایمیل، فایل‌های گرافیکی و فرمت‌های نامحفوظ را تشخیص و شناسایی می‌کند. یکی از قابلیت‌های Symantec DLP این است که می‌توانید آن را برای تشخیص تقریبا هر نوع فایل سفارشی، پیکربندی کنید. این محصول همچنین به شما اجازه می‌دهد که محتوای فایل‌هایی با فرمت مشخص (حتی فرمت‌های رمزنگاری شده) را با استفاده از API استخراج محتوا، خارج کنید.

DATA LOSS PERVENTION:
CONTENT DETECTION TECHNOLOGIES

Described Content Matching

DESCRIBED DATA

Non-indexable data

Lexicons

Data Identifiers

Exact Data Matching

STRUCTURED DATA CUSTOMER DATA

Credit card, Government IDs, Pricing

Partial row matching

Near perfect accuracy

Indexed Document Matching

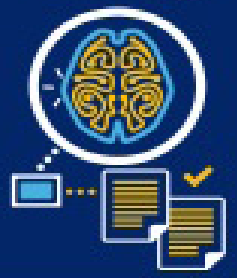
UNSTRUCTURED DATA IP

Designs, Source Code, Financials

Derivative match

Near perfect accuracy

Vector Machine Learning



UNSTRUCTURED DATA IP

Designs, Source Code, Financials

Derivative match

Very High Accuracy

Symantec™

تعریف و پیاده‌سازی سیاست‌های مداوم در محیط

با گسترش داده‌های شما در طیف وسیع‌تری از دستگاه‌ها و فضاهای ذخیره‌سازی، توانایی تعریف و اجرای مداوم سیاست‌ها، مهم‌تر از قبل به نظر می‌رسد. DLP سیمانتک، یک کنسول مدیریتی یکپارچه، پلتفرم اجرای DLP و یک ابزار گزارش‌دهی اطلاعات تجاری دارد. آنالیز IT برای DLP، به شما این امکان را می‌دهد که یک بار، Policyها را مشخص کنید و بعد از آن، این Policyها را همه جا اجرا کرده و ریسک‌ها را کاهش دهید.

نظارت و حافظت از ایمیل و حافظه مبتنی بر فضای ابری

برای بسیاری از شرکت‌ها، انتقال اپلیکیشن‌های نصبی به فضای ابری، یک راهکار هوشمندانه برای افزایش چابکی سیستم و کاهش هزینه‌ها است. اما چطور می‌توان این کار را بدون از دست دادن کنترل اطلاعات حساس انجام داد؟ DLP سیمانتک، این مشکل را با کشف، نظارت و حفاظت قوی و بی‌نظیر خود، برطرف کرده است.

حفاظت کامل از اطلاعات بر روی موبایل

امروزه، تمام کاربران انتظار دارند که به راحتی و با استفاده از هر نوع دستگاهی، به داده‌های مهم سازمانی دسترسی داشته باشند. در واقع، از هر ۵ کارمند، ۲ نفر آن‌ها گفته‌اند که فایل‌های شرکت را روی موبایل یا تبلت خود دانلود می‌کنند. DLP Symantec، این امکان را به شما می‌دهد که کنترل و نظارت لازم را بر دسترسی کاربران داشته باشید و همزمان، از اطلاعات حساس سازمان هم محافظت کنید.

امنیت داده‌ها در Endpoint

اگرچه دستگاه‌های موبایل و حافظه ابری، محبوب‌تر و رایج‌تر شده‌اند، اندپوینت‌ها همچنان نقش ریپازیتوری‌های اصلی را برای اطلاعات سازمان ایفا می‌کنند. این محصول، با ارائه قابلیت کشف، نظارت و محافظت اطلاعات بر روی دسکتاپ‌های سنتی و مجازی، بدون توجه به این که کاربران شبکه سازمانی شما آنلاین باشند یا آفلاین، امنیت اندپوینت‌ها را برای شما به ارمغان می‌آورند.