Symantec Data Loss Prevention

حفاظت کامل داده‌های حساس خود را به دست بگیرید

در یک نگاه

بالاترین سطح حفاظت از اطلاعات

- گسترده ترین محافظت از داده ها برای کانال های ارتباطی: ابر، ایمیل، وب، نقاط پایانی و ذخیره سازی.
- خطای کمتر شناسایی با فناوری های تشخیص جامع.

مدیریت یکپارچه

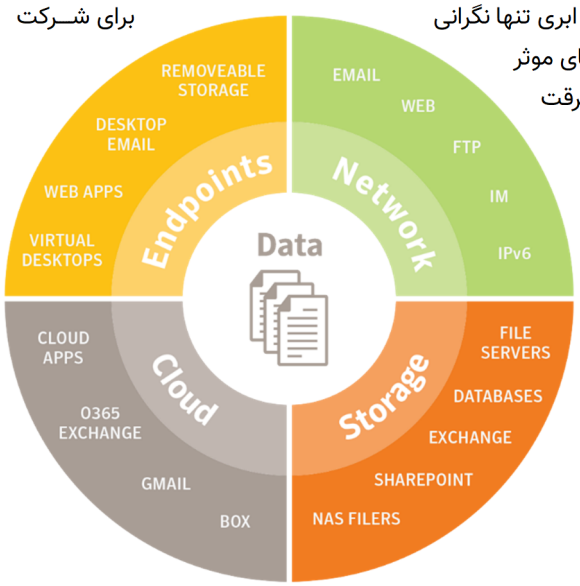
- کنسول واحد برای مدیریت خط مشی، واکنش به حادثه، گزارش دهی و مدیریت.
- مجموعه ای از خط مشی ها و گردش کار برای همه کانال های ارتباطی: ابر، ایمیل، وب، نقاط پایانی و ذخیره سازی.

ادغام با طیف گسترده‌ای از راه‌کارها

- با Symantec Information Centric Security و Cyber Defense Platform ادغام می شود.
- پشتیبانی از یکپارچه سازی گسترده برای رفتار کاربر، رمزگذاری شخص ثالث، طبقه بندی اطلاعات و محصولات مدیریت دسترسی.

با بالاترین سطح حفاظت، از نشت اطلاعات جلوگیری کنید

ایمن و سازگار نگه داشتن اطلاعات هیچ گاه آسان نبوده است. امروزه شرکت ها با مشکلات امنیتی جدید و غیرمنتظره ای روبرو هستند. همانطور که شرکت‌های بیشتری سیستم‌های داخلی خود را با خدمات مبتنی بر ابر جایگزین می‌کنند، اطلاعات شرکت بیشتر در معرض نشت تصادفی توسط کاربران ابری بی‌تجربه قرار می گیرد و در مقابل خطاهای پیکربندی آسیب‌پذیرتر می‌شوند. امنیت ابری تنها نگرانی برای شرکت ها نیست. حملات سایبری هدفمند بسیار رایج شده اند زیرا مجرمان سایبری روش های موثر جدیدی را توسعه می دهند که اقدامات امنیتی قدیمی را دور می زند و از کاربران برای سرقت داده های ارزشمند از شرکت ها سوء استفاده می کنند.

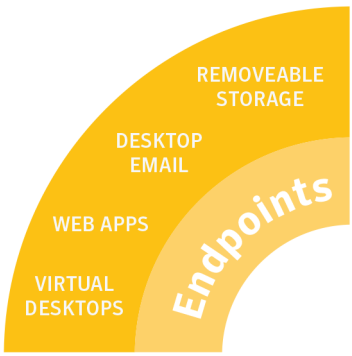


راه کار پیشگیری از نشت اطلاعات Symantec (DLP) بالاترین سطح حفاظتی را که برای جلوگیری از نقض اطلاعات و حفظ اعتبار شرکت خود نیاز دارید، ارایه می دهد. با فناوری پیشرو ما، امکان کشف و نظارت جامع برای شما فراهم می شود و قابلیت‌های حفاظتی به شما دید کاملی از اطلاعات محرمانه خود می هد و کنترل آن ها را امکان پذیر می کند.

پایش اطلاعات موجود در کانال ها: ابر، ایمیل، وب، نقاط پایانی و حافظه ذخیره سازی

نظارت بر نحوه استفاده از اطلاعات در داخل و خارج از شبکه سازمان یا شرکت

محافظت از افشای اطلاعات یا سرقت آن ها در زمان واقعی



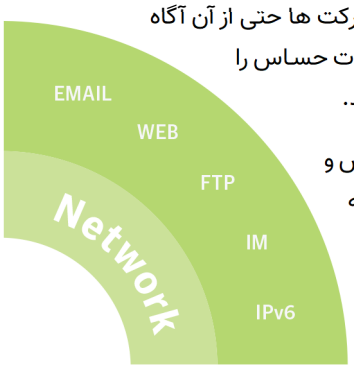
راه حل **Symantec DLP for Endpoint** تمام اقدامات محافظتی مورد نیاز برای ایمن نگه داشـــتن اطلاعات حســـاس در نقاط پایانی را فراهم می کند. قابلیت‌های پایش، نظارت و حفاظت کامل را برای اطلاعات مورد اسـتفاده در طیف وسـیعی از کانال‌ها را فراهم می‌کند؛ از جمله: ایمیل، برنامه‌های ابری، پروتکل‌های شـبکه، حافظه خارجی، دســکتاپ‌ها و ســرورهای مجازی. با Symantec DLP، یک agent ســبک دو ماژول DLP Endpoint Discover و DLP Endpoint Prevent را فعال می‌کند.

Symantec DLP Endpoint Discover دیسک های سخت محلی را اسکن می کند و به شما امکان مشاهده عمیق فایل های حسـاسـی که کاربران در لپ تاپ و دسـکتاپ خود ذخیره می کنند را می‌دهد. همچنین طیف گسـترده‌ای از پاسـخ‌ها از جمله قرنطینه فایل‌های محلی و راه دور، و رمزگذاری مبتنی بر سـیاسـت و مدیریت حقوق دیجیتال که توسط DLP Endpoint FlexResponse API فعال شده است را ارایه می‌کند.

Symantec DLP Endpoint Prevent بر فعالیت های کاربران نظارت می کند و به شما کنترل دقیقی بر طیف وسیعی از برنامه ها، دستگاه ها و پلتفرم ها می دهد. همچنین طیف گسترده ای از پاسخ ها از جمله رمزگذاری مبتنی بر هویت و حقوق دیجیتال برای فایل های منتقل شـــده به USB را ارایه می دهد. با Endpoint Prevent می‌توانید با استفاده از پنجره‌های بازشوی روی صفحه یا اعلان‌های ایمیل، به کاربران در مورد حوادث هشدار دهید. کاربران همچنین می توانند با ارایه یک توجیه تجاری یا لغو اقدام (در صـــورت تشخیص اشتباه) خط مشی ها را لغو کنند.

Browsers	Chrome | Safari | Firefox | IE & Edge
Cloud Apps	Box | Dropbox | Google Drive | Microsoft OneDrive
Email Apps	Outlook | Lotus Notes
Network Protocols	HTTP | HTTPS | FTP
Removable Storage	MSC devices | MTP devices
Virtual Desktops	Citrix | Microsoft Hyper-V | VMware
Others	Print | Fax | Network Share | Clipboard

از جریان اطلاعات در شبکه محافظت کنید



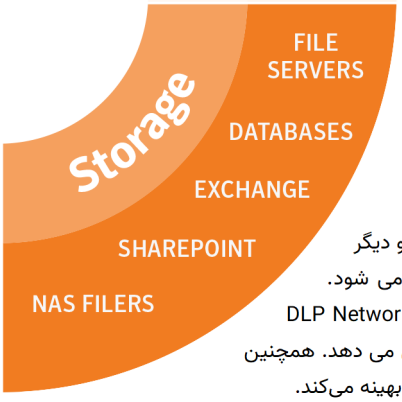
پذیرش گسترده ابزارهای اشتراکی و برنامه های ابری و همراه شدن آن‌ها با رفتار پرخطر کارکنان که ممکن است شرکت ها حتی از آن آگاه نباشند، خطر نشت اطلاعات را در ارتباطات تجاری افزایش می دهد. راه کار **Symantec DLP for Network** اطلاعات حساس را پایش می کند و از افشای آن ها در طیف گسترده ای از پروتکل های ارتباطی در سراسر شبکه شما جلوگیری می کند.

DLP Network Monitor ترافیک خروجی شبکه شرکتی شما را ضبط و تجزیه و تحلیل می کند و محتوای حساس و ابرداده را از طریق پروتکل های اسـتاندارد، غیر اسـتاندارد و اختصـاصـی شـناسـایی می کند. در نقاط خروجی شـبکه مسـتقر شـده و با Network Tap یا آنالیز پورت سـوییچ شـده (SPAN) یکپارچه می شـود. مانیتور شـبکه بازرسـی محتوای عمیق تمام ارتباطات شـبکه را بدون از دسـت دادن هیچ بسـته‌ای انجام می دهد، بر خلاف راه حل های دیگر که بسته ها را در زمان اوج بار نمونه برداری می کنند و شما را در معرض خطر عدم تشخیص قرار می دهند.

DLP Network Prevent for Email از افشـای یا سـرقت پیام‌های حسـاس توســط کارمندان، پیمانکاران و شــرکا محافظت می کند. تمام ترافیک ایمیل شـرکتی را نظارت و تجزیه و تحلیل می کند و به صـورت اختیاری پیام ها را بر اساس محتوای حساس یا سایر ویژگی های پیام تغییر می دهد، هدایت می کند یا مسـدود می کند. Network Prevent for Email در نقاط خروج شـبکه مســتقر شـــده و با عوامل انتقال نامه (MTA) و ایمیل مبتنی بر ابر از جمله Microsoft® Office 365 Exchange یکپـارچـه می شـــود. Network Prevent for Email به عنوان نرم افزار یا ابزار مجازی در دسترس است.

DLP Network Prevent for Web از داده های حساس در برابر نشت به وب محافظت می کند. تمام ترافیک وب شـرکتی را نظارت و تجزیه و تحلیل می کند و به صـورت اختیاری محتوای حسـاس HTML را حذف می کند یا درخواسـت ها را مسـدود می کند. Network Prevent for Web در نقاط خروج شـبکه مسـتقر شـده و با سـرور پروکسـی HTTP، HTTPS یا ftp با استفاده از ICAP ادغام می شود. Network Prevent for Web به صـورت نرم‌افزار، ابزار سـخت‌افزاری یا ابزار مجازی در دسترس است.

اطلاعات بایگانی را در مخزن‌های ذخیره سازی محافظت کنید



حفاظت از اطلاعات بایگانی شده در مخازن ذخیره‌سازی دیجیتال به طور قابل توجهی در حال رشد هستند که عمدتاً به دلیل اسناد تولید شده داخلی است؛ با این حال شرکت‌های کمی به مدیریت و محافظت از آن توجه می کنند. با استفاده از Symantec DLP for Storage می‌توانید اطلاعات حساس بایگانی را کشف و ایمن کنید؛ از جمله: داده‌های ذخیره‌شده در سرورهای فایل، نقاط پایانی، ذخیره‌سازی ابری، اشتراک‌گذاری فایل‌های شبکه، پایگاه‌های داده، شیرپوینت و سایر مخازن اطلاعات.

ابتدا **Symantec DLP Network Discover** اطلاعات محرمانه را با اسکن اشتراک‌گذاری فایل‌های شبکه، پایگاه‌های داده و دیگر مخازن اطلاعات سازمانی پیدا می‌کند که شامل سیستم های فایل محلی در سرورهای Windows، Linux، AIX و Solaris می شود. همچنین Lotus Notes و پایگاه های داده SQL و سرورهای Microsoft Exchange و SharePoint را نیز دربر می گیرد. DLP Network Discover بیش از ۳۳۰ نوع فایل مختلف - از جمله انواع فایل های سفارشی - را بر اساس امضای باینری فایل تشخیص می دهد. همچنین اسکن با سرعت بالا را برای محیط‌های بزرگ و پراکنده فراهم می‌کند و تنها با اسکن فایل‌های جدید یا اصلاح‌شده، عملکرد را بهینه می‌کند.

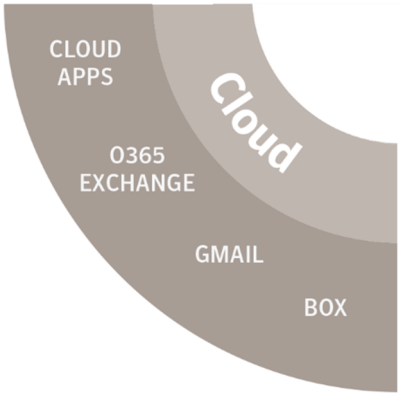
در ادامه **Symantec DLP Network Protect** قابلیت های حفاظتی قوی از فایل را در بالای Network Discover اضافه می کند. Network Protect به طور خودکار تمام فایل‌های در معرض دید را که Network Discover شناسایی می‌کند پاکسازی و ایمن می‌کند و طیف گسترده‌ای از گزینه‌های اصلاحی، از جمله قرنطینه کردن یا انتقال فایل‌ها، کپی کردن فایل‌ها در یک منطقه قرنطینه، یا اعمال رمزگذاری مبتنی بر هویت و حقوق دیجیتالی را ارایه می‌کند. فایل های خاص Network Protect حتی با گذاشتن یک فایل متنی نشانگر در محل اصلی فایل برای توضیح دلیل قرنطینه شدن آن، به کاربران تجاری در مورد نقض خط‌مشی آموزش می‌دهد.

Symantec DLP همچنین دارای یک **FlexResponse API Platform** است که به شما امکان می دهد که برای فایل سفارشی، اقدامات اصلاحی بسازید.

FlexResponse ادغام آسان و یکپارچه سازی با سایر راه کار های امنیتی فایل Symantec و شخص ثالث - از جمله Symantec File Share Encryption و Adobe LiveCycle را فراهم می کند.

File Servers	Windows via CIFS and DFS | Unix via NFS | Local Windows | Local Unix (Linux, AIX and Solaris) | NAS Filers
Distributed Machines	Laptops | Desktops
Document and Email Repositories	SharePoint | LiveLink | Documentum | Lotus Notes | Microsoft Exchange | PST
Web Content and Applications	Corporate Web Sites | Intranet | Extranet | Custom Applications
Databases	Oracle | Microsoft | IBM DB2

محافظت از داده ها در فضای ابری



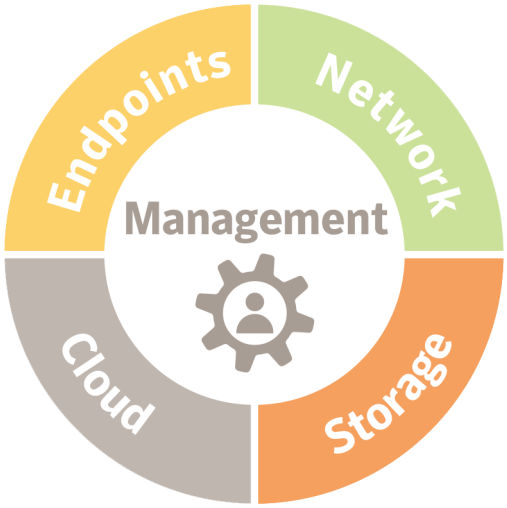
نگرانی‌های امنیتی سازمان ها به دلیل انتقال برنامه‌های قدیمی فناوری اطلاعات به سرویس‌های ابری عمومی همچنان ادامه دارد؛ جایی که دسترسی به سطح دید و کنترل داده‌های حساس مانند سرورهای خصوصی خود دشوار است. با سرویس‌های DLP Cloud Symantec می‌توانید به آسانی کنترل‌های قدرتمند محافظت از اطلاعات را به فضای ابری توسط DLP ارائه‌شده برای آن گسترش دهید. سرویس‌های DLP Cloud Symantec قابلیت‌های پایش، نظارت و حفاظت کامل را برای طیف گسترده‌ای از برنامه‌های ابری و همچنین برنامه‌های کاربردی در محل ارایه می‌کنند.

سرویس تشخیص ابر Symantec DLP محتوای استخراج شده از برنامه های ابری و ترافیک وب را بررسی می کند و به طور خودکار خط مشی های اطلاعات حساس را اعمال می کند. این یکپارچه سازی ابر به ابر پیشرفته با Symantec CloudSOC راه کار پیشرفته ما برای امنیت دسترسی به ابر است که محافظت از اطلاعات در جریان و اطلاعات بایگانی را در بیش از ۱۰۰ برنامه ابری مجاز و غیرمجاز مانند Office 365، G-Suite، Box، Dropbox و Salesforce ارایه می‌دهد. یکپارچه سازی اجازه می دهد تا سیاست های موجود و تشخیص قوی را به برنامه های ابری گسترش دهید و همه حوادث را از کنسول DLP مدیریت کنید. کنترل‌ها شامل عدم اشتراک‌گذاری فایل‌های حساس، قرنطینه، جلوگیری از خروج آن‌ها از برنامه، و همچنین اعمال رمزگذاری مبتنی بر هویت و حقوق دیجیتال به‌طور خودکار برای فایل‌های خاص به اشتراک گذاشته شده با اشخاص ثالث است. سرویس DLP Cloud Detection همچنین یکپارچه سازی پیشرفته با سرویس امنیت وب Symantec برای نظارت بر ترافیک وب - حتی زمانی که رمزگذاری شده است - ارایه می دهد و از کاربران رومینگ و تلفن همراه محافظت می کند.

Symantec DLP Cloud Servic for Email نظارت دقیق و آنی بر ترافیک ایمیل سازمانی را با بهره‌گیری از قابلیت‌های هوشمند داخلی و تشخیص پیشرفته که نتایج اشتباه را به حداقل می‌رساند، ارایه می‌کند. همچنین با مسدود کردن خودکار پیام‌رسانی یا اصلاح پیام برای اعمال رمزگذاری یا قرنطینه پایین‌دستی، محافظت آنی از نشت اطلاعات را فراهم می کند. هنگامی که داده ها با اشخاص ثالث به اشتراک گذاشته می شود، می تواند به طور خودکار رمزگذاری مبتنی بر هویت و حقوق دیجیتال را برای بدنه های ایمیل و پیوست ها فعال کند. سرویس DLP Cloud برای ایمیل از Gmail for Work، Microsoft Office 365 Exchange و Online همچنین Microsoft Exchange Server پشتیبانی می کند که به‌صورت مستقل یا همراه با قابلیت‌های برتر حفاظت از تهدیدات ایمیل سرویس Email Security.cloud در دسترس است.

مدیریت یکپارچه و شفاف

هرچه اطلاعات شما در طیف وسیع‌تری از دستگاه‌ها و محیط‌های ذخیره‌سازی پخش می‌شوند، توانایی تعریف و اجرای مداوم خط‌مشی‌ها حتی حیاتی‌تر می‌شود. Symantec DLP یک کنسول مدیریتی یکپارچه به شما می دهد. **DLP Enforce Platform** به شما امکان می دهد یک بار خط مشی ها را بنویسید و سپس آنها را در همه جا اجرا کنید؛ در تمام کانال هایی که امکان نشت اطلاعات وجود دارد.



با **DLP Enforce Platform** می توانید:

• از یک **کنسول واحد مبتنی بر وب** استفاده کنید تا خط‌مشی‌های از دست دادن داده‌ها را تنظیم کنید، حوادث را اصلاح کنید، و مدیریت سیستم را در تمام نقاط پایانی، دستگاه‌های تلفن همراه، سرویس‌های مبتنی بر ابر، و شبکه‌های داخلی و سیستم‌های ذخیره‌سازی انجام دهید.

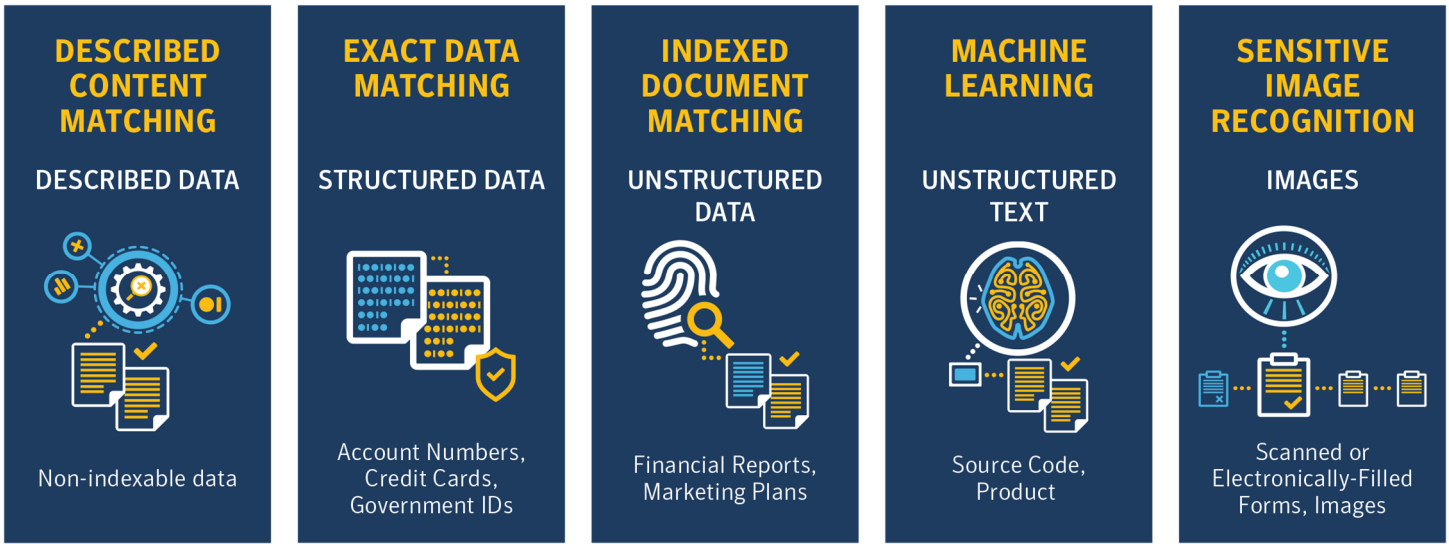
• از بیش از **۷۰ الگوی خط مشی از پیش تعریف شده** و یک **خط مشی ساز** مناسب برای راه اندازی و اجرای سریع سیستم خود بهره ببرید.

• از قابلیت های **جریان کار قوی و تصحیح** برای ساده سازی و خودکارسازی فرآیندهای واکنش به حادثه برای محیط های پرترافیک استفاده کنید.

• از هوش تجاری خود با استفاده از **ابزار تحلیلی پیشرفته Symantec IT Analytics for DLP**، که گزارش‌دهی پیشرفته و قابلیت‌های تجزیه و تحلیل موقت را ارائه می‌دهد برای کاهش ریسک خود استفاده کنید.

دید بی نظیری از اطلاعات محرمانه دریافت کنید

هسته اصلی هر راه کار DLP شناسایی آگاهانه محتوا است. تکنیک‌های تشخیص محتوا، یافتن اطلاعات حساس ذخیره شده در هر مکان و با هر فرمت فایل را ممکن می‌سازد. Symantec DLP جامع‌ترین تشخیص را با یادگیری ماشینی پیشرفته، تشخیص تصویر، اثر انگشت و توصیف فناوری‌هایی ارائه می‌دهد که داده‌ها را به‌طور دقیق طبقه‌بندی می‌کند، بنابراین لازم نیست نگران موارد تشخیص اشتباه و تاثیرگذاری بر کاربران تجاری باشید.



• **Described Content Matching** محتوا را به وسیله مطابقت محتوای توصیف شـده با موارد جسـت‌وجو شـده بر روی کلمات کلیدی خاص، عبارات یا الگوهای منظم و ویژگی‌های فایل، شناسایی می‌کند. Symantec DLP بیش از ۱۳۰ شناسه داده خارج از جعبه را ارایه می دهد، که الگوریتم های از پیش تعریف شـده ای هسـتند که تطبیق الگو را با هوش داخلی ترکیب می کنند تا از تشـخیص اشـتباه جلوگیری کنند.

• **Exact Data Matching** اطلاعات را با انگشـت نگاری یا نمایه سـازی منابع اطلاعات سـاختاریافته مانند پایگاه های داده، سـرورهای دایرکتوری و سـایر فایل های داده ساخت یافته شناسایی می کند.

• **Indexed Document Matching** از روش های انگشت نگاری برای شناسـایی داده های ذخیره شده در اسناد بدون ساختار، از جمله اسناد Microsoft Office، فایل های PDF و فایل های باینری مانند JPEG، طرح های CAD و فایل های چند رسانه ای استفاده می کند. IDM همچنین محتوای «مشتق‌شده» را شناسایی می‌کند، مانند متنی که از یک سند منبع به فایل دیگری کپی شده است.

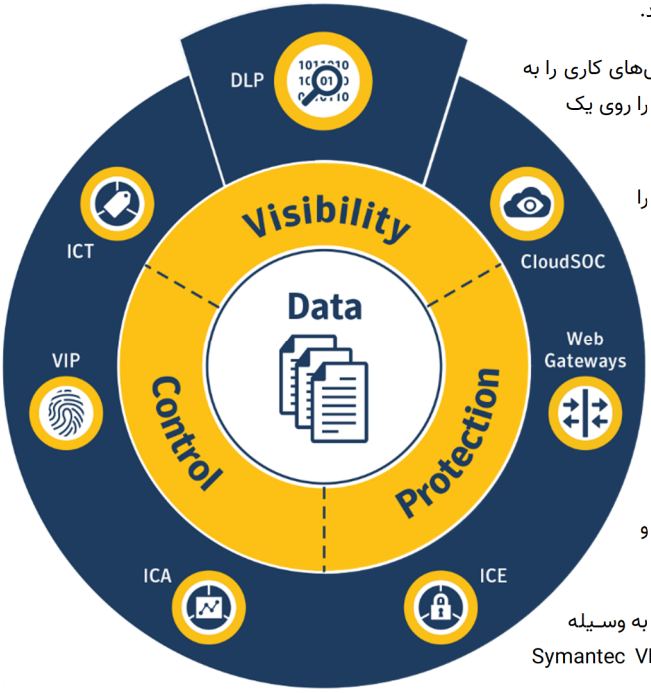
• **Sensitive Image Recognition** متن جاسازی شده در تصاویر مانند فرم های اسکن شده، اسناد، اسکرین شات ها، تصاویر و فایل های PDF را با استفاده از فناوری تشـخیص فرم اختصـاصـی و موتور تشـخیص کاراکتر نوری داخلی (OCR) شناسایی می کند.

• **Vector Machine Learning** از مالکیت معنوی با ویژگی های ظریف محافظت می کند که توصیف آنها گنگ یا دشوار است، مانند گزارش های مالی و کد منبع. برخلاف سایر فناوری‌های تشخیص، یادگیری ماشین برداری نیازی به مکان یابی، توصیف یا اثرانگشت داده‌هایی که برای محافظت از آن نیاز دارید ندارد.

Symantec DLP همچنین مجموعه ای کامل از API های بیرونی و افزودنی را ارایه می دهد تا به شما امکان سفارشی سازی و ادغام با طیف گسترده ای از محصولات امنیتی شـخص ثالث، ابر و برنامه های اختصـاصـی را بدهد؛ از جمله: DLP REST API، DLP FlexResponse API، DLP Content Extraction API، DLP Incident Reporting و DLP API Detection Virtual Appliance و Update API.

گسترش خط‌مشی‌های DLP به برنامه‌های ابری

از آنجایی که اطلاعات حساس با کاربران بیرونی به اشتراک گذاشته می شوند یا به ابر و خارج از محیط مدیریت شده شما منتقل می شوند، در معرض آسیب‌پذیری بیشتری هستند. راه کار Symantec's Information Centric Security با امنیت دسترسی ابری مبتنی بر سیاست، طبقه بندی، رمزگذاری، تجزیه و تحلیل کاربر و دروازه های وب، از اطلاعات شما در سراسر چرخه عمر خود فراتر از محل های مدیریت شده شما محافظت می کند.



• **گسـترش خط‌مشـی‌های DLP به برنامه‌های ابری:** تشـخیص DLP، خط‌مشـی‌ها و گردش‌های کاری را به برنامه‌های ابری از طریق ادغام با Symantec CloudSOC (CASB) گسـترش دهید و حوادث را روی یک کنسول واحد مدیریت کنید.

• **طبقه‌بندی داده‌ها بر اسـاس حسـاسـیت:** کاربران را قادر می‌سـازد تا فایل‌های حسـاس را طبقه‌بندی و برچسـب‌گذاری کنند و با اسـتفاده از راه‌حل طبقه‌بندی داده‌های Symantec از اطلاعات محوری (ICT) آنها بر اساس حساسیت محافظت کنند.

• **محافظت از داده‌ها در صـورت اشـتراک‌گذاری در خارج از شـرکت:** به‌طور خودکار رمزگذاری دائمی و حقوق دیجیتالی را برای داده‌ها هنگام خروج از محل مدیریت شـده اعمال کنید، کنترل کنید چه کسی می‌تواند از آن استفاده کند، آن‌ها را در همه جا ردیابی کند، و در صورت لزوم با رمزگذاری اطلاعات محور (ICE) دسترسی را لغو کنید.

• **سـطح بندی حادثه و مدیریت خط مشـی را سـاده کنید:** زمان و تلاش برای اصـلاح حادثه و مدیریت خط مشـی را کاهش دهید و نیز ریسـک اطلاعات را با تجزیه و تحلیل رفتار کاربر و موجودیت به وسیله Symantec Information Centric Analytics (ICA) کاهش دهید.

• **به اشـتراک گذاری ایمن تر اطلاعات با با دیگران:** از دسـترسـی غیرمجاز به اطلاعات حسـاس به وسـیله احراز هویت قوی هنگامی که اطلاعات با شـرکای تجاری با Symantec VIP Identity and Access Management به اشتراک گذاشته می شوند، جلوگیری کنید.

• **از انتقال اطلاعات به سـایت‌های ناخواسـته جلوگیری کنید:** با اسـتفاده از یکپارچه‌سـازی DLP با دروازه‌های وب امن Symantec از جمله: Symantec ProxySG و Web Security Service، اطمینان حاصل کنید که اطلاعات حساس از طریق ترافیک وب غیرقابل اعتماد، حتی ترافیک رمزگذاری شده، به بیرون درز نمی‌کنند.

حداقل سیستم مورد نیاز

راهکار Symantec DLP شـامل یک پلت فرم مدیریت یکپارچه، عامل نقطه پایانی سـبک وزن و محصـولات قدرتمند تشـخیص محتوا اسـت. ما بیشـترین انعطاف پذیری اسـتقرار را با طیف گسـترده ای از گزینه ها برای هر نوع محیطی ارایه می دهیم: نرم افزار داخلی، لوازم مجازی و فیزیکی، خدمات ابری عمومی، خصوصی و ترکیبی و خدمات مدیریت شده ارایه شده توسط Symantec Partners. بر خلاف راه حل های دیگر، Symantec DLP ثابت شده است که در محیط های توزیع شـده در مقیاس صـدها هزار کار می کند. برای اطلاعات کامل مورد نیاز سـیسـتم Symantec Data Loss Prevention از صـفحه پشتیبانی ما دیدن کنید.

از همین امروز محافظت از اطلاعات خود را شروع کنید

شـرکت رایان سـامانه آرکا آماده اسـت به شـما کمک کند تا سـیاسـت های امنیتی و انطباق خود را فراتر از مرزهای فایروال خود گسـترش دهید تا بتوانید اطلاعات خود را به طور کامل و موثرتر پایش، نظارت و محافظت کنید. با کمترین هزینه سیاسـت های بصـری و ابزارهای مدیریت حادثه و پوشـش جامع در همه کانال های پرخطر شما به صورت پایدار مستقر می شود.

تهران، خیابان شهید بهشتی ، خیابان پاکستان ، کوچه چهارم ، پلاک ۱۱ ، طبقه چهارم ، واحد ۷
تلفن: ۸۸۸۰۴۹۶۱ | دورنگار: ۸۹۷۸۳۷۳۷ | کدپستی : ۱۵۳۱۶۴۵۹۱۸
info@arka.ir www.arka.ir
رایان سامانه آرکا