Solución Symantec Data Loss Prevention

Descubra, monitoree y proteja su información corporativa confidencial

Hoja de Datos: Prevención Contra la Pérdida de Datos

Protegiendo su Información en un Mundo Móvil y Centrado en la Nube

Mantener la seguridad y el cumplimiento de la información corporativa confidencial nunca ha sido fácil. Sin embargo, hoy usted se enfrenta a un conjunto totalmente nuevo de desafíos de protección de los datos. La información confidencial está abandonando la seguridad de su red corporativa, ya que más empleados comparten archivos en los servicios para consumidores de almacenamiento en la nube y acceden a estos archivos en sus propios dispositivos móviles. Las cifras de ataques cibernéticos dirigidos siguen creciendo, a medida que los cibercriminales desarrollan nuevos y efectivos métodos para desafiar las medidas de seguridad tradicionales y robar información corporativa. Con la convergencia de estos factores se vuelve difícil gestionar la información corporativa y protegerla contra la pérdida y el robo.

Entonces, ¿cómo gestiona y protege su información en este desafiador entorno? ¿Cómo sería una estrategia de protección de datos completa y exitosa frente a la aparición de perímetros de seguridad, al aumento de ataques dirigidos y a los hábitos y expectativas cambiantes del usuario?

Symantec Data Loss Prevention (DLP) responde a estas preguntas con un enfoque amplio sobre la protección de la información, que abarca las realidades de hoy en día centradas en la nube y en la movilidad. Con DLP, se puede:

- **Descubrir** dónde son almacenados los datos a lo largo de sus sistemas en la nube, móviles, de red, de extremos y de almacenamiento
- **Monitorear** cómo se utilizan estos datos, estén sus empleados en la red o fuera de ella
- **Proteger** los datos contra la pérdida y la fuga, sin importar en dónde estén almacenados o cómo se utilizan

El enfoque y la tecnología líder en el mercado de Symantec amplían el alcance de sus capacidades de DLP a la nube y a los dispositivos móviles. Le dan la habilidad para extender sus políticas de seguridad y cumplimiento más allá de las fronteras de su propia red. Además, ofrecen el costo de propiedad más bajo, con metodologías de implementación comprobadas, políticas intuitivas y herramientas de gestión de incidentes y un amplio cubrimiento a lo largo de todos sus canales de alto riesgo.

Descubra más Datos con la Detección con Atención en el Contenido

Symantec DLP empieza con una combinación de tecnologías avanzadas que pueden detectar con precisión todos los datos confidenciales en su organización – estén en reposo, en movimiento o en uso. Entre las tecnologías de detección de Symantec DLP están:

- **Exact Data Matching (EDM)** detecta el contenido a través de la huella digital de fuentes de datos estructurados, incluyendo bases de datos, servidores de directorio u otros archivos de datos estructurados.
- **Indexed Document Matching (IDM)** aplica métodos de huella digital para detectar datos confidenciales almacenados en datos no estructurados, incluyendo documentos de Microsoft Office, PDF y archivos binarios, como JPEG, diseños CAD y

archivos multimedia. La IDM también detecta contenido "derivado", como textos que han sido copiados de un documento fuente a otro archivo.

- **Vector Machine Learning (VML)** protege la propiedad intelectual que posee características sutiles, que pueden ser raras o difíciles de describir, tales como reportes financieros y código fuente. La solución detecta este tipo de contenido llevando a cabo un análisis estadístico de los datos no estructurados y comparándolos con contenidos o documentos similares. A diferencia de otras tecnologías de detección, el VML no requiere que usted localice, describa o genere su huella digital para los datos que desea proteger.
- **Described Content Matching (DCM)** detecta contenido buscando coincidencias en palabras clave específicas, expresiones o estándares regulares y propiedades del archivo. Symantec DLP proporciona más de 30 identificadores de datos de uso inmediato, como algoritmos predefinidos que combinan la correlación de estándares con inteligencia incorporada para evitar falsos positivos. El identificador de datos "número de la tarjeta de crédito", por ejemplo, detecta estándares de 16 dígitos y los valida con una "comprobación Luhn".
- La **detección de tipo de archivo** reconoce y detecta más de 330 tipos de archivos diferentes, como correos electrónicos, gráficos y formatos encapsulados. Usted puede configurar su Symantec DLP para reconocer prácticamente cualquier tipo de archivo personalizado y también le permite extraer contenido de formatos de archivo específicos – incluyendo formatos cifrados – usando API de extracción de contenido.

Trabajando juntas, estas tecnologías de detección con atención en el contenido hacen posible la reducción de los falsos positivos, minimizan el impacto de sus esfuerzos en DLP sobre los usuarios finales y encuentran información confidencial almacenada en prácticamente cualquier parte y formato.

Defina y Haga Cumplir Consistentemente las Políticas a lo Largo de Todo su Entorno

A medida de que sus datos se dispersan a lo largo de una amplia gama de dispositivos y entornos de almacenamiento, la habilidad para definir y hacer cumplir consistentemente las políticas se vuelve imprescindible. Symantec DLP cuenta con una consola de gestión unificada, DLP Enforce Platform, y la herramienta de reporte de inteligencia empresarial, IT Analytics for DLP, que le permite escribir sus políticas una vez y después hacerlas cumplir en todas partes, reduciendo de forma medible los riesgos de la información. Con **DLP Enforce y IT Analytics**, se puede:

- Usar una **única consola basada en la web** para definir políticas de pérdida de datos, revisar y corregir incidentes y además llevar a cabo una gestión del sistema a lo largo de todos sus extremos, dispositivos móviles, servicios basados en la nube y sistemas de red y almacenamiento internos.
- Aprovechar más de **60 plantillas de políticas pregeneradas** y un conveniente **generador de políticas** para poner en marcha y ejecutar su solución de DLP rápidamente.
- Aprovechar **las capacidades de flujo de trabajo** robusto y de corrección para agilizar y automatizar los procesos de respuesta a los incidentes.
- Aplicar **inteligencia empresarial** a sus esfuerzos en DLP con **una sofisticada herramienta de análisis** que brinda capacidades de reporte avanzado y de análisis ad hoc. Esto incluye la habilidad para extraer y resumir datos del sistema en cubos multidimensionales y, luego, crear reportes relevantes, paneles y cuadro de mandos para las diferentes partes interesadas de su organización.

Symantec DLP está listo para ayudarle a encontrar y monitorear todos los datos confidenciales en su entorno diverso. Con Enforce Platform también estará seguro de poder aplicar políticas consistentes y tomar las medidas necesarias para mantener la información segura y protegida.

Monitoree y Proteja su Almacenamiento y Correos Electrónicos Basados en la Nube

Para muchas empresas, mover las aplicaciones internas a la nube es una forma inteligente para aumentar la agilidad y reducir los costos. Pero, ¿cómo le sacamos ventaja a la nube sin perder visibilidad o entregar el control de su información corporativa confidencial? **Symantec DLP for Cloud Storage y Cloud Prevent for Microsoft Office 365** solucionan este problema proporcionando capacidades robustas de descubrimiento, monitoreo y protección para sus correos electrónicos y su almacenamiento basados en la nube.

Symantec DLP for Cloud Storage permite la colaboración segura y le proporciona profunda visibilidad de todos los archivos corporativos que los usuarios están almacenando y compartiendo en Box. Proporciona avanzadas capacidades de descubrimiento de contenido para que usted pueda analizar las cuentas Business y Enterprise de Box y comprender qué datos confidenciales se están almacenado, cómo se utilizan y con quién se comparten. Cloud Storage anima incluso a los usuarios a corregir violaciones a la política mediante el uso de etiquetas visuales en archivos de Box, permitiendo la corrección de incidentes desde un portal intuitivo en línea, Data Insight Self-Service Portal.

Symantec DLP Cloud Prevent for Microsoft Office 365 le permite migrar con confianza su correo electrónico a la nube, integrándose impecablemente con Office 365: Exchange Online. Le brinda visibilidad y control profundos sobre correos electrónicos confidenciales enviados por los usuarios con un robusto monitoreo del contenido y capacidades de protección. Con Cloud Prevent se puede detectar información corporativa confidencial y tomar las medidas apropiadas en el momento adecuado, notificando a los usuarios sobre las violaciones a la política, redirigiendo el correo electrónico a una puerta de enlace de cifrado para un envío seguro o bloqueando un correo en tiempo real para evitar la pérdida de datos confidenciales.

Mantenga la Seguridad de los Datos en Extremos Tradicionales

A pesar de que los dispositivos móviles y el almacenamiento en la nube se están volviendo más populares y difundidos, los extremos siguen sirviendo como el principal repositorio para información confidencial corporativa. **Symantec DLP Endpoint Discover y Endpoint Prevent** se asegurarán de que usted pueda mantener toda esa información segura y protegida, dándole la habilidad para descubrir, monitorear y proteger datos confidenciales en escritorios tradicionales y virtuales – estén los usuarios dentro o fuera de la red corporativa.

Con Symantec DLP, un único agente altamente escalable habilita los módulos Endpoint Discover y Endpoint Prevent. Trabajando juntos, le permiten:

- **Llevar a cabo un escaneo, detección y monitoreo local en tiempo real** para un amplio rango de eventos en Windows 7, Windows 8, Windows 8.1 y máquinas Mac OS X.
- **Monitorear datos confidenciales** que se descargan, se copian o se transmiten a/desde computadoras portátiles y de

escritorio. Esto incluye:

- **Aplicaciones:** Outlook
- **Almacenamiento en la nube:** Box, Dropbox, Google Drive y Microsoft OneDrive
- **E-mail:** Outlook y Lotus Notes
- **Protocolos de red:** HTTP/HTTPS y FTP
- **Almacenamiento extraíble:** tarjetas USB, MTP, CF e SD, eSATA y FireWire
- **Escritorios virtuales:** Citrix, Microsoft Hyper-V y VMware

- **Notificar a los usuarios con una ventana emergente de alerta en pantalla** o bloquear acciones específicas cuando se detecta una violación a la política.
- **Escanear discos locales en computadoras portátiles y de escritorio** para brindar un inventario completo de datos confidenciales, para que usted pueda proteger o reubicar archivos expuestos.
- Usar **múltiples opciones de escaneo**, como el escaneo inactivo y el escaneo diferencial, permitiendo un alto desempeño, escaneo paralelo de miles de extremos con un impacto mínimo sobre sus sistemas.
- **Implementar una arquitectura altamente escalable de diferentes niveles** que pueda proteger a cientos de miles de usuarios de extremos.

Extienda la Protección Completa de los Datos a sus Dispositivos Móviles

La política BYOD ("traiga su propio dispositivo") está borrando los límites que separan la vida personal y la laboral. Hoy, los usuarios esperan simplemente ser capaces de acceder a datos corporativos confidenciales en cualquier momento, desde cualquier dispositivo y usando cualquier tipo de conexión. De hecho, 2 de cada 5 empleados admiten que descargaron archivos del trabajo en sus smartphones o tabletas personales. **Symantec DLP for Mobile** le brinda la visibilidad y el control que necesita para abrazar esta tendencia y proporcionar el acceso móvil flexible que los usuarios quieren, sin poner su información en riesgo. Con Symantec DLP for Mobile, se puede:

- **Extender las capacidades de monitoreo y protección de DLP** a todos sus dispositivos iOS y Android, sin importar quién sea el dueño.
- Aprovechar el módulo avanzado **Mobile Email Monitor** para detectar descargas de correos confidenciales en dispositivos Android e iOS a través del protocolo Microsoft Exchange ActiveSync. Estas capacidades de supervisión son implementadas en el punto de salida de su red y se integran con su proxy web inverso para un monitoreo móvil y ininterrumpido del correo.
- Usar el módulo **Mobile Prevent** para monitorear las actividades de los usuarios y evitar la transmisión de datos confidenciales a través del cliente nativo de correo de iOS, del explorador web y de otras aplicaciones, tales como Dropbox y Facebook. Mobile Prevent se conecta a la red de su empresa a través de redes de telefonía celular 3G y 4G, redes Wi-Fi e iOS VPN On Demand. El tráfico móvil de salida es distribuido a través de una red virtual privada (VPN) a su proxy web y luego a Mobile Prevent, que analiza la información y remueve o bloquea automáticamente los datos confidenciales.

Encuentre y Proteja sus Esquivos Datos no Estructurados

Los datos no estructurados están creciendo a una tasa alarmante del 70% al año, por eso, no es una sorpresa que muchas organizaciones luchen para gestionarlos y protegerlos con eficacia. Trabajando juntos, **Symantec DLP Network Discover, Network Protect, Data Insight y Data Insight Self-Service Portal** le permiten tomar las riendas de todos sus datos no estructurados, para que no estén vulnerables a empleados descuidados y atacantes malintencionados.

Primero, **Symantec DLP Network Discover** encuentra y pone al descubierto los datos confidenciales escaneando los archivos compartidos de la red, las bases de datos y otros repositorios de datos de la empresa. Esto incluye sistemas locales de archivos en servidores Windows, Linux, AIX y Solaris; bases de datos Lotus Notes y SQL; y servidores Microsoft Exchange y SharePoint. DLP Network Discover reconoce más de 330 tipos de archivo diferentes – incluyendo archivos personalizados – basado en la firma binaria del archivo. También proporciona un escaneo de alta velocidad para entornos distribuidos y amplios y optimiza el desempeño escaneando solamente de los archivos nuevos o modificados. Network Discover se implementa dentro de su entorno LAN corporativa y comunica información de políticas e incidentes directamente a través de Enforce Platform centrada.

Luego, **Symantec DLP Network Protect** añade capacidades robustas de protección de archivos en Network Discover. Network Protect limpia automáticamente y protege todos los archivos expuestos detectados por Network Discover y ofrece un amplio rango de opciones de corrección, incluyendo poner en cuarentena o moviendo archivos, copiando archivos al área de cuarentena o aplicando un cifrado basado en las políticas y derechos digitales para archivos específicos. Además, Network Protect educa a los usuarios empresariales sobre las violaciones a la política, dejando un marcador de texto en la ubicación original del archivo para explicar por qué está entrando en cuarentena.

Symantec DLP también incluye una **FlexResponse API Platform**, que le permite construir acciones personalizadas de corrección de archivos. FlexResponse proporciona una integración completa con otras soluciones de seguridad de archivos de Symantec y de terceros, incluyendo Symantec File Share Encryption, Microsoft Rights Management Services, Liquid Machines, GigaTrust y Adobe LiveCycle.

Para terminar, **Symantec Data Insight** recopila y analiza eventos de usuario de archivadores de almacenamiento adjunto a la red (NAS), servidores Windows y SharePoint. Esta solución de gobernanza de datos, diseñada específicamente para entornos de datos no estructurados, proporciona inteligencia rica y práctica sobre la propiedad, uso y controles de acceso. Data Insight también se integra con Network Discover para descubrir archivos confidenciales, identificar a los propietarios de los datos, entender los permisos de los archivos y el historial de accesos y lo alerta sobre actividad sospecha de usuarios. Con Symantec Data Insight, puede finalmente encender una luz en lo relacionado con los esquivos “datos oscuros”, comprendiendo exactamente qué datos están en su entorno, cómo se utilizan, quién es el dueño y quién tiene acceso a ellos.

Symantec Data Insight también cuenta con un **Portal de Autoservicio** que añade capacidades eficientes del flujo de trabajo para la corrección de incidentes, dándole a los dueños de los datos, la habilidad de revisar y corregir los incidentes de archivos de la red. Con Data Insight Self-Service Portal, los propietarios de los datos son notificados automáticamente vía correo electrónico en los eventos de violaciones a la política y luego son dirigidos a un portal intuitivo basado en la web para corregir la violación. El equipo de seguridad de TI también puede ver y realizar seguimiento de la actividad de los incidentes a través de la consola de gestión de Enforce Platform.

Juntos, estos cuatro módulos esenciales de DLP le permiten descubrir, proteger y gestionar datos confidenciales a lo largo de prácticamente cualquier sistema de almacenamiento y mantener la seguridad de todos sus datos no estructurados – sin importar que tan rápido crezcan.

Monitoree y Proteja sus Datos en Movimiento

Las investigaciones muestran que cerca de la mitad de los empleados envía por correo electrónico archivos del trabajo a sus cuentas personales, por eso, no es ninguna sorpresa que el correo y la web sean los canales más comunes para la pérdida de datos. **Symantec DLP Network Monitor, Network Prevent for Email y Network Prevent for Web** pueden ayudarle a eliminar este problema casi universal, dándole la habilidad para monitorear un amplio rango de protocolos de red y evitar que, tanto usuarios de red autorizados como no autorizados den un mal uso a los datos confidenciales.

Primero, **Network Monitor** detecta los datos confidenciales enviados a través de un rango de protocolos de red, incluyendo SMTP, HTTP, FTP, IM, NNTP, protocolos personalizados de puerto específico y protocolo de internet versión 6 (IPv6). Realiza una profunda inspección del contenido de todas las comunicaciones de la red sin pérdida de paquetes, a diferencia de otras soluciones que muestrean paquetes durante picos de carga y que lo ponen en alto riesgo de recibir falsos negativos. Network Monitor se implementa en el punto de salida de la red y se integra al puerto de acceso para pruebas de su red (network tap) o a su analizador de puerto conmutado (SPAN).

Luego, **Symantec DLP Network Prevent for Email** inspecciona el correo electrónico corporativo en busca de datos confidenciales, notifica al usuario sobre las violaciones a la política y bloquea o redirige el correo a puertas de enlace de cifrado para un envío seguro. Network Prevent también se implementa en el punto de salida de su red y se integra a su agente de transporte de correo (MTA) compatible con SMTP y servicios en la nube, como Symantec Email Security.cloud.

En última instancia, **Symantec DLP Network Prevent for Web** inspecciona el tráfico de salida enviado a través de HTTP y HTTPS, notifica a los usuarios sobre las violaciones a la política y bloquea o remueve condicionalmente los datos de los mensajes web. Al igual que los otros dos módulos, Network Prevent for Web es implementado en el punto de salida de su red y se integra a proxies web compatibles con ICAP y a servicios en la nube, como Google Apps y Symantec Web Security.cloud.

Comience Construyendo Hoy su Solución Unificada de Protección de la Información

Symantec está lista para ayudarle a extender su prevención contra la pérdida de datos a la nube y a lo largo de todos sus canales con alto riesgo de pérdida de datos, para que usted pueda descubrir, monitorear y proteger su información de manera más completa y eficaz – esté esta en reposo, en movimiento o en uso.

Ingrese a Symantec.com/data-loss-prevention para más información y conozca las ventajas de un enfoque unificado sobre la base de la prevención contra la pérdida de datos diseñada para el mundo móvil y centrado en la nube de los días de hoy.

Requisitos del Sistema

Symantec DLP consiste en una plataforma de gestión unificada, servidores de detección con atención en el contenido y agentes de extremos ligeros. También ofrece una variedad de opciones de implementación flexibles, incluyendo la implementación local, en la nube híbrida y como un servicio gestionado (a través de un socio especializado de Symantec DLP). A diferencia de otras soluciones de DLP, Symantec ha probado su habilidad para trabajar en entornos altamente distribuidos y alcanzar a cientos de miles de usuarios y dispositivos.

Servidores DLP

Sistema Operativo	Microsoft Windows Server 2008, 2012 Red Hat Enterprise Linux VMware ESX y ESXi
Procesador	2 X CPU de 3 GHz
Memoria	6 a 8 GB
Almacenamiento	140 GB
Red	1 de Cobre o Fibra de 1 GB/Ethernet NIC de 100 MB
Base de Datos	Oracle 11g Standard Edition

Agentes de extremos de DLP

Sistema Operativo	Apple Mac OS X Microsoft Windows Microsoft Windows Server 2003, 2008 Citrix XenApp y XenDesktop Microsoft Hyper-V
Procesador	2 X CPU de 3 GHz
Memoria	6 a 8 GB
Almacenamiento	140 GB
Red	1 de Cobre o Fibra de 1 GB/Ethernet NIC de 100 MB
Base de Datos	Oracle 11g Standard Edition

Para más Información

Ingrese a nuestra página

http://go.symantec.com/dlp

Para hablar con un experto del productos en EE.UU.

Llame gratuitamente al 1 (800) 745 6054

Para hablar con un experto del producto fuera de EE.UU.

Para las oficinas de los países y números de contacto específicos, ingrese a nuestra página.

Acerca de Symantec

Symantec Corporation (NASDAQ: SYMC) es una compañía experta en protección de la información que ayuda a personas, empresas y gobiernos que buscan la libertad para abrirse a las oportunidades que trae la tecnología – en cualquier momento y lugar. Fundada en abril del 1982, Symantec, una compañía Fortune 500 que opera una de las redes de inteligencia de datos más grandes del mundo, ha proporcionado soluciones líderes en seguridad, soporte y disponibilidad en lugares donde información vital es almacenada, accedida y compartida. Los más de 20 mil empleados de la compañía residen en más de 50 países. El noventa y nueve por ciento de las compañías Fortune 500 son clientes de Symantec. Durante el año fiscal del 2014, Symantec registró ingresos de US$ 6,7 mil millones. Para más información, ingrese a www.symantec.com o conéctese con Symantec en: go.symantec.com/socialmedia.

Sede Global de Symantec

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

21350666 05/15