



McAfee DLP Prevent

Implemente directivas para proteger su información confidencial.

Ventajas principales

Aprovechamiento de la infraestructura existente

- Protege el correo electrónico de la empresa a través de la integración con gateways MTA que utilizan SMTP con encabezados X para bloquear, devolver, cifrar, poner en cuarentena y redireccionar.
- Proporciona control del tráfico a través de la integración de proxies web compatibles con ICAP para impedir las infracciones de contenido a través de HTTP, HTTPS, mensajería instantánea, FTP y correo web.

Implementación de directivas de forma proactiva para todos los tipos de información

- Protege más de 300 tipos de contenido exclusivos.
- Permite implementar directivas para la información que sabe que es confidencial, así como para la que no es tan obvia.
- Se puede escalar hasta cientos de miles de conexiones simultáneas.

Clasificación, análisis y corrección de fugas de datos

- Permite filtrar y controlar la información confidencial para disponer de protección contra los riesgos conocidos y desconocidos.
- Admite indexación e implementación de directivas de seguridad específicas para todos los tipos de contenido.
- Aplica directivas sobre el acceso a los recursos compartidos de archivos internos para impedir que los usuarios accedan a información o a repositorios sin autorización.

Cuanto mayor sea el número de personas que comparten información de forma electrónica, mayor será la probabilidad de que alguien de manera involuntaria o intencionada envíe información confidencial a una persona no autorizada y ponga en riesgo los datos de la empresa. Ya sea a través del correo electrónico, la Web, la mensajería instantánea o FTP, la información puede salir de la empresa por medio de una gran variedad de canales. Algunos mensajes o transacciones están autorizados, pero deben cifrarse para garantizar la privacidad de los datos. Otros tipos de comunicaciones simplemente no son aceptables en ningún momento y deben bloquearse. La implementación de las directivas adecuadas en el momento justo es esencial para garantizar la seguridad de los datos, el cumplimiento de las normativas y la protección de la propiedad intelectual.

Implementación de directivas de seguridad para los datos en movimiento

En todas las divisiones de todas las empresas, los empleados comparten datos mediante varias aplicaciones y distintos protocolos. Protéjase contra la pérdida de datos inadvertida o intencionada, protegiendo la información confidencial de forma proactiva para evitar que salga de la red, e implemente los procesos empresariales adecuados.

McAfee® Data Loss Prevention (DLP) Prevent le ayuda a implementar directivas para la información que abandona la red a través del correo electrónico, el correo web, la mensajería instantánea, los wikis, los blogs, los portales, y las transferencias HTTP/HTTPS o FTP, todo gracias a la integración con gateways de agente de transferencia de mensajes (MTA) a través de SMTP o proxies web ICAP. Si detecta una infracción de las directivas, McAfee DLP Prevent permite a las empresas adoptar una serie de medidas, como el cifrado, el bloqueo, la redirección, la puesta en cuarentena, etc. Esto permite garantizar el cumplimiento de las normativas en materia de confidencialidad de la información privada y reducir el riesgo de amenazas para la seguridad.

Integración con proxies web y agentes de transferencia de mensajes (MTA) para una mayor protección

McAfee DLP Prevent integra proxies web (que utilizan ICAP) y agentes MTA (que utilizan encabezados X) para llevar a cabo la acción adecuada. Al detener las transacciones no autorizadas a nivel de aplicación, en lugar de limitarse a interrumpir la sesión TCP lo que no alteraría el comportamiento de las aplicaciones, McAfee DLP Prevent alerta a la aplicación de inicio de que se ha rechazado un transmisión debido a la infracción de una directiva. Esto garantiza una mayor protección de su organización, ya que McAfee DLP Prevent "aprende" lo que debe protegerse e impide que la aplicación repita el mismo comportamiento.

Protección de la información confidencial conocida y desconocida

Gracias a la capacidad de clasificar más de 300 tipos de contenido distintos, McAfee DLP Prevent le ayuda a garantizar la seguridad de la información confidencial obvia (números de identificación personal y de tarjetas de crédito, y datos financieros) y aprende que otro tipo de información o documentos no tan obvios deben

Ficha técnica

Especificaciones

Rendimiento del sistema

Hasta 150 Mbits/s de análisis, indexación y almacenamiento de contenido.

Integración en red

Se integra en la red como dispositivo fuera de ruta, que está activo dentro de la ruta de los datos mediante agentes MTA y proxies web compatibles con ICAP.

Tipos de contenido

Admite la clasificación de archivos de más de 300 tipos de contenido, incluidos:

- Documentos de Microsoft Office
- Archivos multimedia
- P2P
- Código fuente
- Archivos de diseño
- Archivos comprimidos
- Archivos cifrados

Protocolos admitidos

Admite los protocolos HTTP, HTTPS, FTP y de mensajería instantánea (IM), a través del protocolo ICAP a un servidor proxy compatible con ICAP. Póngase en contacto con su proveedor de servidor proxy para conocer los protocolos admitidos. Compatible con SMTP a través de la integración con agentes MTA.

Directivas integradas

- Proporciona una amplia gama de directivas integradas para requisitos comunes, incluido el cumplimiento de normativas, la propiedad intelectual y el uso aceptable.
- Permite la personalización total de las reglas para satisfacer las necesidades específicas, aprovechando la base de datos de McAfee.

protegerse, como la propiedad intelectual que es muy compleja. McAfee DLP Prevent incorpora una amplia variedad de directivas, que van desde el cumplimiento de normativas al uso aceptable y la propiedad intelectual, que le permiten comparar documentos completos o parciales con un conjunto de reglas completo, para que pueda proteger toda su información confidencial, tanto la conocida como la desconocida.

Vistas personalizables y reportes de incidentes

La consola de administración McAfee® ePolicy Orchestrator® (McAfee ePO™) le permite personalizar vistas de resumen de los incidentes de seguridad y de las acciones posteriores en función de cualquier pareja de puntos de referencia. También hay disponibles vistas detalladas y listas, así como resúmenes con las tendencias. McAfee DLP Prevent incluye además una gran cantidad de reportes preconfigurados, que pueden visualizarse, guardarse para uso posterior o planificarse para su entrega periódica.

Clasificación de los datos complejos

McAfee DLP Prevent ofrece a su organización la capacidad de proteger todos los tipos de datos confidenciales, desde datos sencillos de formato fijo a datos complejos y muy variables como la propiedad intelectual. Gracias a la combinación de estos mecanismos de clasificación por objeto, McAfee DLP Prevent genera un motor de clasificación detallado, que bloquea la información confidencial e identifica los riesgos ocultos o desconocidos. Los mecanismos de clasificación por objeto incluyen:

- **Clasificación en varios niveles:** cubre tanto la información contextual como el contenido en formato jerarquizado.
- **Registro de documentos:** incluye firmas biométricas de información a medida que cambia.
- **Análisis gramatical:** detecta la gramática o la sintaxis de todo tipo de información, desde documentos de texto a hojas de cálculo y código fuente.

- **Análisis estadístico:** establece cuántas veces se ha producido una coincidencia de firma, gramatical o biométrica en un documento o archivo concreto.
- **Clasificación de archivos:** identifica el tipo de contenido con independencia de la extensión aplicada al archivo o al tipo de compresión.

Especificaciones: Dispositivo McAfee DLP 5500

Componente	Requisito
Procesador	2 x Intel E5-2620 de 6 núcleos, 15 M de caché, 2 GHz, Intel QPI de 7,20 GT/S
Memoria	32 GB DDR3 - 1333 MHz
Fuente de alimentación	2 módulos de alimentación de 760 W intercambiables en caliente
Discos duros	Unidades 8x 2 TB SATA 7,2 K rpm
Tarjeta NIC	Módulo de E/S Ethernet de 1 Gbit/s, de dos puertos (cobre) de Intel
IPMI	Módulos de administración remota 4 de Intel (AXXRMM4)
Tamaño del producto	2 unidades en bastidor (2U)

Especificaciones: Máquina virtual

McAfee DLP Prevent está disponible como un dispositivo virtual que funciona en un entorno VMware. A continuación se indican los requisitos mínimos de hardware para ejecutar el dispositivo virtual.

Componente	Requisito
Procesador	vCPU Intel x86 4x
Memoria	16 GB de RAM
Unidades de disco duro	Unidad 1: tamaño mínimo de 100 GB para el software de máquina virtual Unidad 2: tamaño mínimo de 512 GB para la imagen virtual DLP
Puertos de red	4 NIC virtuales
BIOS	Subproceso con virtualización activa



McAfee. Part of Intel Security.

6205 Blue Lagoon Drive
Suite 600
Miami, Florida 33126
U.S.A.
www.intelsecurity.com

Intel y el logotipo de Intel son marcas comerciales registradas de Intel Corporation en EE. UU. y en otros países. McAfee y el logotipo de McAfee son marcas comerciales o marcas comerciales registradas de McAfee, Inc. o de sus empresas filiales en EE. UU. y en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros. Los planes, especificaciones y descripciones de productos mencionados en este documento se proporcionan únicamente a título informativo y están sujetos a cambios sin previo aviso; se ofrecen sin garantía de ningún tipo, ya sea explícita o implícita.
Copyright © 2013 McAfee, Inc. 60420ds_dlp-prevent_0813B