



# McAfee Data Loss Prevention Monitor

## Protección para los datos esenciales.

### Ventajas principales

#### Identificación y protección de los datos confidenciales

- Identifique rápidamente la información confidencial a través de un motor de búsqueda intuitivo.
- Realice análisis forenses para correlacionar los eventos de riesgo actuales y pasados, detectar tendencias de riesgos e identificar amenazas.
- Cree reglas de forma instantánea para prevenir comportamientos futuros.

#### Identificación y clasificación de todo el tráfico de la red

- Filtre y controle la información confidencial para identificar riesgos ocultos o desconocidos.
- Indexe todos los tipos de contenido y, a continuación, consúltelo y extráigalo para comprender la naturaleza de sus datos confidenciales y dónde se envían.
- Supervise el acceso compartido a archivos internos.

La protección de los datos confidenciales y personales de los clientes y los empleados, como números de tarjetas de crédito y documentos de identificación, es una prioridad para todos hoy día. La divulgación accidental de datos debido a un error del empleado, la pérdida de portátiles o dispositivos USB extraviados plantea problemas para la seguridad de casi cualquier organización. Para complicar aun más las cosas, los datos pueden filtrarse o acabar en manos de quien no deben cuando se transmiten y comparten a través de aplicaciones web como Google Gmail, Yahoo! Mail, las de mensajería instantánea y Facebook. McAfee® Data Loss Prevention (DLP) Monitor es una solución de prevención de pérdida de datos de alto rendimiento que puede analizar todas las comunicaciones a través de Internet y determinar cuándo la información no va al destino adecuado. Ayuda a minimizar la carga de trabajo de su equipo de seguridad, cumplir los requisitos de cumplimiento de normativas y proteger la propiedad intelectual y otros activos vitales.

### Supervisión, análisis y generación de informes sobre los datos en movimiento

Independientemente del tipo de actividad que realice su empresa, necesita disponer de la visibilidad necesaria para identificar la información confidencial en cualquier aplicación, protocolo, puerto y formato, con un alto grado de precisión.

Gracias a McAfee DLP Monitor, puede recopilar y supervisar en tiempo real los datos que se transfieren por la red, generar informes relacionados y, de esta forma, conocer qué información se intercambia entre los usuarios y otras organizaciones, así como

la manera en que se transfiere. McAfee DLP Monitor es un dispositivo de alto rendimiento especializado que detecta de forma exclusiva más de 300 tipos de contenido que transite por cualquier puerto o protocolo, y que permite identificar las amenazas contra los datos y adoptar las medidas necesarias para proteger a la empresa frente a la pérdida de datos. Además, a través de una función de notificación a los usuarios finales, McAfee DLP Monitor puede también servir de utilidad de formación del personal sobre las infracciones que causan la pérdida de datos, con objeto de que modifiquen sus comportamientos sin esfuerzo.

### Creación y ajuste de reglas sofisticadas

- Identifique más de 300 tipos de contenido diferentes en cualquier puerto y aplicación.
- Clasifique el tráfico de red con independencia del puerto.
- Amplíe el soporte a cientos de miles de conexiones simultáneas.

### Especificaciones

#### Rendimiento del sistema

- Clasifique el contenido a una velocidad de hasta 200 Mbits/s, sin muestreo.

#### Integración en red

- Se integra de forma pasiva en la red mediante un puerto SPAN o un dispositivo de escucha en red físicamente en línea (opcional).

#### 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

### Análisis y exploración de la información en tiempo real

Integrado en la red mediante un puerto SPAN o de escucha, McAfee DLP Monitor realiza el análisis y la exploración en tiempo real del tráfico de red. Con más de 150 reglas preconfiguradas, que van desde el cumplimiento de normativas al uso aceptable y a la propiedad intelectual, McAfee DLP Monitor compara documentos completos o parciales (incluida la detección del plagio) con su conjunto completo de reglas. Esto le permite detectar anomalías en el tráfico de red, independientemente del volumen.

### Descubrimiento de riesgos no considerados anteriormente

A través de la clasificación, indexación y almacenamiento detallados de todo el tráfico de red —no solo la información que coincide con sus reglas en tiempo real—, McAfee DLP Monitor le permite aprovechar rápidamente información anterior para identificar qué datos son confidenciales, cómo se utilizan, quién los utiliza y a dónde van. Además, puede realizar una investigación detallada y una inspección histórica de la información para detectar eventos de riesgos y exposición de los datos que pueden no haberse considerado antes. Y cuando se despliega junto con McAfee DLP Discover, también le permite identificar dónde se almacenan los datos en la red y a quién pertenecen.

### Visualización de informes de incidentes para tomar medidas

Una vez que el motor de clasificación analiza, explora y clasifica el tráfico, McAfee DLP Monitor almacena la información adecuada en una base de datos propietario. Gracias a una interfaz de búsqueda intuitiva, puede ver informes completos de la información, quién la envía, a dónde va y de qué forma se envía. De esta forma, puede determinar qué información sale de la empresa, dónde y de qué forma. Con esta información, puede realizar las acciones adecuadas para hacer frente a estas amenazas mediante la aplicación de una serie de medidas destinadas a garantizar el cumplimiento de las normativas y la protección de los datos confidenciales.

### Clasificación de todos los tipos de datos

McAfee DLP Monitor ofrece a su organización la capacidad de analizar 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 Monitor genera un motor de clasificación muy preciso y detallado, que se utiliza para filtrar la información confidencial y realizar búsquedas que identifican los riesgos ocultos o desconocidos.

## Ficha técnica

### Protocolos admitidos

- Admite todas las transmisiones a través de todos los protocolos y puertos que utilizan TCP como protocolo de transporte.
- Incluye identificadores de protocolos para HTTP, HTTPS, SMTP, IMAP, POP3, FTP, Telnet, Rlogin, SSH, correo web, Yahoo! Chat, AOL Chat, MSN Chat, ICY, RTSP, SOCKS, PCAnywhere, RDP, VNC, SMB, Citrix, Skype, IRC, LDAP, DASL, NTLM, Kazaa, BitTorrent, eDonkey, Gnutella, DirectConnect, MP2P, WinMX, Sherlock y eMule, entre otros.

### 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.

Los mecanismos de clasificación por objeto incluyen:

- **Clasificación multinivel:** 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	Descripción
Procesador	2 procesadores 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	8 unidades de 2 TB SATA, 7200 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)

