# McAfee Data Loss Prevention Discover

**Localice, clasifique y proteja sus datos confidenciales dondequiera que residan.**

## Ventajas principales

**Identificación de los riesgos de fuga de datos**

- Analice la información almacenada in situ o en la nube.
- Identifique dónde se encuentran los datos confidenciales y quién es el propietario del contenido.
- Busque y vea todos los datos analizados desde una interfaz intuitiva.

**Directivas e informes personalizados**

- Ejecute consultas y transfiera los resultados a una regla de protección.
- Utilice directivas preconfiguradas para el cumplimiento de normativas, la administración de la empresa y la propiedad intelectual.
- Registre la información confidencial en sistemas de seguridad de la información adyacentes.

**Clasificación, análisis y solución de fugas de datos**

- Filtre y controle la información confidencial con clasificación multivectorial.
- Indexe todo el contenido y, a continuación, consúltelo y extráigalo para comprender la naturaleza de sus datos confidenciales.
- Registre y genere firmas para proteger documentos y la información que contienen, incluso si se plagian o transforman.
- Envíe una notificación de alerta si el contenido infringe las directivas de seguridad.

La información confidencial que reside en portátiles, servidores de archivos compartidos y almacenamiento en la nube puede poner en riesgo a su organización. Es necesario proteger esos ingentes volúmenes de información (terabytes e incluso petabytes). Esta tarea resulta especialmente complicada debido a que la información confidencial no siempre está adecuadamente identificada. Además, en la mayoría de las empresas, no hay forma de saber o comprobar si los datos confidenciales pueden estar en peligro, o de saber dónde han proliferado, incluso cuando se han aplicado controles de acceso. Para complicar aun más las cosas, los datos confidenciales suelen ser tipos de datos no estructurados, como activos de propiedad intelectual que resultan más difíciles de definir que los datos estructurados, como los números de tarjetas de crédito y de documentos de identidad. McAfee® Data Loss Prevention (DLP) Discover le ayuda a localizar y clasificar la información confidencial, a descubrir cómo se utiliza y a protegerla frente a robos o fugas.

## Novedades en McAfee DLP Discover

Ahora McAfee DLP Discover puede analizar y proteger los datos que residen en la nube de Box. Es fácil definir las directivas en el software de administración centralizada McAfee ePolicy Orchestrator® (McAfee ePO™) y los análisis se pueden programar y automatizar de manera anticipada. Hay disponibles informes especiales sobre incidentes y análisis detallados.

**Características principales:**

- El software McAfee DLP Discover ofrece un ahorro adicional de costos, ya que deja de ser necesario emplear un hardware o un dispositivo basado en VM.
- Se puede desplegar y administrar totalmente con el software McAfee ePO. Emplea la misma extensión de administración y directiva de DLP que DLP Endpoint.
- Totalmente compatible con las funciones de clasificación de DLP Endpoint.
- Compatible con Windows Server 2008 y Windows Server 2012.
- Admite despliegues distribuidos que aprovechan la capacidad no utilizada de los servidores existentes y pueden desplegarse en un área geográfica extensa.
- Licencia compatible para el dispositivo DLP Discover versiones 9.3.x o la versión solo software de DLP Discover 9.4.

intel Security

## Especificaciones

**Tipos de contenido**
Soporta la clasificación de archivos de más de 300 tipos de contenido, incluidos:

- Almacenamiento en la nube "Box"
- Documentos de Microsoft Office
- Archivos multimedia
- Código fuente
- Archivos de diseño
- Archivos comprimidos
- Archivos cifrados
- Directivas integradas
- Propiedad intelectual

**Repositorios compatibles**

- Common Internet File System (CIFS)/Server Message Block (SMB)[1]
- Network File System (NFS)
- HTTP/HTTPS
- FTP/FTPS
- Microsoft SharePoint[1]
- EMC Documentum
- Bases de datos: Microsoft SQL, Oracle, DB2, MySQL Enterprise

### Registro de documentos

Los documentos se pueden registrar desde cualquier repositorio. Las firmas de documentos registrados se pueden utilizar de forma local para detectar la proliferación de material confidencial, o para que puedan utilizarlos otros dispositivos de McAfee DLP.

### Informes

El potente motor analítico para visualizar los incidentes y los resultados de las búsquedas permite personalizar vistas resumidas sobre cualquier pareja de puntos de referencia. También hay disponibles vistas detalladas y en formato de lista, así como vistas de resumen con datos de tendencias. El sistema incluye más de 20 informes preconfigurados y personalizables.

## Prevención de la pérdida de información confidencial

El código fuente, los secretos comerciales, los planes estratégicos de la empresa, las direcciones IP y otros activos de información son críticos para la marca, la imagen pública y la competitividad. Es fundamental proteger los datos cuando se transmiten, pero garantizar la seguridad de la información confidencial antes de que se acceda o mueva de forma inapropiada y conocer dónde se encuentra debería ser su primera línea de defensa.

McAfee DLP Discover le ayuda a proteger su empresa frente a la pérdida de datos. A diferencia de otras soluciones precedentes, que parten del principio de que las empresas saben exactamente qué contenido desean proteger, McAfee DLP Discover cubre no solamente la información que debe protegerse de forma obvia, sino que ayuda a identificar los datos menos evidentes.

## Selección de la información que hay que proteger

Para identificar la información y la proliferación de riesgos, McAfee DLP Discover se puede configurar para analizar repositorios específicos e identificar los datos para ofrecer una protección expresa. Además, todos los datos que rastrea McAfee DLP Discover se indexan y puede accederse a ellos a través de una interfaz intuitiva, lo que le permite realizar búsquedas rápidas de información que puede ser confidencial, con el fin de saber a quién pertenece el contenido y dónde se almacena.

## Definición de las directivas de protección

Una vez que sabe la información que hay que proteger, McAfee DLP Discover puede ayudarle a hacerlo de forma precisa. Gracias a la creación de directivas, la generación de informes y la administración de manera intuitiva y unificada, McAfee DLP Discover le ofrece un mayor control sobre su estrategia de protección de los datos en reposo. Las ventajas principales de las directivas, las reglas y la clasificación de McAfee DLP Discover incluyen:

- Un gran número de directivas incorporadas que facilitan el uso inicial sin necesidad de configuración.
- Un potente motor de generación de reglas, que cubre desde los datos de estructura simple (tarjetas de crédito, números de identificación personal) a la información compleja (propiedad intelectual).
- La creación y validación de reglas simplificadas mediante la transferencia del análisis de los resultados de la búsqueda a una regla de protección.
- La integración con vectores de seguridad de la información adyacentes para garantizar una protección coherente.
- La exclusión de documentos públicos y texto común para impedir que esta información inofensiva genere incidentes.

## Análisis de la red para descubrir infracciones

Tras definir las directivas, McAfee DLP Discover puede configurarse para realizar análisis rutinarios de los recursos de la red, con el fin de localizar infracciones de las directivas. Hay disponibles una serie de opciones de planificación flexibles para realizar análisis continuos, a diario, de forma semanal o mensual.

McAfee DLP Discover analiza de forma automática todos los recursos a los que puede accederse, incluidos computadoras portátiles, computadoras de escritorio, servidores, repositorios de documentos, portales y ubicaciones de transferencia de archivos, para localizar posibles infracciones de directivas. Puede definir grupos de análisis basados en direcciones IP o intervalos de direcciones IP, subredes o rutas de red. Asimismo, puede centrar las operaciones de análisis en parámetros específicos; por ejemplo, analizar únicamente la carpeta Mis documentos de todos los usuarios y no las carpetas del sistema, o buscar archivos que pertenezcan a determinados usuarios o de un tipo o tamaño dado.

## Revisión y corrección de infracciones

McAfee DLP Discover elimina o minimiza la proliferación de material confidencial a través del flujo de trabajo de incidentes y la gestión de casos de manera centralizada. Si McAfee DLP Discover encuentra contenido que infringe las directivas de protección, genera incidentes y envía notificaciones. Los incidentes creados por McAfee DLP Discover pueden añadirse a la infraestructura de gestión de casos, que le permite involucrar a especialistas de varios

## Especificaciones: solo software

McAfee DLP Discover está disponible como versión solo software. A continuación se detallan los requisitos mínimos del sistema.

**Requisitos de hardware**

- CPU: Intel Core 2 de 64 bits
- RAM: 4 GB como mínimo
- Espacio en disco: 100 GB como mínimo

**Plataformas compatibles**

- Windows Server 2008 R2 Standard, de 64 bits
- Windows Server 2012 Standard, de 64 bits
- Windows Server 2012 R2 Standard, de 64 bits

**Sistemas de virtualización admitidos**

- vSphere ESXi 5.0 Update 2
- vCenter Server 5.0 Update 2

**Software McAfee ePO y agentes**

- McAfee ePO 4.6.8 o posterior; y 5.1 o posterior
- McAfee ePO 4.8.2 o posterior; y 5.0 o posterior

departamentos dentro de la empresa para que tomen medidas al respecto. Además, los paneles de riesgos permiten al personal de seguridad conocer fácilmente el perfil de las infracciones de directivas y generar informes basados en cualquier parámetro de interés relativo a los de datos en reposo.

## Obtención y análisis de datos almacenados

Además de analizar los recursos de red para detectar infracciones de directivas, McAfee DLP Discover indexa todo el contenido encontrado en reposo en la red y le ofrece la capacidad de realizar consultas y examinar esta información para estudiar sus datos confidenciales. En definitiva, le permite conocer rápidamente sus datos confidenciales, cómo se utilizan, dónde se almacenan y dónde han proliferado.

## Clasificación de datos complejos

McAfee DLP Discover 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 los datos de estos mecanismos de clasificación por objeto, McAfee DLP Discover también es capaz de generar una clasificación multivectorial muy precisa, que se utiliza para filtrar y controlar la información confidencial y para realizar búsquedas que identifican los riesgos ocultos o desconocidos. 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

McAfee DLP Discover está disponible como dispositivo físico o virtual. A continuación se incluyen las especificaciones del dispositivo.

| Componente | Descripción |
|---|---|
| **Procesador** | 2 x Intel E5-2620 de 6 núcleos, 15 MB 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) |

## Especificaciones: máquinas virtuales

McAfee DLP Discover 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<br>Unidad 2: tamaño mínimo de 512 GB para la imagen virtual DLP |
| **Red** | 4 NIC virtuales |
| **BIOS** | Subproceso con virtualización activa |

1. La versión solo software de McAfee DLP Discover 9.4 soporta CIFS, Microsoft SharePoint 2010 y Microsoft SharePoint 2013.

**McAfee. Part of Intel Security.**
6205 Blue Lagoon Drive
Suite 600
Miami, Florida 33126
U.S.A.
www.intelsecurity.com