

Prevención de la pérdida de datos, desde el dispositivo hasta la nube, de McAfee

Protección de datos unificada

Empresas de todos los tamaños contratan servicios basados en la nube, como Microsoft Office 365, para ofrecer a sus empleados mayor flexibilidad y facilitarles el acceso a aplicaciones básicas de la empresa. Las soluciones de protección de datos in situ no suelen tener visibilidad de los datos en servicios en la nube como Office 365 y no pueden controlar la colaboración o el intercambio de archivos en la nube. Muchas empresas se están planteando incorporar una solución de protección de datos independiente para su entorno de nube, pero al hacerlo, fragmentan sus directivas, la generación de informes y la respuesta a incidentes. El resultado es una mayor sobrecarga operativa y una protección de datos incoherente en los distintos dispositivos, redes y servicios en la nube.

La prevención de la pérdida de datos (DLP) desde el dispositivo hasta la nube de McAfee® ofrece protección de datos unificada para endpoints, redes y la nube a través de la integración con dos tecnologías líderes del sector: McAfee® Data Loss Prevention (McAfee DLP) y McAfee® MVISION Cloud. La integración ofrece a las empresas una protección de datos ininterrumpida y unificada, minimizando el riesgo de pérdida de datos y maximizando la eficiencia operativa.

Ineficiencia de las soluciones de protección de datos fragmentadas

La implementación de una solución de prevención de la pérdida de datos en la nube precisaba rediseñar las reglas DLP, creadas para un contexto in situ, de nuevo en la nube. Las reglas DLP in situ también carecían de contexto de colaboración o de intercambio nativo para la nube con

terceros desde los servicios de la nube. Esto provocaba que hubiera que dedicar un tiempo excesivo a replicar trabajo existente ya completado respecto a los datos de los dispositivos y de la red, lo que podía dar lugar a una implementación de directivas potencialmente incoherente desde motores DLP distintos. La pérdida de datos a través de la colaboración o de enlaces compartidos en la nube era invisible para la solución DLP in situ.

Conecte y sincronice fácilmente DLP in situ y DLP en la nube

El software McAfee® ePolicy Orchestrator® (McAfee ePO™) facilita la implementación de DLP, desde el dispositivo hasta la nube. Con MVISION Cloud y el software McAfee ePO trabajando juntos puede proteger datos de cualquier servicio en la nube de manera más rápida que antes, con contexto completo de colaboración e intercambio nativo

Principales ventajas

Integración total

- Clasifique sus datos una vez con el software McAfee ePO y utilice las clasificaciones los contextos de dispositivos, redes y la nube.
- Conexión entre DLP in situ y en la nube con un clic y en menos de un minuto.

Prevención de pérdida de datos sistemática

- Motor de directivas y clasificación común en varios entornos.
- No es necesario realizar cambios en más de una consola.

Vista única para la administración de incidentes y la generación de informes

- Administración centralizada de incidentes en varios entornos.
- No es necesario cambiar de consolas para ver los incidentes y los informes.

Síganos



FICHA TÉCNICA

para la nube. Para conectar las dos soluciones basta un clic y puede realizarse en un minuto¹. Las reglas DLP que cree en el software McAfee ePO para sus dispositivos y red se transfieren a MVISION Cloud, donde pueden aplicarse a cualquier servicio de nube y tráfico nativo de la nube que no pase por su red. Sus clasificaciones de datos se sincronizan, lo que garantiza una prevención de la pérdida de datos coherente en los endpoints y en la nube. Todos los incidentes se envían al software McAfee ePO, lo que le ofrece un flujo de trabajo único para prevención de la pérdida de datos desde el dispositivo hasta la nube.

Cómo consiguen las empresas eficiencia operativa de la prevención de la pérdida de datos (DLP), desde el dispositivo hasta la nube

Los clientes que utilizan el software McAfee ePO han aprovechado esta integración para facilitar al máximo la implementación de DLP en servicios de la nube y simplificar sus operaciones. Por ejemplo, un importante fabricante de servicios alimentarios que utilizaba McAfee DLP en sus endpoints y recursos compartidos de archivos de red necesitaba descubrir dónde residían sus datos en la nube y desarrollar una estrategia para protegerlos. La empresa empezó con McAfee® Web Gateway, y analizó su tráfico web para determinar los principales destinos de los usuarios y dónde se mantenían los datos de la empresa en la nube. Descubrió que la gran mayoría de sus datos estaban en realidad concentrados en Microsoft Office 365.

Los requisitos de protección de datos en la nube de esta empresa no cambiaban respecto las ubicaciones in situ, pero diferencias contextuales como el intercambio de archivos y la colaboración en la nube planteaban nuevos desafíos. Por ejemplo, la empresa necesitaba analizar sus datos en Office 365 bajo demanda, similar al análisis in situ, mientras que implementaba reglas DLP para los

The screenshot shows the McAfee ePO interface for DLP Settings. The top navigation bar includes 'Dashboards', 'System Tree', 'Queries & Reports', 'Policy Catalog', and 'Security Resources'. The main content area is titled 'Data Protection' and 'DLP Settings'. Below this is a tabbed interface with 'MVISION Cloud Server' selected. The settings are organized into sections: 'Last Modified' (May 24, 2019 3:11:19 PM), 'MVISION Cloud Connection' (checked 'Connect to McAfee MVISION Cloud'), 'MVISION Cloud Server' (fields for 'Server name or IP Address', 'User name', and 'Password', with buttons for 'Test Connectivity', 'Sync Classifications', 'Delete Classifications', 'Push DLP policy', and 'Delete DLP policy'), 'Modules' (checked 'Push classification information to MVISION Cloud', 'Pull incidents from MVISION Cloud', and 'Push DLP policy to MVISION Cloud', with a dropdown for 'DLP policy Name' set to 'MVISION Cloud DLP policy'), and 'Status' (connection status 'Success' on August 26, 2019 3:49:16 PM, and a table of synchronization metrics).

General	Advanced	Classification	Incident Manager	Operations Center	Case Management	MVISION Cloud Server	Backup & Restore
Last Modified:		May 24, 2019 3:11:19 PM					
MVISION Cloud Connection		<input checked="" type="checkbox"/> Connect to McAfee MVISION Cloud					
MVISION Cloud Server		Server name or IP Address: <input type="text"/> User name: <input type="text"/> Password: <input type="password"/> Test Connectivity Sync Classifications Delete Classifications Push DLP policy Delete DLP policy					
Modules		<input checked="" type="checkbox"/> Push classification information to MVISION Cloud <input checked="" type="checkbox"/> Pull incidents from MVISION Cloud <input checked="" type="checkbox"/> Push DLP policy to MVISION Cloud DLP policy Name: <input type="text" value="MVISION Cloud DLP policy"/>					
Status		Connection status: Success August 26, 2019 3:49:16 PM Last set of classifications were sent at: August 15, 2019 4:13:20 PM Number of classifications sent: 17 Last incident pulled from MVISION Cloud occurred at: August 5, 2019 3:46:30 PM Number of incidents pulled: 163 Last DLP policy sent to MVISION Cloud at: May 24, 2019 3:11:48 PM DLP policy sent to MVISION Cloud : MVISION Cloud DLP policy (1)					

Figura 1. Sincronización de directivas DLP con MVISION Cloud en McAfee ePO software.

datos que entraban y salían de Office 365, que eran exclusivos de la nube y estaban fuera de la visibilidad de la red. Se determinó que la mejor solución para hacer frente a estos requisitos era un agente de seguridad de acceso a la nube (CASB), y se evaluaron varias de las opciones disponibles en el mercado. Finalmente, la empresa optó por MVISION Cloud por su estrecha integración con las reglas DLP existentes en el software McAfee ePO. Desde el software McAfee ePO, el equipo de seguridad transfirió las clasificaciones de datos in situ a MVISION Cloud y, a continuación, escribió las

FICHA TÉCNICA

directivas para Office 365 utilizando esas clasificaciones prediseñadas. Ahora la empresa utiliza una sola ubicación para administrar las clasificaciones de datos, los incidentes de DLP tanto de los dispositivos como de la nube, así como los informes sobre el tráfico web de McAfee Web Gateway, todo en el software McAfee ePO.

"Elegimos McAfee MVISION Cloud como nuestra solución CASB por la visibilidad que ofrece sobre dónde van nuestros datos y quién accede a ellos, así como por la facilidad con la que podemos comprender el riesgo asociado a un servicio en la nube".

—CISO de un fabricante mundial de dispositivos IoT

Gestión de incidentes y generación de informes centralizadas

El software McAfee ePO le ofrece un panel de visualización único para la gestión de las infracciones de DLP y la generación de informes. No es necesario cambiar de consolas para ver los incidentes y generar informes, con independencia de si las infracciones de prevención de pérdida de datos proceden de dispositivos de la empresa o de aplicaciones en la nube. Esta consola centralizada también ayuda a reducir la complejidad relacionada con auditorías y cumplimiento de normativas gracias a que ofrece visibilidad de los datos confidenciales en varios entornos.



Av. Paseo de la Reforma No.342 Piso 25
Colonia Juárez, México DF
C.P. 06600
+52-55-50890250
www.mcafee.com/mx

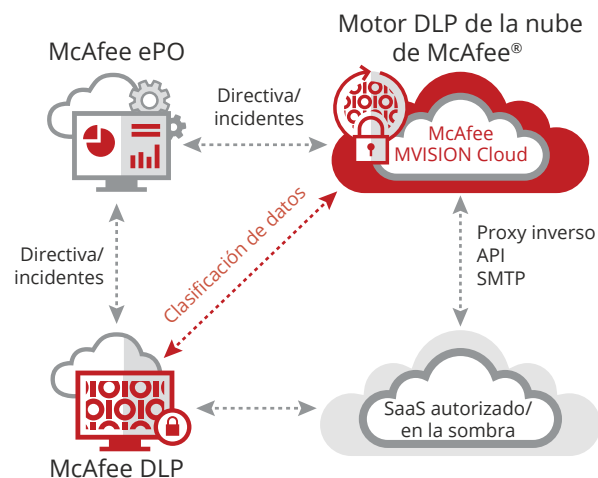


Figura 2. Arquitectura general para la gestión de incidentes de la prevención de la pérdida de datos, desde el dispositivo hasta la nube, de McAfee

Resumen

El importante aumento de los datos que se crean y se envían a la nube a diario hace que sea más importante que nunca disponer de un conjunto de directivas DLP uniformes que protejan los datos de todos los vectores de filtración: endpoints corporativos, dispositivos no gestionados, en la red o en las aplicaciones en la nube.

La prevención de la pérdida de datos (DLP) desde el dispositivo hasta la nube de McAfee ofrece una protección de datos ininterrumpida y unificada de varios entornos, ahorrando tiempo gracias a una mejora de la eficiencia operativa y ayudando a minimizar el riesgo de pérdida de datos.

Más información

Para obtener más información, visite www.mcafee.com/enterprise/es-mx/products/data-protection-products.html

1. Basado en pruebas de laboratorio internas de McAfee, llevadas a cabo de forma sistemática.

McAfee y el logotipo de McAfee, ePolicy Orchestrator y McAfee ePO son marcas comerciales o marcas comerciales registradas de McAfee, LLC o de sus empresas filiales en EE. UU. y en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros.
Copyright © 2019 McAfee, LLC. 4352_0819
AGOSTO DE 2019