McAfee Complete Data Protection—Essential

Solución esencial de cifrado de endpoints

Funciones principales

- Management of Native Encryption
- File and Removable Media Protection

Ventajas principales

- Detenga las pérdidas de datos iniciadas por sofisticado malware que secuestra la información confidencial y los datos personales.
- Proteja los datos almacenados en equipos de sobremesa, portátiles, tablets y en la nube.
- Administre el cifrado nativo de Apple FileVault y Microsoft BitLocker en los endpoints directamente desde el software McAfee® ePolicy Orchestrator® (McAfee ePO™).
- Podrá demostrar el cumplimiento de normativas con funciones avanzadas de auditoría y generación de reportes.
- Supervise los incidentes y genere reportes detallados para demostrar el cumplimiento de los requisitos de las normativas y directivas internas ante auditores, alta dirección y demás interesados.

Los datos confidenciales están en riesgo constante de pérdida, robo y exposición. Muchas veces, los datos simplemente salen por la puerta en una computadora portátil o un dispositivo USB. Las empresas que sufren estas pérdidas de datos se enfrentan a consecuencias importantes, como sanciones, divulgación pública, daños a la imagen de marca, pérdida de la confianza del cliente y pérdidas financieras. Según un reciente reporte de Ponemon Institute, el 7 % de todos los portátiles corporativos serán robados o se perderán en algún momento a lo largo de su vida útil[1]. La rápida proliferación de dispositivos móviles con gran capacidad de almacenamiento y normalmente con acceso a Internet está abriendo nuevas vías para la pérdida o el robo de datos. Por este motivo, proteger la información confidencial, de marca registrada y de identificación personal debe ser una prioridad máxima. McAfee® Complete Data Protection—Essential satisface estas necesidades y muchas otras.

Management of Native Encryption

La función Management of Native Encryption permite a los clientes administrar la funcionalidad de cifrado nativo que ofrece Apple FileVault en Mac OS X y Microsoft BitLocker en plataformas Windows directamente desde el software McAfee® ePolicy Orchestrator® (McAfee ePO™). De esta forma, el producto ofrece compatibilidad inmediata con parches de OS X y Windows, ampliaciones, actualizaciones de firmware de Apple y Microsoft, así como soporte instantáneo para el nuevo hardware de Apple. Esta característica permite a los administradores importar de forma manual claves de recuperación cuando los usuarios han activado FileVault y BitLocker.

Cifrado de soportes extraíbles, archivos y carpetas, y del almacenamiento en la nube

Asegúrese de que determinados archivos y carpetas estén siempre cifrados, con independencia de dónde se editen, copien o guarden los datos. McAfee Complete Data Protection— Essential proporciona cifrado de contenido que codifica de manera automática y transparente los archivos y carpetas que elige, de manera inmediata, antes de que se difundan por su empresa. Puede crear e implementar directivas de manera centralizada en función de los usuarios y grupos de usuarios para cifrar determinados archivos y carpetas, sin la intervención del usuario.

intel Security

Especificaciones

Sistemas operativos Microsoft Windows

- Microsoft Windows 10
- Microsoft Windows 7, 8, 8.1 (todas las versiones de 32/64 bits)
- Microsoft Vista (todas las versiones de 32/64 bits)
- Microsoft Windows XP (solo 32 bits)
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003 (solo versiones de 32 bits)

Requisitos de hardware

- CPU: Pentium III, 1 GHz o superior en portátiles y equipos de escritorio
- RAM: 512 MB como mínimo (se recomienda 1 GB)
- Disco duro: 200 MB de espacio libre en disco como mínimo

Sistemas operativos Apple Mac

- Mac OS X El Capitan, Yosemite, Mountain Lion y Mavericks

Requisitos de hardware

- CPU: portátil Mac Intel con EFI de 64 bits
- RAM: 1 GB como mínimo
- Disco duro: 200 MB de espacio libre en disco como mínimo

Administración centralizada

- Consulte las especificaciones de la plataforma McAfee ePO en su correspondiente ficha técnica.

Administración de la seguridad centralizada y generación de reportes avanzada

Utilice la consola de software centralizada McAfee ePO para implementar directivas de seguridad obligatorias en toda la empresa con el fin de controlar cómo se cifran, supervisan y protegen los datos para evitar fugas. Defina, despliegue, gestione y actualice de forma centralizada las directivas de seguridad que cifran, filtran y supervisan los datos confidenciales, y bloquean el acceso no autorizado.

Funciones de las suites McAfee Complete Data Protection

Management of Native Encryption en sistemas Mac y Windows

- Administre FileVault en cualquier hardware Mac que pueda ejecutar Mac OS X Mountain Lion, Mavericks, Yosemite y El Capitan directamente desde el software McAfee ePO.
- Administre BitLocker en sistemas Windows 7, 8 y 10 directamente desde el software McAfee ePO sin necesidad de un servidor MBAM (Microsoft BitLocker Management and Administration) independiente.
- Comunique el cumplimiento mediante distintos reportes y paneles del software McAfee ePO.

Cifrado de soportes extraíbles

- Cifrado automático e inmediato de prácticamente cualquier dispositivo de almacenamiento móvil, sea o no de la empresa.
- Cifre o bloquee la escritura en soportes extraíbles en las estaciones de trabajo VDI.
- Acceda a los datos cifrados en cualquier ubicación sin necesidad de la instalación de software adicional ni derechos de administración locales en el host del dispositivo.

Cifrado de archivos, carpetas y almacenamiento en la nube

- Mantenga protegidos los archivos y carpetas cualquiera que sea la ubicación donde se guarden, como en discos duros locales, servidores de archivos, soportes extraíbles y servicios de almacenamiento en la nube, como Box, Dropbox, Google Drive y Microsoft OneDrive.

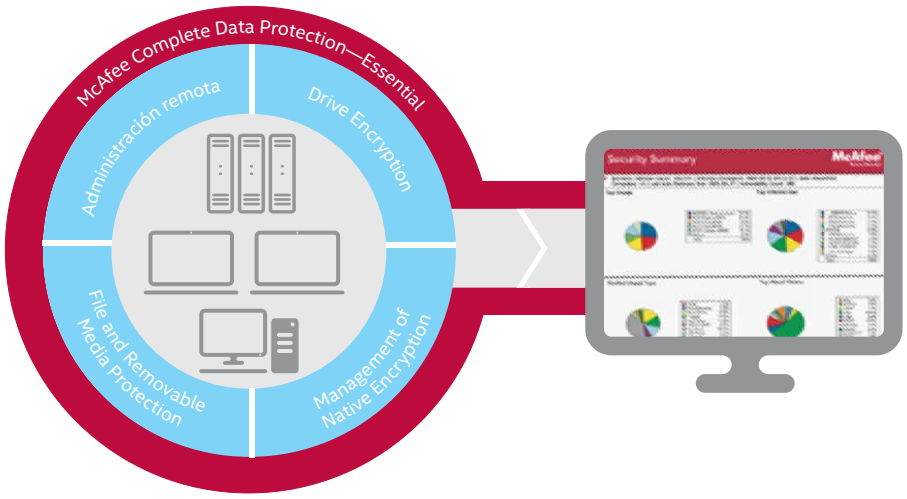

Figura 1. McAfee Complete Data Protection—Essential.

Consola de administración centralizada

- Utilice la infraestructura de software McAfee ePO para administrar el cifrado de discos completos, archivos y carpetas, y soportes extraíbles; controlar la administración de directivas y parches; recuperar contraseñas que se han perdido y demostrar que se cumplen los requisitos de las normativas.
- Sincronice las directivas de seguridad con Microsoft Active Directory, Novell NDS o PKI, entre otros.
- Demuestre que los dispositivos están cifrados con amplias funciones de auditoría.
- Registre las transacciones de datos para conservar información como el remitente, el destinatario, la fecha/hora, pruebas de datos, la fecha y hora del último inicio de sesión, la fecha y hora de recepción de la última actualización y si el proceso de cifrado ha finalizado correctamente.

Para obtener más información sobre la protección de datos de McAfee, visite **www.mcafee.com/mx/products/dataprotection/index.aspx**.

1. *The Billion Dollar Lost Laptop Problem Study* (Estudio sobre el problema de la pérdida de portátiles por valor de miles de millones de dólares), Ponemon Institute, septiembre de 2010.

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

62239ds_complete-data-ess_0116