McAfee ePO Deep Command

Administrar la seguridad más allá del sistema operativo reduce los costos de explotación.

Reduzca las llamadas al servicio técnico y las visitas del centro de asistencia debidas a accidentes de seguridad, brotes u olvidos de las contraseñas de cifrado. Los administradores de seguridad pueden por fin desplegar, administrar y actualizar la seguridad en los endpoints apagados, desactivados o cifrados. El software McAfee® ePO™ Deep Command[1] emplea Intel® vPro™ Active Management Technology (AMT) para proporcionar funciones de administración a un nivel más profundo que el sistema operativo, lo que reduce los costos operativos, mejora la seguridad y el nivel de cumplimiento de normativas, y además acelera la corrección remota de problemas de seguridad en los PC y sistemas de función fija.

Ventajas principales

- **Descubra y aprovisione Intel AMT con rapidez:** identifique fácilmente los PC con Intel vPro y habilite Intel AMT para agilizar la activación.
- **Desbloqueo seguro:** cuando se utiliza con las suites McAfee Complete Data Protection, McAfee ePO Deep Command puede desbloquear y acceder de forma segura al entorno anterior al arranque de un endpoint cifrado.
- **Reduzca el tiempo de reparación:** solucione de forma remota los problemas de cualquier PC o endpoint, en cualquier lugar del mundo, con acceso desde el hardware.
- **Mejore la productividad de los usuarios:** realice las tareas que consumen muchos recursos fuera de horario de oficina para limitar el impacto en los usuarios finales.

Los administradores de seguridad se ven acosados por el aumento de los costos, de las amenazas y de los requisitos empresariales. Cada visita del centro asistencia provocada por una infección de malware u otras amenazas puede llegar a costar hasta 250 dólares. Además del costo, resulta complicado acceder físicamente al equipo de escritorio de cada usuario. Las oficinas remotas, los teletrabajadores y los empleados móviles dependen de las llamadas de asistencia técnica y de los envíos nocturnos al centro de reparaciones. Los usuarios están tan ocupados que a menudo ignoran los problemas, trabajan en sistemas vulnerables que no cumplen las normativas hasta que por efectos del malware se produce un fallo grave, un bloqueo o una interrupción.

Al mismo tiempo, el panorama de amenazas contra los endpoints plantea cada día más retos para la seguridad. Los ciberdelincuentes se mueven rápidamente para aprovechar cualquier nueva vulnerabilidad y utilizan redes de bots y sitios web para propagar malware oculto y de tipo zero-day. Además, ahora hay malware capaz de desactivar la protección a nivel del sistema operativo, con lo que los PC y los dispositivos de función fija del usuario quedan inservibles.

Y por si esto fuera poco, los CIO, presionados para reducir el consumo energético, ven en los equipos de escritorio inactivos una oportunidad de ahorro. Les gustaría apagar los sistemas que no se utilizan, pero necesitan un medio fiable de administrar la seguridad y el cumplimiento de normativas, así que ejecutan los procesos de TI (análisis, actualizaciones o parches) cuando afectan en menor medida a la actividad de los usuarios.

Ventajas principales (continuación)

- **Reduzca los costos de TI:** elimine las frecuentes visitas del centro de asistencia y las largas llamadas de servicio.
- **Reduzca el consumo energético de los endpoints:** adopte programas de ahorro de energía sin dejar de ofrecer acceso para tareas de seguridad o aplicación de parches.

Cómo descubrir y activar sus plataformas Intel vPro

El software McAfee ePO Deep Command le ayuda a obtener el máximo de la tecnología Intel vPro gracias a la función despertador de la tecnología Intel AMT, las funciones de activación remota, la tecnología de teclado, video y mouse (KVM), así como el redireccionamiento IDE. En primer lugar, el módulo Discovery and Reporting de McAfee ePO Deep Command identifica los PC y los endpoints de su entorno compatibles con la tecnología Intel AMT. Unos reportes detallados le ayudan a saber exactamente en cuáles de ellos se puede instalar el agente McAfee ePO Deep Command. McAfee ePO Deep Command también simplifica el aprovisionamiento de Intel AMT para agilizar la activación de dicha tecnología. Una vez que McAfee ePO Deep Command está instalado en los PC y endpoints con tecnología Intel AMT, es posible comenzar a administrarlos de forma remota más allá del sistema operativo, a nivel de hardware.

La administración remota como solución

Ahora, los administradores de seguridad pueden comunicarse y hacerse con el control de los endpoints a nivel de hardware, ya estén apagados, desactivados o cifrados. Esta conexión con el hardware permite administrarlos de manera remota con el fin de implementar las directivas de seguridad y cumplimiento de normativas y reducir los costos derivados de la seguridad. Además de mejorar el nivel de seguridad, estos controles permiten la adopción de programas de administración de energía, que ahorran recursos y garantizan al mismo tiempo el acceso a los endpoints. Gracias a la tecnología Intel vPro AMT, McAfee ePO Deep Command accede a los endpoints sin depender del sistema operativo. Con este acceso a nivel de hardware, los administradores pueden encender los sistemas, ejecutar tareas de seguridad y, posteriormente, devolver los endpoints a su estado anterior de consumo energético. El software McAfee ePO Deep Command permite incluso iniciar de forma segura el proceso de arranque de los endpoints que ejecutan McAfee Complete Data Protection (cifrado de endpoints), sin necesidad de utilizar las credenciales de autenticación del usuario, para realizar tareas de seguridad de manera remota. Estas operaciones pueden tener lugar automáticamente con el "encendido" programado o bajo demanda.

A través de la comunicación con los endpoints independientemente del sistema operativo, McAfee ePO Deep Command permite configurar y resolver los problemas de endpoints difíciles de administrar desde una ubicación central: la conocida plataforma de administración McAfee ePO.

Activar y ejecutar

Los administradores pueden ahora realizar las tareas de mantenimiento de la seguridad, u otras que requieran mucho tiempo, en horario fuera de oficina, sin tener que interrumpir la actividad de los usuarios. Gracias a la función despertador (Alarm Clock) de la tecnología Intel AMT, los administradores de seguridad pueden encender y activar los endpoints, aunque estén cifrados, para ejecutar una serie de tareas de seguridad, incluidas, entre otras:

- Actualizaciones de seguridad y de configuración (incluidos los archivos .DAT)
- Análisis bajo demanda
- Instalación de otros productos de seguridad
- Generación de reportes de eventos
- Aplicación de parches a aplicaciones o al sistema operativo

Requisitos del sistema

- McAfee ePO 4.6 (módulo Discovery and Reporting), McAfee ePO 4.6 (McAfee ePO Deep Command), McAfee ePO 5.0 y superiores
- McAfee Agent 4.5 o superiores
- McAfee Drive Encryption 7.0 y superiores (para las funciones de administración de cifrado remotas)
- Admite Microsoft Windows XP, Windows Vista, Windows 7, 8, Windows Server 2003 y Windows Embedded XP, 7
- Admite Intel vPro AMT versiones 2.2 y superiores
- Intel Setup and Configuration Software (SCS) 8.2 y superiores

Recuperación remota de endpoints desactivados

Cuando se presentan problemas (por ejemplo, un sistema operativo fue desactivado o falló un disco duro), tanto administradores como usuarios pueden disfrutar de la comodidad de la administración integrada activada por McAfee ePO Deep Command. Independientemente de si se trata de un endpoint o PC local o remoto, el administrador puede conectarse al PC o endpoint desactivado y al teclado, video y mouse (KVM) a través de la tecnología Intel AMT para llevar a cabo una acción de corrección remota, como indicar al PC que arranque desde otra imagen ISO de la red. En la mayoría de los casos, no hace falta que el endpoint esté conectado por cable a la red. McAfee ePO Deep Command puede administrar endpoints seguros conectados por Wi-Fi.

La función de solicitud rápida de ayuda de la tecnología Intel AMT proporciona a los usuarios una forma fácil de ponerse en contacto con los administradores de McAfee ePO para solicitar ayuda. El administrador de McAfee ePO puede rápidamente:

- Redirigir el endpoint para que arranque desde una imagen situada en otra ubicación de la red
- Controlar completamente el KVM local
- Restablecer la contraseña de cifrado del usuario
- Limpiar y reparar los sistemas infectados, desactivados o puestos en cuarentena sin necesidad de acceder a ellos físicamente

La seguridad, por delante de las amenazas

Este amplio control proporciona a los equipos de seguridad nuevas opciones para proteger los endpoints antes de que aparezcan las amenazas. Los sistemas pueden actualizarse antes de que se vean afectados por una amenaza potencial, y las medidas pueden activarse de forma remota, lo que impide que sufra la productividad de los usuarios y mantiene protegidos los datos.

Menor costo de consumo energético de los endpoints

Dado que McAfee ePO Deep Command es capaz de activar los endpoints, actualizar las directivas y, posteriormente, devolverlos a su estado de bajo consumo, su empresa puede adoptar con seguridad programas de ahorro de energía y acceder a los incentivos del sector para reducir el consumo energético sin comprometer la seguridad. Póngase en contacto con McAfee para averiguar qué representaría este ahorro para su empresa.

Figura 1. McAfee ePO Deep Command puede descubrir los sistemas vPro y desplegar el software que activa Intel AMT.

Escalabilidad y generación de reportes de nivel empresarial

McAfee ePO Deep Command amplía la plataforma de administración del software McAfee ePolicy Orchestrator® (McAfee ePO™), que ha demostrado ser capaz de adaptarse a cientos de miles de endpoints. Diseñado para admitir arquitecturas distribuidas y equipos de administración de la seguridad, el software McAfee ePO proporciona un entorno unificado de administración de directivas de seguridad y de generación de reportes para toda su infraestructura de seguridad de McAfee. Ahora también puede llevar sus iniciativas de directivas y de cumplimiento más allá del sistema operativo. Gracias a la ampliación de la cantidad de información que puede incluirse en los paneles y reportes del software McAfee ePO, es posible aumentar la visibilidad del grado de cumplimiento de cada endpoint, así como del estado general de seguridad de la empresa. La correlación de datos facilita las auditorías.

Para obtener más información, visite **www.mcafee.com/mx/products/epo-deep-command.aspx**.

El software McAfee ePO Deep Command está disponible como producto independiente y también en las suites McAfee Complete Data Protection. Para obtener más información, visite **www.mcafee.com/mx/products/data-protection/index.aspx**.

Figura 2. McAfee ePO Deep Command permite al centro de asistencia realizar varias tareas, ya sea de forma local o remota.

1. El software McAfee ePO Deep Command está disponible como producto independiente y también en las suites McAfee Complete Data Protection. Para obtener más información, visite **www.mcafee.com/mx/products/data-protection/index.aspx**.

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, el logotipo de McAfee, ePolicy Orchestrator y McAfee ePO 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 © 2014 McAfee, Inc. 61371ds_epo-deep-command_1014