McAfee Embedded Control

Integridad de sistemas, control de cambios y cumplimiento de directivas en una única solución

McAfee® Embedded Control garantiza la integridad de los sistemas permitiendo que solo se ejecute el código admitido y solo se realicen los cambios que han sido autorizados. Crea automáticamente una lista blanca dinámica del "código autorizado" para el sistema incorporado. Una vez creada y activada la lista blanca, el sistema queda bloqueado en la base conocida y correcta, y los programas que no están autorizados no pueden ejecutarse, ni tampoco se pueden realizar cambios no aprobados. McAfee Integrity Control, que combina McAfee Embedded Control y la consola McAfee ePolicy Orchestrator® (McAfee ePO™), proporciona informes integrados de auditoría y de cumplimiento de normativas con el fin de responder a las exigencias de distintas normativas.

McAfee Embedded Control se centra en resolver el problema del aumento de los riesgos para la seguridad derivados de la adopción de sistemas operativos comerciales en los sistemas integrados. McAfee Embedded Control es una solución independiente de las aplicaciones, compacta, que casi no consume recursos y que no requiere ninguna intervención tras su instalación. McAfee Embedded Control convierte los sistemas desarrollados sobre sistemas operativos comerciales en una “caja negra”, de forma que parezca un sistema operativo cerrado. Impide que se ejecuten programas no autorizados que se encuentren en el disco o que se inyecten en memoria, así como que se realicen cambios no permitidos en la base aprobada.

Esta solución ofrece a los fabricantes las ventajas de utilizar sistemas operativos comerciales sin aumentar el riesgo ni perder el control sobre cómo se usan los sistemas en las instalaciones de los clientes.

Integridad de los sistemas garantizada

Control de los ejecutables

Con McAfee Embedded Control solo se ejecutan los programas de la lista blanca dinámica de McAfee. El resto de programas (ejecutables, DLL, secuencias de comandos) no se consideran autorizados. Por lo tanto, se evita que se ejecuten y, de forma predeterminada, se registra el intento de ejecución. Todo ello impide que se ejecuten de manera ilegítima gusanos, virus, spyware y otros tipos de malware que se autoinstalan.

Ventajas principales

- Reduce los riesgos para la seguridad mediante el control de qué se ejecuta en los dispositivos incorporados y protege la memoria de dichos dispositivos.
- Facilita el acceso, mantiene el control y reduce los costes de soporte.
- Permite una aplicación selectiva.
- No requiere procedimientos adicionales tras el despliegue.
- Permite que los dispositivos cumplan las normativas y estén preparados para las auditorías.
- Visibilidad en tiempo real.
- Funciones globales de auditoría.
- Registro de cambios en el que se pueden realizar búsquedas.
- Reparación en bucle cerrado.

Control de la memoria

El control de la memoria garantiza la protección de los procesos en ejecución frente a intentos de ataques maliciosos. Esta función detecta, detiene y registra el código no autorizado inyectado en los procesos en ejecución. De esta forma, se detienen y registran los intentos de controlar el sistema mediante desbordamiento del búfer, desbordamiento del montón, ejecución de la pila y otros ataques similares[1].

Integración con McAfee GTI: la forma más inteligente de enfrentarse a las amenazas globales en entornos aislados

McAfee Global Threat Intelligence (McAfee GTI) es una tecnología exclusiva de McAfee que supervisa, en tiempo real, la reputación de los archivos, mensajes y remitentes mediante millones de sensores desplegados en todo el mundo. Esta función emplea información alojada en la nube para determinar la reputación de todos los archivos de su entorno informático y clasificarlos como legítimos, maliciosos o desconocidos. Gracias a la integración con McAfee GTI, sabrá con exactitud si un archivo de malware ha sido incluido en una lista blanca de manera inadvertida. Se puede acceder a la información sobre reputación que ofrece GTI desde entornos con conexión a Internet y desde entornos con el software McAfee ePO aislados.

Control de cambios

McAfee Embedded Control detecta los cambios en tiempo real, ofrece visibilidad de las fuentes del cambio y verifica que los cambios se hayan llevado a cabo en los sistemas adecuados. Además, proporciona una pista de auditoría de los cambios y solo permite que se realicen los cambios a través de los medios autorizados.

McAfee Embedded Control permite aplicar procesos de control de cambios mediante la definición de los medios de modificación autorizados. Se puede controlar quién puede aplicar cambios, qué certificados se necesitan para autorizarlos, qué puede modificarse (por ejemplo, los cambios pueden estar limitados a ciertos archivos o directorios) y cuándo pueden aplicarse (por ejemplo, es posible que la actualización Microsoft Windows solo sea posible a ciertas horas durante la semana).

De forma preventiva, los cambios se verifican antes de aplicarlos a los sistemas de destino. Cuando este módulo está activado, las actualizaciones de los sistemas de software solo pueden realizarse de forma controlada.

El módulo de seguimiento de cambios en tiempo real registra todas las modificaciones sufridas por el estado de un sistema, lo que incluye las que afectan al código, la configuración y el registro. Los cambios se registran cuando se producen, en tiempo real, y se envían al módulo supervisor del sistema para su incorporación y registro.

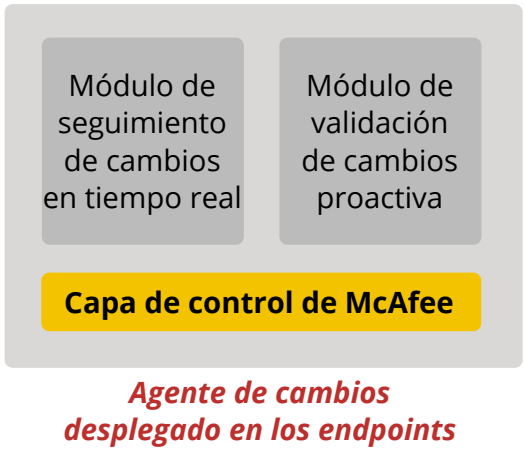

Figura 1. Capa de control de McAfee.

El módulo supervisor del sistema gestiona la comunicación entre el controlador del sistema y los agentes. Agrega y guarda la información de los cambios procedente de los agentes en el sistema de registro independiente.

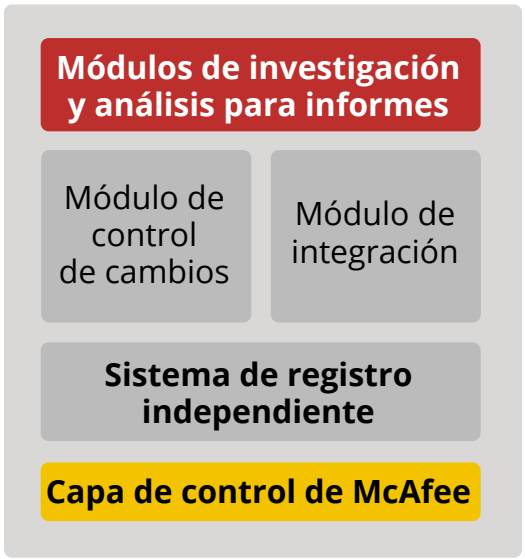

Figura 2. Módulos de informes, investigación y análisis.

Auditoría y cumplimiento de normativas

McAfee Integrity Control ofrece paneles e informes que ayudan a cumplir los requisitos de las normativas a través de la consola McAfee ePO, que está provista de una interfaz web para usuarios y administradores.

McAfee Embedded Control ofrece herramientas integradas, de bucle cerrado y en tiempo real para el cumplimiento de normativas y las auditorías, que se complementan con un sistema de seguridad que registra las actividades autorizadas y los intentos no autorizados.

Acerca de las soluciones de seguridad integrada de McAfee

Las soluciones de seguridad integrada de McAfee permiten a los fabricantes garantizar que sus productos y dispositivos están protegidos frente a las ciberamenazas y los ataques. Las soluciones de McAfee incluyen una amplia gama de tecnologías, como las de listas blancas de aplicaciones, protección antivirus y antimalware, administración de dispositivos, cifrado y gestión de riesgos, y cumplimiento de normativas. Todas ellas aprovechan la información de McAfee Global Threat Intelligence, líder del sector. Nuestras soluciones pueden personalizarse para satisfacer las necesidades específicas de diseño de los dispositivos y las arquitecturas de los fabricantes.

Pasos siguientes

Para obtener más información, visite **www.mcafee.com/es/partners/oem-alliances/index.aspx** o póngase en contacto con su representante local de McAfee.

Función	Descripción	Ventajas
Integridad de los sistemas garantizada		
Protección frente a amenazas externas	Garantiza que solo se ejecute el código autorizado. El código no autorizado no puede inyectarse en la memoria, y el código autorizado no puede manipularse.	▪ Acaba con la aplicación de parches de emergencia, reduce la cantidad y la frecuencia de los ciclos de aplicación de parches, permite realizar más pruebas antes de aplicarlos y reduce el riesgo para la seguridad de los sistemas en los que es difícil aplicarlos. ▪ Reduce el riesgo para la seguridad que suponen los ataques de tipo zero-day y polimórficos, que se propagan por medio de malware, como gusanos, virus y troyanos, y de inyección de código, como los casos de desbordamiento del búfer, del montón y de la pila. ▪ Preserva la integridad de los archivos autorizados, lo que garantiza que el estado del sistema productivo se conoce y se ha verificado. ▪ Reduce los costes operativos mediante la reducción del período de inactividad por aplicación de parches no planificados y recuperación, además de mejorar la disponibilidad de los sistemas.
Protección frente a las amenazas internas	La función de restricción de acceso a los administradores locales ofrece la flexibilidad necesaria para que ni siquiera ellos puedan cambiar lo que está autorizado para que se ejecute en un sistema protegido, a menos que presenten una clave auténtica.	▪ Ofrece protección frente a las amenazas internas. ▪ Bloquea lo que se ejecuta en los sistemas integrados de los entornos productivos e impide su modificación, incluso a los administradores.

FICHA TÉCNICA

Función	Descripción	Ventajas
Control de cambios avanzado		
Protección de las actualizaciones autorizadas de los fabricantes	Garantiza que en los sistemas integrados en producción solo puedan aplicarse las actualizaciones autorizadas.	▪ Garantiza que no se puedan aplicar cambios fuera de banda en los sistemas en producción. Impide que se realicen cambios no autorizados en los sistemas para evitar que puedan provocar tiempos de inactividad y requieran la asistencia del soporte técnico. ▪ Los fabricantes pueden optar por conservar el control de todos los cambios, o bien autorizar solo a agentes de confianza en los clientes para que lleven a cabo dicho control.
Verifica que los cambios se realizan dentro del período aprobado	Permite garantizar que los cambios no se realizan fuera de los períodos de cambios autorizados.	▪ Impide que se realicen cambios no autorizados durante períodos asociados a las obligaciones fiscales o durante las horas de mayor productividad para evitar interrupciones y/o el incumplimiento de las normativas.
Actualizadores autorizados	Garantiza que solo realicen cambios en los sistemas de producción los actualizadores autorizados (personas o procesos).	▪ Garantiza que no se aplique ningún cambio fuera de banda en los sistemas de producción.
Funciones de auditoría y cumplimiento de normativas en tiempo real y de bucle cerrado		
Supervisión de los cambios en tiempo real	Realiza un seguimiento de los cambios en toda la empresa en cuanto se producen.	▪ Garantiza que no se aplique ningún cambio fuera de banda en los sistemas de producción.
Auditoría global	Obtiene información completa de cada uno de los cambios realizados en los sistemas: quién, qué, dónde, cuándo y cómo.	▪ Ofrece un registro exacto, completo y definitivo de todos los cambios realizados en los sistemas.
Identificación del origen de los cambios	Relaciona todos los cambios con su origen: quién los efectuó, la secuencia de eventos que condujeron al cambio y el proceso o programa que intervinieron.	▪ Valida los cambios aprobados, identifica con rapidez los cambios no autorizados e incrementa la tasa de éxito de los cambios.
Reducción de los costes operativos		
Instalar y listo	El software se instala en unos minutos y no requiere una configuración inicial. Tampoco es necesario modificar la configuración posteriormente de forma periódica.	▪ Está listo para usarse tras la instalación. Empieza a funcionar inmediatamente después de la instalación. No tiene gastos de mantenimiento, por lo que es una opción ideal para configurar una solución de seguridad con unos costes operativos reducidos.
No tiene reglas, firmas ni período de aprendizaje, y es independiente de las aplicaciones	No depende de reglas ni de bases de datos de firmas, es eficaz en todas las aplicaciones de inmediato, sin período de aprendizaje.	▪ Requiere muy poca atención de los administradores durante el ciclo de vida del servidor. ▪ Protege los servidores sin parches o hasta que se aplican los parches, con costes operativos reducidos. ▪ Su eficacia no depende de la calidad de las reglas o de las directivas.
Ocupa poco espacio y requiere pocos recursos para su ejecución	Necesita menos de 20 MB de espacio en disco. No afecta al tiempo de ejecución de las aplicaciones.	▪ Se ofrece listo para su despliegue en cualquier sistema de producción esencial, y no afecta a sus tiempos de ejecución ni a su espacio de almacenamiento.

FICHA TÉCNICA

Función	Descripción	Ventajas
Garantiza que no se producirán falsos positivos ni falsos negativos	Solo se registra la actividad no autorizada.	▪ La precisión de los resultados reduce los costes operativos en comparación con otras soluciones de prevención de intrusiones en el host, ya que disminuye drásticamente el tiempo necesario para analizar los registros diaria o semanalmente. ▪ Mejora la eficiencia de los administradores y reduce los costes operativos.

1. Disponible solo para plataformas Microsoft Windows.

Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas, Madrid, España
+34 91 347 85 00
www.mcafee.com/es