McAfee Application and Change Control

Protección integral frente a cambios imprevistos o no autorizados, y control de aplicaciones, endpoints, servidores y dispositivos de función fija

Las amenazas persistentes avanzadas (APT) que llegan a través de ataques remotos o ingeniería social dificultan cada vez más la protección de la empresa y pueden dar lugar a violaciones de la seguridad, pérdidas de datos y caídas de sistemas. En especial en los entornos de servidores y de la nube actuales, que evolucionan continuamente, los cambios malintencionados pueden pasar desapercibidos. Si tiene una tolerancia cero a las amenazas persistentes avanzadas (APT) debe considerar el software McAfee® Application and Change Control.

McAfee® Application Control ayuda al equipo de TI a burlar a los ciberdelincuentes y a mantener la seguridad y la productividad del negocio. Mediante el uso de un modelo de confianza dinámico y de la inteligencia de reputación local y global, los análisis de comportamiento en tiempo real y la inmunización automática de los endpoints, esta solución de McAfee frustra de manera inmediata las amenazas persistentes avanzadas, sin necesidad de complicadas administraciones de listas ni actualizaciones de firmas.

El software McAfee® Change Control bloquea los cambios no autorizados en archivos de sistema, configuraciones y directorios críticos, mientras racionaliza la implementación de directivas nuevas y las medidas de cumplimiento de normativas. McAfee Change Control, que incluye supervisión de la integridad de archivos y prevención de cambios, implementa las directivas de cambios y ofrece una supervisión continua de los sistemas esenciales. Además, detecta y bloquea los cambios no deseados realizados en ubicaciones distribuidas y remotas. Su intuitiva interfaz de búsqueda ayuda a los usuarios a localizar rápidamente la información sobre eventos de cambio.

La solución McAfee Application and Change Control garantiza la integridad de los sistemas, ya que solo permite el acceso autorizado a los dispositivos, bloqueando los ejecutables no autorizados, y con un enfoque sistemático de la supervisión y la prevención de cambios en el sistema, el registro y las cuentas de los usuarios. De esta forma se garantiza una detección y una protección continuas, eficaces y en toda la empresa.

Ventajas principales

- Uso de McAfee Global Threat Intelligence y McAfee Threat Intelligence Exchange para proporcionar reputación de archivos y aplicaciones global y local.
- Mejora de la seguridad y reducción del coste de propiedad con listas blancas dinámicas que aceptan de manera automática el software nuevo que se ha agregado a través de los canales de confianza.
- Implementación de controles en los servidores, las máquinas virtuales, los endpoints, los dispositivos fijos, como los terminales punto de venta, y los sistemas heredados, tanto conectados como no conectados.
- Compatibilidad con nuevas aplicaciones en función de su calificación o la autoaprobación para facilitar la continuidad de la actividad empresarial.

Síganos

Listas blancas inteligentes

Evite los ataques zero-day y de amenazas avanzadas persistentes, bloqueando la ejecución de aplicaciones no autorizadas y permitiendo solamente la ejecución de las reconocidas como legítimas, incluidas en listas blancas. McAfee Application and Change Control agrupa los archivos binarios (.EXE, DLL, controladores y scripts) de toda la empresa, por aplicación y proveedor, y los muestra en un formato intuitivo y jerárquico, clasificados como aplicaciones legítimas conocidas, desconocidas y maliciosas conocidas.

Implementación del estado de seguridad adecuado

Para ofrecer más flexibilidad de aplicaciones en el mundo empresarial actual que hace uso de la nube y las redes sociales, McAfee Application and Change Control ofrece a las empresas tres opciones para sacar el máximo partido de su estrategia de listas blancas con el fin de mejorar la prevención de amenazas:

Figura 1. Tres formas de maximizar la estrategia de listas blancas.

Respuesta rápida y completa

El uso de las listas blancas se complementa con la inteligencia de McAfee® Global Threat Intelligence, una exclusiva tecnología de McAfee que supervisa, en tiempo real, la reputación de los archivos, mensajes y remitentes mediante millones de sensores desplegados en todo el mundo. McAfee Application Control utiliza esta información para determinar la reputación de los archivos en un entorno informático y clasificarlos como legítimos, maliciosos o desconocidos.

Cuando se despliega con McAfee® Threat Intelligence Exchange, un módulo opcional que se vende por separado, McAfee Application and Change Control actualiza la lista blanca según la información de reputación local, para combatir las amenazas al instante. Además, utiliza McAfee Threat Intelligence Exchange para coordinarse con McAfee® Advanced Threat Defense para analizar de forma dinámica el comportamiento de las aplicaciones desconocidas en un entorno aislado (o sandbox) e inmunizar automáticamente manera todos los endpoints frente al malware que se acaba de detectar.

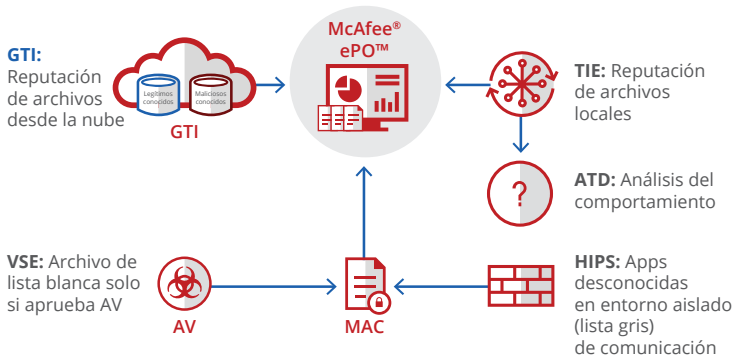

Figura 2. McAfee Global Threat Intelligence y McAfee Threat Intelligence Exchange proporcionan reputación global y local para McAfee Application Control.

Principales ventajas (continuación)

- Visibilidad constante y en tiempo real de los cambios en archivos del sistema, de configuración y de contenido esenciales.
- Prevención de las alteraciones de archivos críticos y claves del registro por parte de personas no autorizadas
- Implementación estricta de directivas, gracias al bloqueo proactivo de los cambios ajenos al proceso actual y no deseados antes de que se produzcan.

Información integrada y de gran utilidad

Las búsquedas en inventario y los informes predefinidos ayudan a los usuarios a gestionar con facilidad los problemas de vulnerabilidades, cumplimiento de normativas y seguridad en entornos y archivos relacionados con aplicaciones. Además, pueden descubrir información de utilidad, como las aplicaciones que se han añadido recientemente, los archivos binarios no certificados, los archivos con reputación desconocida y los sistemas que ejecutan versiones de software anticuadas.

El modo de inventario, que es nuevo en McAfee Application and Change Control 8.3, mantiene continuamente inventarios actualizados de todos los sistemas y dispositivos. De esta forma, se reduce el uso de recursos de CPU y de sistemas y dispositivos, mientras que se garantiza el cumplimiento de SWAM/CPE y PCI-DSS. El modo de inventario permite a los usuarios hacer un seguimiento de los cambios en archivos y binarios en el endpoint a lo largo del tiempo. Common Platform Enumeration (CPE) ofrece la opción de comparar los datos de NIST CPE con inventarios recopilados, y utilizar esa información en la creación de listas blancas y en los informes de cumplimiento.

Sin perjudicar la continuidad de la actividad empresarial

Para evitar interferencias con la actividad empresarial, las nuevas aplicaciones se permiten automáticamente en función de su reputación. En el caso de las aplicaciones desconocidas, una interfaz de sugerencias recomienda nuevas directivas de actualizaciones basadas en modelos de ejecución en los endpoints. Es una forma excelente de gestionar las excepciones que generan las aplicaciones bloqueadas. Tras investigar las excepciones y los detalles de las aplicaciones bloqueadas, basta con aprobar el archivo y asignarlo a la lista blanca, o bien ignorarlo para que se bloquee la aplicación.

Participación activa de los usuarios

En el caso de las aplicaciones desconocidas, McAfee Application and Change Control explica a los usuarios por qué no se permite el acceso a las aplicaciones no autorizadas y les permite realizar pasos para aprobar la aplicación, de forma autónoma o a través de solicitudes.

Sistemas actualizados

Es importante mantener los sistemas actualizados con los últimos parches. El modelo de confianza dinámico de McAfee Application and Change Control puede actualizar los sistemas automáticamente, sin afectar a la continuidad de la actividad empresarial. Mantenga los sistemas al día con usuarios y grupos locales de confianza, así como certificados, procesos y directorios de confianza. McAfee Application Control impide igualmente que las aplicaciones incluidas en la lista blanca puedan sufrir ataques por desbordamiento del búfer en sistemas Microsoft Windows.

Prevención de cambios y supervisión de la integridad

A menudo, existe la posibilidad de que se modifique la configuración y no hay visibilidad de quién ha realizado el cambio, lo que puede dar lugar a violaciones de la seguridad, pérdida de datos e interrupciones de la actividad. McAfee Application and Change Control puede bloquear o restringir los intentos de cambios realizados en sistemas y dispositivos, que no se ajusten

Plataformas compatibles

McAfee Application and Change Control

- 8.3.x, 8.2.x, 8.1.x, 8.0.x, 7.0.x (sistemas operativos basados en Windows)
- 6.4.x, 6.3.x (sistemas operativos basados en Linux) 6.2.x, 6.1.x (sistemas operativos basados en Windows y en UNIX)
- Linux
- Microsoft Windows

a las directivas. Los cambios intentados se guardan en el registro y se ofrece visibilidad en tiempo real de los eventos relacionados con cambios. El módulo supervisor del sistema gestiona la comunicación entre el controlador del sistema y los agentes.

Supervisión de la integridad de archivos de un nivel superior

McAfee Application and Change Control permite la implementación del software File Integrity Monitoring (FIM) en tiempo real y la validación del cumplimiento de PCI DSS de una forma eficaz y rentable. FIM de McAfee Application and Change Control proporciona información sobre quién, cuándo, qué y por qué, incluidos el nombre del usuario, la hora del cambio, el nombre del programa y el contenido del archivo/registro, todo en una única ubicación y en tiempo real. Además, puede ayudar a identificar las causas principales de una caída del sistema durante tareas de solución de problemas.

Seguimiento de los cambios de contenido

McAfee Change Control permite al equipo de TI realizar un seguimiento de los cambios realizados en el contenido y en los atributos de los archivos. Los cambios en el contenido de los archivos pueden visualizarse y compararse en paralelo, para ver lo que se ha añadido, eliminado o modificado. Se pueden configurar filtros de inclusión/exclusión de manera que únicamente se capten los cambios pertinentes y procesables. También se pueden limitar los cambios en sistemas y dispositivos, por usuarios, grupos de usuarios locales, aplicaciones, certificados y/o servicios web. Los cambios en dispositivos y sistemas se pueden incluso restringir a determinadas fechas y horas (por ejemplo, permitir que se apliquen actualizaciones de Windows solamente entre las 2 y las 4 de la mañana los martes). Asimismo, los mecanismos de alerta especiales informan al equipo de TI al instante de los cambios críticos, para que pueda impedir las interrupciones relacionadas con la configuración —una de las mejores prácticas recomendadas por la biblioteca ITIL (Information Technology Infrastructure Library). También se proporcionan formularios QSA (Qualified Security Assessor, Asesor de seguridad cualificado) para simplificar la generación de informes PCI.

Prevención de interrupciones asociadas a cambios no planificados

McAfee Change Control permite al personal de TI resolver fácilmente los incidentes, automatizar los controles de cumplimiento de normativas y prevenir las interrupciones asociadas a cambios. Además, ayuda a eliminar la necesidad de directivas de cumplimiento manuales, que requieren muchos recursos y propensas a errores, a menudo asociadas a la ley Sarbanes-Oxley (SOX). McAfee Application and Change Control permite a los usuarios generar una infraestructura automatizada de control de TI en la que toda la información necesaria para verificar el cumplimiento de normativas está disponible en un único sistema de generación de informes. Los cambios que contravienen las autorizaciones pueden validarse automáticamente. Las reparaciones de emergencia y otros cambios ajenos al proceso se documentan y concilian automáticamente para facilitar las auditorías.

Administración centralizada de la seguridad y el cumplimiento de normativas

El software McAfee® ePolicy Orchestrator® (McAfee ePO™) consolida y centraliza la administración, proporcionando de esta forma una visión global de la seguridad de la empresa. Esta galardonada plataforma integra McAfee Application and Change Control con McAfee® Host Intrusion Prevention y otras soluciones de seguridad de McAfee, como el antimalware para listas blancas. Además, McAfee Application and Change Control puede desplegarse y actualizarse en un solo paso desde Microsoft System Center. Se pueden activar nuevos perfiles en todo momento para reforzar la protección; desde una supervisión sencilla hasta una implementación de alta seguridad.

Pasos siguientes

Bloquee o limite con confianza la ejecución de aplicaciones no autorizadas que pongan los datos en riesgo, y emplee un enfoque sistemático para supervisar y prevenir los cambios en el sistema de archivos, el registro y las cuentas de los usuarios. McAfee Application and Change Control garantiza la integridad del sistema, ya que solamente permite el acceso autorizado a los dispositivos y bloquea los ejecutables no autorizados.

Para obtener más información, visite www.mcafee.com/es/products/application-control.aspx o llámenos al 0080012255624.

Más información

Para obtener más información, consulte la Guía para entornos admitidos—KB87944.

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