

McAfee Application Control

Reduzca los riesgos asociados a las aplicaciones no autorizadas para controlar los endpoints, servidores y dispositivos fijos.

Las amenazas persistentes avanzadas ejecutadas mediante ataques remotos o ingeniería social complican cada vez más la protección de su empresa. McAfee® Application Control le ayuda a burlar a los ciberdelincuentes y garantizar la seguridad y la productividad de su negocio. Mediante el uso de un modelo de confianza dinámico y de innovadoras funciones de seguridad, como 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 emplear las complicadas administraciones de listas ni las actualizaciones de firmas. McAfee Application Control es la solución ideal para protegerle de las amenazas de tipo zero-day.

Listas blancas inteligentes

McAfee Application Control previene los ataques de tipo zero-day y de amenazas persistentes avanzadas mediante el bloqueo de la ejecución de las aplicaciones no autorizadas. Con nuestra función de inventario, es fácil localizar y gestionar los archivos de aplicaciones. Agrupa todos los binarios (EXE, DLL, controladores y secuencias de comandos) en su empresa por aplicación y proveedor, y los muestra en un formato jerárquico intuitivo clasificándolos de forma inteligente como aplicaciones bien conocidas, conocidas y poco conocidas. Mediante el uso de listas blancas, puede evitar ataques de malware desconocido permitiendo la ejecución únicamente de aplicaciones bien conocidas de la lista blanca.

Implementación del estado de seguridad adecuado

En un momento en el que los usuarios demandan más flexibilidad para utilizar las aplicaciones en el entorno empresarial a través de la nube y las redes sociales, McAfee Application Control ofrece a las empresas tres opciones para potenciar su estrategia de lista blanca con el fin de mejorar la prevención de amenazas como se muestra a continuación:

Principales ventajas

- Protección contra amenazas persistentes avanzadas y de tipo zero-day sin actualizaciones de firmas.
- 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 costo 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.
- Control eficaz del acceso a las aplicaciones con el software McAfee® ePolicy Orchestrator® (McAfee ePO™), una plataforma centralizada para la administración de las soluciones de seguridad de McAfee.
- Reducción de los ciclos de aplicación de parches gracias a listas blancas seguras y a la protección avanzada de la memoria.

FICHA TÉCNICA



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

Información integrada y de gran utilidad

Con las búsquedas en inventario y los informes predefinidos, puede localizar y resolver fácilmente los problemas de vulnerabilidades, cumplimiento y seguridad en su entorno. Además, puede descubrir información de gran utilidad, como cuáles son las aplicaciones que se han agregado recientemente, los archivos binarios no certificados, los archivos con reputación desconocida o los sistemas que ejecutan versiones de software obsoletas, entre otros datos, con el fin de identificar rápidamente las vulnerabilidades y validar la conformidad de las licencias de software.

Respuesta rápida y completa

El uso de las listas blancas se complementa con la inteligencia global sobre amenazas que aporta McAfee Global Threat Intelligence (McAfee GTI), 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 de su 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 Control actualiza la lista blanca según la información de reputación local para combatir las amenazas al instante. Gracias a McAfee Threat Intelligence Exchange, McAfee Application Control se coordina con McAfee Advanced Threat Defense para analizar de forma dinámica el comportamiento de las aplicaciones desconocidas en un entorno aislado (o sandbox) e inmuniza de manera automática a todos los endpoints frente al malware que se acaba de detectar.

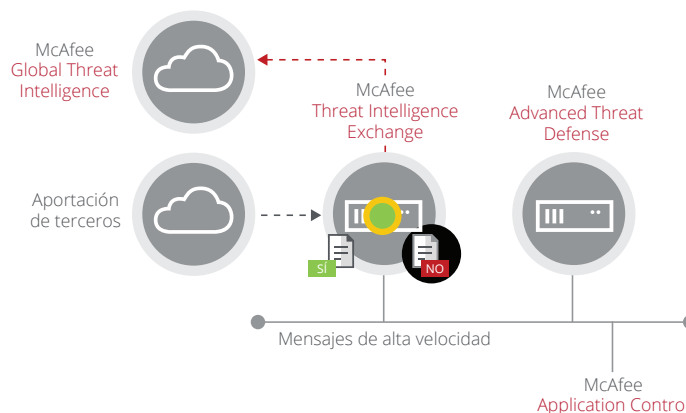


Figura 2. McAfee GTI supervisa constantemente la reputación de los archivos y remitentes. Cuando se despliega con McAfee Threat Intelligence Exchange, McAfee Application Control actualiza automáticamente la lista blanca según la inteligencia de reputación local y puede coordinarse con McAfee Advanced Threat Defense si se necesita más información sobre un archivo.

Principales ventajas (continuación)

- Actualización continua de los sistemas con los últimos parches mediante actualizadores de confianza.
- Controles en servidores conectados o desconectados, máquinas virtuales, endpoints, dispositivos fijos, como terminales puntos de venta, y sistemas heredados como los de Microsoft Windows XP.
- Compatibilidad con nuevas aplicaciones en función de su calificación o la autoaprobación para facilitar la continuidad de la actividad empresarial.
- Mantenimiento de la productividad de los usuarios y el rendimiento del servidor gracias a una solución que utiliza pocos recursos.
- Protección sencilla de sistemas heredados e inversiones en tecnologías modernas.

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. Se trata de una forma extraordinaria 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 Control ofrece a los departamentos de TI varias formas de permitir a los usuarios la instalación de nuevas aplicaciones.

- **Notificaciones a usuarios:** los usuarios pueden recibir un mensaje informativo en el que se explica por qué no tienen acceso a aplicaciones no autorizadas. Estos mensajes invitan a los usuarios a solicitar la aprobación por correo electrónico o a través de los centros de asistencia.
- **Autoaprobaciones de usuarios:** los usuarios con privilegios pueden instalar nuevo software sin esperar a la aprobación del departamento de TI. Este departamento inspecciona las autoaprobaciones y crea directivas para toda la empresa destinadas a prohibir o permitir el uso de la aplicación en todos los sistemas.

Mantenga actualizados sus sistemas

Sabemos que es importante mantener sus sistemas actualizados con los últimos parches. Por eso ofrecemos un modelo de confianza dinámico para actualizar automáticamente los sistemas sin afectar a la marcha de su actividad empresarial. Mantenga los sistemas al día con usuarios, 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 de 32 y 64 bits.

Control de ejecución avanzado

Para mejorar la protección, McAfee Application Control le permite combinar reglas según el nombre de archivo, nombre de proceso, nombre de proceso principal, parámetros de línea de comandos y nombre de usuario. Puede utilizar el control de ejecución avanzado para detener los ataques que consiguen sortear el modo interactivo de bloqueo de entrada/salida de archivos para intérpretes de sistemas, y evitar que se hackeen las herramientas del sistema. Además, disfruta del algoritmo SHA-256, que es más fuerte y eficaz para crear directivas.

Plataformas compatibles

Microsoft Windows (32 y 64 bits)

- Sistemas incrustados: Windows XPE, 7 Embedded, WEPOS, POSReady 2009, WES 2009, Embedded 8, 8.1 Industry, 10
- Servidor: Windows Server 2008, 2008 R2, 2012, 2012 R2
- Sistemas de sobremesa: Windows NT, 2000, XP, Vista, 7, 8, 8.1, 10

Linux

- Red Hat/CentOS 5, 6, 7
- SUSE/openSUSE 10, 11
- Oracle Enterprise Linux 5, 6, 7
- Ubuntu 12.04

FICHA TÉCNICA

Software McAfee ePolicy Orchestrator: un panel único de visibilidad

El software McAfee ePO consolida y centraliza la administración, proporcionando de esta forma una visión global de la seguridad de la empresa, sin ángulos muertos. Esta galardonada plataforma integra McAfee Application Control con McAfee Host Intrusion Prevention y otras soluciones de seguridad de McAfee, como antimalware para listas blancas. Además, McAfee Application Control puede desplegarse y actualizarse en un solo paso desde Microsoft System Center.

Un modo de observación para optimizar su experiencia

El modo de observación le ayuda a descubrir las directivas destinadas a entornos de escritorio dinámicos sin aplicar el bloqueo de listas blancas. Le permite desplegar McAfee Application Control en entornos de preproducción o durante la fase inicial de producción sin perturbar el funcionamiento de las aplicaciones. Gracias a McAfee Application Control, los administradores pueden utilizar una sola página de descubrimiento de directivas para definir directivas y observaciones, así como solicitudes de autoaprobación.

Proteja los sistemas heredados y las inversiones en tecnología reciente

¿Necesita proteger sistemas operativos antiguos, como Microsoft Windows NT, 2000 y XP? Aunque Microsoft y otros proveedores de soluciones seguridad no admiten estos sistemas, con el software McAfee Application Control no tiene de qué preocuparse. Además, McAfee Application Control admite los últimos sistemas operativos, como Microsoft Windows 10.

Pasos siguientes

Para obtener más información, visite www.mcafee.com/mx/products/application-control.aspx.



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

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 © 2017 McAfee, LLC. 2183_1216
DICIEMBRE DE 2016