

McAfee Enterccept Standard Multi-Platform Server Agent

Prevención de Intrusiones para Sistemas Esenciales

El desafío

El número de nuevas vulnerabilidades y la velocidad con que los ataques pueden comprometer sistemas esenciales aumentan a cada año, aumentando así los riesgos a la disponibilidad, a la integridad y a la confidencialidad de los sistemas.

Desafortunadamente, los productos antivirus y de IDS de *host* tradicionales son reactivos y no hacen nada para bloquear ataques desconocidos que utilizan vulnerabilidades recién descubiertas. Además, las empresas, independientemente de su tamaño, sufren intensas presiones legislativas para asegurar la privacidad de datos confidenciales y controlar el acceso a sistemas y aplicaciones.

Para proteger preventivamente los sistemas contra los sofisticados ataques de hoy, las empresas necesitan implementar una prevención contra intrusiones que cuente con varios niveles de protección. McAfee® Enterccept® es la solución de prevención contra intrusiones más completa, precisa y flexible del mercado, que permite que las empresas reduzcan los riesgos, aseguren la disponibilidad de los negocios y reduzcan su costo total de propiedad.

La solución McAfee Enterccept

Los Agentes Multiplataforma Estándar Enterccept protegen los sistemas contra ataques conocidos y desconocidos, con una premiada tecnología patentada. Cada agente administrado centralmente utiliza una poderosa combinación de tecnologías de prevención de intrusiones para bloquear ataques con inigualable precisión:

- Reglas de comportamiento protegen contra ataques desconocidos dirigidos a nuevas vulnerabilidades — sin necesitar actualizaciones
- Las firmas protegen el *host*, identificando con precisión tráfico hostiles conocidos, reduciendo considerablemente el número de falsos positivos
- El *firewall* de sistema (sólo en las versiones para Windows®) controla el acceso a sistema y aplicaciones, bloqueando el tráfico que entra o sale del sistema, según la dirección IP, el protocolo o el puerto.

Beneficios

Completo

- Bloquea ataques desconocidos sin ninguna actualización, reduciendo significativamente la criticidad de la distribución de parches contra nuevas amenazas
- Tecnologías complementarias protegen la disponibilidad, la integridad y la confidencialidad de servidores y datos
- La prevención de intrusiones, aliada al *firewall* de sistema blindo las aplicaciones esenciales contra ataques



McAfee Enterccept utiliza reglas conductuales, archivos de características y un firewall de sistema para prevenir ataques conocidos y desconocidos.

Preciso

- La configuración de *aplicaciones confiables* permite que las empresas eliminen el riesgo de falsos positivos de aplicaciones esenciales
- Las firmas contienen descripciones específicas detalladas de eventos
- Políticas previamente configuradas que se pueden personalizar reducen el número de falsos positivos y liberan valiosos recursos humanos de seguridad

Flexible

- Administra hasta 10 000 agentes con un único administrador
- Administración opcional por McAfee ePolicy Orchestrator® 3.5
- Instalación y actualización imperceptibles, sin reinicio, que asegura protección continua
- Niveles personalizables de protección, desde el registro hasta el bloqueo

Cómo funciona McAfee Enterccept

Cada agente viene con un modelo predefinido de políticas totalmente configurado, y brinda protección sin la necesidad de otras configuraciones. Los agentes también poseen poderosos recursos de personalización que permiten a los profesionales de seguridad crear y ajustar políticas personalizadas específicas para sus entornos y reducir el número de falsos positivos.

El agente examina llamadas específicas al sistema y a las API, usadas por todas las aplicaciones para solicitar servicios al sistema operativo. Compara de forma ágil y eficaz sus reglas de comportamiento y características de ataques conocidos con un gran número de información sobre cada llamada (por ejemplo, el proceso que hizo la llamada, el contexto de seguridad en que se ejecuta el proceso, el recurso accedido, etc.). Entonces, el agente bloquea todas las llamadas de comportamientos o programas malintencionados.



La consola de administración de Enterecept presenta un resumen panorámico de las amenazas y de la situación del sistema.

Recursos

Prevención de ataques desconocidos — Enterecept impide ataques nuevos y nunca vistos, a través de sus poderosas reglas de comportamiento. Las reglas de comportamiento fiscalizan el comportamiento adecuado del sistema operacional y de aplicaciones y bloquean nuevos ataques que violen las políticas, sin ninguna necesidad de actualizaciones.

Prevención de la explotación de desborde de buffer — Una tecnología patentada impide la ejecución de programas como resultado de un desborde de buffer. Los agentes protegen los servidores esenciales contra dichas explotaciones peligrosas, que son la mayor fuente de vulnerabilidades de seguridad de los servidores.

Prevención de ataques conocidos — Bloquea explotaciones conocidas e impide que se causen daños a los servidores, comparando la actividad con su amplia base de datos de ataques conocidos. Los agentes acceden automáticamente a las actualizaciones de nuevas firmas de ataques.

Protección de recursos — Protege la disponibilidad, la integridad y la confidencialidad de los sistemas, bloqueando sus recursos esenciales (archivos, configuraciones, claves de registro, servicios, etc.).

Firewall de Sistema (sólo en las versiones para Windows) — Bloquea el tráfico de red que entra y sale del sistema, a través de un filtro de paquetes altamente individualizado y del *firewall*. Puede bloquear el tráfico que entra y sale del sistema, según el puerto, el protocolo y la dirección IP.

Blindaje/Empaquetamiento de Servidores de Web y de Base de datos — El blindaje impide la invasión y el uso inadecuado de recursos de aplicaciones esenciales (archivos, usuarios, registro, etc.). El empaquetamiento impide que la aplicación protegida realice actividades malintencionadas fuera de su comportamiento normal (por ejemplo, acceder a datos de otras aplicaciones).

Protección de HTTP y SQL — La protección de HTTP bloquea ataques dirigidos contra servidores de Web Apache, Sun o Microsoft®, por medio de un exclusivo mecanismo de descomposición de HTTP. La protección de SQL protege servidores SQL 2000 contra técnicas de inyección de SQL, a través de un exclusivo mecanismo de consulta de SQL.

Distribución y Monitoreo por McAfee ePO™ 3.5 — Opciones de instalación, actualización y monitoreo de agentes.

Sistema necesario

Windows (sólo para las versiones del SO en inglés, francés y alemán)

- Windows Server 2003
- Windows XP SP2
- Windows 2000 Server y Advanced Server
- Windows NT 4 Server o Enterprise Server, SP 6A
- Microsoft SQL Server 2000
- Microsoft IIS 4, 5 y 6

Sun

- Solaris 7, 8 y 9 (kernels de 32 y 64 bits)
- Sun ONE/iPlanet 3.6, 4.0, 4.1 y 6.0

HP-UX

- HP-UX II.0, Ili (PA-RISC de 64 bits)

Apache

- Apache 1.3.6 y posteriores, 2.0.42 y posteriores

McAfee PrimeSupport

El programa McAfee PrimeSupport® es esencial para sacar el máximo provecho de su inversión en las Soluciones de Protección de Sistemas y Redes de McAfee. El equipo PrimeSupport de McAfee cuenta con todos los recursos correctos y está lista para llevar a usted la solución de servicios que necesita. Entre los recursos del PrimeSupport están: autorización de acceso a todas las versiones de mantenimiento y actualizaciones de productos disponibles, acceso a una amplia gama de otros recursos de autoatención remota, soporte telefónico en directo al que se puede acceder 24/7/365, gerentes de cuenta de soporte asignados y disponibles, además de una amplia gama de soluciones de soporte de software y hardware que se pueden adaptar a sus necesidades.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

Los productos de McAfee® denotan años de experiencia y compromiso con la satisfacción del cliente. El equipo McAfee PrimeSupport® de técnicos de soporte colaboradores y altamente cualificados brinda soluciones hechas a la medida, brindando asistencia técnica detallada para administrar el éxito de proyectos esenciales — todo eso con niveles de servicio que atienden a las necesidades de todas las empresas clientes. McAfee Research, líder mundial en sistemas de información e investigaciones de seguridad, sigue encabezando la innovación en el desarrollo y el refinamiento de todas nuestras tecnologías.

McAfee, Enterecept, ePolicy Orchestrator y PrimeSupport son marcas comerciales, registradas o no, de McAfee, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. El color rojo asociado a la seguridad es marca distintiva de los productos que llevan la marca McAfee®. Todas las otras marcas comerciales, registradas o no, mencionadas en este documento pertenecen exclusivamente a sus respectivos propietarios. © 2004 Network Associates Technology, Inc. Todos los derechos están reservados. 1-sps-ese-005-1204