

McAfee Enterecept Desktop Agent

Prevención de intrusiones para *notebooks* y *desktops*

El desafío

Por sí mismos, los productos antivirus tradicionales no logran asegurar la disponibilidad, integridad y confidencialidad de sistemas portátiles y *desktops*. Estos sistemas contienen los mismos datos propietarios o regulados que se encuentran en servidores corporativos y, además frecuentemente se encuentran fuera de la protección de herramientas corporativas de seguridad tales como *firewalls* y sistemas de prevención de intrusión de redes, por lo cual resultan ser como puertas abiertas para brechas de seguridad.

Las empresas necesitan defender sus sistemas más vulnerables con medidas avanzadas y preventivas contra amenazas y ataques que explotan las vulnerabilidades. Los productos antivirus tradicionales son reactivos y no hacen nada para bloquear los 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.

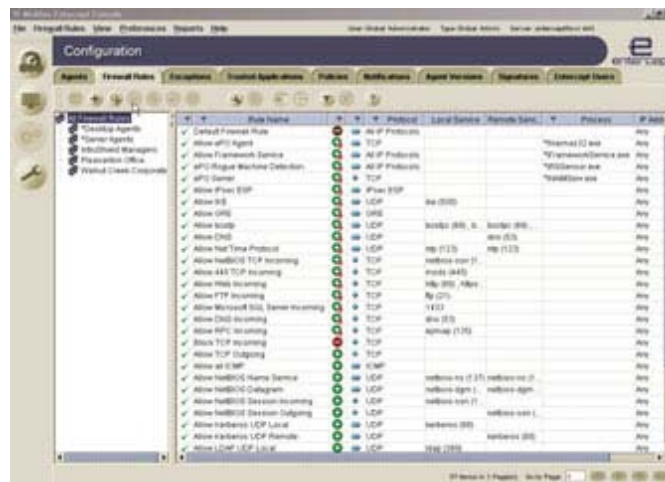
Para proteger de forma amplia y preventiva sus sistemas portátiles y *desktops*, las empresas necesitan implementar una prevención de nivel profesional contra intrusiones. McAfee® Enterecept® es la solución de prevención contra intrusiones más precisa y flexible para *desktops* y sistemas portátiles 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 Enterecept para *notebooks* y *desktops*

Los agentes de McAfee Enterecept protegen sistemas portátiles y *desktops* contra ataques conocidos y desconocidos con la misma tecnología patentada y premiada disponible en los agentes Enterecept para servidor. Los agentes Enterecept para *desktop* cuentan con reglas de comportamiento desarrolladas específicamente para proteger las aplicaciones de *desktop* más explotadas, tales como Microsoft® Internet Explorer y Outlook contra explotaciones desconocidas, sin ninguna actualización.

Cada agente administrado de forma centralizada utiliza una combinación exclusiva de tres tecnologías de prevención de intrusiones para bloquear ataques contra aplicaciones y servicios de *desktop*, con precisión inigualable:

- Reglas de comportamiento protegen contra ataques desconocidos dirigidos a nuevas vulnerabilidades o explotaciones para las cuales todavía no existe ningún parche, reduciendo la urgencia de la distribución de parches.
- Firmas protegen el *host*, identificando con precisión contenidos hostiles conocidos en los datos, además de bloquear cargas peligrosas antes que estas sean procesadas, reduciendo considerablemente los falsos positivos.
- El Firewall de Sistema protege aplicaciones y datos, bloqueando el tráfico que entra o sale del sistema, según la dirección IP, el protocolo o el puerto.



Enterecept es completamente invisible al usuario final, con políticas individualizadas y personalizables controladas por los administradores.

Ventajas

Completo

- Bloquea ataques desconocidos, sin actualizaciones
- Reduce considerablemente la criticidad de la distribución de parches contra nuevas amenazas
- Protege la disponibilidad, la integridad y la confidencialidad de datos y sistemas
- La prevención de intrusiones más la protección de *firewall* asegura sistemas portátiles y *desktops* contra ataques

Preciso

- Las Aplicaciones Confiables permiten que las empresas eliminen los falsos positivos de aplicaciones críticas
- Las firmas reducen significativamente el número de falsos positivos y generan descripciones exactas y detalladas de los eventos
- Políticas personalizables permiten adaptarse a cualquier entorno

Flexible

- Administra hasta 10 000 agentes con un único administrador
- Administración opcional por McAfee ePolicy Orchestrator® 3.5
- Instalación silenciosa y actualizaciones sin reinicio o intervención del usuario final eliminan la posibilidad de violación de políticas
- La reacción automática a eventos de seguridad y la ausencia de una interfaz local para el usuario impiden que los usuarios finales permitan brechas accidentalmente

Cómo funciona McAfee Enterecept

Cada agente Enterecept viene con modelos predefinidos de políticas totalmente configurados, que brindan 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 específicas para sus entornos y reducir el número de falsos positivos.

El agente examina llamadas específicas al sistema y llamadas a la API (ambas usadas por todas las aplicaciones para solicitar servicios del sistema operativo). Compara de forma rápida y eficaz sus reglas de comportamiento y firmas de ataques conocidos con un gran volumen 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.). El agente bloquea entonces todas las llamadas de comportamientos maliciosos o programas malintencionados.

Los agentes toman automáticamente las actualizaciones cifradas y autenticadas del sistema de administración, asegurando que cada uno tenga las políticas y firmas de ataques más recientes.



Enterecept asegura la disponibilidad, la integridad y el sigilo de sistemas portátiles y desktops.

Recursos

Prevención de Ataques desconocidos — Enterecept impide ataques nuevos y nunca vistos, a través de sus poderosas reglas de comportamiento que no necesitan actualización para bloquear los ataques desconocidos. Este abordaje basado en comportamiento fiscaliza el correcto comportamiento del sistema operativo y de las aplicaciones, además de bloquear nuevos ataques que violan políticas.

Prevención de la Explotación de desborde de buffer — Una tecnología patentada impide la ejecución de programas como resultado de un desborde de buffer, que es la mayor fuente de vulnerabilidades de seguridad de los sistemas.

Prevención de Ataques conocidos — Detecta y bloquea explotaciones conocidas e impide que se causen daños a los sistemas, comparando la actividad con su amplia base de datos de

ataques conocidos, automáticamente actualizada, además de presentar un análisis forense detallado.

Firewall de Sistema — Bloquea el tráfico que entra y sale del sistema, a través de un filtro de paquetes altamente granular y del *firewall*. Puede bloquear el tráfico que entra y sale del sistema, según el puerto, el protocolo y la dirección IP.

Protección de Recursos — Protege los sistemas contra comprometimientos, bloqueando sus recursos esenciales (archivos, configuraciones, claves de registro, servicios, etc.), impidiendo inclusive a los usuarios que poseen derechos administrativos de saltarse las políticas de seguridad.

Invisible a los Usuarios finales — Los agentes son completamente invisibles a los usuarios finales, y no requieren ninguna interacción durante la instalación, las actualizaciones o para reaccionar a eventos de seguridad.

Control local de acceso — Bloquee el acceso a unidades de memoria USB, unidades de disquete, etc.

Blindaje/Empaquetamiento de aplicaciones — El blindaje impide la intrusión y el uso inadecuado de los recursos del Internet Explorer y del Microsoft Outlook (archivos, usuarios, registro, etc.) El empaquetamiento impide que dichas aplicaciones realicen actividades malintencionadas fuera de su comportamiento normal (por ejemplo, acceder a datos de otras aplicaciones).

Políticas ágiles de prevención paso a paso listas para usar — Una consola intuitiva de administración permite que las empresas muevan los agentes a través de niveles incrementales de sensibilidad, logrando así, incrementar su postura de seguridad, paso a paso. El resultado es un nivel de casi cero falsos positivos y muy pocos ajustes en el largo plazo.

Administración centralizada — El sistema de administración permite que las empresas fiscalicen configuraciones de seguridad entre sus aplicaciones, grupos de usuarios y agentes para reducir el costo de instalación y mantenimiento.

Requerimientos del Sistema

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

- Windows XP SP2, Windows 2000 Workstation o Windows NT 4 Workstation

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 listo 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 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-ent-dta-001-1204