

# McAfee Entercept Management System

## Administración de Clase Empresarial para McAfee Entercept Intrusion Prevention

### El desafío

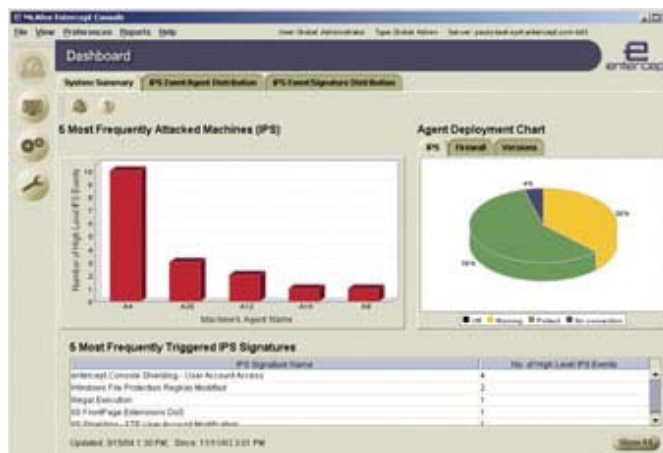
Las empresas enfrentan la atemorizante tarea de proteger las redes de hoy, que son geográficamente dispersas y heterogéneas. Necesitan manejar ataques combinados sofisticados que emplean varios vectores para penetrar en la infraestructura de seguridad. También necesitan cumplir exigencias legales de protección de la integridad y confidencialidad de los datos en sus sistemas y aplicaciones principales. Además, necesitan documentar para la alta gerencia el valor de sus inversiones en seguridad.

Las empresas necesitan implementar un sistema de administración de seguridad que sea capaz de administrar - con riqueza de recursos- miles de agentes, brindar protección inigualable contra amenazas y reducir el tiempo necesario para administrar el sistema. McAfee® Entercept® Intrusion Prevention es la solución del mercado más completa, precisa y flexible para la protección contra amenazas, que ayuda a las empresas a reducir los riesgos, asegurar la disponibilidad de los negocios y disminuir el costo total de propiedad.

### La solución Entercept

Entercept Management System brinda administración completa, de nivel empresarial para los agentes de prevención de intrusiones de Entercept. El Sistema de Administración ofrece una infraestructura de administración flexible, robusta y fácil de usar, capaz de controlar hasta 10000 agentes por servidor de administración.

Todos los agentes Entercept (Desktop y Servidor) comparten la misma infraestructura de administración que provee el Sistema de Administración. Las empresas pueden aprovechar fácilmente las configuraciones de seguridad entre aplicaciones, grupos de usuarios y agentes para reducir el costo de instalación y mantenimiento. Los administradores de seguridad pueden importar y exportar configuraciones entre varios servidores de administración, lo que asegura una fiscalización uniforme de las políticas. Entercept protege varias plataformas (Windows, HP-UX y Solaris), y brinda una protección uniforme y confiable contra intrusiones del host para los actuales entornos heterogéneos de servidor.



McAfee Entercept Management System posee un tablero de control resumido para exhibir un panorama del status del sistema.

### Cómo funciona Entercept Management System

Entercept Management System consiste en un servidor y una consola de administración altamente flexibles. El servidor de administración actúa como una capa intermedia entre los agentes Entercept y la consola, coordinando las comunicaciones y almacenando la base de datos de eventos y configuraciones. Varias consolas en ubicaciones geográficamente distribuidas pueden conectarse simultáneamente con el servidor de administración para administrar y monitorear los agentes.

Cuando los agentes detectan y bloquean los ataques, envían la información respectiva al servidor de administración Entercept. El servidor encamina los datos respectivos a las consolas, además de almacenarlos en la base de datos SQL central. La consola agrega eventos semejantes para reducir el volumen de datos brutos exhibidos, presentando un resumen de la situación general del sistema en un único tablero de control.

- El Sistema de Administración posee un amplio conjunto de opciones de reacción y notificación, incluso alertas por e-mail, por pager, capturas de SNMP, y disparo de un proceso. La consola se comunica con los agentes a través de canales cifrados y autenticados. Entercept Management System fiscaliza activamente las políticas de seguridad de la empresa con su premiada tecnología de prevención de intrusiones, bloqueando ataques y, al mismo tiempo, brindando recursos inigualables de reportes y análisis de datos.

## Ventajas

### Completo

- Reduce la criticidad de la distribución de parches contra nuevas amenazas
- Bloquea ataques conocidos y desconocidos
- Protege la integridad y la privacidad de datos confidenciales
- Fiscalización activa y automática de políticas, sin requerir la intervención del usuario final
- Protege sistemas Windows, Solaris y HP-UX con una premiada tecnología patentada
- Blindaje/Empaquetamiento de aplicaciones — El blindaje impide la intrusión y el uso inadecuado de los recursos de servidores de Web, de base de datos y de aplicaciones de desktop (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).

### Preciso

- Una poderosa combinación de reglas de comportamiento, firmas y firewall de sistema brinda protección contra ataques tales como explotaciones de desborde de buffer y reduce el número de falsos positivos
- Asistentes crean reglas y características personalizadas que se adaptan a cualquier entorno
- La ausencia de interacción del usuario final elimina las llamadas a la central de soporte de TI
- La búsqueda, el filtrado y la agrupación permiten que los administradores identifiquen tendencias y descubran posibles amenazas

### Flexible

- Administre miles de agentes con un único administrador
- Distribución y monitoreo de agentes a través del McAfee ePolicy Orchestrator<sup>®</sup> 3.5 (opcional)
- Aprovecha configuraciones entre aplicaciones, grupos de usuarios o agentes
- Instalación/actualización imperceptibles, sin la necesidad de reiniciar la máquina
- La agregación de eventos consolida eventos repetidos en un único artículo en la consola
- El rastro de auditoría de la consola registra todas las alteraciones de configuración realizadas por los administradores
- Niveles personalizables de protección, desde el registro hasta el bloqueo

## Requerimientos de Sistema

### Configuración recomendada

#### Servidor de Administración

- Pentium IV de 1,5 GHz o mejor
- 1 GB de RAM
- 20 GB de espacio libre en el disco duro
- Windows Server 2003
- Windows 2000 Server o Advanced Server (SP 2 o posterior)
- SQL Server 2000 (SP 2 o posterior)
- Dirección IP estática
- Ninguna otra aplicación instalada
- Puertos TCP 443 y 5005 disponibles (el 443 se utiliza si no se define nada de otra forma, pero se la puede alterar)

#### Consola

- Pentium III de 800 MHz o mejor
- 256 MB de RAM
- 100 MB de espacio libre en el disco duro
- Windows XP SP 2
- Windows 2000 Professional, Server o Advanced Server
- Windows NT 4 Server o Workstation, SP 6a

## McAfee PrimeSupport

McAfee viene adoptando la estrategia de proveer tecnología de primera clase para cada tipo de aplicación de administración de rendimiento — pero la Estrategia Protection-in-Depth™ es más que sólo distribuir e implementar las mejores soluciones hoy. La prevención es, seguramente, la prioridad número uno, pero, inevitablemente, ¿usted necesitará reaccionar a algún problema!

El programa McAfee PrimeSupport<sup>®</sup> 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](http://www.mcafee.com)

Los productos de McAfee<sup>®</sup> denotan años de experiencia y compromiso con la satisfacción del cliente. El equipo McAfee PrimeSupport<sup>®</sup> 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<sup>®</sup>. 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-mgt-003-1204