



Endpoint Access Manager de ControlGuard



Los datos de su empresa están expuestos a robo y uso indebido

El robo de información y la filtración de datos confidenciales son noticia frecuente hoy en día. Importantes organizaciones se han visto obligadas a informar al público respecto a documentación privada de clientes que ha sido comprometida.

La mayoría de los casos de filtración y robo de datos son atribuidos a personal interno y no siempre son intencionadas. Mientras que las redes de la empresa están generalmente protegidas por diversas aplicaciones de seguridad, PCs y ordenadores portátiles (terminales) se dejan a menudo expuestos a amenazas internas. Cualquier persona con acceso a estos terminales puede descargar fácilmente información confidencial o infectar su Pc con virus u otros tipos de programas dañinos (malware), utilizando dispositivos extraíbles como CD, Memory Sticks e iPods. Estos dispositivos portátiles y medios extraíbles no controlados representan una seria amenaza de seguridad. ControlGuard ofrece una solución para afrontar esta amenaza: Endpoint Access Manager.

Endpoint Access Manager impide la filtración de datos y el acceso no autorizado a TODO dispositivo o interfaz.



Endpoint Access Manager de ControlGuard protege eficazmente sus datos



- ➔ **Controlando** y monitorizando la forma en que se descarga información en los terminales.
- ➔ **Defendiendo** su red contra malware copiado a los terminales desde medios extraíbles y dispositivos portátiles.
- ➔ **Asegurando** su red contra la exposición al mundo externo a través de módems inalámbricos, Wifi, Bluetooth y otros interfaces.

Protección de los datos de su empresa

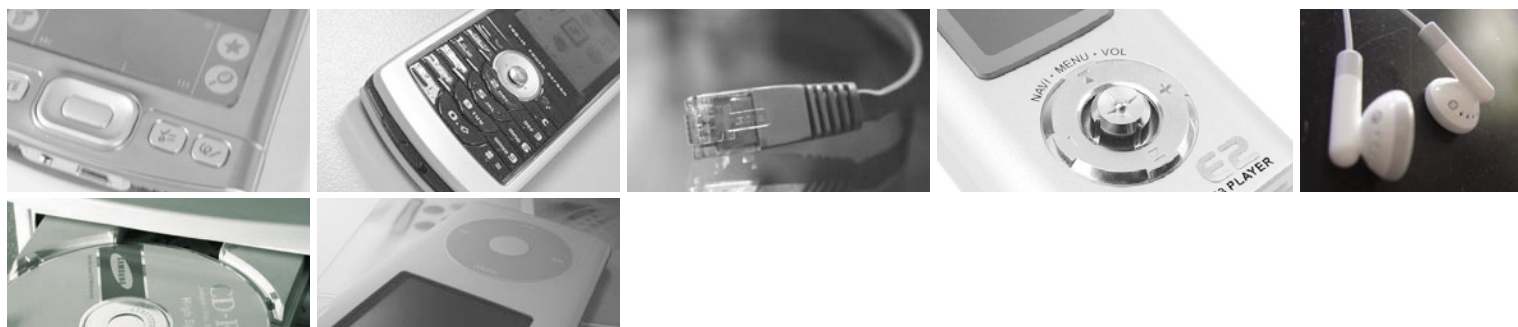
Endpoint Access Manager es una solución a nivel de empresa para controlar, monitorizar y registrar cómo se carga y descarga información en los terminales. Mediante la implementación de una política de control de acceso a terminales para dispositivos portátiles y medios extraíbles, la solución de ControlGuard impide eficazmente el uso no autorizado de datos de la empresa.

Endpoint Access Manager se instala y administra de forma centralizada. Los administradores de seguridad definen directivas que se distribuyen automáticamente a los terminales. Estas directivas se hacen cumplir y todos los eventos relevantes se reportan al Management Server. Una rigurosa integración con los directorios y sistemas de gestión de la empresa facilitan la instalación y hacen posible un detallado registro y una gran potencia de generación de informes.



I/O devices

- Internal Modems
- External Modems
- PDA's
- Network Printers
- Local Printers
- MP3 Players
- Tape Devices
- Biotech Devices
- CD/DVDs, Burners
- Memory Sticks
- LAN Adapters
- Camcorders
- Digital Cameras
- Scanners
- iPods
- Optical Devices
- Smart Phones
- Floppy Disks
- Mass Storage
- SD Cards
- Zip/Jazz Drives

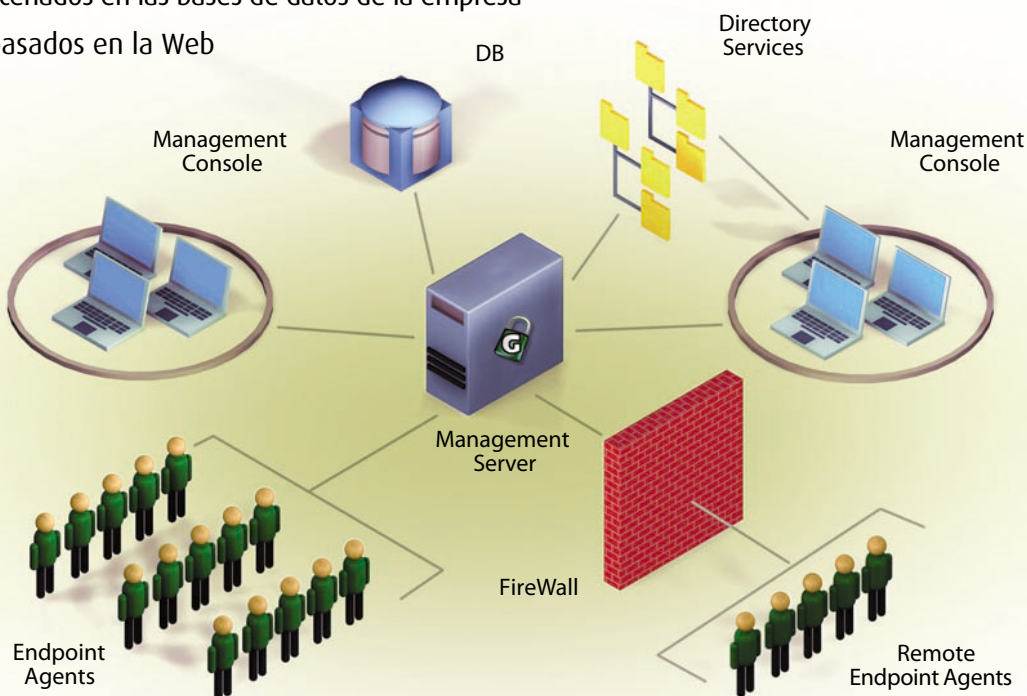


Implementación de Endpoint Access Manager

Endpoint Access Manager incluye un Management Server, una Management Console y Endpoint Agents. Management Server se instala en una ubicación central dentro de la red de la empresa. Los Agentes Endpoint se instalan sin dificultad en los terminales utilizando herramientas estándar de distribución de la empresa. Management Server comunica en forma inteligente las directivas de seguridad a los agentes. Los agentes hacen cumplir las directivas, monitorizan las actividades de los terminales y comunican los datos relevantes al Management Server.

Management Console ofrece sólidas herramientas para visualizar y analizar las actividades de los terminales, que incluyen:

- ➔ Notificaciones en tiempo real
- ➔ Registros de auditoría almacenados en las bases de datos de la empresa
- ➔ Informes personalizados basados en la Web



Management Console muestra las configuraciones de los terminales y revela los dispositivos conectados y las interfaces de medios. Toda actividad de entrada y salida en el terminal es controlada por las directivas definidas, además de ser registrada inmediatamente y mostrada en la Management Console. Endpoint Agent es responsable de que estas directivas se cumplan y de transmitir la información adecuada al Management Server. Las directivas pueden limitarse a la monitorización solamente o pueden permitir una acción específica, en un conjunto específico de dispositivos, para usuarios específicos.

Los Agentes Endpoint son módulos inteligentes e independientes que permanecen activos incluso cuando el terminal no está conectado a la red. Están protegidos contra ataques de procesos, servicios u otros controladores y los usuarios de los terminales no los pueden eludir, incluso si tienen derechos administrativos en el terminal.

Endpoint Access Manager se integra rigurosamente con los servicios de directorio, con los sistemas de gestión de la empresa, con la infraestructura de las aplicaciones y con los sistemas de distribución, facilitando la instalación y minimizando los gastos generales de administración.

Características clave

Directivas inteligentes y granulares

Endpoint Access Manager permite autorizar dispositivos, medios e interfaces específicos para PCs y usuarios, dentro y fuera de la red corporativa. Las directivas se comunican a los terminales en tiempo real y los Endpoint Agents hacen que se cumplan inmediatamente. Los administradores pueden otorgar permisos temporales a usuarios en línea y a usuarios móviles.

Distribución inteligente

Los Endpoint Agents se distribuyen e instalan eficazmente y sin dificultad en la red. Los agentes se pueden distribuir también mediante herramientas comunes de distribución de software de la empresa como Microsoft System Management Server.

Acepta conexión en caliente

Los Endpoint Agents monitorizan los controladores de los dispositivos Plug-and-Play instalados en el terminal. En función de las directivas de dicho terminal, el agente informará del dispositivo recientemente instalado al Management Server y hará que se cumplan los permisos adecuados de acceso.

Acepta usuarios móviles

Los terminales de los usuarios móviles también se monitorizan y protegen. El Endpoint Agent sigue haciendo que se cumplan las directivas incluso cuando el terminal no está conectado a la red. Puede aplicar distintos permisos de acceso a interfaces (como WiFi) cuando el terminal no está conectado a la red. Los administradores de seguridad pueden autorizar excepciones y otorgar a usuarios remotos el acceso temporal a un dispositivo extraíble requerido.

Notificaciones y auditoría en tiempo real

Todas las actividades de entrada y salida de datos de los terminales gestionados se notifican en tiempo real al Management Server y se registran en la base de datos. Los eventos se muestran en la Management Console y se comunican a los administradores de seguridad en varios formatos, tales como mensajes emergentes y correo electrónico. Los eventos se ponen también a disposición de sistemas de gestión de la empresa en capturas SNMP.

Acerca de ControlGuard

ControlGuard es proveedor líder de soluciones de seguridad para terminales a nivel de empresa. Empresas de todo el mundo se dirigen a ControlGuard para que proteja sus terminales contra violaciones de seguridad. El equipo de ControlGuard tiene vasta experiencia en seguridad de información y gestión de empresas, complementada por colaboraciones con proveedores de soluciones clave en este terreno. Para obtener más información acerca de las soluciones de ControlGuard, visite www.controlguard.com.

Agente de seguridad avanzado

El Endpoint Agent está protegido contra ataques de procesos, controladores, servicios y códigos dañinos en su terminal. Incluso usuarios que tienen privilegios administrativos en su terminal no lo pueden eludir.

Mecanismo de LiveUpdate

La función LiveUpdate controla la versión de software de los Endpoint Agents. Cuando es necesario, instala automáticamente actualizaciones, minimizando de este modo los gastos generales de administración.

Integración de directorios

Endpoint Access Manager se integra perfectamente con la infraestructura de directorios de la empresa como Microsoft Active Directory y Novell eDirectory. Esto permite a los administradores emplear eficazmente el diseño lógico organizacional existente de objetos y grupos. Asimismo, esto permite descubrir en forma dinámica nuevos objetos que se han agregado a la red e instalar opcionalmente un agente en cualquier terminal nuevo.

Integración de sistemas de gestión de la empresa

Endpoint Access Manager se integra perfectamente con sistemas de gestión de la empresa tales como CA Unicenter, CA eTrust y HP OpenView. Esto permite a los administradores emplear eficazmente la infraestructura de gestión existente y agrupar eventos de seguridad de terminales en registros unificados y en consolas de gestión existentes.

Exhaustivo generador de informes

Endpoint Access Manager registra todos los eventos de E/S de los terminales en una base de datos SQL. Un módulo de informes flexible e intuitivo permite a los administradores enviar consultas personalizadas y generar informes detallados sobre terminales y actividades de usuarios finales.

ControlGuard Ltd. - Headquarters:
1 Abba Eban Blvd.
Herzlia 46725 Israel
Tel +972-9-9578781
sales@controlguard.com

ControlGuard Inc. - US
1200 Route 22 East, Suite 2000
Bridgewater, NJ 08807
Tel +1-908-203-4685
sales@controlguard.com

Mayorista e importador para España:
Ireo - Mayorista de ITSM y Seguridad
Tel.: (+34) 902 32 11 22
www.ireo.com
info@ireo.com

www.controlguard.com