Secured eDevice - Ficha Técnica

DESCRIPCIÓN SOLUCIÓN

La Solución **Secured eDevice** ofrece una protección flexible y escalable a todos los equipos de cómputo de su red al permitirle de forma centralizada controlar, monitorear y registrar el acceso de Dispositivos Portátiles, Medios de Almacenaje Extraíbles, e Interfaces de los Equipos de Cómputo. **Secured eDevice** funciona a través de una Consola Central de Administración y un Agente de Seguridad que es instalado en los equipos de cómputo, portátiles, servidores, etc., que permite hacer cumplir las políticas de seguridad de la compañía y proteger la Información Confidencial.

Con tecnología avanzada que permite la balanza de carga (load balancing) y un diseño inteligente, **Secured eDevice** permite la distribución de las operaciones del día a día entre su personal especializado de Seguridad Informática. La definición de las políticas de seguridad de los equipos de cómputo y los dispositivos portátiles es un proceso eficiente que se integra con el Directorio Activo de la compañía tales como Microsoft Active Directory y Novell eDirectory.

Secured eDevice es una aplicación fácil de utilizar, desarrollada con tecnología de vanguardia, que permite la definición de políticas de seguridad a lo largo y ancho de la Organización, soportando múltiples Consolas de Administración para configurar y administrar las políticas de seguridad relacionadas con los equipos de cómputo de la red, los dispositivos portátiles, y los tipos y tamaños de información que son permitidos para ser transferidos.

BENEFICIOS

- Totalmente Escalable – no hay límite del número de PC's de la Red de Cómputo
- Capacidad de visualización remota del contenido de los dispositivos
- Política restrictiva de copia para hacer cumplir la encriptación en los dispositivos de almacenaje removibles
- Detección de dispositivos no autorizados ó del uso de puertos o periféricos no autorizados
- Capacidad de bloqueo de contenido a través del Filtro de Expresiones Regulares (DLP)
- Control de Redes Inalámbricas (WiFi) permitidas a través de la definición del MAC Address/SSID/Secure Network por equipo o red específica
- Monitoreo en tiempo real de los equipos de cómputo y su uso.
- Capacidad de alertas y registro de eventos incluyendo mensajes personalizables, SMTP traps y correo electrónico.
- Bloqueo y autenticación de grupos de usuarios, usuarios, computadores, y dispositivos a través de un identificador único
- Ofrece balanceo de carga (load balancing) asegurando la disponibilidad del servidor de seguridad cuando algún otro servidor esté ocupado o no disponible
- Soporta la aplicación de políticas de seguridad en Máquinas Virtuales VMware
- Trabaja como una medida adicional de protección contra software maligno, descarga de información confidencial en dispositivos portátiles, etc. (el medio electrónico o dispositivo no pueden aprovechar la vulnerabilidad del autorun)
- El Agente de Seguridad incluye un mecanismo avanzado anti-tampering que previene que sea detenido ó desinstalado, protegiendo y haciendo cumplir las políticas de seguridad

- Mantiene y aplica las políticas de seguridad y el registro de eventos en los equipos aún cuando el computador no está conectado a la red ó los servidores no están disponibles (online o offline)
- Protección basada en políticas de varias capas que incluye políticas negativas y positivas de seguridad (Lista Blanca – Permitido/Lista Negra – No Permitido).
- Aplicación de Políticas de Seguridad en Conexión en Caliente (hot-plugging) y dispositivos plug-and-play
- Cambio dinámico de políticas (automáticamente aplica políticas offline y online)
- Integración con los Directorios Activos tales como Microsoft Active Directory y Novell eDirectory
- Módulo completo de reports y búsquedas de eventos y actividades
- 100% Tiempo Real en registro de eventos, notificaciones, acciones y auditoría
- Permite brindar permisos temporales utilizando un sistema de código de desbloqueo para los usuarios de equipos portátiles y remotos

DISPOSITIVOS, PUERTOS E INTERFACES SOPORTADAS

Almacenaje Removible:

1. MP3 Players
2. MP4 Players
3. SD Cards
4. Flash Memory Cards
5. SDHC Cards
6. Micro SD Cards
7. Compact Flash
8. CF Cards
9. Memory Sticks
10. Mini SD Cards
11. Mini DV Tape
12. Iomega Zip Disk
13. Magneto Optical Disk
14. DLT Tape Cartridge
15. LTO Tape Cartridge

Modems:

1. Internal Modems
2. External Modems
3. Datacard Modems
4. ADSL Modems
5. UMTS Modems
6. GPRS Modems
7. Cable Modems

Medios de Almacenaje CD/DVD:

1. CD-R
2. CD-RW
3. DVD-R
4. DVD+R
5. DVD-RW/+RW
6. HD DVD
7. Mini DVD-R
8. Blu-ray Disk
9. Dual Layer DVD-R

Dispositivos con Encriptación:

1. U3
2. Secure USB Devices

Adaptadores Inalámbricos WIFI:

1. Internal Wireless
2. External Wireless

Dispositivos PDA:

1. PDAs con Sistema Operativos Windows CE
2. PDAs con Sistema Operativo Windows Mobile
3. PDAs con Sistema Operativo Palm

Teléfonos y Dispositivos RIM:

1. Blackberries
2. Smartphones
3. Dispositivos Wireless Handheld

Puertos:

1. USB
2. FireWire
3. Infrared
4. Serial
5. Parallel
6. RS-232 Port

Dispositivos Tape:

1. DV Tape
2. Iomega Zip Tape
3. Magneto Optical Tape
4. LTO Tape

Dispositivos de Imágenes:

1. Webcams
2. Camcorders
3. Scanners

Impresoras:

1. Impresoras Locales
2. Impresoras de Red
3. Impresoras Virtuales

Otros:

1. Floppies
2. Smart Card Readers
3. Keyloggers

RAZONES DE PESO PARA ELEGIR SECURED EDEVICE

- Si usted necesita asegurar sus accesos remotos a través de VPNs al aplicar una política diferente que cuando sus usuarios están conectados a la red (Online) o desconectados (Offline).
- Si usted quiere hacer cumplir la inspección del contenido de documentos digitales salientes que son copiados en los dispositivos de almacenamiento extraíbles.
- Si usted quiere controlar que tipo de archivos y que tamaño de archivos están autorizados sus usuarios a copiar fuera de su red de cómputo.
- Si usted quiere evitar la impresión de pantallas (print screen) dentro de su red de cómputo para algunos usuarios.
- Si usted necesita administrar el uso de los dispositivos no únicamente en usuarios del Directorio Activo (LDAP - Active Directory) sino también en usuarios administradores locales.
- Si administrar en el esquema de Active Directory es inaceptable y quiere gestionar todo dentro de una consola centralizada.
- Si usted quiere instalar las nuevas versiones del producto sin tener que desinstalar primero todos los agentes, reiniciar todas las máquinas, y luego reinstalar los nuevos agentes.
- Si usted quiere auditar eventos en tiempo-real sin depender de las limitaciones de GPO (Group Policy Objects).
- Si usted quiere reducir las tareas de soporte y mesas de ayuda al personalizar Mensajes Emergentes a sus usuarios.
- Si usted quiere tener la capacidad de hacer un 'Clic-Derecho' y instalar o desinstalar el agente.
- Si usted quiere Notificaciones en Tiempo-Real al definir eventos críticos y enviar alertas a los administradores a través de email o mensajes emergentes.

- Si usted quiere tener la capacidad de suspender cualquier política en situaciones críticas con solo realizar un 'Clic-Derecho'.
- Si usted tiene un centro de soporte y usted desea brindarles a ellos una interface tipo Web para administrar sus políticas de puntos finales sobre la marcha.
- Si usted necesita auditar las acciones de sus usuarios en archivos sensitivos utilizados en los dispositivos removibles de almacenaje.
- Si usted requiere tener una visualización clara de todos los computadores de su red con el estatus de su política.
- Si usted quiere bloquear el uso de los dispositivos de almacenaje extraíbles dentro de sus equipos de cómputo VMware.
- Si la política de lista blanca no es suficiente y usted quiere usar ambas, las políticas de lista blanca y lista negra.
- Si usted quiere prevenir la impresión no únicamente en impresoras locales sino también en impresoras compartidas e impresoras de red.
- Si en algunos casos usted quiere tomar acción contra usuarios no autorizados al reinicializar sus equipos o correr un script cuando una violación a la política de seguridad haya ocurrido.
- Si usted necesita una copia forense de todos los archivos que han sido copiados a los dispositivos removibles de almacenaje, en violación de las políticas de seguridad.
- Si desea mostrar una rápida navegación del contenido de un equipo remoto y tomar control completo sobre el contenido de su punto final.
- Entre muchas otras ….

REQUERIMIENTOS TÉCNICOS DE SOFTWARE Y HARDWARE

Server Hardware and Software Requirements

- CPU: Intel Pentium 4-class or higher, 450 MHz minimum 2.8 GHz
- Disk space: 2GB free
- RAM: 1 GB RAM minimum, 2 BB recommended
- Server: Microsoft IIS with ASP.NET 2.0
- OS: MS Windows® Server 2003 Std. or Ent. SP 0-2 and R2, MS Windows Server 2008
- Browser: Microsoft Internet Explorer® 5.5 or greater
- Database Applications: MSDE 2000 (included default), Microsoft Express® 2005, Microsoft SQL® 2000 SP 3 and above, or Microsoft SQL® 2005

SECURED EDEVICE Agent - desktop/laptop clients

- CPU: Pentium III 1 GHz or greater
- Network Connection: TCP/IP for remote access
- RAM: 512 MB
- Disk Space: 200 MB minimum
- OS: MS Windows 2000 Pro. SP 4, 2000 Server SP 4, 2000 Advanced Server SP 4, MS Windows 2003 Std. or Ent. SP 0-2 and R2, XP Professional SP 0-3, XP Tablet PC Edition SP 0-3, Vista® Ent.\Ultimate\Business SP 0-1, Windows 7, MSI Ver. 2 or higher

Para mayor información o realizar un demo de nuestra solución, por favor contáctenos:

Fertech Corporation • info@fertechcorp.com • www.fertechcorp.com