

*Data leak prevention, anytime, anywhere...*



# Secured eDevice

.....

Secured eDevice es nuestra solución calificada para empresas que ofrece el control de dispositivos que proactivamente protege la información más confidencial de su empresa. Controla, supervisa y registra de qué manera su data es descargada y cargada a usuarios finales y permite a los usuarios crear políticas reforzadas de seguridad, observa resultados y actividad en tiempo real, además de supervisar de manera central cualquier tipo de medios extraíbles, dispositivos de almacenamiento portátil y una interfaz de comunicación.

Las políticas basadas en control de acceso de usuarios finales del Secured eDevice para dispositivos de almacenamiento portables y medios extraíbles previene efectivamente el uso no autorizado de data empresarial y refuerza las políticas de seguridad de los usuarios finales, que cumplen con las normas de seguridad requeridos tales como: Sarbanes-Oxley, California SB1386 o el Health Insurance Portability And Accountability Act (HIPAA).

Secured eDevice es implementado y supervisado de manera central permitiendo que los administradores de seguridad definan políticas que son automáticamente distribuidos a los usuarios finales utilizando los llamados Agentes de Usuario Final. Estas políticas son rígidamente cumplidas y todo evento relevante es comunicado al Administrador del Servidor. La perfecta integración con los directores de la empresa y el sistema de administración permite una fácil implementación y un extensa supervisión y reporte.

## Características Principales

---

### Agente de Seguridad Avanzado

El agente de usuario final es protegido de ataque por procesos, servicios, código malicioso en su puerto. No puede ser violado ni siquiera por usuarios que tienen privilegios administrativos en sus puertos.

### Administración de Cualquier Dispositivo o Interfaz

Secure eGuard puede trabajar con módems internos o externos, PDSs, iPods, impresores en red y locales, MP3s, dispositivos cassette, dispositivos biotech, CD/DVDs, quemadores, USBs, adaptadores LAN, camcorders, cámaras digitales, scanners, dispositivos ópticos, smartphones, floppy disks, almacenamiento masivo, SD Cards y zip/jazz drives. Interfaz de Comunicación, tales como; USB, WiFi, Bluetooth, PCI ISA, haces ópticos, digital protegido, PCMCIA, COMs serial, LPTs paralelo, IrDA y FireWire.

### Mecanismo de Actualización Real

La función de actualización real controla la versión de aplicación de los agentes de usuario final. Automáticamente implementa actualizaciones cuando es necesario, minimizando los gastos generales de administración.

### Integración del Directorio

El administrador de acceso a usuario final está bien integrado con el directorio de la infraestructura de la empresa como Microsoft Active Directory y Novell eDirectory.

### Integración del Sistema de Administración de la Empresa

La administración del acceso a usuario final está bien integrado con sistemas de administración empresarial como : CA Unicenter, CA eTrust y HP OpenView.

### Reportes Integrales

La administración del acceso a usuario final registra todo evento de usuario final in una base de datos SQL.

Los reportes flexibles e intuitivos permiten a los supervisores personalizar búsquedas y generar informes integrales de los usuarios finales y sus actividades.

### Políticas Inteligentes y Detalladas

Permite la autorización de dispositivos USB individuales, media e interfaz para pc específicas y usuarios que utilizan los servicios del directorio empresarial.

La información que las políticas de seguridad comunican a los usuarios finales en tiempo real e inmediatamente son reforzadas por los agentes del usuario final. Los administradores pueden autorizar permisos temporales para usuarios de celular o que están en línea.

### Soporte a Usuarios de Celular

Este tipo de usuario es supervisado y protegido. El Agente de usuario final continúa reforzando la política de seguridad aún cuando el usuario no esté conectado a la red.

### Notificaciones en Tiempo Real y Auditoría

Toda actividad de los usuarios finales son notificadas en tiempo real al servidor de administración y registrados en una base de datos.

Los eventos son desplegados en la administración. La comunicación y la consola para la administración de seguridad en una variedad de formatos como mensajes popup, y correos electrónicos. Los eventos están también disponibles para el sistema de administración empresarial en SNMP traps.

### Hot-Plug Support

Los agentes monitorean los drivers de los dispositivos plug-and-play que son instalados en las terminales. Basándose en la política del terminal, el agente reportará al servidor de administración los nuevos dispositivos instalados y aplicará los permisos de acceso apropiados.

### White and Black List Support of Device

El administrador de acceso del Endpoint permite la creación de las políticas para aprobar los dispositivos específicos - la lista blanca y el control de funcionalidad de un dispositivo, como la aprobación de una marca específica de USB flash, que tenga la disponibilidad de leer/escribir y denegar - o una lista negra teniendo control de funcionalidad del dispositivo.