



Circuitos Cerrados de información:
360° de protección de la información
para la empresa

Esta página se dejó en blanco intencionalmente.

Resumen ejecutivo

La combinación poderosa de legislación, comunicados de prensa negativos y responsabilidad legal ha garantizado que la protección de información sea, quizás, el reto tecnológico e informático más importante que enfrentan las organizaciones en la actualidad. El panorama de soluciones se desborda con opciones que prometen abordar un solo aspecto de la protección de información; pero para el Director General de una típica empresa, amplia y con poco presupuesto, la implantación de múltiples soluciones simplemente no es una opción práctica.

Secuware *Security Framework* (SSF) está diseñado para resolver dichos problemas y ofrecer un sistema operativo de seguridad global que cubra y se integre con Windows para proteger la información de la organización, sin importar dónde esté almacenada. SSF proporciona "Circuitos Cerrados de Información", y así asegura que sólo los individuos autorizados que usan aplicaciones autorizadas en dispositivos autorizados puedan acceder a la información autorizada. Permite la aplicación de políticas con alta seguridad para almacenar y acceder a información en dispositivos fijos o extraíbles, así como en carpetas de red, de modo que la información esté disponible para las personas autorizadas, pero para nadie más. Estas protecciones y controles se implantan en un diseño central de información, que minimiza el trabajo administrativo y se integra firmemente con el Directorio Activo y otros servicios de directorio basados en LDAP (protocolo de acceso a directorios).

Antes de revisar y analizar con detenimiento Secuware *Security Framework* y la forma cómo éste se puede implantar para resolver los problemas más críticos sobre protección de información que hoy día enfrentan las organizaciones, en este documento se analizan los problemas de protección de información y el historial de Secuware en el mercado de seguridad de la información.

Tabla de Contenido

Circuitos Cerrados de información:	1
360° de protección de la información para la empresa	1
Resumen ejecutivo	3
El problema de la protección de información	5
El alto costo de la información insegura	5
¿Cuál es problema de la protección de información y cómo se puede resolver?	5
Secuware Security Framework	6
Visión general y beneficios	6
Cientes Clave de SSF	8
Secuware Security Framework más a fondo	9
Arquitectura del producto	9
Despliegue y administración simple y escalable	10
Distribución del cliente	13
Creación y revisión de las políticas de seguridad del usuario	13
Creación y revisión de las políticas de la computadora	13
Creación y revisión de las políticas para encriptación del disco duro local	14
Creación y revisión de las políticas para el almacenamiento externo	14
Creación y administración de controles de acceso a la información para dispositivos específicos	15
Controles de acceso a aplicaciones	15
Protección transparente de información para sistemas de usuario final	15
Inicio del sistema operativo (<i>booting-up</i>)	15
Uso normal del sistema	17
Tecnologías clave	18
Tipos de encriptación	18
Autenticación previa al inicio del sistema operativo (<i>pre-booting</i>)	19
Control de aplicaciones	20
Comparación con las alternativas disponibles en el mercado	21
En conjunto	21
Problemas relacionados con Infraestructura de Clave Pública	21
Microsoft Vista BitLocker	21
Especificaciones de producto	23
Cliente	23
Consola de gestión	23
Servidores soportados	23
Directorios soportados	23
Historia y antecedentes de la empresa	24

El objetivo de este reporte sólo es informativo. Secuware no otorga ninguna garantía, expresa o implícita, en este documento.

El cumplimiento de todas las leyes de derechos de autor es responsabilidad del usuario. Sin limitarse a los derechos de autor, no está autorizada la reproducción, el registro o la introducción en un sistema de recuperación de información (electrónico, mecánico, fotoquímico, por fotocopia, o cualquier otro), o la transmisión de este documento, en parte o su totalidad, sin el permiso escrito de Secuware Inc.

© 2007 Secuware Inc. Todos los derechos reservados. Secuware y el logotipo de Secuware son marcas registradas de Secuware, Inc. Secuware Security Framework y Crypt2000 son marcas registradas de Secuware, Inc. Las demás marcas son propiedad de sus respectivos dueños.

El problema de la protección de información

El alto costo de la información insegura

En la última *Encuesta sobre Crimen y Seguridad Informática* de 2006 realizada por CSI/FBI¹, la “protección de la información” ocupó el primer lugar en la lista de los problemas más críticos de los siguientes dos años”. En contraste a la preocupante ilustración de la importancia del problema de la protección de información, el *spam* resultó ser un problema crítico para sólo el 15% de los encuestados.

Esta respuesta difícilmente es sorprendente respecto al ambiente legal y regulatorio que hoy día enfrentan los Directores Generales de las empresas. En sectores de negocios tan diversos como los servicios financieros, de manufactura, comercio por Internet, así como en el Gobierno, una infracción o pérdida de información debe reportarse, incluso si sólo es una sospecha. Para 2006, las leyes de notificación de incumplimiento en la seguridad habían sido introducidas en mínimo 35 estados², y las multas por incumplimiento pueden ser hasta de millones de dólares. Todos estamos conscientes de las numerosas historias publicadas sobre la pérdida o el robo de computadoras portátiles y CD's con información confidencial de cientos de miles, incluso millones de personas.

Las consecuencias no financieras de la pérdida de información o el incumplimiento de privacidad incluyen la vergüenza pública, la pérdida de buena fe y el daño a la reputación. Las consecuencias no financieras son tales que incluso algunas organizaciones nunca se recuperan, entre éstas se encuentran los gastos legales, de investigación y administración, así como las reacciones adversas de los accionistas y clientes, la pérdida de oportunidades y el manejo de la crisis; después está el costo de retener clientes a través de la provisión de líneas de información y suscripciones de monitoreo de crédito complementarias³. Un estudio concluyó que 20% de los clientes afectados por el incumplimiento de la protección de información terminó su relación con la empresa, y 5% contrataría a un abogado⁴. Tal vez, en la actualidad, la peor pesadilla de un Director General sea la posibilidad de ver el nombre de su empresa en un periódico de *Wall Street* en un artículo sobre pérdida de información.

¿Cuál es problema de la protección de información y cómo se puede resolver?

La protección de información abarca la privacidad de la información y el control del acceso a ésta, lo que claramente es un amplio problema de varias facetas con muchos inconvenientes y dificultades para la empresa:

- Computadoras portátiles pérdidas o robadas fuera de la oficina con información confidencial⁵.
- Empleados que copian información sin autorización a dispositivos extraíbles, como unidades flash.
- “Trabajos internos” realizados por empleados que hacen mal uso de la información confidencial para ganancia personal, o ciber-criminales que se infiltran en el negocio⁶.
- Empleados que bajan aplicaciones para uso personal, las cuales contienen virus o Troyanos diseñados para robar información corporativa.
- Recursos limitados para el refuerzo de la seguridad.

“Sólo pocos de los casos de infracción a la protección de información reportados al Comité (Reforma Gubernamental) fueron causados por hackers infiltrados al sistema informático en línea. La gran mayoría de los casos de pérdida de información surgieron del robo físico de computadoras portátiles, unidades y discos, o por el uso de la información por empleados no autorizados.” – Comité de Reforma Gubernamental, Reporte de personal, Octubre 13, 2006

En la actualidad, el reto clave que enfrentan los departamentos de tecnología de la información (TI) y la administración de la información es la identificación y el despliegue de una solución que proteja la privacidad de la información y controle el acceso a ésta a pesar de su ubicación, y que sea efectiva en la operación. Una solución compleja y excesiva no ofrecerá una seguridad efectiva, ya que nunca será mantenida o soportada de manera adecuada en una era de reducción de presupuestos. Los usuarios finales simplemente se negarán a trabajar con productos de seguridad que generen muchos obstáculos entre ellos y su productividad, a pesar de los beneficios prometidos.

En el desarrollo y la implantación de una solución de completa privacidad de la información y control de acceso, el director general y su personal se enfrentan con un desconcertante número de opciones; la mayoría son sólo soluciones parciales. Es casi seguro que una combinación de diferentes productos vaya a sufrir de traslapes y espacios funcionales, múltiples consolas de gestión, y duplicación de tareas administrativas. El resultado inevitable es la confusión, los costos altos de mantenimiento y la vulnerabilidad de seguridad. La solución preferida es una que ofrezca resultados.

- Protección total de información y control de acceso en una sola solución flexible
- Bajo mantenimiento en general (Personal con habilidades y especialización)
- Transparencia con el usuario final
- Integración justa con la infraestructura existente de TI

Secuware Security Framework (SSF) es una solución empresarial diseñada desde los cimientos para proteger la información corporativa y el acceso de control a ésta a pesar de la ubicación o el medio de almacenamiento.

Secuware Security Framework

Visión general y beneficios

Secuware Security Framework (SSF) asegura que sólo los “individuos autorizados” con los “dispositivos autorizados” y las “aplicaciones autorizadas” podrán acceder a la “información autorizada”. Mientras que SSF se integra directamente con todos los servicios principales de directorio basados en LDAP, el Directorio Activo se usa como un ejemplo de implantación en este documento.

Un proceso de autenticación previo al inicio del sistema operativo (pre-boot), integrado firmemente con Windows y el Directorio Activo, asegura el requerimiento de una autenticación de usuario más fuerte para cualquier acceso a información o sistema. Este proceso refuerza la inversión en la infraestructura existente de seguridad y elimina la necesidad de un sistema separado de administración de identidad.

Un acercamiento centrado en información a la encriptación de medios y archivos refuerza la privacidad de la información y los controles de acceso. Los controles de acceso adicionales permiten al sistema la entrada sólo a dispositivos USB o FireWire autorizados. El control de aplicaciones limita el acceso del usuario a una lista predeterminada de programas aprobados. Como un beneficio complementario, el control de aplicaciones ofrece una capa suplementaria de defensa contra virus, Troyanos y otros malware (software perjudicial), al prevenir la activación accidental o deliberada de archivos ejecutables no aprobados. También contribuye en gran manera a la estabilidad del sistema, como siempre han sabido los usuarios, a las configuraciones de aplicación probadas.

Esta combinación de controles crea “Circuitos Cerrados de Información”, zonas de seguridad que protegen la información corporativa casi como un sistema de circuito cerrado de televisión desplegado.

imágenes sólo en un área restringida. La firme integración con Windows resulta en un “sistema operativo seguro” que protege la información de procesos de inicio adelantados.

La arquitectura de SSF es escalable y baja en costos, comprende un Cliente de Windows y una Consola de gestión. No requiere su propio servidor o una base de datos exclusiva o un servidor de base de datos. El cliente es desplegado con facilidad con herramientas estándares de administración de software.

La configuración y administración de seguridad (creación de políticas) se realiza a través de consolas de gestión de directorio. La administración del sistema (asignación de políticas a usuarios y sistemas) se maneja a través de consolas estándar de directorios.

Las políticas de seguridad, en forma de perfiles de usuario y computadora con claves de encriptación, se almacenan en el directorio como extensiones esquema. Por seguridad, las claves de encriptación no están disponibles directamente para los administradores de seguridad o sistema. Las políticas entran en efecto en el siguiente acceso al sistema (login) o activación de un Grupo de políticas.

Circuitos cerrados de información

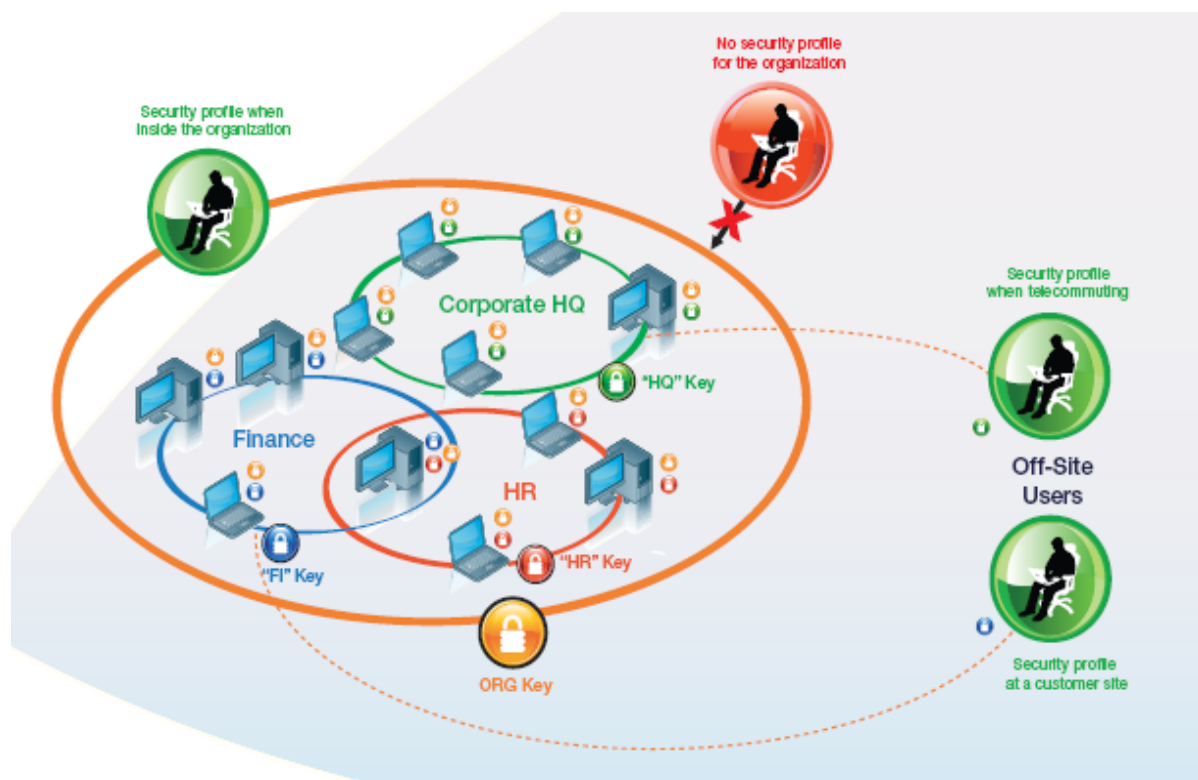


Figura 1: Secuware Security Framework crea Circuitos Cerrados de Información

SSF ofrece protección de información con claves de encriptación simétricas. Se usa una clave para la encriptación del disco duro local y se asignan claves de encriptación adicionales para el almacenamiento externo, incluyendo dispositivos extraíbles, dispositivos USB, FireWire y carpetas de red. Cada clave de encriptación está relacionada con un “dispositivo nombrado”; puede haber múltiples dispositivos nombrados para un tipo de dispositivo en específico, como CD/DVD. Se pueden asignar dispositivos nombrados a un número de distintos usuarios y perfiles de computadora, permitiendo la aplicación de políticas de alta granularidad y seguridad. Este acercamiento elegante y franco elimina la complejidad en

los problemas que se asocian con Infraestructura de Clave Pública, como se menciona en la sección de problemas relacionados con este tema.

SSF proporciona controles adicionales de acceso a la información a través de perfiles para dispositivos y aplicaciones autorizados. Si un perfil de dispositivo autorizado está efectivo, sólo los dispositivos con autorización previa se podrán comunicar con un sistema, esté o no esté encriptada la información en el dispositivo. Si un perfil de aplicaciones autorizadas está configurado, el usuario sólo podrá correr las aplicaciones con previa autorización del administrador de seguridad.

Clientes Clave de SSF

SSF es usado por más de 300 clientes Corporativos y Gubernamentales alrededor del mundo, dando protección a más de 500,000 sistemas en Windows.

La Agencia Estatal de Administración Tributaria (AEAT; la IRS española) ha implementado SSF en 35,000 sistemas para proteger la información confidencial de los contribuyentes. La AEAT ha implementado Circuitos Cerrados de Información para prevenir la fuga de información de discos duros locales, discos 3 1/2, CD/DVD's, dispositivos USB y carpetas de red.

Wal-Mart México usa SSF para la protección de información en bancos ubicados en sus tiendas mexicanas. Debido a que el Directorio Activo está ubicado en las oficinas corporativas en Estados Unidos, Wal-Mart México ha desplegado el ADAM (Modelo de Aplicación de Directorio Activo) para permitir a los administradores de seguridad y sistemas en México administrar los despliegues locales de SSF. (Consulte la sección sobre Despliegue y administración simple y escalable más adelante.)

Warner Brothers México usa SSF para proteger la propiedad intelectual de sus clientes y evitar la piratería con el refuerzo de los controles de acceso en las computadoras portátiles de sus empleados.

Telefónica Móvil (compañía en telefonía celular española) ha implementado SSF en 10,000 estaciones de trabajo para garantizar la confidencialidad de toda la información de sus clientes almacenada en sus sistemas, lo que evita la conexión de dispositivos no autorizados a los sistemas de Telefónica, así como la ejecución de aplicaciones no autorizadas.

Iberdrola, la compañía de servicio público más grande en España, cuenta con clientes en toda Europa del sudoeste y ha desplegado SSF en 12,000 sistemas para proteger la cadena de suministro de energía del ciber-terrorismo y otras amenazas electrónicas.

BBVA, uno de los bancos más grandes de España con sucursales en muchos países de Europa, América Latina y Estados Unidos, ha implantado SSF para proteger la información confidencial en las computadoras portátiles de sus ejecutivos de alto rango.

Secuware Security Framework más a fondo

Arquitectura del producto

SSF comprende un módulo de administración implantado como una consola de gestión de Directorio Activo MMC, y cuatro módulos separados de clientes, como se muestra en la Figura 2 a continuación. Tres de los módulos de clientes crean y refuerzan las políticas, y los cuatro registran todos los eventos de seguridad importantes para el análisis posterior para propósitos forenses y de seguridad.

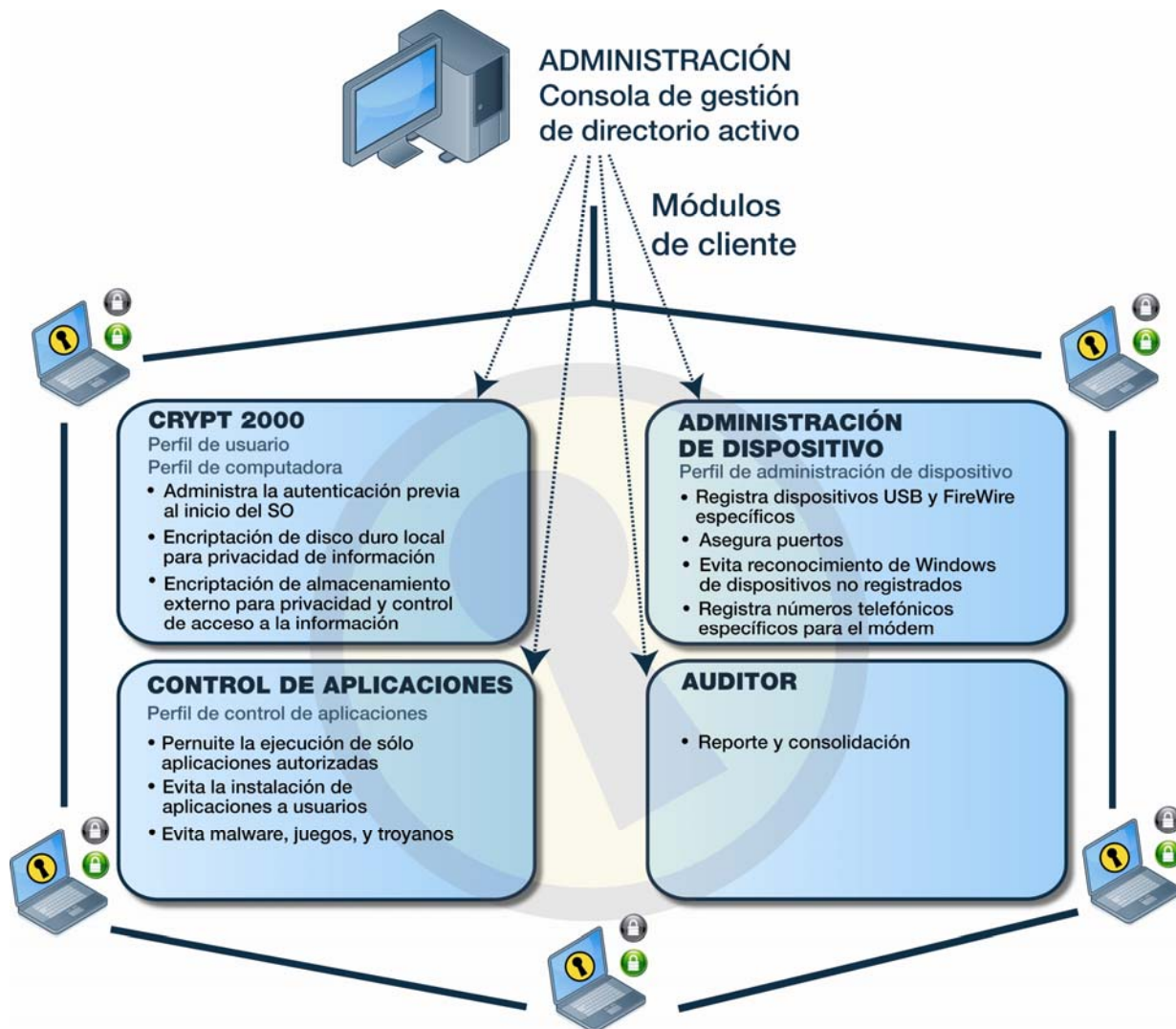


Figura 2: Módulos de clientes SSF; pueden instalarse en cualquier combinación y ejecutar políticas creadas por el módulo de administración.

El despliegue de SSF puede iniciar con cualquiera de los tres módulos de políticas, aunque en la práctica la mayoría de las empresas empiezan con Crypt2000. El módulo de administración siempre es requerido, y es usado para crear y administrar políticas. La Figura 3 a continuación muestra cómo cada módulo protege el acceso a la información durante las distintas etapas de la operación del sistema, desde antes del inicio del sistema operativo hasta el apagado del sistema.

Como se mencionó con anterioridad, no se requiere un servidor de seguridad o una base de datos de políticas, lo que simplifica bastante el despliegue y reduce los costos de implantación.

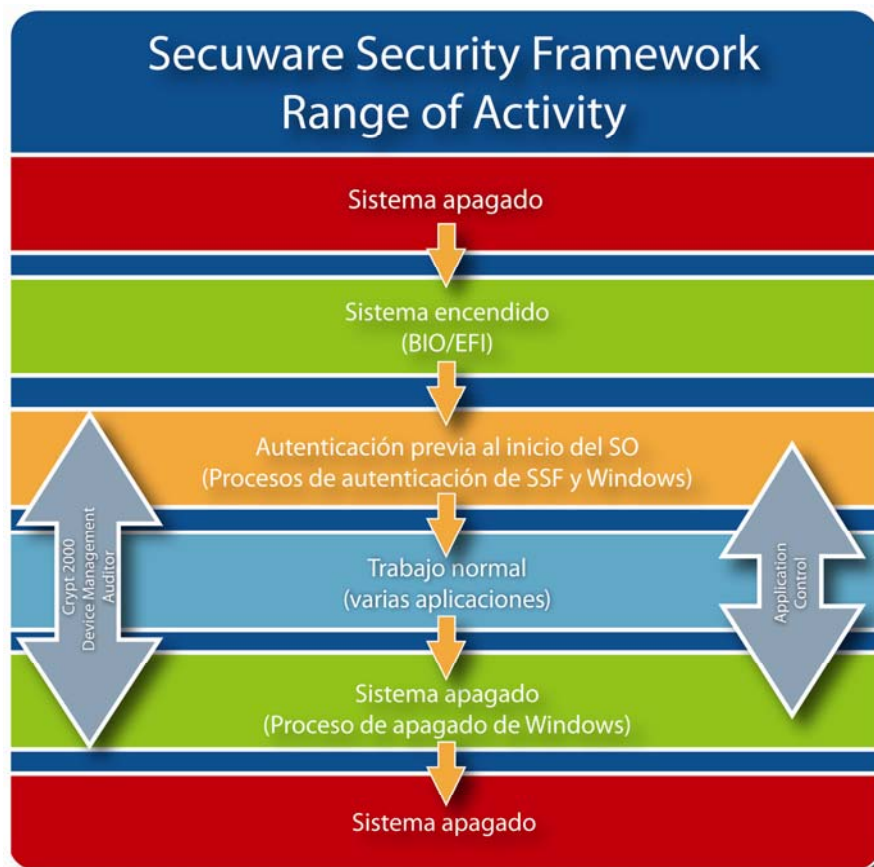


Figura 3: SSF ofrece una protección activa todo el tiempo que el sistema esté activo.

Despliegue y administración simple y escalable

Las políticas de datos administradas centralmente por sistemas finales son el corazón de SSF. Las políticas son creadas y almacenadas como extensiones al esquema de usuarios y computadoras del Directorio Activo. Una vez almacenadas en el directorio activo, las políticas son eliminadas para los usuarios en el próximo acceso al sistema o actualización de Política de grupo.

Toda la configuración del directorio activo, en términos de árboles, dominios, sitios, número de objetos, relaciones de confianza, población de sistemas, delegación de responsabilidades, etc., es completamente transparente para SSF.

Nota: Para los clientes que no quieren aplicaciones de terceros para extender el esquema del directorio activo, o que quieren implantar una delegación de responsabilidades descentralizada, SSF también soporta ADAM⁷.

El Modelo de Aplicación de Directorio Activo (ADAM por sus siglas en inglés) fue diseñado por Microsoft para abordar los escenarios de despliegue relacionados con las aplicaciones de directorios habilitados. Es una versión del Directorio Activo que puede correr como un servicio simple de usuario en Servidores Windows 2003 o incluso en Windows XP con SP1. Para simplificar el uso, ADAM usa muchas de las mismas herramientas administrativas que un Directorio Activo. ADAM usa los mismos APIs que un Directorio Activo para la fácil integración de la aplicación.

La Tabla 1 a continuación resume cómo los diferentes aspectos de la protección de la privacidad de la información y los accesos a ésta se implantan dentro del Directorio Activo:

Área de política de seguridad	Perfil SSF (módulo)	Clase de objeto del Directorio de Aplicación
Autenticación previa al inicio del sistema operativo	Perfil de computadora (Crypt2000)	Sistemas
Opciones de autenticación y encriptación de disco local	Perfil de computadora (Crypt2000)	Sistemas
Protección de privacidad de la información para el disco duro	Clave para encriptación de dispositivos (Crypt2000)	Sistemas (vía perfil de computadora)
Protección de privacidad de información y control de acceso a la información para dispositivos extraíbles (CD/DVD, USB, FireWire, disco 3 ½)	Claves para encriptación de dispositivos, una por nombre de dispositivo. (Crypt2000) Asignada a uno o más perfiles de usuario.	Usuarios (vía perfil de usuario) Sistemas (vía perfil de computadora)
Acceso a la información para dispositivos específicos USB/FireWire	Perfil de administración de dispositivos	Usuarios Sistemas
Control de aplicaciones	Perfil de control de aplicaciones	Usuarios Sistemas

Tabla 1: Implantación de políticas de seguridad con SSF

SSF hace cumplir una división de responsabilidades entre el administrador de seguridad y el administrador de sistema. Sólo el administrador de seguridad puede crear y modificar las políticas, crear claves de encriptación y asignar claves de encriptación al usuario y los perfiles de sistema. Sólo el administrador de sistema puede implantar las políticas de seguridad SSF con usuarios y computadoras. Esta división de responsabilidades garantiza la realización de tareas por parte de los administradores dentro de sus respectivas áreas de experiencia; de este modo se refuerza toda la seguridad corporativa a través de la eliminación de un solo punto de falla (humano).

Esta división de responsabilidades se resume en la Tabla 2 a continuación.

Administrador de seguridad	Administrador de sistema
Implantación de políticas de seguridad corporativa para mayor autenticación	Creación de usuarios Creación de sistemas
Implantación de políticas de seguridad corporativa para privacidad y acceso a información	Aplicación de políticas a usuarios y sistemas
Creación de listas (perfil de administración de dispositivos) de dispositivos USB y FireWire registrados y aprobados	Aplicación del perfil de administración de dispositivos a usuarios
Creación de listas (perfil de control de aplicaciones) de aplicaciones aprobadas	Aplicación de perfil de aplicación a usuarios
Creación de perfil de auditoría para archivos y carpetas Revisión de reportes de auditoría para incidentes de seguridad	Aplicación de perfil de auditoría a usuarios

Tabla 2: SSF hace cumplir una división estricta de responsabilidades entre los administradores de seguridad y sistemas.

El administrador de seguridad usa la consola de gestión del Directorio Activo MMC de Secuware mostrado en la Figura 4. Todas las políticas son creadas y administradas por el administrador de seguridad a través de esta consola. Sólo los administradores de seguridad del sistema deben instalar la consola de gestión de SSF.



Figura 4: El administrador de seguridad crea y administra las políticas de seguridad a través de una consola de gestión de Directorio Activo

El administrador del sistema implanta las políticas de seguridad con las extensiones esquema de los cuatro esquemas de usuarios y computadoras en el Directorio Activo, como se muestra en la Figura 5. Para cumplir con la división de responsabilidades, esta consola de sistema de directorio activo no debe ser accesible para los administradores de seguridad.

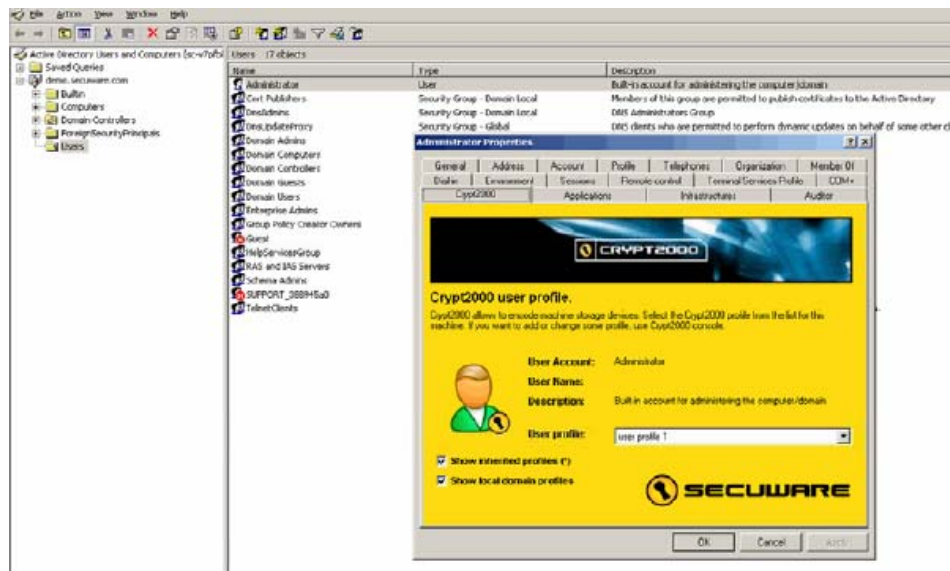


Figura 5: El administrador del sistema usa las cuatro pestañas de extensión creadas por SSF en el esquema de usuarios y computadoras para aplicar las políticas a los usuarios y sistemas.

Distribución del cliente

El cliente SSF es un módulo instalador de Microsoft que puede desplegarse e instalarse automáticamente con cualquiera de las principales herramientas de distribución de software basadas en red, como Microsoft SMS o equivalentes de Tivoli, Computer Associates, etc. De forma alternativa, el cliente SSF puede instalarse con un acceso al sistema.

Creación y revisión de las políticas de seguridad del usuario

El administrador de Seguridad crea los perfiles de políticas y las claves de encriptación de dispositivos con el elemento Crypt2000 de la consola de gestión de SSF. Una vez creadas, el administrador del sistema puede asignar estas políticas al usuario o grupos de usuarios con la ventana de propiedades administrativas para usuarios y computadoras, como se muestra en la Figura 5 anterior.

A los usuarios se les asigna un sólo perfil de usuario Crypt2000, eliminando la confusión acerca de cuáles políticas aplican a qué usuarios, lo cual simplifica la creación, el cumplimiento y la administración de políticas. Un perfil de usuario Crypt2000 es obligatorio; de forma opcional se puede asignar a los usuarios como un perfil de Administración de dispositivos y/o de aplicaciones.

El administrador de sistema puede asignar un perfil de usuario a:

- Todo el dominio
- Múltiples dominios dentro de un directorio activo
- Una unidad organizacional dentro de un dominio; por ejemplo, un departamento o ubicación
- Un usuario individual
- Cualquier combinación de las opciones antes mencionadas

No existe un límite superior práctico al número de diferentes perfiles de usuario que pueden crearse para un Directorio Activo. Sin embargo, en la práctica, un cliente grande de Secuware (más de 10,000 usuarios) ha creado sólo tres políticas de usuarios, una para la administración directiva, otra para la administración gerencial y una para los demás empleados. Otras organizaciones han creado varios perfiles, con perfiles separados para empleados en distintas organizaciones funcionales.

Creación y revisión de las políticas de la computadora

Cada sistema tiene un perfil de computadora relacionado que aplica a todos los usuarios del sistema. Este perfil se usa para el cumplimiento de la fuerte autenticación a través de la autenticación previa al inicio del sistema operativo, para establecer opciones para los permisos de autenticación permitidos, para habilitar / deshabilitar opciones de autenticación avanzadas de Windows, y para forzar / no forzar a los usuarios a introducir un nombre en cada acceso al sistema. Este perfil también tiene la clave para la encriptación del disco duro local y la selección de perfiles del usuario para cuando el usuario esté o no esté conectado al dominio.

Una vez que se ha completado el proceso de autenticación previa al inicio del sistema operativo, la clave de encriptación del disco duro local, contenida en el perfil de computadora, se usa para descryptar los archivos requeridos. (Observe que el disco en sí siempre permanece encriptado, protegiendo todos los archivos, incluso si el sistema se apaga abruptamente durante el funcionamiento normal.)

Creación y revisión de las políticas para encriptación del disco duro local

El administrador de seguridad puede especificar si el disco duro se encripta o no; primero debe crear un “dispositivo nombrado”, como se muestra en la Figura 6. Entonces este “dispositivo nombrado” se asigna a uno o más perfiles de computadora. El administrador del sistema asigna los perfiles de computadora a los sistemas, como se mencionó con anterioridad.



Figura 6: SSF puede crear un nuevo “dispositivo nombrado” para su uso con uno o más perfiles de usuario y computadora.

Creación y revisión de las políticas para el almacenamiento externo

El administrador de seguridad puede especificar qué tipos de dispositivos de almacenamiento externo pueden utilizarse para acceder a la información protegida. El almacenamiento externo incluye CD/DVD’s, dispositivos USB y FireWire, discos 3 1/2 y carpetas de red.

Para permitir políticas granulares de alta seguridad, se “ nombra ” a cada control de acceso para dispositivos de almacenamiento externo. Puede haber múltiples “ nombres ” para cierto tipo de dispositivo de almacenamiento, y se crea una clave de encriptación simétrica y única para cada control de dispositivos.

Una vez que se han creado los controles de dispositivos nombrados, estos son asignados por el administrador de seguridad a uno o más perfiles de usuario y computadora. Todos los usuarios o todas las computadoras con un perfil específico comparten una clave de encriptación para dispositivos, y por ende tienen acceso a los archivos y dispositivos protegidos con esa clave de encriptación para dispositivos nombrados. Debido a que un dispositivo nombrado puede incluirse en múltiples perfiles de usuario y computadora, los usuarios o las computadoras con distintos perfiles pueden acceder a los mismos archivos o dispositivos. A los demás usuarios y computadoras, con diferentes perfiles que no contengan la clave de encriptación de un dispositivo nombrado, se les niega el acceso a estos archivos y dispositivos.

Para dispositivos extraíbles, discos 3 1/2, CD/DVD, y unidades USB y FireWire, cada dispositivo usado en una de estas unidades está encriptado con una encriptación física para máxima seguridad. (Consulte la sección de Encriptación física y dispositivos extraíbles más adelante.)

Creación y administración de controles de acceso a la información para dispositivos específicos

El módulo de Administración de dispositivos se utiliza para crear listas de perfiles para administración de dispositivos específicos al filtrar puertos USB, FireWire y de módem. Sólo se puede tener acceso a los dispositivos incluidos en la lista, estén o no estén encriptados los archivos de información en estos dispositivos.

El perfil de administración de dispositivos también puede filtrar la marcación de números para módems, permitiendo al administrador de seguridad limitar un usuario de módem a sólo destinos de marcación aprobados con anterioridad.

El administrador de seguridad registra un dispositivo específico y el número de serie registrado. Una vez que el dispositivo está incluido, el administrador del sistema asigna los dispositivos autorizados a los usuarios al relacionar ese perfil de administración de dispositivos con un usuario.

Controles de acceso a aplicaciones

El control de aplicaciones asegura que los usuarios sólo puedan correr las aplicaciones y *plug-ins* del navegador aprobados por el administrador de seguridad. No se pueden ejecutar o instalar otras aplicaciones o *plug-ins*, incluso cualquiera descargado por el usuario.

El módulo de control de aplicaciones puede implantarse en una variedad de formas, desde mínimo o sin efecto hasta despliegues selectivos a un despliegue total. Debido a que el control de aplicaciones controla firmemente el uso

del sistema, puede ser de gran utilidad restringir grupos de empleados específicos, como contratistas, para correr ciertas aplicaciones, especialmente en empresas donde sólo se despliegan unas cuantas configuraciones de sistema estandarizadas a muchos grupos diferentes de empleados.

Cada política de aplicaciones diferentes está contenida en un perfil de aplicación creado por el administrador de seguridad; dicha política es aplicada a los usuarios por el administrador del sistema.

Potencial para granularidad en las políticas de seguridad de SSF

Los perfiles de usuario, computadora, administración de dispositivos y administración de aplicaciones no dependen uno del otro. Distintos perfiles de usuario y computadora pueden tener algunas claves de encriptación en común, pero otras que son únicas o diferentes.

Protección transparente de información para sistemas de usuario final

Inicio del sistema operativo (*booting-up*)

SSF controla la PC desde el momento que se enciende. La autenticación previa al inicio del sistema operativo asegura que sólo el usuario autorizado pueda iniciar el sistema o acceder a los contenidos del disco duro local.

El proceso de autenticación previa al inicio del sistema operativo previene que un intruso traspase el disco duro interno e inicie el sistema con técnicas como:

- Disco de Rescate creado por Windows⁸ o por utilidades anti-virus o de partición de disco
- Instalación de dispositivos de Windows
- Unidad *flash* USB de inicio, cargado con Windows⁹
- CD con un “Sistema Operativo” auto-contenido, como Knoppix¹⁰

Este acercamiento también evita que un individuo quite el disco duro SSF-encryptado y lo coloque en otro sistema como un disco duro secundario, debido a que no podrá completar con éxito el procedimiento de autenticación previa al inicio del sistema operativo que permite la descriptación de archivos en el disco duro.

Una vez que el sistema completa el inicio de BIOS (o EFI), SSF despliega una pantalla de acceso al sistema personalizada similar a la mostrada en la Figura 7 a continuación.



Figura 7: El proceso de autenticación previo al inicio del sistema operativo abre el sistema e inicia Windows en un solo paso.

La ventana de autenticación previa al inicio del sistema operativo puede personalizarse para:

- Publicar mensajes corporativos y otro material motivacional,
- Recordar a los empleados las políticas claves de seguridad o corporativas,
- Ofrecer la información del contacto de ayuda.

El proceso de autenticación previa al inicio del sistema está totalmente integrado con el proceso normal de acceso de Windows. Los usuarios proporcionan su identificación y contraseña de Windows, tarjeta inteligente, o *token* USB, para autenticarse.

Acceso si el sistema está conectado a un dominio

- Un Directorio Activo valida los permisos del usuario.
- Windows se inicia normalmente.
- El perfil de usuario se carga desde el Directorio Activo.
- El perfil de computadora se carga desde el Directorio Activo.

Acceso si el sistema no está conectado a un dominio

El proceso es el mismo que cuando el sistema está conectado a un dominio, excepto porque:

- Los permisos del usuario son validados con una copia en caché de la información de permisos de Windows almacenada de forma encriptada en un disco duro.
- Se carga un perfil de usuario distinto, el cual por lo regular es más restringido que el cargado cuando el sistema está conectado a un dominio por el riesgo de que el usuario ya no trabaje con la empresa o de que haya reportado la pérdida del sistema, el cual se bloquearía con una autenticación en línea, pero no un acceso al sistema fuera de línea si el usuario fuera descuidado con sus permisos.

Uso normal del sistema

Una vez que ha entrado a Windows, el usuario puede realizar todas las funciones normales permitidas por las políticas establecidas para su trabajo.

La protección de información y el control de acceso a ésta son completamente transparentes para el usuario autorizado, quien tendrá acceso total a la información autorizada. No tendrá la necesidad de pulsar en iconos o seleccionar artículos en menús para encriptar o desencriptar un archivo. Toda la encriptación y desencriptación de archivos se hace automáticamente, en segundo plano. El usuario podrá utilizar todos los dispositivos autorizados para almacenar y recuperar información y podrá correr todas las aplicaciones autorizadas, lo que le permitirá:

- Crear archivos nuevos
- Acceder y modificar archivos existentes
- Borrar archivos
- Copiar / mover archivos a / desde cualquier parte del disco duro local
- Copiar / mover archivos a / desde un dispositivo de almacenamiento extraíble, como un CD-R o una memoria USB
- Copiar / mover archivos a / desde una carpeta de red.

Los empleados que usan su sistema para realizar funciones laborales, nunca enfrentarán ninguna restricción en las actividades de trabajo; SSF será 100% transparente para estos usuarios. El usuario encontrará límites en las acciones sólo si intenta acceder a información o usar dispositivos o correr una aplicación para los cuales no está autorizado.

Por ejemplo, como se muestra en la Figura 8:

- Un empleado del departamento de finanzas no tendrá acceso a ninguna de las carpetas de red de las oficinas centrales corporativas, pero tendrá acceso a carpetas de red seleccionadas de finanzas. Las carpetas de red de las oficinas centrales corporativas y la mayoría de las carpetas de red de recursos humanos y su contenido serán visibles en el Explorador de Windows para un empleado de finanzas, pero los archivos en sí no serán legibles.

Circuito Cerrado de Información

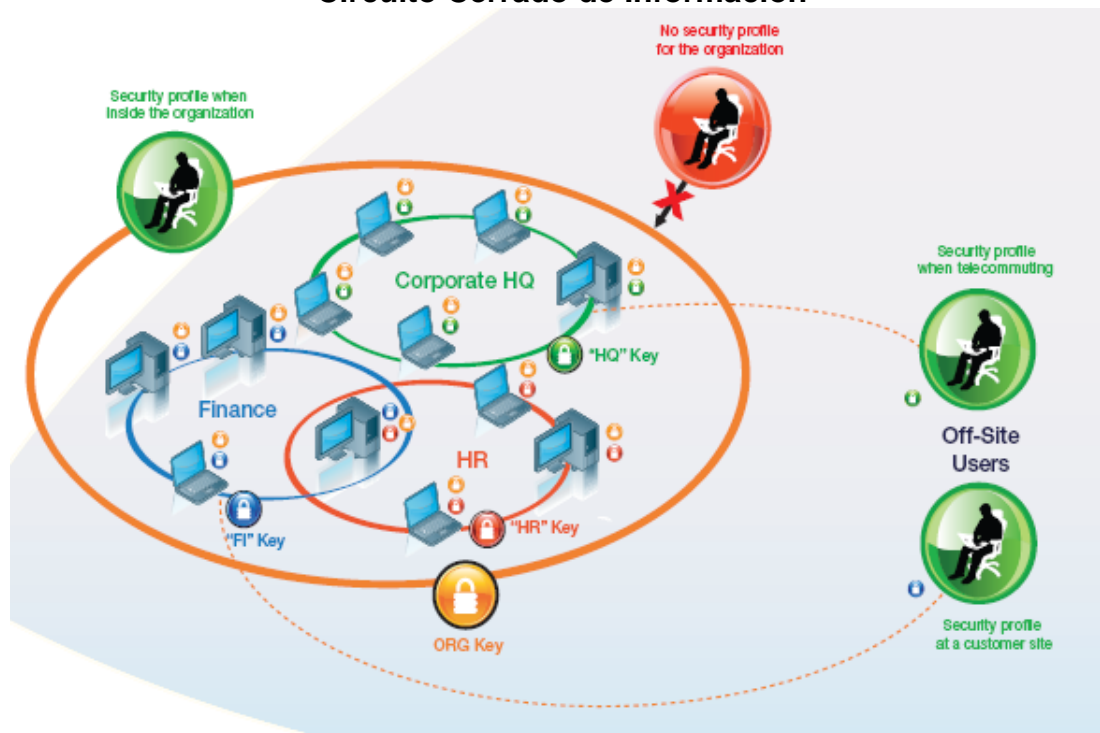


Figura 8: Los usuarios sólo pueden acceder a información y aplicaciones que estén dentro de su circuito cerrado de información autorizado.

- Si un empleado en las oficinas centrales utilizó una unidad *flash* o CD para transferir información a un empleado de finanzas, el receptor no podrá leer, modificar o imprimir ese archivo. Lo mismo sucedería si el mismo empleado utilizó la unidad *flash* o CD para transferir el archivo alguien fuera de la empresa.
- Si cualquier usuario descargó una aplicación de un sitio *web*, esa aplicación no podrá ejecutarse, incluso si el usuario pudo instalarla con éxito.

La política de autorización está totalmente fuera del control del usuario. El usuario no puede configurar el cliente SSF, y éste no crea ningún archivo de inicio o hace ninguna entrada de registro que un usuario técnico o un *malware* puedan modificar.

Gracias a que SSF es tan transparente, los usuarios finales por lo regular no requieren capacitación, ni antes ni después del despliegue, excepto, quizás, para reforzar las políticas de seguridad de la organización.

Tecnologías clave

Tipos de encriptación

SSF usa dos tipos de encriptación al crear Circuitos Cerrados de Información: encriptación física y encriptación local.

Encriptación física

Disco duro local

Los discos duros locales son encriptados a nivel sector para proporcionar un nivel mayor de protección y evitar el acceso a la información en el disco si el sistema es iniciado por diferentes dispositivos, como una unidad flash o CD.

Si toda la información en el disco duro está encriptada, todo lo almacenado en ese disco está protegido, incluso los archivos temporales y otra información de rastreo (archivos *swap*, etc.) que no estén protegidos por los procesos y programas tradicionales de protección de información. Esto evita la posibilidad de la explotación no autorizada y por lo tanto disminuye los riesgos.

La mayoría del *software* de encriptación usa Windows Crypto API o un kit de herramientas crypto, que consiste de DLLs (*Dynamic Link Libraries*). Estos DLLs se cargan después de haber iniciado Windows, y son vulnerables al ataque.

Una preocupación común sobre la encriptación total del disco duro local es el impacto en el desempeño del sistema. El SSF usa algoritmos de bloques de cifras simétricos (IDEA 128 bits o AES 265 bits), usados para el alto desempeño y el bajo uso de recursos, para evitar este problema. En la práctica, Secuware ha determinado que su implantación de encriptación simétrica impone sólo un 0.15% en general en archivos de lectura o escritura protegidos. El resultado neto es que la diferencia de desempeño entre un sistema con discos duros encriptados y uno sin ellos es mínima.

Dispositivos extraíbles

La encriptación total de dispositivos extraíbles a nivel sector proporciona el medio de lectura sólo en sistemas con SSF instalado y para usuarios con el perfil adecuado. Este diseño evita la fuga de información, accidental o deliberada, a cualquier entidad fuera de los canales autorizados de la organización. Este nivel de control es transparente para los usuarios durante el curso normal de operaciones, y la información siempre está protegida, a pesar de que esté ubicada dentro o fuera de la empresa.

Encriptación lógica (archivos y carpetas base red)

La encriptación lógica se usa para encriptar información a nivel archivo, de modo que la información encriptada puede almacenarse en cualquier dispositivo no formateado a nivel físico, sobre todo carpetas de red.

La encriptación lógica se selecciona a nivel carpeta, y todos los archivos almacenados en dicha carpeta están encriptados con la misma clave. Es posible proteger múltiples carpetas con la misma clave de encriptación, pero sólo se puede usar una clave de encriptación para una determinada carpeta.

Las copias de respaldo de archivos en carpetas de red protegidas permanecerán encriptadas, ya que fueron encriptadas al ser escritas originalmente en la red. Cualquier administrador puede crear respaldos, puesto que los usuarios no autorizados no podrán leer el contenido de las carpetas protegidas.

Autenticación previa al inicio del sistema operativo (*pre-booting*)

En la instalación, SSF modifica el MBR (*Master Boot Record*) para iniciar el sistema con un proceso de autenticación previa al inicio del sistema operativo en lugar del inicio del registro para la parte activa.

El proceso de autenticación previa al inicio del sistema operativo usa su propio protocolo de red TCP/IP para comunicarse con el Directorio Activo incluso después de la activación de Windows. Este acercamiento elimina los ataques de *hackers* con base en la modificación o el reemplazo de DLLs clave en la autenticación normal de usuario de Windows, y evita que los golpes de tecla de los usuarios en Windows capturen las identificaciones y contraseñas de los usuarios.

Si no hay una red disponible, o no se puede ubicar un nodo de Directorio Activo, se usa una copia en caché local de los permisos del usuario para la autenticación.

Control de aplicaciones

El módulo de control de aplicaciones usa las firmas de aplicación para verificar si ésta está autorizada, si no ha sido alterada, y si puede ejecutarse.

El administrador de seguridad utiliza el módulo de control de aplicaciones para seleccionar y pre-aprobar el SO de Windows y las carpetas de aplicación seleccionadas. De forma alternativa, al lidiar con unas cuantas imágenes de sistema estándar usadas en toda la organización, todos los archivos en el disco duro pueden seleccionarse.

Entonces, el módulo de control de aplicaciones calcula 5 fracciones de 128-bit MD para todos los archivos dentro de las carpetas seleccionadas, las cuales están agrupadas como un archivo de firma, archivo relacionado con un perfil de control de aplicaciones.

El administrador de sistema asigna el perfil de control de aplicaciones a los usuarios seleccionados. Cada vez que un usuario intenta iniciar una aplicación, o si una aplicación intenta cargar un DLL, se calcula la fracción MD5 de ese ejecutable y se compara contra las fracciones en el archivo de firma. Si no se encuentra una fracción igual se permite la ejecución; de lo contrario, el archivo no se podrá ejecutar.

Comparación con las alternativas disponibles en el mercado

En conjunto

SSF difiere de otras soluciones para protección de información en varias formas:

- Implanta protección de privacidad de información y controles de acceso a ésta, a pesar de la ubicación de la información.
- Ofrece controles de acceso a la información en los que Windows puede reconocer dispositivos USB y FireWire.
- Controla qué aplicaciones pueden ejecutarse en cualquier dispositivo específico.

La protección de SSF está activa aun cuando se apaga el sistema; los usuarios deben pasar por un proceso de autenticación previo al inicio del sistema operativo, integrado con Windows, para obtener acceso al sistema y sus archivos. De manera similar, la protección de SSF está activa incluso cuando el sistema o los dispositivos extraíbles están fuera de la red corporativa.

El acercamiento unificado y centrado en información de SSF implica que sólo son necesarios una consola de gestión y tres módulos de clientes para crear, establecer y cumplir las políticas para la protección de información y el acceso para todas las clases de usuarios y sistemas, dispositivos USB y Firewire, y aplicaciones. La consola de gestión se utiliza para aplicar estas políticas a cualquier usuario o sistema en la red corporativa. Otras soluciones requieren muchos módulos más para lograr lo mismo o menos.

SSF está integrado firmemente con Windows y los servicios LDAP, dando como resultado una arquitectura ligera y escalable que fortalezca, en vez de duplicar, las inversiones existentes de una organización en infraestructura de seguridad.

Problemas relacionados con Infraestructura de Clave Pública

En la Infraestructura de Clave Pública, la administración del ciclo de vida clave es crítica para la seguridad total de la aplicación. La Infraestructura de Clave Pública requiere atención a los siguientes problemas, ninguno de los cuales es una preocupación para el cliente SSF:

- Creación segura de un par clave
- Almacenamiento seguro del cliente (El registro de Windows no protege adecuadamente una clave privada.)
- Distribución de certificados X.509 con claves públicas
- Respaldo o custodia de claves de entrada (Las claves de entrada no necesitan una custodia)
- Renovación / reemplazo de claves privadas y certificados al caducar los certificados anteriores.

Microsoft Vista BitLocker

BitLocker es una función de seguridad introducida en Windows Vista que ofrece la total encriptación del disco para discos duros locales. Sin embargo, como el BitLocker no soporta la encriptación de carpetas de red, no soporta la encriptación lógica. El soporte de BitLocker sólo es proporcionado en Windows Vista Enterprise, no para Windows Vista Business. Además, Microsoft recomienda que el sistema tenga un TPM [módulo de plataforma confiable] v1.2¹¹, el cual todavía no está disponible para muchos sistemas utilizados en el mercado de negocios. Para sistemas sin un TPM, Microsoft ha definido un acercamiento alternativo con el uso de Bitlocker con dispositivo flash USB como parte del proceso de inicio del sistema operativo. Este acercamiento ha sido, de modo nada sorprendente, criticado por un experto en seguridad como "improvisado"¹².

Una ventaja clave que SSF ofrece sobre el BitLocker es que éste último sólo sirve para proteger de ataques fuera de línea al disco duro local de una computadora portátil o de un sistema de escritorio que corra Vista Enterprise. SSF puede proteger la información en cualquier dispositivo de almacenamiento a través de una amplia gama de plataformas Windows y protege la información cuando está ubicada fuera del sistema local. Además, SSF ofrece controles de acceso a la información para dispositivos USB o FireWire, e implanta controles en el uso de aplicaciones, ninguno de los cuales es soportado por BitLocker.

La Tabla 3 a continuación resume estas diferencias:

	<i>Secuware Security Framework</i>	<i>Windows Vista BitLocker</i>
Plataformas		
Soporta la plataforma final de Windows	Windows 2000 Professional Windows XP Vista (anuncios futuros)	Windows Vista Enterprise
Autenticación		
Métodos de autenticación	Identificación y contraseña del usuario Tarjeta inteligente <i>Token</i> USB	TPM v1.2 presente en el sistema Dispositivo flash USB
Protección de información		
Relaciones de confianza	Autenticación del usuario	Autenticación del sistema, pero no del usuario
Protección de la información en el sistema del disco duro	Todas las particiones Todos los discos físicos	Sólo la partición C en el disco físico primario
Protección de información en CD-R	Sí	No
Protección de información en dispositivo flash USB	Sí	No
Protección de información en carpetas de red	Sí	No
Permisos para compartir información encriptada con individuos autorizados	Sí	No
Administración clave		
Clave de recuperación requerida	No (Consulte la sección sobre problemas de información pública clave)	Sí
Reparación del sistema (<i>e.g.</i>) El reemplazo de la tarjeta madre evita el acceso del usuario a la información.)	No es un problema	Requiere clave de recuperación
El cambio de disco duro del usuario a otro sistema evita el acceso del usuario a la información.	No es un problema	Requiere clave de recuperación
Administración del acceso de dispositivos		
Sólo dispositivos USB y FireWire autorizados y reconocidos por Windows	Sí	No
Control de aplicaciones		
El usuario sólo puede correr aplicaciones autorizadas	Sí	No

Tabla 3: SSF ofrece protección y control de acceso a la información completa para todos los sistemas Windows 2000 y XP, mientras que el BitLocker ofrece protección sólo contra pérdida o robo del sistema y sólo para Vista Enterprise.

Especificaciones de producto

Cliente

Plataformas soportadas:

- Windows 2000 Professional SP 4
- Windows XP
- Windows Vista (durante 2007)

Espacio de disco duro

- 10 MB

Consola de gestión

Plataformas soportadas:

- Windows 2000 Professional SP 4
- Windows 2000 Servidor SP 4
- Windows XP
- Windows 2003 Servidor

La consola de gestión puede co-residir en el mismo sistema que cualquiera de los módulos de cliente SSF.

Espacio de disco duro

- Mínimo

Servidores soportados

- Windows 2000 Servidor SP 4
- Windows 2003 Servidor

Directorios soportados

- Directorio Activo de Microsoft
- Modelo de aplicación de Directorio Activo de Microsoft
- Novell eDirectory

Historia y antecedentes de la empresa

En 1988, Carlos Jiménez fundó Secuware en Madrid, España, para ofrecer una solución de seguridad pro-activa al Ministerio de Defensa Español. Su objetivo era crear una “red de seguridad” que pudiera adaptarse y desarrollarse en respuesta a los cambios del comportamiento humano y las amenazas emergentes. Jiménez fundó Secuware después de vender su empresa anterior, Anyware, que en 1988 produjo productos anti-virus para McAfee.

Secuware *Security Framework* fue lanzado en 1998. En la actualidad, cuenta con más de 300 clientes Corporativos y Gubernamentales en Europa y América Latina, ofreciendo una protección total a 500,000 sistemas Windows en computadoras portátiles y de escritorio. La empresa tiene oficinas en Madrid, España; Dorfen, Alemania; Ciudad de México, México; Bogotá, Colombia, y ahora en Sunnyvale, California, EUA.

¹ <http://www.gocsi.com/> (Seleccione la liga y complete el cuestionario para poder realizar la descarga.)

² Knowledge Services Group, *Violación de la seguridad de la información: Contexto y resumen de incidentes*, actualizado en septiembre 28, 2006, pg 2, Reporte para el Congreso del Sistema de Control y Reportes (CRS por sus siglas en inglés), Servicio de investigación del Congreso, La Biblioteca del Congreso, Código de orden RL 33199. http://digital.library.unt.edu/govdocs/crs//data/2005/upl-meta-crs-8258/RL33199_2005Dec16.pdf

³ El reporte del fenómeno muestra un marcado aumento en el costo de la violación de información, <http://complianceandprivacy.com/News-Penomenon-data-breach-cost-study.asp>

⁴ Anne Saite, Aviso: Víctimas arremeten contra empresas comprometidas, http://searchcrm.techtarget.com/originalContent/0.289142.sid11_gci1131245.00htmlm Septiembre 27, 2005.

⁵ Gartner Group, Computadoras portátiles robadas y aumento en el incumplimiento de la seguridad de la información para una mayor educación, Marzo 10, 2006, número de identificación G0013873.

⁶ Gartner Group, Las mejoras en la seguridad alentarán un incremento en la colaboración interna de ciber-ataques, Noviembre 14, 2006, número de identificación G00144683.

⁷ *Introducción al modo de aplicación del Directorio Activo*, Microsoft Corporation, agosto 2003.

<http://www.microsoft.com/windowsserver2003/techinfo/overview/adam.msp>

⁸ Microsoft Corp., <http://support.microsoft.com/kb/314079/en-us>. *Cómo usar archivos de sistema para crear un disco de inicio como protección para evitar el inicio de Windows XP.*

⁹ Brian M. Posey MCSE, <http://articles.techrepublic.com.com/5100-6346-5928902.html>. *Inicio de Windows XP desde una unidad flash USB.*

¹¹ Microsoft Corp. <http://technet.microsoft.com/en-us/windowsvista/aa906017.aspx> *Encriptación de BitLocker: Visión técnica general, Versión 1.02, abril 4, 2006.*

¹² www.scheier.com/blog/archives/2006/05/BitLocker.html.