

La seguridad efectiva y el cumplimiento de las regulaciones requiere una gestión centralizada para configurar e implementar políticas de forma coherente, especialmente en entornos mixtos de TI. Los administradores deben modificar las políticas continuamente para satisfacer requisitos en constante cambio y a la vez garantizar que la seguridad es transparente. SafeGuard Management Center reduce los costes de

SafeGuard Management Center es un módulo funcional de SafeGuard Enterprise, una solución centralizada para gestionar la seguridad de los datos en entornos mixtos de TI. SafeGuard Management Center es la plataforma de administración central y funciona junto con otros módulos funcionales de SafeGuard Enterprise para proporcionar un control total de seguridad y gestión para todos los dispositivos y usuarios conectados. Permite la gestión de la encriptación total de datos y prevención de filtración de datos (DLP) desde una consola única para una sólida seguridad multinivel.

Las principales funciones de gestión son:

- Las políticas de seguridad centralizadas implantan reglas coherentes de encriptación, autenticación, privilegios de usuarios, individuos y grupos en numerosos dispositivos en entornos mixtos de TI.
- Es fácil gestionar y distribuir políticas de seguridad a los dispositivos endpoint de los usuarios de forma rápida y cómoda. Puede importar fácilmente usuarios, grupos, dispositivos y unidades de organización ya configuradas en Microsoft Active Directory.
- La gestión centralizada de claves en entornos mixtos permite a los usuarios y administradores compartir con facilidad y recuperar datos en diferentes grupos y dispositivos.
- Los registros de auditoría e informes garantizan la conformidad con las políticas internas y las regulaciones externas.
- La recuperación de datos/contraseñas es compatible con las herramientas forenses y de recuperación estándares, lo que reduce la carga de trabajo del helpdesk.

Ventajas

- Gestiona de forma central las políticas de encriptación y de prevención de filtración de datos (DLP)
- Gestiona la encriptación de datos y la prevención de la filtración de datos en una única consola
- Administra usuarios y dispositivos en entornos mixtos de TI de forma coherente
- La gestión de usuarios basada en roles permite la aplicación de una política granular
- Accede a registros e informes de auditoría detallados e imprimibles para la conformidad con las regulaciones
- Recupera fácilmente contraseñas y datos
- Encripta y gestiona ordenadores de sobremesa, portátiles y medios extraíbles

Gestión de claves vanguardista

- Gestión de claves centralizada desde una única consola
- Almacenamiento, intercambio y recuperación segura de claves en entornos mixtos de dispositivos y sistema operativo

Ventajas clave

Administración centralizada de políticas de seguridad

- » Administración de seguridad centralizada y multiplataforma con definición jerárquica de políticas de seguridad
- » Los mecanismos de herencia de la política modular permiten la mayor flexibilidad y eficiencia en la gestión
- » Conjunto de políticas resultantes (RSOP): la política final heredada se calcula para cada usuario u ordenador
- » Distribución automática de políticas de seguridad en todas las plataformas
- » Reglas asignadas a unidades de organización (OU) y activadas para grupos de usuarios/ordenadores
- » Los dispositivos que no contacten con el servidor en un intervalo de tiempo predefinido o en un número fijo de intentos de inicio de sesión pueden ser bloqueados; el desbloqueo se realiza mediante desafío/respuesta
- » Administración de responsables de seguridad
- » Acceso basado en roles; roles de responsable de seguridad predefinidos y personalizados
- » Autorización de dos responsables para acciones críticas
- » Autenticación de dos factores opcional mediante tokens o tarjetas inteligentes
- » Responsables de seguridad de SafeGuard seleccionables de Active Directory
- » La consola de gestión tiene capacidad de multisesión
- » Soporte multitenerencia

Arquitectura de seguridad modular y flexible

- Se adapta a las necesidades gracias a los módulos adicionales SafeGuard Enterprise
- API de gestión con numerosas funcionalidades para aplicaciones del cliente
- Soporta Windows Vista™ BitLocker™ Drive Encryption
- Integración con el servicio de directorio Microsoft Active Directory® a través de LDAP; soporta entornos Novell
- Compatible con tarjetas inteligentes y tokens de terceros
- Comunicación basada en XML/SOAP: sin reconfiguraciones de cortafuegos, soporta la distribución de la carga de tráfico

Gestión completa de Windows Vista™ BitLocker™ Drive Encryption

- Se pueden aplicar políticas de seguridad coherentes en entornos mixtos de SO y dispositivos
- Gestiona de forma centralizada las claves para la copia de seguridad y la recuperación
- BitLocker™ Drive Encryption se puede seleccionar como opción
- SafeGuard Enterprise informa sobre el estado del dispositivo BitLocker

Soporte de servicios de directorio

- Se pueden importar datos de infraestructura (usuarios, ordenadores, grupos, certificados X.509, etc.) de directorios LDAP
- Soporte de Microsoft Active Directory:
 - no se requieren cuentas específicas de usuario de SafeGuard Enterprise
 - Responsables de seguridad de SafeGuard Enterprise seleccionables de los usuarios de Active Directory
- Soporta entornos Novell

Instalación automatizada

- Soporta mecanismos de distribución de software estándar a través de paquetes MSI, distribuidos e instalados automáticamente mediante sistemas

de gestión de software existentes (p. ej. Altiris, Microsoft SMS, NetInstall)

- La configuración por defecto permite una rápida implementación en entornos de prueba

Opciones de helpdesk

- Asistente de recuperación desafío/respuesta integrado para contraseñas de usuario olvidadas
- Helpdesk basado en web para entornos subcontratados
- Autoayuda en web para que los usuarios finales restablezcan contraseñas sin contactar con el helpdesk
- API para la integración personalizada del helpdesk

SafeGuard Management API soporta

- Operaciones de directorio, sincronización automática
- Asignación usuario a dispositivo
- Asignación de claves a dispositivos/usuarios
- Procesamiento de registros, inventarios e informes
- Gestión de certificados y tokens
- Desafío/respuesta para aplicaciones personalizadas de helpdesk

Estado en tiempo real, registros e informes de seguridad

- Todas las actividades/estados de los clientes, acciones de administración y eventos de seguridad se registran y almacenan de forma central
- Los tipos de registros y la ubicación del almacenamiento están definidos por el usuario
- Los administradores pueden filtrar, visualizar e imprimir informes de registro
- La herramienta autónoma opcional SGNState informa del estado de encriptación a consolas externas (p. ej. LANDesk o soluciones de control de acceso a la red [NAC])

Requisitos del sistema

Sistemas operativos (32 bit)1

- » Microsoft Windows XP (Service Pack 2, Service Pack 3)
- » Microsoft Windows Vista™ (Service Pack 1, Service Pack 2)
- » Microsoft Windows Server 2003
- » Microsoft Windows Server 2008

Certificaciones

- » FIPS 140-2
- » Habilitado para Aladdin eToken

Estándares y protocolos

- » Encriptación simétrica: AES 128/256 bits
- » Encriptación asimétrica: RSA
- » Funciones de hash: SHA-256, SHA-512
- » Contraseñas, padding, PKCS #1, PKCS #5v2
- » Tarjeta inteligente/token: PKCS #11, PKCS #15, Microsoft CSP, PC/SC, Kerberos
- » PKI: Certificados PKCS #7, PKCS #12, LDAP, X.509
- » Transferencia de datos: SOAP, XML, SSL

Idiomas

- » Inglés, francés, alemán, japonés

Comunicación cliente-servidor XML/SOAP

- » Comunicación segura a través de servicios web basados en XML/SOAP
- » Entre las ventajas figura el equilibrio de carga de los servicios en entornos amplios
- » Sin cambios en las configuraciones del cortafuegos

Gestión de licencias por parte de administradores

- » Activar nuevos módulos de SafeGuard simplemente actualizando la licencia
- » Monitorizar el uso de los módulos de SafeGuard Enterprise para cumplir con la licencia
- » Los tipos de registros y la ubicación del almacenamiento son servicios web basados en SOAP definidos por el usuario

Bases de datos soportadas

Para más detalles, visite www.sophos.com

