Data Leak Prevention

safetica

ESET TECHNOLOGY ALLIANCE

Safetica

El software de seguridad Safetica ofrece una solución integral para la prevención de la fuga de datos (DLP, por sus siglas en inglés), que abarca una amplia gama de amenazas de seguridad originadas por una misma fuente: el factor humano. Safetica brinda protección ante fugas de datos accidentales o intencionales, las malas intenciones del personal interno, los problemas de productividad, los riesgos de la implementación de políticas BYOD (llevar el dispositivo personal al trabajo), entre otros problemas.

La filosofía de seguridad de Safetica se basa en tres pilares: la integridad, la flexibilidad y la facilidad de uso.

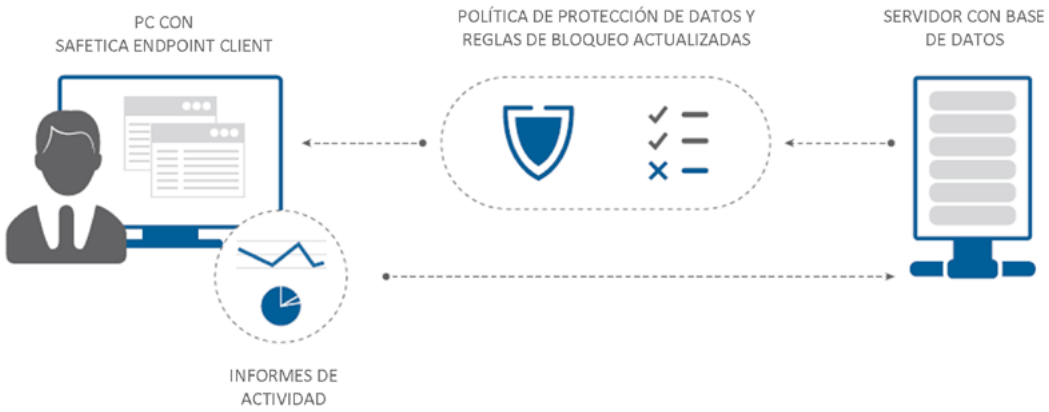
Safetica les suministra a los administradores una solución completa para prevenir la fuga de datos a nivel corporativo, incluyendo la elaboración de informes exhaustivos de la actividad y haciendo cumplir las políticas de seguridad de la empresa respecto a las acciones de los usuarios. Safetica ofrece un conjunto completo de herramientas de seguridad en un solo paquete de software que de lo contrario requeriría la instalación de varias soluciones de seguridad de diferentes proveedores.

VENTAJAS PRINCIPALES

Solución de DLP integral	que cubre todos los canales principales por los que se pueden filtrar los datos. Safetica proporciona DLP para endpoints con funcionalidades de DLP para redes.
Beneficios en poco tiempo	El enfoque flexible de Safetica para el bloqueo de los canales de extracción de datos hace que tenga el tiempo de despliegue más rápido entre todos los productos de su clase.
Alta resistencia ante la manipulación indebida	que garantiza una seguridad consistente, a la vez que asigna derechos de administrador para proteger el sistema ante los usuarios.
Protección ante funciones especiales de extracción de datos	Safetica protege los datos ante la extracción de capturas de pantalla, el robo de los datos del portapapeles, la impresión virtual, las transformaciones de archivos, y las funciones de compresión y cifrado de archivos.
Enfoque agnóstico	La protección de datos que suministra Safetica no se limita al uso de protocolos y de aplicaciones individuales.
Políticas de datos claramente definidas	con Zonas seguras. Los gerentes simplemente seleccionan las ubicaciones desde donde los datos no tienen que salir; Safetica se encarga de la seguridad.
Seguimiento preciso de la actividad	Que se haya abierto no significa que se haya usado en forma activa. Los informes de actividad suministrados por Safetica muestran el tiempo real que los usuarios pasaron en sitios Web visitados o en aplicaciones.
Evaluación y notificación automáticas	Safetica selecciona los registros más importantes y envía un informe resumido a los destinatarios designados. En caso de ser necesario, también están disponibles los detalles completos.

CÓMO FUNCIONA

La estación de trabajo es donde transcurre la acción. Los usuarios trabajan con datos críticos de la empresa, acceden a Internet, leen correos electrónicos, envían documentos a la impresora y conectan sus medios extraíbles. Safetica despliega un agente (Safetica Endpoint Client) en las endpoints deseadas y mantiene una conexión periódica con ellas a través del servidor (Safetica Management Service). Este servidor crea una base de datos con la actividad de las estaciones de trabajo, y distribuye nuevas políticas y reglamentos de protección de datos a cada una de ellas.



FUNCIONALIDADES PRINCIPALES

Prevención completa de la fuga de datos	Safetica protege todos los canales de fuga de datos, y además es fácil de instalar y operar. Para conocer la amplia cobertura de Safetica, consulte la sección Protección de eventos en las endpoints.
Generación de perfiles de tendencias y productividad	Les advierte a los gerentes de la empresa si detecta cambios repentinos en la actividad de los empleados y muestra las variaciones de productividad por departamento a través del tiempo. Ambos cambios son indicios de posibles riesgos de seguridad.
Informes de actividad	Detecta brechas de seguridad en muchos frentes mediante el control de todas las actividades del usuario en busca de cualquier signo de peligro potencial, incluso antes de concretar la transferencia de datos.
DLP de correo electrónico	Asegura que los datos protegidos no lleguen a buzones equivocados. Registra adónde se envían los archivos confidenciales y almacena esta información para informes futuros.
Control de aplicaciones con reglas de tiempo	Habilita los paquetes seleccionados de aplicaciones relacionadas con el trabajo y bloquea las demás para que el entorno sea más seguro. Se puede hacer que las aplicaciones estén disponibles solo durante un período de tiempo especificado.
Filtrado de la Web	Hace cumplir fácilmente las políticas de uso aceptable de la empresa mediante categorías cuidadosamente preseleccionadas y filtrado de palabras clave.
Control de la impresión	Limita lo que se puede imprimir y por quién, y establece cuotas de impresión para usuarios individuales y departamentos.
Control de dispositivos	Impide que los empleados conecten dispositivos no autorizados en el trabajo. Los puertos comunes se pueden habilitar para ciertos dispositivos específicos o bloquear para todos por igual.
Gestión del cifrado	Safetica ofrece el cifrado de disco completo o de particiones enteras, y crea unidades virtuales locales o de red para el almacenamiento seguro de los archivos. Además de los métodos de contraseñas y claves de acceso, Safetica ofrece discos de viaje protegidos y una funcionalidad para "cifrar cuando se copia", que protege los datos cuando salen de la Zona segura.
Modo informativo y de prueba	Ayuda a las empresas a ir integrando en forma progresiva la protección de datos mediante la implementación de pruebas para todos los tipos de situaciones posibles, sin detener las operaciones de la empresa.
Clasificación de datos sobre la marcha	Protege la información nueva inmediatamente tras su creación o su recepción.
Consola de administración unificada	La consola de administración de Safetica permite gestionar la seguridad y presentar informes desde un mismo lugar. Integra toda la protección de datos de la empresa, la elaboración de informes y las políticas de bloqueo.
Inspección de SSL/HTTPS	Verifica y protege las líneas de comunicación seguras, incluyendo los sitios Web que utilizan el protocolo HTTPS, las aplicaciones de mensajería instantánea con conexiones protegidas y la transmisión de correo electrónico seguro.
Mínimo costo total de la propiedad	Exime a los usuarios de la necesidad de comprar dispositivos de seguridad adicionales. Los agentes para endpoints desplegados en Safetica también proporcionan funciones de prevención de la fuga de datos para las redes corporativas.
Uso flexible	Safetica protege cualquier aplicación, protocolo de mensajería instantánea o servicio de correo basado en la Web gracias a su exclusivo enfoque universal.

Alianza Tecnológica de ESET

El objetivo de la Alianza tecnológica de ESET es mejorar la protección corporativa mediante una serie de soluciones de seguridad informática. Les proporcionamos a los clientes una mejor opción en el entorno de seguridad, que se halla en cambio constante, mediante la combinación de nuestra tecnología de confianza comprobada por el tiempo con otros productos que constituyen los mejores en su campo.

Alianza Tecnológica de ESET – **Prevención de fuga de datos** con Safetica

PROTECCIÓN DE EVENTOS EN LAS ENDPOINTS

Informes y bloqueo de actividades

- Todas las operaciones con archivos
- Tendencias a largo plazo y fluctuaciones de la actividad a corto plazo
- Sitios Web (todos los navegadores son compatibles, incluyendo el tráfico HTTPS): tiempo de actividad e inactividad
- Correo electrónico y correo electrónico basado en la Web (prácticamente todos los proveedores)
- Palabras clave buscadas (la mayoría de los motores de búsqueda son compatibles, incluyendo Windows Search)
- Mensajería instantánea (independiente de la aplicación utilizada; todos los protocolos)
- Uso de las aplicaciones indicando tanto el tiempo de actividad como el de inactividad
- Impresoras virtuales, locales y de red
- Actividad de la pantalla (captura inteligente)
- Registrador de pulsaciones

Prevención de la fuga de datos

- Todos los discos rígidos, unidades USB, FireWire, tarjetas SD/MMC/CF, unidades SCSI
- Transferencia de archivos en la red (sin protección, con protección)
- Correo electrónico (protocolos SMTP, POP, IMAP, Microsoft Outlook/MAPI)
- SSL/HTTPS (todos los navegadores y aplicaciones con administración de certificados estándar)
- Copiar y pegar, portapapeles, arrastrar y soltar
- Impresoras virtuales, locales y de red
- Bluetooth, IR/COM/puertos paralelos
- Lectoras y grabadoras de CD/DVD/BluRay
- Controla el acceso a los archivos por las aplicaciones

CASOS DE USO

Protección de la información vital de la empresa	Una vez que se han establecido zonas seguras para todos los datos protegidos, Safetica controla en silencio cada interacción con estos archivos y, en el caso de detectar una operación prohibida, la bloquea o lleva a cabo otras acciones preseleccionadas. Entre las acciones definidas por la empresa se incluyen informarle al gerente de seguridad sobre cada evento, cifrar los datos y ofrecer otro lugar seguro para los datos. Los datos también se protegen en los equipos portátiles y en las unidades USB incluso cuando se encuentran fuera de la empresa.
Gestión de dispositivos extraíbles	Safetica le ofrece a los administradores el control final sobre quién conecta qué en los equipos corporativos, eliminando posibles canales para la fuga de datos y reduciendo drásticamente la cantidad de intervenciones requeridas.
Cumplimiento de las normativas	Con Safetica Endpoint Client en los equipos de la empresa y la gestión de políticas activada en la consola de administración de Safetica, podrá cumplir con las normativas que regulan los movimientos y el uso de datos confidenciales.
Cifrado de datos	Safetica ofrece cifrado de disco completo, es capaz de supervisar un sistema de almacenamiento de archivos cifrado y protegido, gestionar las memorias conectadas, y evitar que los datos se almacenen en lugares no seguros.
Control de la productividad	Incluso sin necesidad de utilizar directamente la interfaz gráfica de la consola de administración de Safetica, los administradores pueden recibir informes periódicos con un resumen de la actividad de usuarios o grupos preseleccionados.

1. Se utiliza una aplicación de agente pequeña para registrar las acciones y hacer cumplir las políticas normativas (que opcionalmente puede ocultarse del usuario).

2. Los datos de los equipos en red se transfieren automáticamente al servidor y los datos de los equipos portátiles se sincronizan cuando se conectan a la red. Las configuraciones de los equipos cliente se sincronizan desde el servidor.

3. Todos los datos se pueden ver desde la consola de administración. Desde allí también se pueden configurar todos los ajustes.

4. Safetica admite la administración de múltiples sucursales desde una única consola.

Requisitos del sistema

Safetica Endpoint Client
(software agente)

- Procesador dual-core de 2,4 GHz y 32 bits (x86) o 64 bits (x64)
- 2 GB de memoria RAM
- 2 GB de espacio libre en disco
- Instalación en el equipo cliente
- MS Windows XP SP3, Vista, 7, de 32 y 64 bits
- Paquete de instalación MSI

Safetica Management Service
(componente del servidor)

- Procesador dual-core de 2 GHz y 32 bits (x86) o 64 bits (x64)
- 2 GB de memoria RAM
- 10 GB de espacio libre en disco
- Instalación en el servidor de la aplicación o en un servidor exclusivo (permite la virtualización)
- Disponibilidad de más servidores para equilibrar mejor la carga
- Admite Active Directory, pero su uso no es indispensable
- MS Windows Server 2003 SP2, 2008, 2008 R2, de 32 y 64 bits
- Requiere conectarse con el servidor mediante MS SQL 2008 o posterior

MS SQL
(componente del servidor para la instalación estándar)

- Procesador de 1 GHz y 32 bits (x86) o 64 bits (x64)
- 4 GB o más de memoria RAM (componente crítico para el rendimiento)
- 200 GB de espacio libre en disco (ideal 500 GB o más, según la configuración del monitoreo y la cantidad de equipos cliente; detalles en http://calc.safetica.com)
- Servidor compartido o exclusivo MS Windows Server 2003 SP2, 2008, 2008 R2, de 32 y 64 bits