

# Forware Anti-Leak Suite DataSheet

## Problema de la Fuga de Información

La información hoy en día, es uno de los activos más importantes, ya no sólo para las empresas y organizaciones, sino también para cada individuo. Por este motivo, la misma requiere ser asegurada y protegida de forma apropiada.

Con el paso del tiempo, los profesionales también nos hemos dado cuenta de que el verdadero problema en la seguridad de la información no se encuentra tanto en el exterior como dentro de nuestras empresas y, más concretamente, en el uso inadecuado o no autorizado de información sensible por parte de empleados.



### QUIÉNES SOMOS

Forware es una compañía española de Tecnologías de la Información cuya misión es mejorar la seguridad y la productividad de las organizaciones. Es el primer fabricante que evita de forma sencilla e integral la fuga de información, gracias a la integración de las tecnologías DLP (Data Leakage Prevention), ERM (Enterprise Rights Management), EPP-Control de dispositivos y Token.

## Forware Anti-Leak Suite

Forware AntiLeak Suite es una solución para evitar la fuga de información. La protección se lleva a cabo de forma automática mediante la localización de los ficheros sensibles en el computador del empleado, la encriptación y la asignación de derechos de acceso a los mismos. La solución evita que los ficheros informáticos de la empresa sean accedidos por personas no autorizadas y ayuda al cumplimiento normativo de la organización y al cumplimiento de leyes sobre la protección de datos.

## Beneficios

VULNERABILIDADES Y AMENAZAS CUBIERTAS							
Empleados insatisfechos		Competidores desleales		Gestión integral de riesgos		Infraestructura insegura	Datos disgregados
FICHEROS PROTEGIDOS							
Documentos de Negocio		Datos Personales		Propiedad Intelectual		Documentos Operativos	Bases de Datos
ALCANCE DE LA PROTECCIÓN							
 En la oficina		 En casa		 En itinerancia		 En terceros	
CUMPLIMIENTO DE NORMATIVAS							
LOPD		SB-1386		HIPAA		GLBA	US PII
						PCI	Sarbanes-Oxley
EXPERIENCIA DE EMPLEADO: SENCILLO							
Rápido 1ms/acceso		Transparente Imperceptible		No requiere formación		Cómodo, protección automática	
EXPERIENCIA DEL ADMINISTRADOR: SENCILLO							
Cómodo, gestión centralizada		Eficiente, propagación de políticas inmediata		Rápida formación, medio día		Flexible, no intrusivo y escalable	
NIVEL DE SEGURIDAD							
Encriptación AES 128/256		Control de Acceso por Token con CriptoArquitectura		Control de Seguridad de claves criptográficas		Actualizaciones de seguridad periódicas	Auditoría para análisis forense

Forware AntiLeak Suite incorpora lo mejor de cada tecnología para conseguir un entorno de trabajo productivo en el que la información permanezca segura.

DATA LEAKAGE PREVENTION (DLP)	Localizar ficheros sensibles y asignar automáticamente derechos de acceso	ENDPOINT PROTECTION PLATFORM (EPP)	Bloquear de forma selectiva el uso de dispositivos: USB, impresoras, grabadoras CD/DVD
	Controlar los flujos de información		
	Educar a los usuarios en las políticas de seguridad de la empresa		
	Auditar el uso que cada usuario hace de la información		
ENTERPRISE RIGHTS MANAGEMENT (ERM)	Cifrar ficheros sensibles	TOKEN	Velar por la integridad del computador del usuario
	Administrar los derechos de acceso a la información		Evitar la suplantación de identidad mediante el control de acceso
	Compartir de forma segura ficheros con otros usuarios fuera de la organización		Gestionar los derechos de acceso en un entorno seguro libre de corrupción

Seguridad

- Encriptación robusta: algoritmo AES 128/256, implementado en Criptoprocesador / CriptoArquitectura.
- Ubicuidad: protección de información dondequiera que esté, en contraposición a la seguridad perimetral, que acota el ámbito de actuación.
- Almacenamiento seguro: la información siempre está cifrada en disco y sólo se descifra parcialmente bajo demanda en memoria RAM.
- Control de los canales de entrada/salida: imprimir pantalla, copiar, pegar, imprimir, CD/DVD, USB y Bluetooth.
- Comunicación segura entre los módulos de la solución.
- Control de acceso, gestión de derechos y control de la integridad mediante un Token físico o virtual.

Productividad

- Localización automática de ficheros sensibles mediante búsqueda de patrones en su contenido:
  - Frecuencia de una palabra en el texto.
  - Distancia de dos palabras en el documento.
  - Cualquier combinación de las anteriores mediante operadores lógicos.
- Asignación automática de derechos de acceso a los ficheros sensibles localizados.

Elementos Protegidos

- Ficheros informáticos, independiente de su formato.
- Aplicaciones informáticas con las que se abren los archivos.
- Sistemas de almacenamiento local y en red.
- Grupos de trabajo, independientemente de su tamaño y necesidades de escalabilidad.

Adaptabilidad

- Control de acceso mediante políticas de seguridad, compuestas por cualquier combinación de:
  - Lista blanca de aplicaciones de confianza.
  - Extensiones de ficheros.
  - Ruta de almacenamiento.
  - Fecha de caducidad.
  - Conectividad del Endpoint Agent con el Administration Server via TCP/IP (online/offline).
  - Patrones en el contenido del fichero.
- Organización en grupos: agrupación de usuarios que comparten políticas.
- Jerarquía de grupos: de acuerdo a la organización de la empresa, simplifican la herencia de políticas.
- Granularidad: especialización de políticas para un usuario, con precedencia sobre las heredadas.

Administración

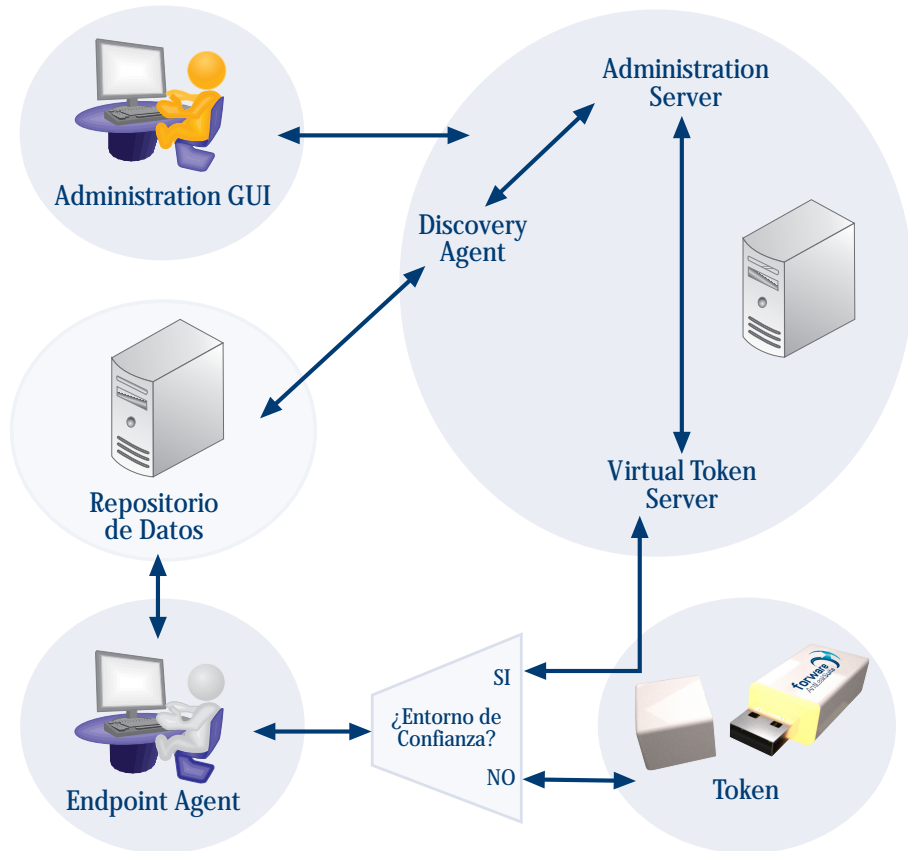
- Gestión centralizada de políticas de seguridad, usuarios y grupos.
- Auditoría: filtrado de eventos según usuario, dirección IP, archivo, proceso, tipo de evento, fecha y canal.
- Gestión de Tokens físicos y virtuales.
- Seguimiento de licencias del software.
- Descarga, aprobación y distribución de actualizaciones.

Sistemas operativos

- Windows XP SP2 y posteriores
- Espacio en disco
- Software de servidor: 90 MB
- Software de usuario: 70 MB

## La solución está formada por los siguientes componentes:

- **Administration GUI:** interfaz gráfico para la administración centralizada de políticas de seguridad, usuarios, derechos de acceso y auditoría de sucesos.
- **Software de Servidor:**
  - **Administration Server:** aplicación de servidor a la que se conectan remotamente los Endpoint Agents para mantener actualizado su software anti-fugas y sus derechos de acceso, así como sincronizar su historial de sucesos.
  - **Virtual Token Server:** aplicación de servidor a la que se conectan remotamente aquellos Endpoint Agents que no dispongan de un Token físico y precisen uno virtual.
  - **Discovery Agent:** localización automática de la información sensible en repositorio de datos.
- **Software Endpoint Agent:** aplicación instalada en el computador de cada usuario que haciendo uso del Token evita la fuga de información desde el equipo del usuario, cualquiera que sea el canal de salida.
- **Token Hardware (opcional):** se entrega a cada usuario para el acceso a la información cifrada. Es un mecanismo para evitar la suplantación de identidad, y que al mismo tiempo proporciona la máxima protección gracias a la CriptoArquitectura hardware.



Declaración CE de conformidad

De acuerdo con la directiva EMC 89/336/ECC, este producto está conforme con las siguientes normas armonizadas:

- \* EN55022
- \* EN55024