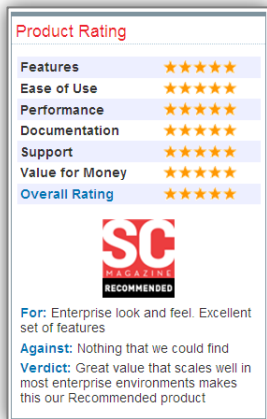


CLEARSWIFT SECURE Web & Email Gateway

CLEARSWIFT SECURE Web & Email Gateway ES LA PASARELA DE EMAIL Y WEB QUE PROPORCIONA SEGURIDAD UNIFICADA (ANTIMALWARE Y DLP) EN AMBOS ENTORNOS

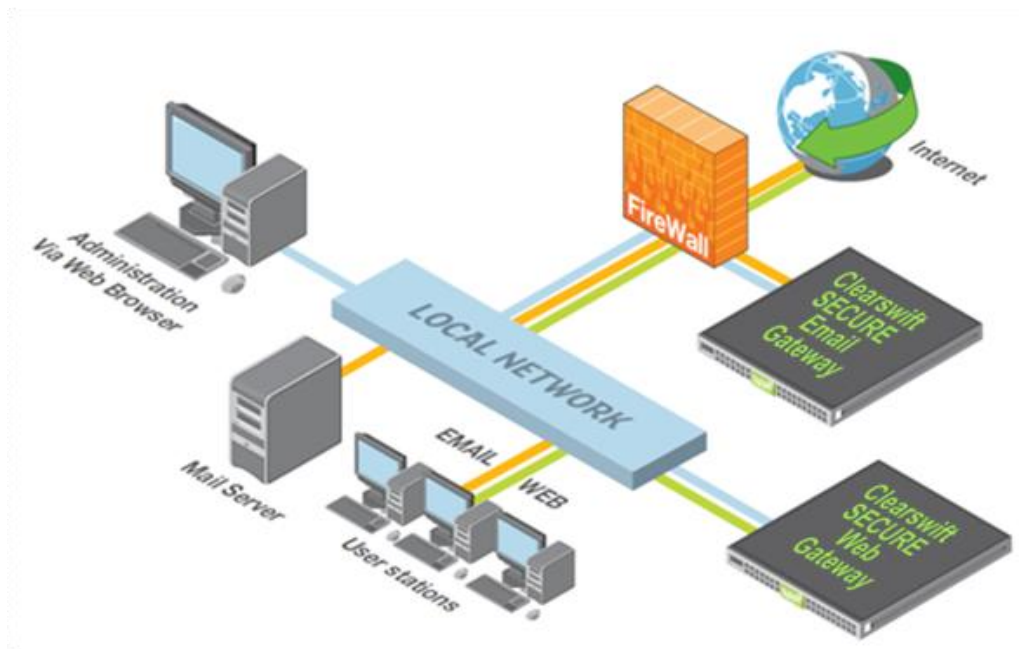


Gracias a sus más de 15 años de especialización en el control de contenidos, **Clearswift** ofrece en sus productos unas capacidades de análisis del tráfico tanto entrante como saliente difícilmente igualables.

La gestión totalmente integrada* para los entornos de **Email y Web** posibilita la creación de **políticas coherentes** entre ambos entornos. Se hace posible de esta forma la definición de verdaderas políticas de control de contenidos para la compañía, al abarcar los dos métodos de acceso a Internet habituales de los usuarios.

Ahora, con **Clearswift SECURE Web & Email Gateway**, puede disfrutar de una **plataforma de gestión unificada** para proteger y controlar tanto los flujos de correo electrónico como de navegación Web, con una gestión unificada y preparada para los entornos más exigentes.

*Disponible también de forma separada como pasarela para correo o navegación independiente



BENEFICIOS CLAVE

- Integración Web y Email
- DLP perimetral
- Anviti-virus y Anti-spyware
- Potente Antispam
- Categorización de URLs
- Gestión Centralizada
- Política Granular
- Inspección HTTPS
- Web 2.0 Ready
- Sencillo Manejo
- Cache de contenido Web
- Solución consolidada

Con **Clearswift SECURE Web & Email Gateway**, podrá afrontar los retos actuales de seguridad, fuga de información y cumplimiento de normativa de una forma eficiente y sencilla.

Analice y controle en la pasarela todos los flujos de tráfico Web y Email. Gracias a la **consola y política común para Web & Email** podrá desplegar su política de control de contenidos corporativa, permitiéndole:

- **Protegerse ante amenazas externas**, tanto de virus, spam, spyware, phishing, y en general, cualquier tipo de
- **Mejorar la productividad de sus empleados**, gracias al control granular e integrado con sus sistemas corporativos de directorios de usuarios
- **Evitar fugas de información (DLP)**, mediante el más avanzado motor DLP de pasarela de Clearswift
- **Mejorar el cumplimiento normativo**, detectando contenido al que aplica normativa legal y definiendo acciones para su control
- **Implementar la solución eficientemente** mediante: HW, SW & Virtual Appliance

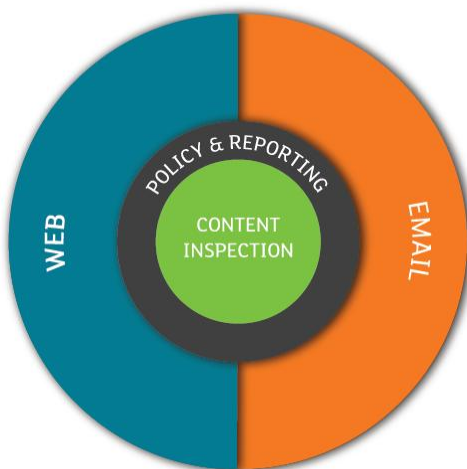
Clearswift SECURE Web & Email Gateway: Solución eficiente a problemas reales

Clearswift SECURE Web & Email Gateway realiza una aproximación práctica y eficiente al grueso de las causas de la fuga de información, evitando daños directos a la empresa, problemas de imagen e incumplimiento normativo.

Gracias a sus más de 15 años de especialización en el control de contenidos, Clearswift ofrece en sus productos unas capacidades de análisis del tráfico tanto entrante como saliente difícilmente igualables. La disponibilidad de productos en formato Appliance para los entornos de Email y Web que disponen del mismo motor de inspección, posibilita la creación de políticas coherentes entre ambos entornos. Se hace posible de esta forma la definición de verdaderas políticas de control de contenidos para la compañía, al abarcar los dos métodos de acceso a Internet de los que disponen los usuarios.

Las soluciones Clearswift, por sus características, permiten ahorrar tiempo y costes mediante:

- **Una consola común para Web & Email** que permite a los administradores monitorizar y controlar eficientemente toda la actividad así como el despliegue/modificación de políticas de manera rápida y sencilla y de forma coherente para web y mail. Esto les permite además identificar y controlar políticas relativas a la información sensible así como el grado de cumplimiento normativo en ambos entornos.
- **Múltiples opciones de despliegue** que incluyen HW, SW y Virtual Appliance. De esta forma, es posible optimizar la inversión en HW y adaptarla a la evolución de las necesidades, garantizando un bajo coste de propiedad (TCO) y un rápido retorno de la inversión (ROI).
- **La integración de Seguridad de Contenidos** (antivirus, antispam, antispyware,...) y el más eficiente motor **DLP** permiten aplicar medidas de Prevención de Fugas de Información de manera rápida, segura y económica.



Los appliances de Clearswift están basados en un sistema Linux securizado y optimizado para obtener el máximo rendimiento. Su sencillez de instalación y gestión incluye los entornos con múltiples appliances, en los que ningún elemento adicional es necesario al estar toda la funcionalidad consolidada en los appliances.

La inclusión de nuevos appliances en el grupo, se realiza de forma rápida y sencilla, en configuraciones **activo-activo** pudiéndose gestionar todos los

appliance desde la consola web de uno cualquiera de ellos. Se proporciona de este modo un grado de escalabilidad difícilmente igualable. Asimismo, las avanzadas capacidades de generación de informes permiten consolidar la información procedente de todos los appliances desplegados de forma sencilla y sin necesidad de herramientas, licencias o servidores adicionales.



La trayectoria de Clearswift y la calidad de nuestros productos, han sido reconocidos por diversos prestigiosos medios del sector.

Fuga de Información: ¿Un problema real?

Mucho se ha hablado sobre la fuga de información (DLP, por sus siglas en inglés), pero ¿debemos estar preocupados? ¿Cómo puede afectar a mi empresa? ¿Cuál es el coste de implantar medidas que eviten la fuga de información?

Hasta hace algún tiempo, las organizaciones tenían un control más efectivo sobre la información. La mayoría del contenido corporativo se encontraba en bases de datos y aplicaciones corporativas con acceso muy limitado.

Hoy en día, la información está repartida, y alrededor del 80% del contenido no está estructurado, residiendo en cuentas de correo electrónico, webmails, hojas de cálculo, ficheros varios, aplicaciones, o servidores de documentación. Esta información viaja libremente a través de las organizaciones sin ser inspeccionado.

Esta movilidad de la información incrementa la posibilidad de fugas de información e incumplimientos de normativa legal. Estos son algunos ejemplos de incumplimientos relevantes:

- 42 millones de números de tarjetas de crédito y débito fueron filtradas de una cadena de ventas minorista incumpliendo así PCI DSS, costándole 256 millones de dólares, y 130 millones de dólares en denuncias de pagos por bancos y clientes afectados. Cualquier compañía que almacene, procese, o transmita información de una tarjeta debe cumplir con PCI DSS y realizar auditorías periódicas.
- 4,2 millones de números de tarjetas de crédito y débito fueron filtrados de una cadena de supermercados por malware instalado en equipos internos.
- Desde un centro de I+D de una compañía de software, se enviaron al exterior los documentos de diseño y código fuente de los últimos proyectos de innovación, con el grave impacto asociado.
- Un empleado de un hospital envió por equivocación una lista que contenía 4.500 pacientes de SIDA y 2.000 pacientes con HIV positivo, incumpliendo así las normativas y exponiendo información privada de los pacientes.

Estos y otros muchos casos muestran la gravedad tanto por el daño a la compañía como por el riesgo de incumplir normativa e incurrir en las correspondientes sanciones.

Pero ¿cuáles son las principales causas de fuga de información? Según un estudio realizado por Clearswift, las cuatro principales causas son:

- **Fuga accidental:** ¿Cuántas veces se ha autocometido una dirección de correo y ha enviado información a otra persona? ¿Ha reenviado un correo que tenía en el histórico información que no debía haber salido de la compañía? ¿Ha enviado alguna vez información de la compañía desde una cuenta de webmail porque el correo corporativo no funcionaba correctamente?
- **Malware:** ¿Cómo llega el malware a los equipos corporativos? ¿Dispone de barreras de entrada de malware por Email y Web? ¿Y de filtros que eviten que el malware se comuniquen con el exterior?
- **Trabajadores propios:** ¿Se ha planteado cuántos de sus trabajadores se envían información al exterior para guardar “su” trabajo? ¿Qué ocurre cuando un empleado deja la compañía?
- **Ataques de seguridad dirigidos:** ¿Está controlando qué información sale de su compañía? ¿Podría detectar una cantidad inusual de información sensible en los flujos de información?

El impacto de cualquiera de estas fugas puede no pasar de la anécdota, pero en muchas ocasiones no se trata únicamente del daño directo que pueda causar al negocio, sino que se puede incurrir en incumplimientos de normativas que suelen tener serios impactos económicos.

Este problema afecta a cualquier organización. Independientemente del tamaño de su empresa, si trata con información personal le aplicará el cumplimiento de LOPD, si trata de algún modo tarjetas de crédito deberá cumplir PCI DSS,...

Existen un gran número de casos que ilustran cómo el incumplimiento de estas normativas incluso de forma accidental, ha ocasionado graves perjuicios económicos a entidades de pequeño tamaño¹.

¹ En www.agpd.es se pueden consultar los casos y sanciones impuestas por incumplimiento de LOPD

CARACTERÍSTICA	BENEFICIO
POLÍTICA	
Generación de políticas flexibles y granulares	Defina políticas avanzadas para controlar los flujos de comunicaciones Web & Email regulando cómo se comparte, almacena y distribuye la información de su organización, además de proteger frente a amenazas
Política de navegación por franja horaria o cuotas	Permite definir tanto las franjas horarias como el tiempo diario de navegación por usuario para cada zona de Internet
Control centralizado	Actualización automática de políticas entre varios appliances de Clearswift
Integración con LDAP y Directorio Activo	Defina la política por usuario, grupo, dominio, o cualquier otra combinación basada en los datos del directorio corporativo
Política de uso aceptable de Internet	Página de información periódica de la política de uso aceptable de Internet, donde el usuario debe aceptar previo a la navegación
HIGIENE	
Anti-malware bidireccional	Bloqueo efectivo del malware conocido y desconocido tanto entrante como saliente
Anti-spyware bidireccional	Bloqueo de spyware, adware, key loggers y spyware call-home, identificando los equipos y usuarios infectados
Filtro de URL incluyendo categorías de Riesgo de Seguridad	Evita el acceso a sitios de alto riesgo por Malware, Phishing, Proxies remotos, y Hacking
TRUSTmanager™	Filtro de conexión por reputación de alta efectividad con bloqueo de hasta el 80% del spam
SpamLogic™	Tecnología anti-spam basada en múltiples motores con un grado de efectividad en la detección de al menos 99,5%
Cifrado en conexiones	Inspección de los flujos de tráfico HTTPS para una protección completa
Inspección de contenidos	Bloqueo de ejecutables, incluyendo ActiveX, incluso ante intentos de ofuscación
INSPECCIÓN DE CONTENIDOS	
Detección de tipo de contenido a nivel binario	Identificación real y efectiva a nivel binario de los tipos de contenidos en los flujos de comunicación, o incrustados en la información, para su aplicación en la política
Inspección HTTPS y control de puertos	Aplicación del completo filtro antimalware e inspección de contenidos a los flujos cifrados HTTPS
Detección de expresiones léxicas y regulares	Búsqueda efectiva de patrones y palabras clave en el contenido, adjuntos, cabeceras, URL, e incluso partes de documentos. Se incluyen patrones y tokens de detección avanzados, como números de tarjetas de crédito
Diccionarios incorporados	Listados multi-lenguaje para lenguaje inapropiado, así como diccionarios editables de cumplimiento normativo GLBA, HIPAA, SEC, SOX, PCI y PII
GESTIÓN Y GENERACIÓN DE INFORMES	
Intuitivo interfaz web de gestión	Completo y sencillo de utilizar, evitando la necesidad de utilizar línea de comandos
Plantillas de informes predefinidas	Informes sencillos de visualizar, modificar y compartir, con posibilidad de profundizar
Programación de informes	Permite la definición inicial y programación periódica para distribuir por correo electrónico
Informes multi-appliance	Vista consolidada de la actividad de los usuarios para facilitar la gestión, supervisión y análisis de la información de seguridad
Actualizaciones automáticas	Mantiene al sistema preparado, a la vez que disminuye los tiempos de administración
Alertas SNMP y SMTP	Simplifica la gestión desatendida, al alertar frente a gran cantidad de eventos

Clearswift Global Support

Clearswift Global Support provides access to technical support that covers all the components within our solutions.

Clearswift Global Support is available as 'Standard Support' on a 24x7 basis