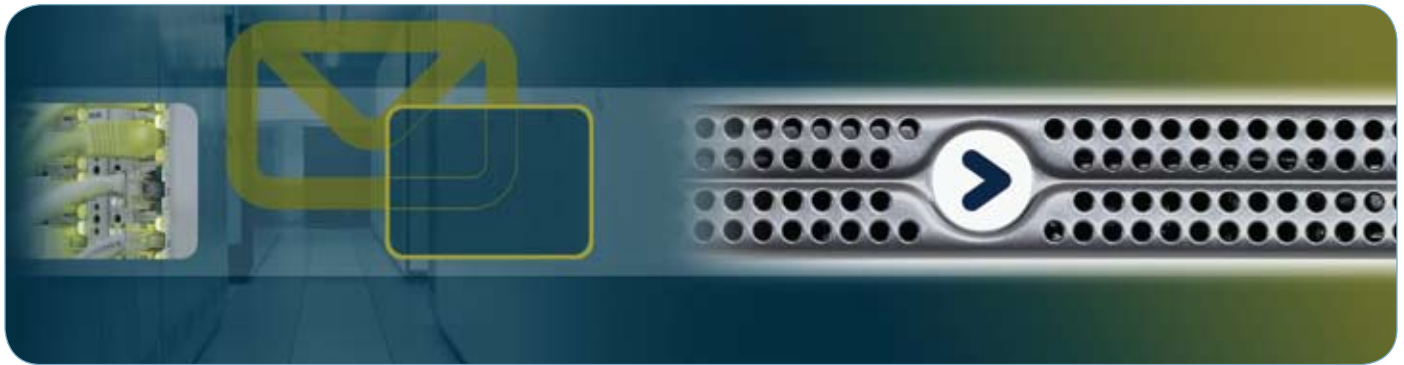


# Proofpoint: a la vanguardia en seguridad de correo electrónico y prevención de pérdida de datos



En sitio o bajo demanda, Proofpoint le permite controlar los riesgos del correo electrónico



Ya sea que se implementen bajo demanda o en sitio, las soluciones de seguridad de correo electrónico de Proofpoint protegen de las amenazas de mensajería entrante, previenen la fuga de información delicada, encriptan mensajes y contribuyen a optimizar su infraestructura de mensajería. Su arquitectura unificada, defensas modulares y su interfaz de gestión de políticas protegen a las organizaciones contra todo tipo de riesgos de correo electrónico, a nivel gateway de las empresas.

## defiende, previene, encripta, analiza

¿Por qué comprar otra solución puntual? La plataforma unificada de seguridad de correo electrónico y prevención de pérdida de datos de Proofpoint proporciona protección integral contra amenazas entrantes y riesgos de seguridad de contenidos salientes, y la arquitectura modular de Proofpoint le permite implementar fácilmente nuevas defensas a medida que sus necesidades van cambiando.

Todas las funciones de Proofpoint (incluidos el antispam, el antivirus, la seguridad de contenidos en múltiples protocolos, la encriptación basada en políticas y características de generación de informes) se gestionan de manera centralizada desde una única GUI administrativa y se despliegan en una arquitectura unificada. Las funciones pueden implementarse en prácticamente cualquier configuración para ajustarse a las necesidades particulares de su organización.

Ya sea que su implementación involucre una única ubicación o múltiples ubicaciones distribuidas en todo el mundo, todas las tareas de gestión y administración de políticas se controlan a través de la consola de administración centralizada basada en la web de Proofpoint.

## opciones flexibles de implementación

Las soluciones de seguridad de correo electrónico y prevención de pérdida de datos de Proofpoint pueden implementarse bajo demanda, en sitio o en configuraciones híbridas para máxima flexibilidad:

- **SaaS:** las soluciones de software como servicio Proofpoint ENTERPRISE™ y Proofpoint PROTECT™ proporcionan las funciones de DLP y seguridad de correo electrónico de Proofpoint, como un servicio a pedido, rentable. Hospedadas en los centros de datos de primera línea de Proofpoint, estas soluciones a demanda proporcionan máxima seguridad con el menor costo total de propiedad.
- **Dispositivo de hardware:** Proofpoint Messaging Security Gateway es un dispositivo mejorado, seguro y de fácil despliegue que se instala en minutos. Hay una cantidad de modelos disponibles que soportan empresas de cualquier tamaño.
- **Dispositivo virtual:** el dispositivo Virtual Edition de Proofpoint proporciona, al igual que los dispositivos de hardware de Proofpoint, la mejor protección en su clase, conjuntamente con los diversos beneficios en términos de ahorro y administración propios de la virtualización. El dispositivo virtual opera en cualquier x86 estándar utilizando un servidor VMware o una infraestructura VMware.
- **Software:** Proofpoint Protection Server proporciona la plataforma de seguridad de correo electrónico de Proofpoint como software para el sistema operativo Red Hat Enterprise Linux.

## Seguro, efectivo y de fácil despliegue

Éstas son solamente algunas de las formas de describir la plataforma unificada para la seguridad del correo electrónico y la prevención de pérdida de datos de Proofpoint. Se trata de la solución más poderosa en la industria, desplegada como SaaS, dispositivo, dispositivo virtual o software, y ofrece:

- Detección de spam y administración de conexión insuperables.
- Protección de primera clase contra virus y botnets.
- Prevención de pérdida de datos y seguridad de contenidos integrales en múltiples protocolos.
- Encriptación de correo electrónico basada en políticas.
- Generación de reportes y análisis avanzados.
- Gestión de políticas unificada.
- Rendimiento de nivel empresarial.
- Rápida implementación y puesta a punto.
- Arquitectura con óptima escalabilidad.

**“Pacific Sunwear evaluó una cantidad significativa de productos antispam, antivirus y de exploración de contenidos, y Proofpoint fue la primera compañía en proporcionar una plataforma que resuelve todos nuestros desafíos relativos al correo electrónico y la mensajería con una única solución de fácil manejo y despliegue. El dispositivo Messaging Security Gateway ha devuelto nuestro canal de correos electrónicos a su posición legítima como conducto estratégico para las comunicaciones comerciales y no como puerta giratoria para las amenazas contenidas en los mensajes”.**

**Ron Ehlers**  
VP de Sistemas de Información  
Pacific Sunwear

# Proofpoint: a la vanguardia en seguridad de correo electrónico y prevención de pérdida de datos

## protección total

### Tecnología Proofpoint MLX

#### Aprendizaje automático avanzado

La potencia que subyace a las soluciones de seguridad para mensajería empresarial de Proofpoint (Proofpoint MLX) es un sistema de aprendizaje automático avanzado, cuya patente está en trámite, desarrollado por científicos en el Proofpoint Attack Response Center. Basado en técnicas estadísticas avanzadas, incluidos la regresión logística y el análisis de la información obtenida, Proofpoint MLX permite la clasificación e identificación adecuadas de contenido no estructurado, según se presenta en correos electrónicos y otros documentos.

#### Precisión incomparable

Proofpoint MLX despliega la incomparable precisión antispam de Proofpoint Spam Detection. Mediante el uso de MLX, Proofpoint analiza cientos de miles de atributos estructurales, de imágenes, de contenidos y de reputación para diferenciar con precisión el spam de los mensajes válidos. Las soluciones antispam tradicionales evalúan únicamente una cantidad limitada de atributos y no son capaces de clasificar definitivamente el spam, lo que se traduce en una baja efectividad y una tasa alta de falsos positivos.

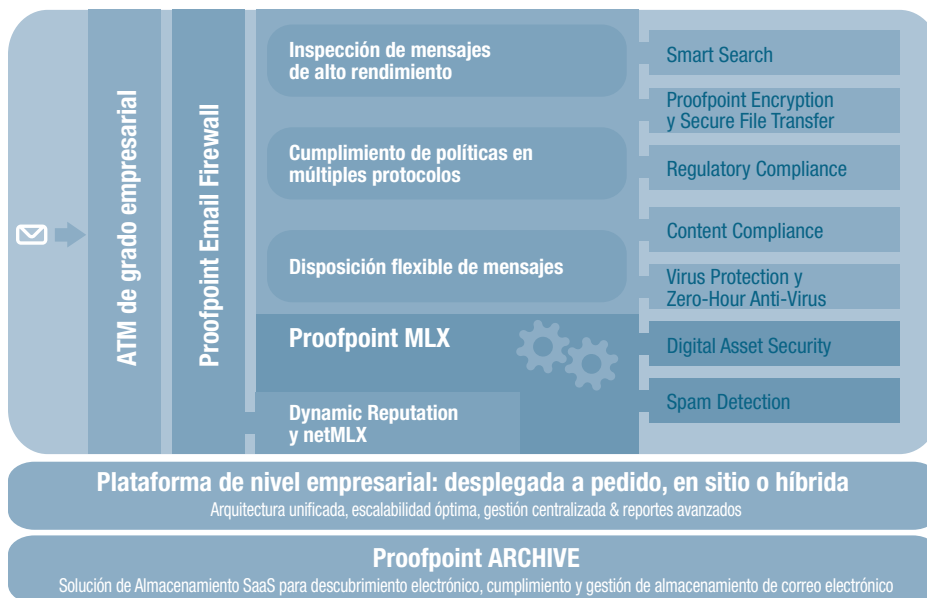
#### Inteligencia a prueba del futuro

La tecnología antispam de Proofpoint se actualiza permanentemente para defenderse de nuevas formas de spam. El autoaprendizaje permanente y las nuevas técnicas desarrolladas por los científicos de Proofpoint le permiten a MLX predecir y adaptarse a las nuevas formas de spam a medida que van apareciendo. Las actualizaciones de MLX se entregan automáticamente a todos los clientes de forma continua.

Como resultado, Proofpoint MLX ofrece una efectividad de 99,8% o superior, aun contra formas difíciles de spam, incluidos PDF, archivos adjuntos, backscatter y spam en idioma extranjero.

A diferencia de otras soluciones antispam, la capacidad de protección de Proofpoint contra ataques de spam no se deteriora con el tiempo, y las actualizaciones del motor antispam MLX se envían automáticamente a su empresa en forma regular. Proofpoint MLX está en continua evolución para contrarrestar las amenazas emergentes y se asegura de que su infraestructura de mensajería permanezca segura contra los spammers actuales y los que puedan surgir en el futuro.

Proofpoint MLX acciona también las funciones avanzadas de seguridad de contenido de Proofpoint Digital Asset Security y las funciones inteligentes de seguridad perimetral del servicio Proofpoint Email Firewall y Dynamic Reputation. Proofpoint es el único proveedor que aplica estas poderosas técnicas de aprendizaje automático a la seguridad del correo electrónico y la prevención de pérdida de datos.



## protección contra amenazas entrantes

### Detección avanzada de spam desarrollada por Proofpoint MLX™

Desarrollado con tecnología de aprendizaje automático Proofpoint MLX, **Proofpoint Spam Detection™** examina cientos de miles de atributos en cada correo electrónico, incluidos el título del asunto y la estructura, las imágenes, la reputación del remitente así como también el contenido no estructurado en el cuerpo del mensaje, para bloquear el spam, el spam basado en imágenes y los ataques de fraude electrónico, y se adapta automáticamente a los nuevos ataques a medida que van apareciendo. **Proofpoint Dynamic Update Service™** actualiza automáticamente su protección contra spam y asegura una máxima efectividad en todo momento. Las puntuaciones del spam controlado en forma individual y del contenido adulto le permiten reforzar las políticas de tolerancia cero contra el spam pornográfico. Las funciones antifraude electrónico (incluida la firma DKIM de correos electrónicos salientes) evitan la propagación del fraude electrónico y evitan el robo de la información personal de los empleados. Las funciones de gestión del rebote, incluida la admisión de la especificación de la Validación de Etiquetas de Direcciones Rebotadas (BATV), bloquean el 100% de spam backscatter (mensajes de informes de no entrega).

Proofpoint Spam Detection es multilingüe y ofrece una precisión extraordinaria contra el spam en cualquier idioma, incluidos los idiomas de caracteres multibyte, difíciles de analizar, como el japonés y el chino. Las políticas antispam pueden personalizarse en forma global, grupal o por usuario. La integración con LDAP (protocolo de acceso ligero a directorio) o Directorio Activo simplifica la administración continua.

### Protección integrada Email Firewall

**Proofpoint Email Firewall™** proporciona una protección de primera línea con control de estado contra spam y conexiones maliciosas, sometiendo a prueba puntos de datos con distintos niveles de conexión, incluidos DNS, verificación de registro MX, SPF, verificación del receptor, información de Proofpoint Dynamic Reputation y datos netMLX (reputación de la red) opcionales.

### Manejo innovador de las conexiones

Todos los despliegues Proofpoint proporcionan un análisis integrado, predictivo y de comportamiento del tráfico local IP que responde en tiempo real para eliminar los picos de tráfico de correo electrónico causados por ataques a objetivos y para bloquear o regular conexiones maliciosas de botnets.

**Proofpoint Dynamic Reputation™** o el servicio **Proofpoint SHIELD™** pueden reducir los volúmenes de conexiones entrantes en un 80% o más. Proofpoint constituye la base de datos de reputación de direcciones IP que envía correos electrónicos por Internet más precisa y actualizada de la industria. Es el único servicio de reputación de correo electrónico que utiliza una combinación de datos locales de comportamiento predecible y la reputación observada internacionalmente, analizada por algoritmos

# Proofpoint: a la vanguardia en seguridad de correo electrónico y prevención de pérdida de datos

## protección contra amenazas entrantes (continuación)

de aprendizaje automático poderosos, para bloquear las conexiones entrantes de direcciones IP maliciosas. Cada minuto, se analizan en detalle cientos de puntos de datos para todas las direcciones IP con algoritmos de aprendizaje automático avanzado para generar una puntuación representativa de la reputación del remitente. Proofpoint Dynamic Reputation utiliza entonces estas puntuaciones, combinadas con datos locales de comportamiento, para tomar decisiones inteligentes en cuanto a la aceptación, restricción o rechazo de las conexiones de correo electrónicos entrantes.

### Virus Protection y Zero-Hour Anti-Virus Defenses

Mediante alianzas estratégicas con los proveedores líderes de antivirus, **Proofpoint Virus Protection™** proporciona una funcionalidad completa de exploración para la identificación de virus. Los motores de virus están completamente integrados con la plataforma de Proofpoint, la que proporciona una administración adecuada y centralizada de las políticas antivirus desde la misma interfaz utilizada para manejar las políticas de spam y de contenidos. Los mensajes se exploran de manera eficiente para identificar virus, simultáneamente con el contenido de mensajes y el spam, protegiendo a los usuarios finales de virus, gusanos y otros códigos maliciosos. Adicionalmente, **Proofpoint Zero-Hour Anti-Virus™** protege contra virus emergentes en las primeras etapas de su proliferación y los detiene mucho antes de que las soluciones de la competencia empiecen a reaccionar.

### previene filtraciones de información en múltiples protocolos

Las funciones de prevención avanzada de pérdida de datos de Proofpoint pueden proteger los correos electrónicos salientes, así como también los flujos de mensajes adicionales, incluidos los correos electrónicos basados en la web, publicaciones en blogs, publicaciones en foros y otras actividades basadas en HTTP o FTP.

### Content Compliance: imponga fácilmente las políticas de uso aceptables

**Proofpoint Content Compliance™** facilita la definición e imposición de políticas de uso corporativas aceptables para el contenido de los mensajes y los archivos adjuntos. Una práctica interfaz point-and-click (señala y marca) simplifica el proceso de definición de reglas complejas relacionadas con los tipos de archivos, el tamaño de los mensajes y el contenido de los mensajes. Estas funciones pueden utilizarse para identificar y prevenir una gran variedad de violaciones entrantes y salientes de políticas, incluidos el lenguaje ofensivo, el acoso, el intercambio de archivos y las violaciones de reglamentaciones externas.

### Regulatory Compliance: mantenga seguros los datos privados

Hoy más que nunca, las empresas necesitan salvaguardar la privacidad y seguridad de los datos referidos a los clientes y los empleados. **Proofpoint Regulatory Compliance™** implementa las mejores prácticas para asegurar los datos privados y protege a su organización de las responsabilidades asociadas con las reglamentaciones relativas a la privacidad y la seguridad de datos—como la HIPAA (Ley de Responsabilidad y Transferencia de Seguros Médicos), GLBA (Ley Gramm-Leach-Bliley), PCI (Interconexión de Componentes Periféricos), normas SEC (Comisión de Valores y Bolsa de EE. UU.)—. Se utilizan normas personalizadas, diccionarios gestionados e “identificadores inteligentes” para explorar automáticamente la información no de dominio público, como información sobre la salud protegida e información financiera personal, y para rechazar o encriptar mensajes según corresponda.

Los identificadores inteligentes de Proofpoint son más sofisticados que las simples expresiones regulares. Buscan la cantidad correcta de dígitos o caracteres, pero además realizan un procesamiento algorítmico complejo para asegurar una gran precisión en la detección y minimizan, al mismo tiempo, los falsos positivos.

### Digital Asset Security: protección de documentos confidenciales

Así como el correo electrónico, el webmail y otros sistemas de mensajería se han transformado en las vías de comunicación más importantes, éstos se han transformado también en un canal que expone información sensible o confidencial. **Proofpoint Digital Asset Security™** evita que los valiosos activos corporativos y los datos confidenciales se filtren fuera de su organización a través del correo electrónico y otros protocolos de mensajería. La poderosa tecnología de aprendizaje automático MLX analiza y clasifica sus documentos confidenciales, y luego controla esa información (o partes de esa información) en el flujo de mensajes salientes y detiene las infracciones de seguridad de contenidos antes de que se produzcan.

### Prevención de pérdida de datos en múltiples protocolos

Extienda la potencia de las funciones de prevención de pérdida de datos de Proofpoint a los flujos HTTP y FTP con la adición de **Proofpoint Network Content Sentry™**.

## Gestión centralizada

### Gestión de políticas, administración y controles de usuarios finales basada en la Web

Proofpoint Messaging Security Console™ proporciona una interfaz de administración centralizada y basada 100% en la web para el marco de la gestión unificada de las políticas de Proofpoint, la que asegura la aplicación sistemática de las políticas corporativas de mensajería. La consola facilita el monitoreo y control de su infraestructura de mensajería y define las políticas de mensajería. Puede incluso definir e imponer distintas políticas para distintos grupos de usuarios finales o dominios. A medida que añade funciones adicionales de Proofpoint a su despliegue, se utiliza la misma práctica interfaz para la gestión de políticas.

La interfaz basada en Ajax le proporciona una personalización de tipo drag and drop (arrastra y suelta) de los informes, la información de estado, los alimentadores RSS y otros componentes que puedan aparecer. Puede incluso crear mashups de información de fuentes externas.

La excepcional facilidad de uso de Proofpoint se extiende también a los usuarios finales. Los informes y controles fáciles de entender, así como el resumen para el usuario final de Proofpoint, la cuarentena basada en la web y los listados de seguridad y bloqueo personalizados proporcionan a los usuarios el control total sobre sus propias preferencias de spam. Las interfaces de usuario final pueden personalizarse fácilmente con el uso del GUI administrativo de Proofpoint.

### Sólida generación de reportes

La consola proporciona también acceso a más de 60 reportes y alertas gráficas en tiempo real que le permiten visualizar en su totalidad el sistema de mensajería de su empresa. Los informes pueden enviarse por correo electrónico o publicarse fácilmente como HTML o XML. Los informes “activos” de Proofpoint suministran información clave, pero también permiten a los administradores accionar inmediatamente (p. ej., pulsar simplemente un enlace para bloquear un remitente abusivo).

## Administración cero

### Protección permanentemente actualizada, máxima facilidad de administración

Los dispositivos Proofpoint aprovechan la potencia de los recursos informáticos “en las nubes” de Proofpoint para mantener su empresa segura y minimizar el mantenimiento continuo. Proofpoint Dynamic Update Service asegura que su red disponga siempre del máximo nivel de protección contra las amenazas contenidas en los correos electrónicos. Proporciona actualizaciones permanentes para cada componente de su despliegue Proofpoint, incluidos el SO (sistema operativo) reforzado y el ATM (agente de transporte de correo electrónico), los motores de spam y virus, los diccionarios de cumplimiento, los componentes de las aplicaciones y las reparaciones “en caliente” personalizadas.

# Proofpoint: a la vanguardia en seguridad de correo electrónico y prevención de pérdida de datos

## encripte información sensible

**Proofpoint Encryption™** añade poderosas capacidades de encriptación de correos electrónicos basadas en políticas a su despliegue Proofpoint y encripta sus mensajes automáticamente según las políticas de su organización. Aplica de forma automática y sistemática sus políticas de encriptación sin que los usuarios finales deban tomar medidas especiales. La solución Proofpoint ENTERPRISE SaaS, y el hardware y dispositivos virtuales de Proofpoint, admiten también certificados digitales y habilitan la transferencia y recepción de correos electrónicos seguros de gateway a gateway mediante el uso de la Seguridad de la Capa de Transporte (TLS, por sus siglas en inglés).

## optimice su infraestructura de mensajería

Amplíe su despliegue Proofpoint con una variedad de mejoras que perfeccionan la facilidad de uso y el manejo de su infraestructura de correo electrónico.

La solución de archivo de correos electrónicos a pedido **Proofpoint ARCHIVE™** enfrenta los desafíos de la gestión de almacenamiento, la producción de prueba y el cumplimiento de normativas sin el desgaste involucrado en el manejo de un archivo de correo electrónico interno. La tecnología patentada DoubleBlind Encryption™ protege sus datos en tránsito o “en las nubes”. **Proofpoint Smart Search™** mejora las funciones de registros integrados e informes de Proofpoint con rastreo avanzado de mensajes y con capacidades de análisis de registros y técnicas forenses, ofreciendo una visibilidad sencilla en tiempo real de los flujos de mensajes. Busque, analice y exporte registros de mensajes desde una GUI adecuada, fácil de usar, incluso entre despliegues de Proofpoint distribuidos internacionalmente. **Proofpoint Secure File Transfer** añade capacidades de transferencia segura y archivos pesados a su despliegue. Permite a los usuarios finales enviar rápida y fácilmente archivos pesados o archivos que requieren una máxima seguridad, manteniendo al mismo tiempo esos archivos adjuntos fuera del servidor de su correo electrónico.

## alto rendimiento, fácil despliegue, óptima escalabilidad

Proofpoint fue diseñado para satisfacer las necesidades únicas de grandes empresas, ISP (proveedores de servicios de Internet), universidades y organizaciones gubernamentales. Ya sea que lo despliegue como SaaS, appliance o software, Proofpoint ofrece todas las funciones de rendimiento, flexibilidad, escalabilidad, personalización y control de usuarios finales necesarios en los despliegues a gran escala.

Todos y cada uno de los componentes del sistema Proofpoint están diseñados para satisfacer las rigurosas exigencias de rendimiento empresarial. Desde el sistema operativo de mensajería optimizado y reforzado, hasta la arquitectura única sin cola de Proofpoint que permite que todas las funciones de exploración de mensajes se lleven a cabo en la memoria, Proofpoint proporciona el alto rendimiento y la seguridad requeridos incluso en los despliegues más sofisticados.

Los dispositivos Proofpoint pueden escalarse indefinidamente para admitir millones de mensajes diarios. Pueden desplegarse fácilmente en configuraciones maestro/agente para admitir centros de datos complejos o distribuidos geográficamente, lo que ofrece la seguridad de una redundancia del 100% combinada con la conveniencia de una única interfaz administrativa. Proofpoint admite incluso el trabajo simultáneo de despliegues híbridos con hardware, dispositivos virtuales y SaaS.

La arquitectura de escalabilidad óptima de Proofpoint le permite manejar todos los servidores agentes desde una única consola maestra. La propagación automática de la configuración, una cuarentena centralizada de mensajes y la generación centralizada de informes simplifican el mantenimiento y reducen el coste total de propiedad.

Proofpoint reduce adicionalmente el coste total de propiedad al integrarse fácilmente con cualquier infraestructura IT, sin importar cuál sea su distribución. Una consola de comando LDAP basada en GUI y la constatación de que admite Microsoft Active Directory® facilitan la integración con los servidores de directorios. Proofpoint es compatible también con soluciones de servidores de correo electrónico sobrecargadas, incluidos Microsoft Exchange®, Lotus Notes® o cualquier otro servidor de correo electrónico SMTP, y minimiza la carga sobre éstos.

## Versión de prueba gratuita, ¡pruébela ahora mismo!

Compruebe usted mismo el poder de Proofpoint. Visite [www.proofpoint.com/trial](http://www.proofpoint.com/trial) y regístrese para descargar una versión de prueba por 45 días del dispositivo Virtual Edition de Proofpoint; o visite [www.proofpoint.com/trypod](http://www.proofpoint.com/trypod) para registrarse para una prueba gratuita de nuestra solución bandera de seguridad de correo electrónico SaaS, Proofpoint ENTERPRISE.

## Proofpoint habla su mismo idioma

Además de proporcionar un desempeño excepcional contra el spam en cualquier idioma, la política y motores de búsqueda de contenidos detectan y “comprenden” texto en cualquier idioma, inclusive los idiomas de múltiples bytes. Las políticas de prevención de pérdida de datos pueden establecer correspondencias entre palabras claves que no están en inglés y términos del diccionario escritos en caracteres internacionales, incluidos el japonés, el chino y el cirílico. Los administradores pueden crear políticas que se activan en base al idioma detectado en el contenido del correo electrónico. Por ejemplo, se pueden adjuntar exenciones de responsabilidad específicas a un mensaje saliente según el idioma en el que haya sido escrito.

Las interfaces para usuarios finales para resúmenes de mensajes y cuarentenas basadas en la web se encuentran disponibles en chino (tradicional y simplificado), holandés, inglés, finlandés, francés, alemán, italiano, japonés, polaco, portugués, ruso, español y sueco.

La GUI administrativa de Proofpoint, la documentación del producto y la ayuda en línea se encuentran actualmente disponibles en sus versiones en inglés y en japonés. Así como con las interfaces para usuarios finales de Proofpoint, los administradores pueden establecer sus preferencias de idioma individualmente.

## Versiones de dispositivos

El dispositivo Proofpoint Messaging Security Gateway se encuentra disponible en una variedad de configuraciones de hardware para admitir despliegues de cualquier tamaño. Para obtener información actualizada sobre los modelos de dispositivos Proofpoint, visite: [www.proofpoint.com/products/msg.php](http://www.proofpoint.com/products/msg.php)

## Navegadores admitidos

Todas las tareas de configuración y de administración se manejan a través de la interfaz de Proofpoint basada en un 100% en un navegador. Los navegadores admitidos son: Microsoft® Internet Explorer 6.0 o superior  
Mozilla Firefox 2.0 o superior  
Safari 3.1.1 (interfaz para usuario final únicamente)

©2009 Proofpoint, Inc. Proofpoint y Proofpoint Protection Server son marcas registradas de Proofpoint, Inc. en Estados Unidos y otros países. son marcas comerciales de Proofpoint, Inc. en los Estados Unidos y otros países. Proofpoint on Demand, Proofpoint Messaging Security Gateway, Proofpoint Email Firewall, Proofpoint Spam Detection, Proofpoint Virus Protection, Proofpoint Content Compliance, Proofpoint Digital Asset Security, Proofpoint Regulatory Compliance, Proofpoint Dynamic Update Service, Proofpoint MLX, Proofpoint Dynamic Reputation, Proofpoint netMLX, Proofpoint Smart Search, Proofpoint ENTERPRISE, Proofpoint PROTECT, Proofpoint SHIELD, Proofpoint ARCHIVE y Proofpoint Messaging Security Console son marcas de Proofpoint, Inc. en Estados Unidos y otros países. Todas las otras marcas incluidas aquí son propiedad de sus respectivos titulares. 09/09