

RETARUS EMAIL SECURITY

Alojado en la nube, **Retarus Email Security** aporta varias funcionalidades de seguridad y gestión de correo electrónico que permiten ofrecer un servicio de calidad, diferenciación y gran valor añadido.



Las ventajas que aporta Retarus son:

- No requiere infraestructura física en la red del cliente.
- Análisis anti-malware con motores de 4 fabricantes diferentes.
- Actualizaciones automáticas, a prueba de fallos.
- Pago por uso con facturación mensual, a precios asequibles.
- Sin compromiso de permanencia.

Las soluciones de Retarus se comercializan a través de Proveedores de Servicios autorizados, en modo pago por uso con facturación mensual.

Essential Protection with MultiScan

Un servicio de seguridad completa para el correo electrónico, a un precio asequible. Alojado en la nube, es muy fácil de implantar y de administrar. Este servicio incluye las siguientes prestaciones:

- Antivirus MultiScan x4
- Anti-spam Management
- Phishing Filter
- External Sender Visibility Enhancement
- Attachment Blocker
- Directory Filter
- Large Email Handling

Ninguna otra solución del mercado ofrece esta funcionalidad, a un precio tan atractivo.

PVP recomendado: 1 euro por usuario/mes*

Premium Protection

La versión Premium aporta toda la funcionalidad de Essential Protection con MultiScan, más una serie de prestaciones avanzadas tales como Sandboxing, mitigación de ataques de día cero, y mucho más:

- Deferred Delivery Scan
- Sandboxing
- Time of Click Protection
- CxO Fraud Protection
- Patient Zero Detection
- Patient Zero Detection Reacting Process

Este servicio está diseñado para las empresas más exigentes que quieren una protección avanzada de su correo electrónico. Se trata de un servicio de gama alta, a un precio muy competitivo.

PVP recomendado: 3,50 euros por usuario/mes*

* PVP recomendado para un volumen de 25 usuarios. El partner se beneficia de descuentos por volumen según el total número de usuarios activos.

Funcionalidades incluidas en Retarus Essential Protection with MultiScan

Antivirus MultiScan x4

Los mensajes entrantes y salientes (incluyendo ficheros adjuntos) se analizan con sistemas anti-malware de 4 fabricantes diferentes, ofreciendo así las mejores tasas de detección de malware.

Anti-spam Management

Se analizan los mensajes entrantes con un sistema avanzado anti-spam, que combina diferentes reglas y algoritmos de detección.

Phishing Filter

El sistema anti-phishing de Retarus analiza las URLs que contienen los mensajes entrantes y los contrasta con fuentes conocidas de Phishing.

External Sender Visibility Enhancement

El sistema detecta posibles casos de Spoofing y los marca visiblemente, avisando al usuario de que debe prestar especial atención.

Attachment Blocker

Esta funcionalidad permite bloquear o meter en cuarentena los mensajes que contienen ficheros adjuntos peligrosos (ejecutables, ficheros Office con macros, etc).

Directory Filter

Se rechazan los mensajes dirigidos a destinatarios incorrectos, protegiendo la empresa de ataques DoS y Directory Harvesting. Asimismo, utiliza validación SPF y DKIM para detectar remitentes no legítimos.

Large Email Handling

En caso de superar el límite establecido del tamaño de ficheros adjuntos, no se bloquea el mensaje entero: los usuarios recibirán un mensaje, con un enlace que les permitirá descargar los ficheros por separado.

Opciones adicionales

Quiet Time

Se pueden definir periodos de tiempo durante los cuales no se entregarán mensajes externos a los usuarios.

Inbox Assist

Esta opción permite a ciertos usuarios reenviar automáticamente los mensajes entrantes a otra persona, y delegar la gestión de su correo.

Email Signature

Esta funcionalidad permite gestionar las firmas y textos legales que deben aparecer al final de cada mensaje, asegurando el cumplimiento de la política corporativa.

Funcionalidades adicionales incluidas en Retarus Premium Protection

Deferred Delivery Scan (DDS)

El módulo DDS facilita la detección de ataques de día cero. Los mensajes que contienen ficheros adjuntos, son analizados cuando llegan y, tras un periodo de tiempo establecido, son analizados de nuevo, antes de entregar el mensaje.

Sandboxing

Los emails que contienen ciertos tipos de ficheros son sometidos a un análisis profundo. El código ejecutable se copia a un entorno virtualizado, y se ejecuta para ver su comportamiento; de esta forma se analiza lo que el fichero hace, y no solo lo que contiene.

Time of Click Protection

Se modifican las URLs que llegan a través del correo electrónico, de modo que cuando el usuario hace clic, el tráfico es dirigido a la plataforma de Retarus para que se pueda verificar si representa un peligro para el usuario o la organización.

CxO Fraud Detection

Se trata de un sistema que identifica ataques utilizando los métodos de from-spoofing y domain-spoofing (falsificación de remitente).

Patient Zero Detection (PZD)®

Se trata de una tecnología propietaria y patentada de Retarus, que permite identificar malware en los mensajes que ya han sido entregados y avisar al destinatario.

PZD Reacting Process

Al detectar un malware en un email que ya ha sido entregado, permite responder rápidamente, minimizando el riesgo de contagio. Es posible eliminar los mensajes del servidor de forma automática, e incluso notificar a las personas que han recibido una copia en caso de que el usuario lo haya reenviado.

Más información

Para más información, visite www.retarus.com/es/ o desde la web de IREO, su mayorista en España: www.ireo.com.

Si tiene alguna pregunta o necesita más información, póngase en contacto con IREO enviando un correo electrónico a info@ireo.com o llamando al teléfono 91 312 13 86.