

## Lo nuevo en Outpost Firewall Pro 4.0

### La solución definitiva en protección proactiva

La nueva versión de **Outpost Firewall Pro** de Agnitum es la solución definitiva para la protección de la información electrónica vulnerable.

Con este lanzamiento, se introduce un nuevo estándar para las aplicaciones de seguridad informática: Outpost brinda a los usuarios el más alto nivel posible, en protección proactiva, contra programas espías provenientes de Internet, aplicaciones que obtienen claves de acceso, troyanos y otras tentativas desautorizadas de tener acceso a los datos del ordenador - incluso de aquellos que funcionan con tecnología **Windows** de 64-bits.

Principales novedades en esta versión de Outpost Firewall Pro:



#### Tecnología para prevenir la fuga de información, realmente efectiva

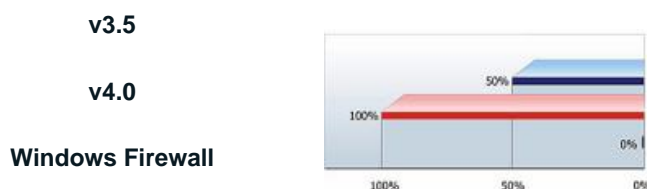
Las pruebas de fuga (*Leak test*) comprueban la eficacia de una aplicación cortafuegos, en la prevención de la pérdida de información personal, a través de los filtros de salida.

Outpost Firewall Pro 4.0 puede bloquear todas las técnicas existentes utilizadas para el robo de datos confidenciales del ordenador de un usuario, como, por ejemplo, los programas espía.

✍ Para más información sobre las pruebas de fuga, [consulte nuestro documento específico](#).

Además de las funciones expuestas, para la prevención de fugas, las nuevas características de Outpost Firewall Pro 4.0, en esta materia, incluyen:

#### Cantidad de pruebas de fuga superadas



#### Prevención personalizada contra intentos, no autorizados, de controlar aplicaciones confiables

Los usuarios pueden modificar la lista de las aplicaciones confiables para realizar transferencias de datos y prevenir tentativas de acceso de programas enmascarados como legítimos.

#### Supresión de los intentos de apertura de un navegador, a través de ejecución de parámetros por línea de comandos

Muchos programas se pueden configurar para que abran ventanas de navegación cuando un usuario pulsa en un vínculo a una dirección de Internet, como por ejemplo, en Microsoft Outlook, Microsoft Office e ICQ, entre otros. Para evitar, que programas maliciosos realicen estas aperturas indeseadas, los usuarios pueden modificar la lista de las aplicaciones que tienen permiso para abrir este tipo de ventanas.

#### Control configurable sobre la utilización de la memoria por parte de las aplicaciones

Los usuarios pueden modificar la lista de aplicaciones confiables y evitar que códigos maliciosos utilicen el espacio de memoria asignado a uno de estos programas durante su ejecución.

## Control sobre el escritorio activo

Los componentes del escritorio activo pueden contener código malicioso que transfiera datos confidenciales, hacia el exterior, en nombre del explorador de Windows.

Outpost evita la instalación o ejecución de dicho código.

## Prevención de intentos de controlar las ventanas de otras aplicaciones

Los programas maliciosos pueden emular la pulsación de teclas, en otras ventanas del programa, y hacer transferencias de datos no autorizadas, entre dichas ventanas.

Outpost Firewall Pro 4.0 detecta, ahora, tales tentativas, las comprueba para saber si hay legitimidad y bloquea cualquier intento ilegítimo de transferir datos.

## Prevención de intentos de modificar entradas críticas del registro

El registro de Windows contiene casi todos los parámetros de configuración de las aplicaciones instaladas. Los usuarios pueden personalizar la lista de aquellas que tienen permitido realizar cambios en dicho elemento fundamental del sistema operativo.

## Doble control en la resolución de DNS

Las técnicas avanzadas de piratería permiten que los intrusos roben datos mediante peticiones DNS malformadas, que ahora se bloquean completamente.

## Control de acceso a la red de bajo nivel

El código malicioso, una vez instalado en el sistema del usuario, puede simular una actividad normal y así iniciar conexiones salientes ilegítimas. Outpost detecta tales tentativas, alerta al usuario y exhibe un aviso para actuar en consecuencia.



## Insuperable control anti-espía

Los ingenieros de Agnitum han aumentado perceptiblemente el nivel de protección contra aplicaciones espía. Así es cómo la monitorización de Outpost Firewall Pro 4.0 se realiza ahora con mayor eficacia, detectando y quitando toda aplicación espía, sea conocida o desconocida:

## Mejora en el rendimiento del sistema

Se ha implementado un nuevo método para comparar los programas con la base de datos de aplicaciones espía, lo que aumenta perceptiblemente la velocidad del análisis.

## Protección adicional que ahora cuenta con la opción “Análisis previo a la ejecución”

Todos los programas, sin excepción, son analizados antes de otorgarles permiso de ejecución.

Para hacer esto, Outpost Firewall Pro 4.0, simula la ejecución del programa en un contenedor seguro, permitiendo la realización, controlada, de pruebas sobre programas sospechosos (*Sandbox*) para legitimarlo, antes de permitir o de bloquear su ejecución real.

El rendimiento del sistema no se ve afectado.

## Nuevo analizador de firmas de programas espía

El desarrollo de nuevos algoritmos, más exactos y precisos, para la detección de programas espía, aumentan la protección de los usuarios contra código malicioso conocido y desconocido.



## Autoprotección

Outpost Firewall Pro 4.0, incluye ahora, un modo de autoprotección que actúa como defensa, alrededor del programa, para evitar que la aplicación cortafuegos, sea desactivada por virus, troyanos o programas espía.

Incluso se detectan y detienen las tentativas de cerrar la aplicación cortafuegos, simulando pulsaciones del teclado.

Outpost supervisa continuamente sus propios archivos en los discos duros, así como también sus entradas en el registro del sistema, estado de la memoria, ejecutando el programa *servicesand*, utilizado para bloquear cualquier cambio promovido por programas malintencionados. Este modo de autoprotección puede ser activado y desactivado por el usuario, permitiendo la instalación de nuevos complementos y otros ajustes de la configuración realizados por usuarios más experimentados.



## Mejoras en ImproveNet

En la versión 4.0, **ImproveNet** recopila información a nivel del ordenador local sobre cómo se produce la interacción entre los diversos programas.

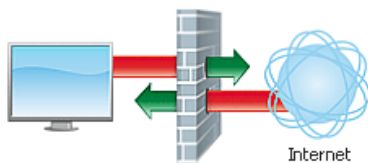
Estas nuevas reglas locales se actualizan de forma automática para usuarios que han habilitado el servicio ImproveNet y, se utiliza para distinguir entre las actividades seguras e inseguras.

Este acercamiento proporciona un nuevo nivel de seguridad para los procesos locales.

**ImproveNet** fue introducido en una versión anterior de Outpost Firewall Pro, como el medio para ahorrar tiempo y proporcionar seguridad adicional, recogiendo, aprobando y redistribuyendo reglas de uso general, entre usuarios de la aplicación.

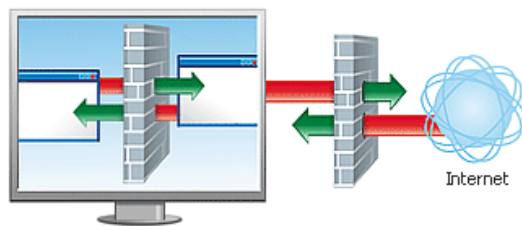
### ImproveNet 3.5

En Outpost Firewall Pro 3.51, las reglas que reciben los usuarios suscriptos a ImproveNet, afectan las conexiones de entrada y de salida.



### ImproveNet 4.0

En Outpost Firewall 4.0, los usuarios reciben un nuevo nivel de protección, ya que además de las características mencionadas, la interacción entre los programas se encuentran controladas por reglas de seguridad, que son distribuidas, globalmente, entre los usuarios suscriptos a este servicio.



## Mejoras en la usabilidad

### Modo entretenimiento

Cuando un usuario está interactuando con juegos sumamente intensos o está mirando una película en línea, no desea ser interrumpido por peticiones de la aplicación cortafuegos, para tomar una decisión respecto de permitir o rechazar una conexión en particular.

Outpost Firewall Pro 4.0 ofrece ahora el modo **Entretenimiento**, que suprime los mensajes emergentes de la aplicación cortafuegos cuando se están ejecutando determinados programas específicos de una lista configurable por el usuario. El cambio al modo Entretenimiento no afecta el nivel de seguridad de la aplicación cortafuegos y permite a los usuarios concentrarse en su tarea específica.

### Para usuarios experimentados:

#### Reglas para adaptar la aplicación cortafuegos

Outpost Firewall Pro 4.0 incluye ahora la posibilidad de definir guiones para los programas; esto le permite, a los usuarios, indicar manualmente y en forma individual las reglas de seguridad para las aplicaciones y los servicios basados en Windows.

Por ejemplo, ahora es posible elegir establecer limitaciones a las peticiones DNS, de la lista de servicios DNS indicados en el adaptador de red.

Si el proceso de resolución DNS está intentando alcanzar un servidor que no se encuentra habilitado, se le consultará al usuario respecto de permitir o bloquear esta acción.

## Conclusión

Con el lanzamiento de Outpost Firewall Pro 4.0, los usuarios de ordenadores personales alrededor del mundo, pueden experimentar en profundidad, las ventajas de poseer lo último en protección proactiva y con un excelente nivel de usabilidad, en un cortafuegos personal de bajo coste, y además, disponible también para sistemas operativos con tecnología de 64 bits.

## Actualización a la versión 4.0

Los usuarios que tengan su licencia aún vigente, podrán actualizar a la versión 4.0 sin coste alguno.

Consulte en la página de [soporte](#) las instrucciones correspondientes.

## ¡Ahora sí, pruebe Outpost Firewall y no lo abandonará jamás!

[Descargue](#) la versión de evaluación de Outpost Firewall Pro totalmente funcional y válida por 30 días, y acceda a la mejor protección para su ordenador y sus datos.

☑ Para continuar usándolo posteriormente, sólo será necesario activar el producto, adquiriendo la correspondiente licencia.