

## Hoja de ruta de Outpost Security Suite 5.0

### ¿Por qué es necesaria la protección proactiva?

La situación de Internet actual, merece un enfoque completamente nuevo hacia la seguridad: prácticamente todo está interconectado, y sucediendo en tiempo real. Y esto incluye las amenazas.

Una aplicación de seguridad eficaz, debe estar alerta permanentemente ante la aparición de códigos maliciosos novedosos y arteros.

Las nuevas clases de amenazas requieren nuevos tipos de protección. Los gusanos y virus de distribución masiva están cediendo el camino a los ataques motivados por intereses económicos. Estos están diseñados para robar identidades, dinero y otras mercancías, valiéndose de técnicas especializadas de fraude en línea (*phishing*) y de la ingeniería social.

Para ofrecer una protección completa ante estas nuevas amenazas, una solución de seguridad eficaz debe desplegar una estrategia de varios niveles, ofreciendo un bloqueo proactivo y que contemple el comportamiento de los procesos, además de la detección tradicional basada en firmas. También debe ser fácil de usar, o en caso contrario los usuarios no la utilizarán.

**Outpost Security Suite Pro**, la nueva aplicación de Agnitum construida en base a la aclamada protección de Outpost Firewall Pro, combina lo mejor de ambos enfoques en un único producto integral, que brinda protección personalizada y confiabilidad absoluta.

**Outpost Security Suite Pro** protege sus preciados tesoros electrónicos las 24 horas del día, los siete días de la semana, sin importar las actividades que esté realizando.

### Beneficios clave



El cortafuegos multipremiado controla las conexiones de su ordenador con otras máquinas, bloqueando códigos maliciosos e intrusiones de piratas informáticos.



La protección del *host* monitoriza las interacciones y el comportamiento de los programas, para defender proactivamente al sistema contra actividades no autorizadas, bloqueando troyanos y programas espía sin necesidad de verificar firmas.



Los archivos ejecutables y componentes internos de la aplicación son bloqueados, para asegurar así que no podrán ser desactivados o interrumpidos por un ataque dirigido.



El analizador multipropósito contra códigos maliciosos detecta y elimina programas espía, virus, gusanos y otras amenazas, utilizando un único motor integrado para asegurar un trabajo eficiente, y minimizar el impacto en el rendimiento del sistema.



El módulo contra correo no solicitado mantiene la bandeja de entrada libre de mensajes indeseados, y gracias a su capacidad de autoaprendizaje, su rendimiento mejora aún más con el paso del tiempo.

Protección proactiva significa que su ordenador está asegurado contra la mayoría de las amenazas existentes y futuras, incluyendo *rootkits*, virus del tipo *zero-day*, y troyanos que registran pulsaciones de teclas, incluso antes de conectarse a Internet.

**Outpost Security Suite Pro** ha sido diseñado para satisfacer las exigencias de los usuarios más experimentados, que comprenden la necesidad de una seguridad robusta y eficiente.

Además de brindar la mejor protección inmediatamente, **Outpost Security Suite Pro** también incluye una amplia variedad de opciones y parámetros adaptables para que los usuarios avanzados configuren la aplicación a su medida.

Para los usuarios menos expertos, Outpost permite definir y aplicar automáticamente la mayoría de las opciones y definiciones, eliminando así potenciales errores de configuración.

Sus controles accesibles, y la intuitiva interfaz, aseguran la facilidad de manejo, independientemente del nivel de experiencia del usuario.

## Características clave

### Salvaguardias proactivas

#### Protección superior contra amenazas

La **protección del host** de Outpost Security Suite Pro monitoriza la actividad de los programas, bloqueando transacciones no autorizadas y los intentos del código malicioso por operar directamente o secuestrando otras aplicaciones.

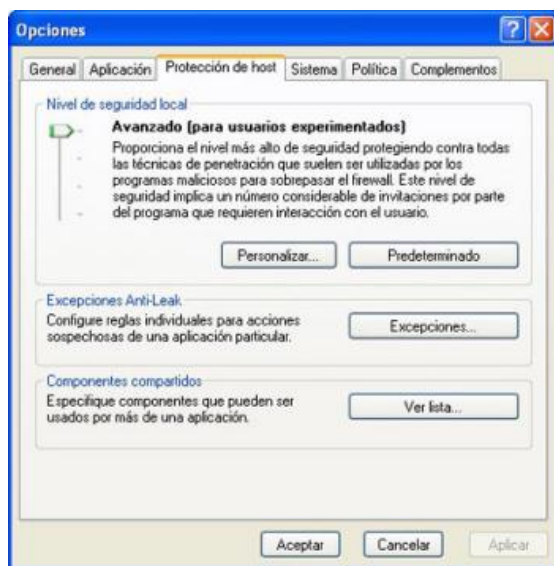
Esta es la primera línea de defensa contra las nuevas técnicas de las amenazas actuales, que podrían escapar al control de las tradicionales soluciones basadas en verificación de firmas.

#### Protección contra intrusiones

La tecnología proactiva de detección de ataques, detecta y rechaza automáticamente todo tipo conocido de ataques de piratas informáticos.

#### Autoprotección

Al incorporar una sólida defensa contra la manipulación de todos sus componentes, Outpost Security Suite Pro asegura que nadie podrá deshabilitar la protección activa, excepto el usuario del programa autorizado.



### Eficiencia contra el código malicioso

#### Defensa total contra el código malicioso

Un nuevo motor universal contra códigos maliciosos proporciona una mayor capacidad de defensa antivirus y contra programas espía.

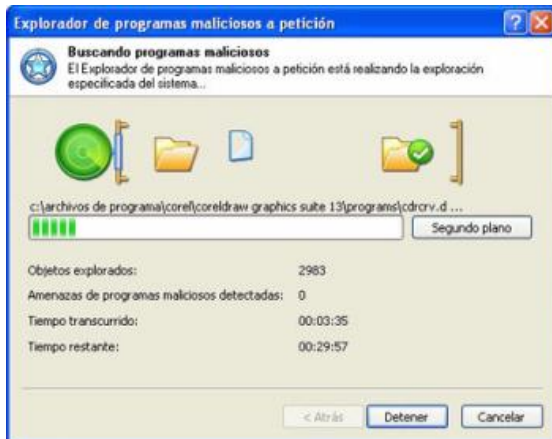
El monitor de acceso residente elimina o aísla instantáneamente cualquier objeto malicioso que encuentre en las áreas clave del ordenador.

Conjuntamente, el analizador a petición del usuario, permite verificar y desinfectar amenazas en los discos duros, carpetas de red, discos ópticos y dispositivos de almacenamiento externos, cuando se crea conveniente. El usuario puede especificar ubicaciones o tipos de archivos que desea excluir de los análisis regulares, si tiene la certeza de que estos no son vulnerables a una infección.

Los archivos adjuntos en los mensajes de correo electrónico se verifican en tiempo real, apenas llegan o antes de ser enviados. También se puede mover manualmente al área de cuarentena un documento sospechoso, para su revisión posterior.

El motor universal no tiene impacto alguno sobre el rendimiento general del sistema, y trabajará en segundo plano mientras el usuario realiza sus tareas habituales.

**SmartScan**, el monitor inteligente, analiza solamente las porciones del sistema de archivos que se han modificado. De este modo, evita repetir la verificación de elementos que no han cambiado desde el último control.



## Continuidad y seguridad de la red

### Seguridad de las conexiones

El cortafuegos de doble dirección monitoriza las conexiones entrantes y salientes del ordenador, y previene intrusiones no autorizadas en la red, tanto locales como remotas.

Al ocultar los puertos de acceso, mantiene invisible su presencia en Internet.

El módulo de protección específicamente diseñado, resguarda las conexiones de la red de área local (LAN, *Local Area Network*), y evita el sabotaje interno controlando la transmisión de los datos que circulan en ella. Esto elimina el posible riesgo de que los datos contenidos en ventanas de conversación (*chat*) o en sesiones autenticadas del navegador, sean entregados al destino equivocado, o interceptados en el camino.

### Control de acceso a las aplicaciones

El cortafuegos controla cuáles son los programas que tienen permiso para acceder a Internet, protegiendo proactivamente el ordenador contra los intentos del código malicioso por establecer conexiones ilegítimas, y las amenazas del tipo *zero-day*.



## Control y monitorización

### Monitorización de la actividad de la red

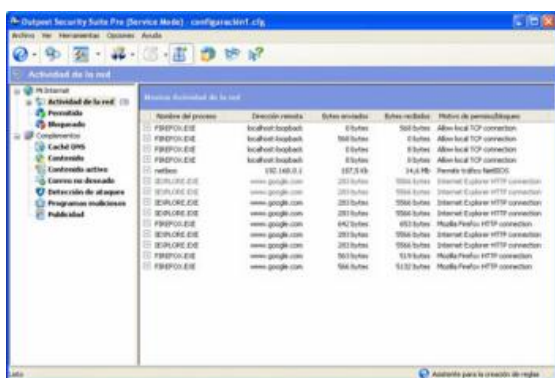
El monitor de actividad de la red muestra todas las conexiones que el ordenador establece con otras máquinas en Internet o en la red local. Así, es posible controlar permanentemente las acciones que se están llevando a cabo, y cerrar rápidamente cualquier enlace no autorizado.

### Registro de eventos

El visor de registros muestra el historial completo y detallado de la actividad del ordenador, para que el usuario pueda revisar qué ha ocurrido en el sistema en el pasado, o identificar un problema tempranamente y corregirlo. La personalización de los filtros asegura que solo se verá la información deseada, obviando eventos irrelevantes o reiterados. Incluso puede configurarse la exclusión de ciertos tipos de comunicaciones, como el tráfico NetBIOS.

### Protección por contraseñas, configuración de múltiples perfiles

Es posible definir contraseñas para proteger su configuración de modificaciones accidentales o deliberadas, así como también crear y utilizar múltiples perfiles que se adapten a los niveles de riesgo o de tolerancia particulares. Los usuarios experimentados pueden construir varios puntos de restauración gracias al comando de configuración guardar/cargar.



## Compatibilidad y flexibilidad

### Reglas adaptables del cortafuegos

Al viajar con ordenadores portátiles, o cambiar el proveedor de servicios de Internet, no es necesario ajustar manualmente la seguridad para la nueva conexión, porque Outpost lo hará automáticamente. Con solo designar parámetros de conexión específicos (por ejemplo servidores de nombres de dominio o de direcciones de puertos de enlace) como variables de entorno, el ordenador está automáticamente equipado para proteger las conexiones nuevas tan pronto como registra el cambio.

### Modo entretenimiento para no interrumpir sesiones de juego o de reproducción de vídeos

Al ejecutar juegos en pantalla completa, o mirar vídeos en el ordenador, el modo entretenimiento de Outpost asegura que la aplicación no interrumpirá al usuario con alertas si detecta alguna actividad nueva. Estas notificaciones se manejan en segundo plano, sin afectar los niveles de protección establecidos. Es posible configurar las aplicaciones que activarán automáticamente el modo entretenimiento.



## Privacidad

### Protección contra el correo no solicitado

El nuevo motor contra el correo basura mantiene la bandeja de entrada libre de mensajes indeseados.

Utilizando sofisticados algoritmos bayesianos camuflados bajo una interfaz de usuario simple, el sistema puede ser entrenado para reconocer y usar definiciones personales de correo no solicitado. Esto lo hace aún más eficiente, y un gran aliado para ahorrar tiempo a medida que se utiliza.

### Protección de datos personales

Ningún tipo de información confidencial, como números de cuentas bancarias y contraseñas, que el usuario defina utilizando el bloqueo de ID, podrá sobrepasar los límites del ordenador a través de rutas de comunicación tales como mensajería instantánea, Internet o correo electrónico.

Esto aumenta sensiblemente la protección contra el robo de identidad y otras técnicas de estafa en línea (*phishing*). Además, asegura que nadie más, incluyendo niños y familiares, pueda divulgar esta información accidental o deliberadamente en la Red.

### Navegación más clara y confidencial

Gracias al control de *cookies*\* y de referencias a páginas previamente visitadas, se puede mantener un alto nivel de privacidad al navegar por sitios de compras, entretenimiento o noticias, y al mismo tiempo, permitir que los sitios de confianza obtengan solamente los datos de los hábitos de navegación del usuario necesarios para personalizar sus páginas.

☑ Una *cookie* es un pequeño archivo de texto, que un sitio web coloca en el disco duro del ordenador que lo visita, y que queda almacenado. Este archivo sirve para identificar al usuario cuando se conecta de nuevo a dicha página.

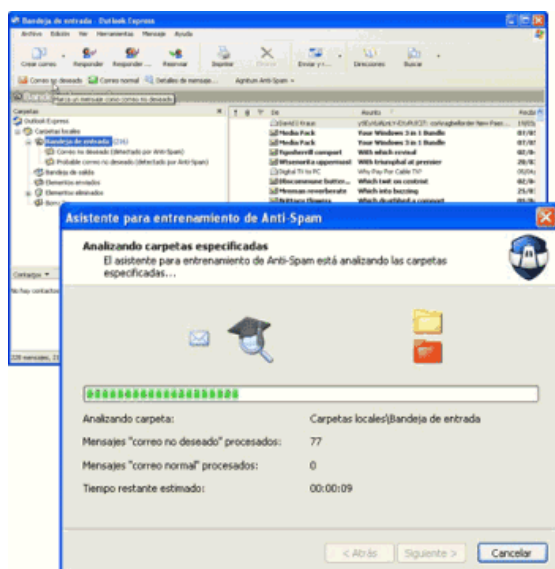
Además, **Outpost Security Suite Pro** proporciona la posibilidad de limitar los elementos que se muestran en las páginas web, bloqueando selectivamente imágenes, publicidad, avisos emergentes, controles ActiveX o ejecución de guiones, para que la navegación sea más rápida y libre de estorbos.

### Administración de contenido

Los usuarios pueden definir una lista de palabras y frases que serán bloqueadas, y no se mostrarán en los sitios donde aparezcan.

Esta característica es particularmente valiosa para los padres que no quieren que sus hijos estén expuestos a contenidos inapropiados.

También existe la opción de bloquear el acceso a sitios específicos.



## Conveniencia y facilidad de uso

### Configuración automática para mayor simplicidad

Para la mayoría de los programas que acceden a Internet, las reglas se aplican automáticamente, aliviando al usuario el trabajo de cargar las reglas manualmente cada vez que una aplicación nueva se conecta a la Red, o interacciona con otro programa.

Existe un amplio rango de políticas de acceso predefinidas, asignadas a programas particulares. La opción de incluir aplicaciones que acceden a Internet al inicio o en otro momento, también contribuye con la funcionalidad de Outpost.

### Servicio ImproveNet para facilitar la configuración

ImproveNet es un sistema voluntario de distribución e incorporación de configuraciones del programa, que refleja las situaciones reales en las que las personas usan la aplicación.

Las reglas remitidas por los usuarios de Outpost, después de ser revisadas y aprobadas por los ingenieros de Agnitum, se distribuyen a todos los suscriptores. De esta forma, se obtienen las reglas más seguras y actualizadas.

### SmartAdvisor: ayuda inmediata y sensible al contexto

Si ImproveNet no tiene la respuesta, **SmartAdvisor** está permanentemente a disposición del usuario, para ayudarle a tomar la decisión correcta al configurar la información de acceso para una aplicación.

### Instalación automática

Todo el proceso de instalación y la configuración inicial son automatizados, con el fin de facilitar su uso para los usuarios con menos conocimientos técnicos.

El asistente de instalación, recomendado para quienes tengan más experiencia en instalar y configurar cortafuegos, permite la personalización y selección de parámetros de operación específicos.

### Actualizaciones sin intervención del usuario

Siempre que se lance una actualización de **Outpost Security Suite Pro** durante el periodo de validez de la licencia del producto, el módulo de actualización del programa automáticamente descargará la última versión desde el servidor de Agnitum, y la aplicará tan pronto como el usuario dé su autorización.

