

Hoja de ruta de Outpost Network Security

Desafío de seguridad

Todos los meses, alguno de los ordenadores corporativos conectados a Internet se enfrenta con alrededor de doscientas nuevas amenazas a la seguridad.

Las medidas de protección tradicionales, como los antivirus y los sistemas de detección de intrusos, ya no son suficientes, especialmente cuando un código malicioso como el gusano *Slammer* puede propagarse en pocos minutos antes que se libere una actualización de una firma de virus.

Además, el usuario está bajo amenaza por parte de los agentes espía, los troyanos de acceso remoto, los componentes maliciosos insertados en las páginas de Internet, *zombis* destructivos y ataques distribuidos por piratas informáticos.

Teniendo en cuenta que estas amenazas pueden venir tanto desde afuera como desde adentro del perímetro de una red, no se puede subestimar el desafío de lograr una seguridad completa e integral.

Lo que resulta más preocupante de todo esto, es que esas amenazas imparables y automatizadas, no reconocen si se enfrentan a sólo una pequeña red con algunos ordenadores o a una gran corporación con cientos de equipos.



La mejor elección

La mejor decisión posible para una corporación, es implementar medidas de seguridad proactivas que no dependan de actualizaciones como los antivirus y los sistemas de detección de intrusiones.

La solución recomendada es la tecnología del cortafuegos, que constantemente controla y regula el tráfico que los ordenadores reciben y envían.

A diferencia del programa antivirus, un cortafuegos reconoce a un código malicioso no por su "descripción" sino por su "comportamiento".

Los cortafuegos físicos son una buena opción para empezar a construir la seguridad, pero no son tan flexibles como las aplicaciones cortafuegos y, además, no pueden encargarse de las amenazas internas.

Outpost Network Security de Agnitum ofrece una solución económica para proteger, a los ordenadores terminales de una red corporativa, de las amenazas externas e internas.

Outpost Network Security está basado en nuestro mejor cortafuegos personal, proporcionando un arsenal de defensa superior, al mismo tiempo que permite al usuario, implementar, configurar y actualizar centralmente el programa en cada ordenador cliente.

Esto hace de Outpost Network Security el elemento central de una protección de varias capas dentro de las medidas de seguridad modernas.

Cómo reducir los riesgos

Outpost Network Security protege la oficina de todos los peligros conocidos de Internet, implementándose automáticamente y configurando el cliente, en las estaciones de trabajo seleccionadas a través de la red corporativa. Inmediatamente después de ser instalado, el cortafuegos cliente comienza a proteger las terminales, a través del control de la información entrante y saliente y, aplicando reglas específicas para cada tipo de información.



Filtrado de aplicaciones

Outpost Network Security filtra todas las aplicaciones que acceden a la red al enviar o recibir información.

Si se utilizan las reglas del cortafuegos, los administradores de la red podrán aplicar políticas específicas de seguridad, a través de la restricción de puertos y protocolos determinados para las aplicaciones. Esto no sólo ayuda a reforzar la seguridad del puesto de trabajo, sino que también evita el mal uso de la red por parte de los empleados.

Prevención de ataques

El complemento **Detección de ataques** automáticamente evita todos los ataques conocidos de Internet contra un ordenador cliente.

Permite una configuración flexible por puertos y proporciona una alta seguridad contra las intrusiones de los piratas informáticos.

El cortafuegos brinda protección contra todas las brechas conocidas de seguridad: supera todas las últimas pruebas de fuga, asegurando que la protección del cliente sea completa y sólida, para que no exista ninguna fuga de información privada.

Protección contra códigos maliciosos

Por medio del empleo de las tecnologías: **Control de componentes**, **Control de procesos ocultos**, y **Control de procesos abiertos**, Outpost no permite que las aplicaciones maliciosas se activen como parte de programas legales, y de esta forma protege a los clientes de: troyanos, programas espía y tantos otros peligros.

Además, el complemento **Cuarentena de archivos adjuntos** analiza los correos electrónicos entrantes en busca de adjuntos peligrosos y les cambia el nombre a aquellos sospechosos.

Esta característica evita que los usuarios abran ocasionalmente ficheros maliciosos y así protege a los ordenadores cliente de virus y gusanos.

Protección de la privacidad

Actualmente, cualquier página de Internet visitada por los empleados puede tener contenido malicioso.

En tal caso, la toma de control (de forma silenciosa) por sólo una de las estaciones de trabajo, causaría consecuencias severas en la red corporativa entera.

Los complementos integrados en Outpost Network Security Client permiten que la privacidad del cliente esté bien protegida:

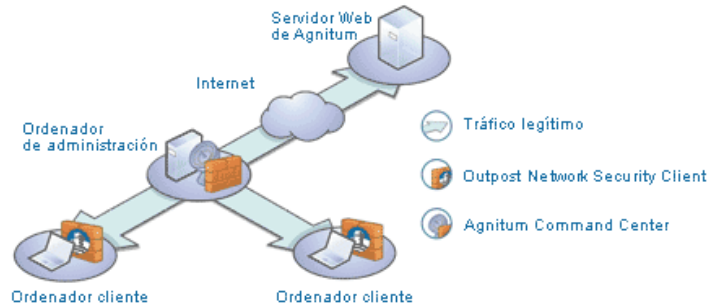
- El complemento **Contenido activo** es el encargado de controlar el código de los sitios de Internet, limitando o bloqueando la activación de guiones y otros elementos dinámicos que pudieran ser dañinos para el sistema del cliente.
También protege el historial de navegación del usuario por medio de la obstrucción flexible de *Cookies* y referencias (*referrers*).
- El complemento **Publicidad**, ahorra tiempo de navegación a los clientes así como reduce el consumo de ancho de banda al quitar las imágenes publicitarias de los sitios de Internet accedidos.
- El complemento **Contenido** permite el bloqueo de las páginas de Internet con contenido objetable o indeseado.

Eficacia en los costes

El Centro de comando de Agnitum (*Agnitum Command Center*) simplifica tres procedimientos importantes:

- Implementación
- Administración
- Actualización.

Esto ahorra tiempo y simplifica las tareas tradicionales realizadas por el administrador de la red.



Fácil de implementar

Outpost Network Security no es necesario que esté instalado en un servidor o en un controlador de dominios. Todas las herramientas de administración pueden instalarse en cualquier estación de trabajo dedicada, que cumpla con los requerimientos del sistema.

Además, el producto permite una fácil instalación y configuración masiva de las estaciones de trabajo a través de una red, y de esta forma ahorra mucho tiempo del administrador en grandes y medianas organizaciones.

Se puede utilizar la Política de grupo de Windows para la instalación automática del cortafuegos cliente en el dominio de Windows 2000 o superior.

Administración centralizada

El Centro de comando de Agnitum permite el control de la protección de las estaciones de trabajo individuales desde una ubicación central.

Toda la administración, solución de problemas y las tareas de control son realizadas desde una ubicación centralizada, ahorrando tiempo y esfuerzo del administrador, ya que así se evita visitar cada instalación y realizar las mismas operaciones varias veces.

Rápidas actualizaciones

El Servicio de actualización de Agnitum (*Agnitum Publisher Service*) proporciona actualizaciones centralizadas para los cortafuegos cliente, permitiendo la instalación múltiple, programada y desde un solo archivo. Así, se reduce el impacto del tráfico de Internet en el ancho de banda de la red, al utilizar la descarga de una sola actualización y la instalación de la misma en todos los clientes simultáneamente.

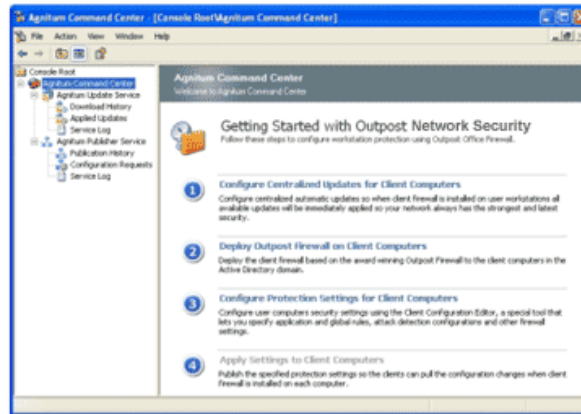
Fácil de utilizar

Outpost Network Security brinda una interfaz de usuario familiar.

La principal aplicación de administración, Agnitum Command Center, está implementada como un complemento de la Consola de administración de Microsoft (MMC).

Los parámetros de funcionamiento del cortafuegos cliente son heredados de Outpost Network Security y, el proceso de configuración de los cortafuegos cliente, es efectuado de forma rápida y sencilla.

Para más detalles sobre el proceso de administración, por favor consulte la [Guía del administrador de Outpost Network Security](#).



Requerimientos de sistema

Outpost Network Security está diseñado para ser instalado bajo sistemas operativos Microsoft Windows:

- **Especificaciones generales:**

- **Procesador**

Intel Pentium o compatible. 450 MHz o superior

- **Espacio disponible en disco duro**

50 MB

- **Memoria RAM**

- **Módulo servidor**

256 MB

- **Módulo cliente**

64 MB RAM para Windows 98 / Me

128 MB RAM para Windows 2000 / XP / 2003 Server

- **Ratón**

Microsoft o dispositivo compatible

- **Monitor**

VGA 256 colores o superior

- **Red**

Conexión de red o Internet

- **Sistema operativo:**

- **Servidor Outpost Network Security**

Windows XP / 2000 Pro ó 2003 Server

Para permitir la instalación remota:

Windows 2000 ó 2003 con controlador de dominio

- **Ordenadores cliente**

Windows 98 / 98SE / ME / 2000 / XP ó 2003 Server

Soporte Técnico

Para cualquier consulta adicional sobre Outpost Network Security visite la [página principal de soporte](#), donde encontrará una variedad de recursos y formas de contacto, a su disposición.