Aranda 360 ENDPOINT SECURITY®

STANDARD & ENTERPRISE EDITION

Proteja su infraestructura informática de las amenazas de red, asegurando completamente los datos y archivos importantes de su organización además de la información confidencial.

Beneficios

Protección frente a la posible contaminación de las aplicaciones.

Protección permanente en la navegación interna y externa de red.

Refuerzo de políticas y control de acceso a las redes de trabajo.

Administración de permisos para el uso y acceso de dispositivos.

Defensa a mayor nivel de los puntos finales, sin importar dónde y cómo sea usada la estación.

Características

Protección actualizada permanentemente.

Control de acceso a la red.

Control de instalación, acceso y uso de las aplicaciones.

Control de almacenamiento de dispositivos removibles.

Control de comunicaciones inalámbricas.

Actualmente las redes de trabajo corporativas se encuentran medianamente protegidas por tecnologías de seguridad. Es por ello que los delincuentes informáticos han cambiado sus estrategias dirigiendo sus ataques a los puntos finales de las empresas (servidores, estaciones de trabajo, portátiles), ya que representan el punto más crítico de los sistemas de seguridad.

El medio más recurrente para la ejecución de los ataques es la Web, gracias al rápido e ilimitado acceso a Internet, lo que está generando un incremento considerable del uso inapropiado, peligroso e improductivo de los medios informáticos, mediante descargas multimedia, P2P, mensajería instantánea, spywares, entre otros.

Los sistemas de reconocimiento de firmas de amenazas informáticas conforman la primera capa de protección para los puntos finales en las organizaciones, pero sin duda alguna no son suficientes para superar las nuevas amenazas, debido al gran número, la rapidez y la diversidad de dichos ataques.

Mientras la organización es atacada por nuevos virus, gusanos informáticos, troyanos, desbordamientos de memoria o intromisiones malintencionadas en la red, ya es muy tarde para que los software de seguridad puedan actuar.

Por esta razón, una compañía debe ser capaz de asegurar la productividad de sus usuarios así como de proteger su información, es entonces cuando la defensa eficiente de los puntos finales se convierte en prioridad para la organización y por tanto es nuestra principal misión.

La única respuesta efectiva

Aranda 360 ENDPOINT SECURITY presenta una nueva y radical solución para proteger las organizaciones tanto de los ataques externos, como de las falencias en las políticas corporativas de seguridad para el uso de las estaciones de trabajo.

Este es el primer sistema de defensa que se caracteriza por ser proactivo, automático, y con múltiples capas en un tiempo real. **Aranda 360 ENDPOINT SECURITY** no necesita esperar las actualizaciones de las firmas para proporcionar una protección completa e integrada de las estaciones de trabajo.

Un agente es el encargado de reforzar el perfil de cada política aplicada a las estaciones de trabajo, así sean usadas fuera o dentro de la red corporativa, en línea o fuera de ella. El agente desarrolla esta tarea sin necesidad de interrumpir el trabajo de cada usuario.

Beneficios estratégicos para su organización

- Su organización tendrá un alto nivel de seguridad informática sin precedentes, lo que le generará confianza en el registro de la información.
- Control total de seguridad en sus estaciones de trabajo.
- Complemento y refuerzo de las aplicaciones de antivirus existentes en la red.

© 2004-2007. Todos los derechos reservados. Aranda Software, el logotipo de Aranda Software, Aranda 360 ENDPOINT SECURITY y todos sus módulos componentes son marcas registradas de Aranda Software Corporation.

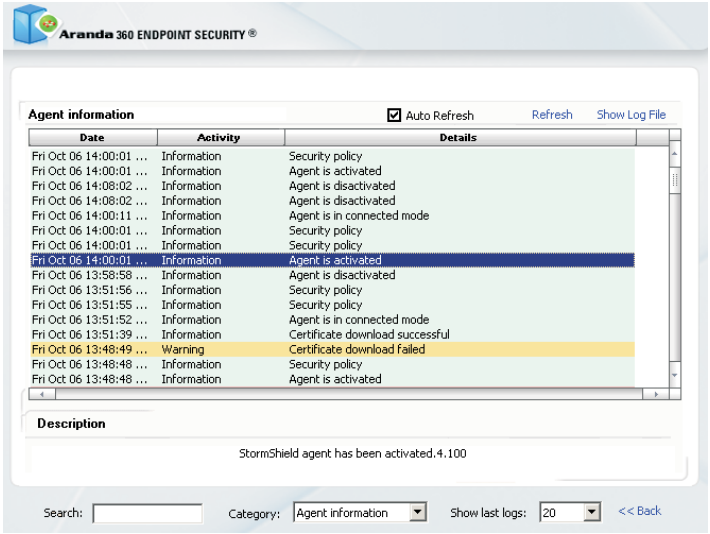
- Información crítica y/o confidencial de la compañía permanentemente asegurada y protegida.
- Aumento de la productividad gracias a la disposición de los recursos en buen estado.

Funcionalidades

Protección de archivos y aplicaciones (Standard & Enterprise Edition)
Files and Applications Protection

Controla las aplicaciones de los usuarios (acceso a listas blancas y listas negras) y el acceso a los diferentes tipos de archivos. Así mismo, limita los procesos de descarga y restringe archivos multimedia.

Establece permisos de acceso detallados para cada aplicación, registros y archivos, también permite la configuración de permisos de acceso a la red. Como valor agregado controla la instalación de software no permitido y previene la contaminación binaria de aplicaciones existentes.



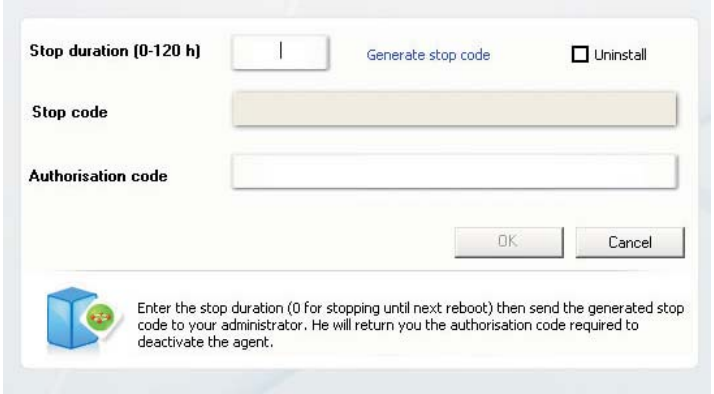
Soporte múltiple a los dispositivos (Standard & Enterprise Edition)
Multiple Devices Control

Permite el control de diferentes dispositivos de almacenamiento removibles, como por ejemplo, USB flash drives, cámaras digitales, reproductores MP3 o discos duros externos, asegurando el control sobre quién tiene acceso a ellos y bajo qué condiciones.

Bloquea los dispositivos de almacenamiento sin bloquear los puertos y controla el dispositivo de acuerdo con el distribuidor, el serial o el modelo.

Control de comunicaciones inalámbricas (Standard & Enterprise Edition)
Wireless Security

Se protege el sistema al encriptar la información mediante diferentes métodos (WEP, WPA, WPA2) y definiendo los puntos de acceso autorizados (SSID, MAC). Además, mediante técnicas de análisis de comportamientos se detectan intromisiones o posibles rechazos a las solicitudes de servicio. También administra y controla las comunicaciones inalámbricas. Por ejemplo, encender o apagar las conexiones WiFi y Bluetooth.



Control centralizado (Standard & Enterprise Edition)
Centralized Control

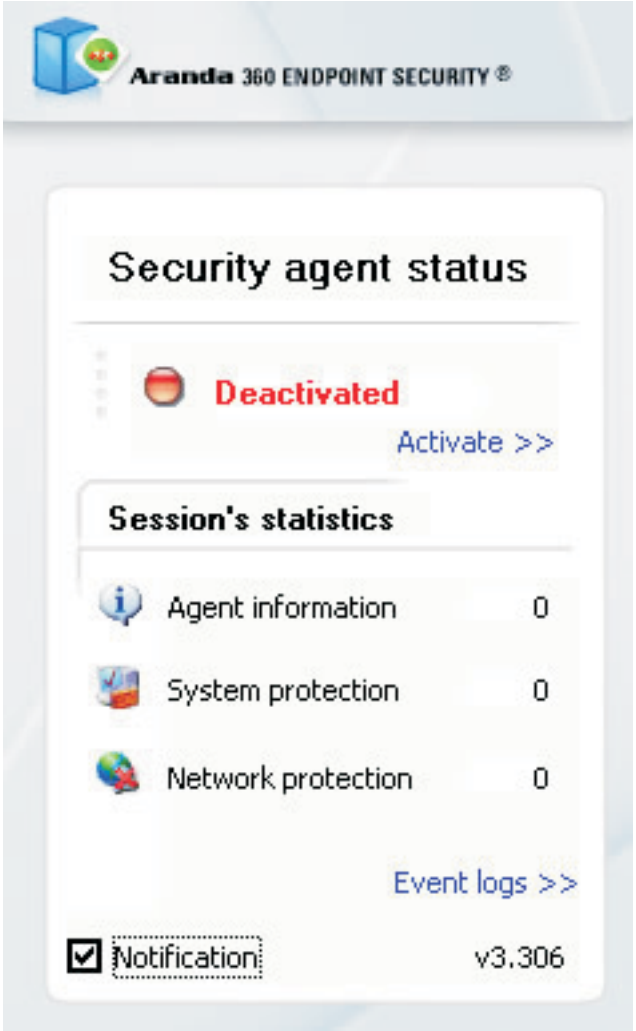
Permite establecer una o más políticas del sistema por grupo de trabajo además de monitorear y generar reportes permanentemente. **Aranda 360 ENDPOINT SECURITY** es una solución administrada de acuerdo con el perfil asignado del usuario y permite ejecutar todas sus funciones desde una consola de administración. Adicionalmente, es posible identificar un punto específico mediante el directorio activo, la dirección IP o el nombre del host.

Protección del Sistema (Enterprise Edition)
System Protection

Protege de ataques que podrían generar un desbordamiento de memoria, el cual constituye el primer paso utilizado frecuentemente para infiltrarse en un sistema e instalar un Troyano. Además, defiende los medios críticos del sistema operativo como reinicios provocados por intrusos, uso excesivo de la CPU, archivos, carpetas y registros del sistema.

© 2004-2007. Todos los derechos reservados. Aranda Software, el logotipo de Aranda Software, Aranda 360 ENDPOINT SECURITY y todos sus módulos componentes son marcas registradas de Aranda Software Corporation.

Bloquea automáticamente los intentos de programas espías para capturar la digitación en el teclado (keyloggers). Así mismo, protege el sistema operativo de la instalación de numerosos tipos de rootkits que sin ser detectados, pueden tener acceso a los documentos, archivos y carpetas de una estación de trabajo.



Protección de red (Enterprise Edition)
Network Protection

Se activa un filtro de alta profundidad en el sistema operativo cuando el tráfico de información ingresa al punto final (protocolos múltiples sobre IP, TCP/UDP/ICMP y Ethernet, y filtro de MAC/IP); además, complementa el firewall de la red, estableciendo reglas de comunicación para ésta en cada aplicación.
Detecta los accesos no autorizados a una estación de trabajo o a una red mediante el IDS (sistema de detección de intrusos) y protege la red del escaneo de puertos.

Aplicación dinámica de las políticas (Enterprise Edition)
Stateful Policies Enforcement

Se controla la instalación de aplicaciones para proteger el sistema de la ejecución de software no autorizado, incluso para usuarios con derechos administrativos. Además, se protegen las aplicaciones del uso no adecuado.

Tres mecanismos de protección

Aranda 360 ENDPOINT SECURITY tiene tres tipos de mecanismos de protección que brindan el nivel más alto de seguridad en una estación de trabajo:

- Protección basada en reglas.
- Protección automática
- Protección monitoreada basada en el perfil.

Protección basada en reglas

Este mecanismo permite definir privilegios de una protección basada en reglas, así como establecer privilegios asociados con las aplicaciones de las estaciones, archivos, registros y la comunicación de la red.

Una política de seguridad explícita puede ser desplegada por distintos grupos de estaciones de trabajo. **Aranda 360 ENDPOINT SECURITY** posee reglas predefinidas, de tal manera que las políticas pueden ser aplicadas inmediatamente por parte del administrador. No obstante, estas reglas de omisión podrían ser modificadas en cualquier momento para ser adaptadas a las políticas que una organización específica necesite.

Protección automática contra cualquier actividad sospechosa

La protección automática cubre todos los mecanismos constituyentes de **Aranda 360 ENDPOINT SECURITY**, detectando y bloqueando cualquier tipo de actividad sospechosa. Este tipo de protección no requiere de ninguna configuración por parte del administrador, sin embargo, él puede definir el grado de la misma.

© 2004-2007. Todos los derechos reservados. Aranda Software, el logotipo de Aranda Software, Aranda 360 ENDPOINT SECURITY y todos sus módulos componentes son marcas registradas de Aranda Software Corporation.

Dos categorías de gran importancia en cuanto a mecanismos de protección automática están incluidas dentro del producto. La primera categoría cubre las actividades del sistema y de la aplicación; esta se encarga pues, de proteger la estación de trabajo contra intentos de corromper archivos ejecutables, así como el acceso a servicios del sistema, o datos específicos.

La segunda categoría se constituye por un Sistema de Detección de Intromisiones (IDS), de tal manera que la estación de trabajo se puede proteger a si misma de ataques provenientes de la red. Los mecanismos implementados para detectar ataques del sistema o de la red de trabajo, por el sistema de protección automática se mantienen activos de manera permanente.

El tratamiento que **Aranda 360 ENDPOINT SECURITY** genera ante estos eventos puede ser controlado por el administrador. Dependiendo del tipo de evento que se presente, el sistema enviará una alerta, o implementará ciertas medidas automáticamente, según se haya definido en un principio.

Protección basada en el perfil

El último mecanismo de defensa se refiere a una protección monitoreada basada en el perfil. Este depende en una capacidad avanzada de monitorear sistemas mediante llamadas hechas por cada aplicación. Durante la fase de aprendizaje, estas llamadas son memorizadas como si se estuviera construyendo un perfil estándar de una aplicación. Las acciones desempeñadas por una aplicación que está corriendo son entonces comparadas con su perfil para detectar cualquier posible discrepancia que pueda surgir.

La protección basada en el perfil, constituye una tercera línea de defensa que está especialmente organizada para prevenir ataques así como nuevos gusanos informáticos de alta velocidad. Cualquier ataque basado en aplicaciones o servicios de sistema operativo corruptos serán totalmente bloqueados, independientemente de si un mecanismo de detección de firmas, o cualquier otro medio que busque defender el sistema de estos ataques, estén o no disponibles.

Requerimientos Técnicos

En el cliente

Procesador	SP1/SP2, Pentium III 600 Mhz
Espacio en disco duro	20 MB
Sistema Operativo	Windows 2000 SP4, XP

En el servidor

Procesador	Pentium III 850 MHz
Espacio en disco duro	50 MB
Sistema Operativo	Windows 2000, XP, 2003

En la consola

Sistema Operativo	Windows 2000, XP SP1/SP2
Espacio en disco duro	15 MB

Solicite información adicional sobre éste u otros productos de Aranda Software al correo electrónico info@arandasoft.com, consulte a su distribuidor autorizado o visite nuestro sitio en Internet **www.arandasoft.com.**

© 2004-2007. Todos los derechos reservados. Aranda Software, el logotipo de Aranda Software, Aranda 360 ENDPOINT SECURITY y todos sus módulos componentes son marcas registradas de Aranda Software Corporation.