



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

- *Disponibilidad 24x7 e integridad en las estaciones de los usuarios.*
- *Aranda 360 dispone de una suite de módulos integrados, que garantiza la seguridad proactiva, eficaz y en tiempo real de sus puntos finales.*
- *Protección basada en el comportamiento de la estación y la red, para evitar “ataques de día cero”, o cualquier tipo de ataque desconocido.*
- *Implementación segura de nuevas aplicaciones, herramientas y actualizaciones que incrementan la productividad en la compañía.*
- *Tranquilidad de los usuarios de TI cuando las actualizaciones necesitan ser instaladas.*

## Características

- *Control de acceso a la red.*
- *Control de instalación, acceso y uso de las aplicaciones.*
- *Control de dispositivos removibles de almacenamiento y de comunicaciones inalámbricas.*
- *Definición de políticas de seguridad compatibles con los puntos finales de su organización.*
- *Posibilidad de encriptar datos vulnerables y archivos confidenciales.*

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 vulnerable 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 de archivos multimedia, uso de redes P2P, mensajería instantánea, spyware, 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, en la medida en que este tipo de soluciones ya no dan abasto con el gran número, la rapidez y la diversidad de dichos ataques.

Mientras la organización es atacada por nuevos virus, gusanos informáticos, troyanos, explotaciones de vulnerabilidades o intromisiones malintencionadas en la red, ya es muy tarde para que los sistemas basados en las firmas de amenazas puedan actuar.

Por esta razón, una compañía debe ser capaz de asegurar la productividad de sus usuarios así como de salvaguardar 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.

## Una 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 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, en casa o en el camino. El agente desarrolla esta tarea sin necesidad de interrumpir el trabajo de cada usuario.

## Beneficios estratégicos para su organización

- *Aplicación de políticas de seguridad informática, basadas en el contexto específico de su organización.*
- *Bajo costo total de propiedad (TCO), gracias a que se utiliza un agente, una consola, y una sola implementación, dirigidos a cubrir toda suerte de situaciones que puedan afectar la seguridad informática en su empresa.*
- *Integración inmediata con la infraestructura TI pre-existente (aplicaciones, antivirus, herramientas de seguridad y de monitoreo).*



- Control total de la seguridad en sus estaciones de trabajo.
- Su organización tendrá un nivel de seguridad informática sin precedentes, lo que le generará confianza en el registro de la información.
- 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 del Sistema (Enterprise & Premium Editions)

#### Host Intrusion Prevention System

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 de ataques tales como reinicios provocados por intrusos, uso excesivo de la CPU, archivos, carpetas y registros del sistema.

También 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.

### Firewall Dinámico (Enterprise & Premium Editions)

#### Stateful Firewall

Aranda 360 ENDPOINT SECURITY protege su infraestructura TI por medio de un firewall propio que se fundamenta en el kernel del sistema operativo.

### Control de Aplicaciones (Enterprise & Premium Editions)

#### Applications Control

Aranda 360 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 el acceso a archivos multimedia.

Establece permisos de acceso detallados para cada aplicación, para los registros y los archivos y permite la configuración de permisos de acceso a la red. Además, controla la instalación de aplicaciones y previene la corrupción binaria de aplicaciones existentes.

### Aplicación Dinámica de las Políticas (Enterprise & Premium Editions)

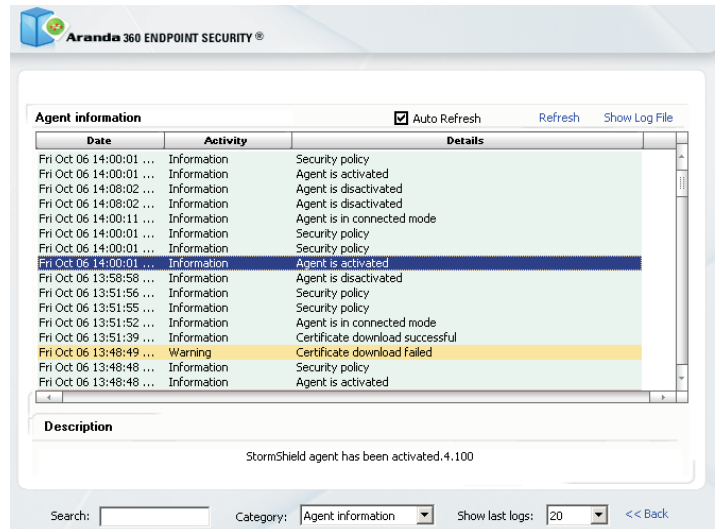
#### Stateful Policies Enforcement

Controla la instalación de aplicaciones para proteger el sistema de la ejecución de software no autorizado, incluso para usuarios con derechos administrativos. De la misma forma, protege las aplicaciones del uso no adecuado, salvaguardando su integridad, y define políticas de seguridad, de acuerdo con los requerimientos específicos de cada organización.

### Protección de Red (Enterprise & Premium Editions)

#### Network Access Control

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 direcciones MAC e IP).





Además, complementa el firewall de la red, estableciendo reglas de comunicación para ésta en cada aplicación. Detecta los accesos no autorizados a un computador o a una red mediante el IDS (Sistema de Detección de Intrusos) y protege la red del escaneo de puertos.

### **Control de Dispositivos Móviles (Enterprise & Premium Editions)** **Wireless Security**

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

Se protege el sistema al limitar la conexión a dispositivos inalámbricos que utilizan diferentes métodos de encriptación y autenticación (WEP, WPA, WPA2), y se definen redes de conexión inalámbricas autorizadas mediante su nombre SSID o su dirección MAC.

También administra y controla las comunicaciones móviles. Por ejemplo, restringe la activación o desactivación de las conexiones WiFi y Bluetooth.

### **Monitoreo de Puntos Finales (Enterprise & Premium Editions)** **Endpoint Monitoring**

Permite controlar la compatibilidad de las políticas de seguridad con el punto final, dependiendo de los criterios específicos y el entorno de cada organización. Adicionalmente, es posible implementar acciones correctivas, tales como la actualización de programas de antivirus y las de Windows.

### **Encriptación de Archivos y Carpetas (Premium Edition)** **File and Folder Encryption**

Permite encriptar cualquier tipo de información confidencial de la organización de manera transparente para el usuario, por medio del estándar de encriptación avanzada AES (por sus siglas en inglés Advanced Encryption Standard).

## **Cuatro Módulos Independientes de Protección**

La suite de protección de Aranda 360 garantiza el control absoluto del manejo y la seguridad de sus estaciones de trabajo, portátiles y dispositivos móviles, mediante la protección integrada de sus cuatro soluciones independientes de protección:

- Aranda 360 SYSTEM PROTECTION
- Aranda 360 DYNAMIC POLICY
- Aranda 360 DEVICE CONTROL
- Aranda 360 DATA ENCRYPTION

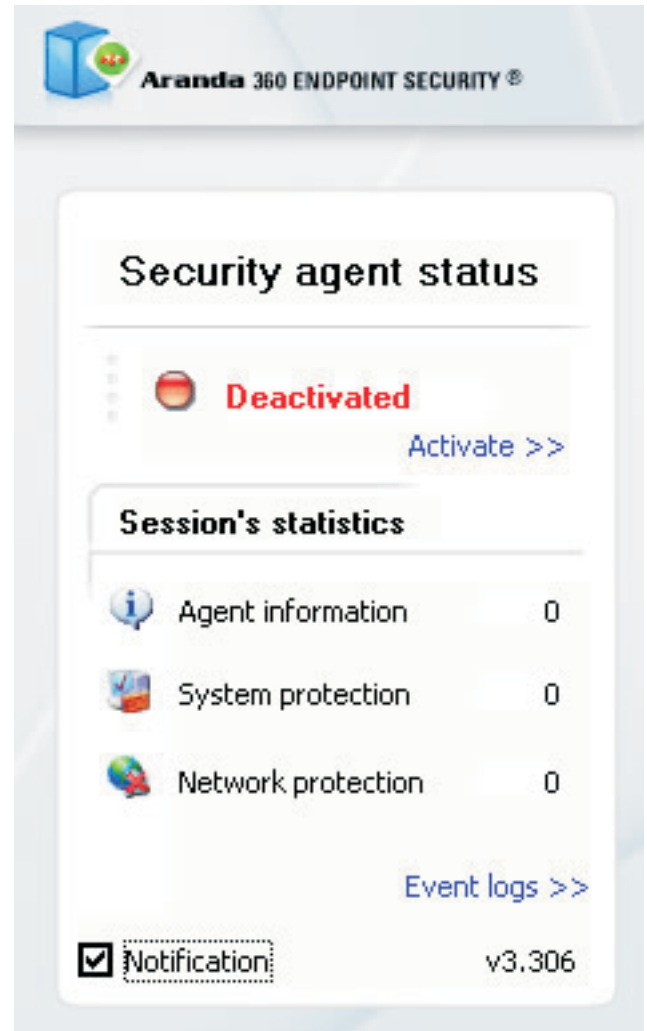
### **Aranda 360 SYSTEM PROTECTION**

Esta solución garantiza una protección basada en reglas, que controla el acceso a archivos ejecutables, carpetas y paneles del sistema, y monitorea las conexiones de la aplicación.

Adicionalmente, detecta, alerta y bloquea cualquier mecanismo de ataque genérico como desbordamientos de memoria o escaneo de puertos.

### **Aranda 360 DYNAMIC POLICY**

Esta solución determina la compatibilidad existente entre las políticas





de seguridad establecidas desde la misma y sus puntos finales implementando a estos últimos, procedimientos de actualización. Además, es posible definir políticas perfectamente adaptadas a las necesidades específicas de cada red corporativa.

### Aranda 360 DEVICE CONTROL

El control de dispositivos permite establecer permisos de acceso y uso a dispositivos de almacenamiento de acuerdo con criterios puntuales. De igual forma, monitorea las operaciones llevadas a cabo en éstos, y controla los diversos tipos de conectividad inalámbrica existentes en la red corporativa, tales como Wi-Fi y Bluetooth.

### Aranda 360 DATA ENCRYPTION

La encriptación de datos y archivos confidenciales es una de las funciones más representativas de Aranda 360 ENDPOINT SECURITY. Por medio de este módulo, es posible encriptar y desencriptar de manera transparente para el usuario cualquier tipo de archivo, crear archivos encriptados auto-extraíbles, y eliminar de manera segura y definitiva cualquier tipo de información de la estación de trabajo. De esta forma, será posible aumentar el nivel de seguridad de su red corporativa.

## 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](mailto:info@arandasoft.com), consulte a su distribuidor autorizado o visite nuestro sitio en Internet [www.arandasoft.com](http://www.arandasoft.com).