

1. Generalidades

- ¿Qué tipo de amenazas ponen en peligro la infraestructura de mi PC?
- ¿Cómo Aranda 360 protege la infraestructura de mi PC?
- ¿Puedo usar Aranda 360 sin un antivirus?
- ¿Puedo usar Aranda 360 sin un firewall personal?
- ¿Cómo obtener más información acerca de Aranda 360? ¿Cómo puedo adquirir esta solución?

2. Seguridad

- ¿De qué manera Aranda 360 protege mi PC de gusanos informáticos?
- ¿Con qué mecanismos Aranda 360 protege de troyanos e intentos de tomar el control de la estación de trabajo?
- ¿De qué forma Aranda 360 protege de intentos de robo de información confidencial?
- ¿De qué manera Aranda 360 protege la estación de trabajo de ataques a la red?
- ¿El usuario es notificado cuando Aranda 360 bloquea una operación en la estación de trabajo?
- ¿La herramienta consulta al usuario para autorizar o prohibir acciones sospechosas?
- ¿Al usar Aranda 360 no debo instalar parches?
- ¿Aranda 360 puede protegerse contra ataques?
- ¿Un usuario puede desinstalar o detener Aranda 360 ENDPOINT SECURITY?

3. Políticas de Uso

- ¿Qué es una política de uso?
- ¿Se puede prohibir el uso de dispositivos de almacenamiento removibles?
- ¿Es posible prohibir el uso de archivos específicos?
- ¿Es posible prohibir el uso de aplicaciones específicas?

4. Distribución e Integración

- ¿Cómo se implementa Aranda 360?
- ¿De que manera puede ser desplegada una política de seguridad con Aranda 360?
- ¿Aranda 360 es compatible con Windows XP Sp2? ¿Aranda 360 es compatible con el firewall SP2?
- ¿Con qué antivirus se ha probado Aranda 360?

5. Configuración y Administración

- ¿Cuánto tiempo toma configurar Aranda 360?
- ¿Qué conocimientos son indispensables para utilizar el producto?
- ¿Existen algunos modelos de configuración disponibles?
- ¿Por qué algunos productos no necesitan de configuraciones previas para proteger Pcs?

6. Arquitectura

- ¿Cuáles son los requisitos de Aranda 360?
- ¿Cuáles son los componentes de la solución?
- ¿Cómo se comunican los componentes de la solución entre sí?
- ¿Cuál es el tamaño del ejecutable de un agente?
- ¿Es posible instalar el servidor en una máquina que es utilizada para otras tareas, o es necesario tener un servidor dedicado para esta aplicación?
- ¿Es necesaria una base de datos? Puede ser usada una base de datos ya existente?
- ¿La instalación de los componentes de A360 puede ser organizada de acuerdo con las necesidades del administrador en una o más máquinas?

7. Desempeño

- ¿Qué impacto tiene Aranda 360 en el desempeño de la estación de trabajo?
- ¿Qué ancho de banda debería ser destinado para comunicarse con los agentes de Aranda 360?
- ¿Es posible gestionar y optimizar esta comunicación?
- ¿Cómo escala Aranda 360? ¿Cuántas estaciones puede proteger?

8. Actualizaciones

- ¿Aranda 360 requiere de firmas para funcionar?
- ¿Existe alguna manera de verificar si un agente de A360 ha sido actualizado en la estación de trabajo?

9. Monitoreo

- ¿Qué información específica es registrada en la consola?
- ¿La información de seguridad es enviada inmediatamente a la consola de administración?
- ¿Aranda 360 tiene funcionalidades integradas para seguridad y generación de reportes?
- ¿Es posible generar alertas y acciones en las consolas de monitoreo de la red?
- ¿Los datos de seguridad pueden ser usados junto con otros análisis y herramientas de reporte, como por ejemplo, objetos de negocios o Crystal Reports?

Generalidades

¿Qué tipo de amenazas ponen en peligro la infraestructura de mi PC?

Las estaciones de trabajo se han convertido en el punto más débil e inseguro de los sistemas de información en red. Indudablemente, éstas se encuentran totalmente expuestas a cualquier tipo de amenaza y se hacen cada vez más vulnerables, por medios tales como la facilidad de movilidad de PCs, la conectividad inalámbrica, así como un número cada vez mayor de elementos de comunicación.

Los nuevos ataques son ahora mucho más agresivos, difíciles de detectar, y más rápidos que nunca (de tal manera que los sistemas de reconocimiento de firmas de amenazas informáticas ya no tienen tiempo suficiente para reaccionar).

Los ataques en la actualidad ya no se limitan solamente a dañar la estación de trabajo, o tal vez a disminuir la capacidad de la red. Por el contrario y cada vez con más frecuencia, tienden a tomar el control del PC, con el fin de realizar espionaje industrial, transferencia ilícita de fondos, presentación de Pop-Ups publicitarios, entre otros.

De otra parte, los usuarios autorizados también propician la perpetuación de estos ataques y también ciertos problemas legales cuando usan sus estaciones de trabajo para acciones tales como: cargar ciertas aplicaciones de contenido inconsistente o peligroso, utilizar aplicaciones vulnerables, transferir documentos de tipo ilegal, etc.

¿De qué manera Aranda 360 protege la infraestructura?

A360 protege de manera proactiva e independiente su infraestructura informática contra ataques conocidos o desconocidos. Proactiva, implica que esta solución no depende de firmas, parámetros, u otras actualizaciones, para poder bloquear un nuevo ataque. Independiente, se refiere a que esta herramienta no requiere de la intervención de un usuario o un administrador para bloquear actividades que son consideradas como peligrosas.

Por esta razón, se dice que ésta es una solución de defensa autónoma que, en tiempo real, usa una combinación de técnicas innovadoras para detectar y bloquear todas aquellas acciones que puedan hacer peligrar la integridad del sistema, las aplicaciones ó la comunicación en una estación de trabajo y su respectivo ambiente. A360 es una solución de tipo empresarial, ya que una consola de manejo central puede definir e implementar políticas, tanto de uso, como de seguridad para cientos o miles de PCs.

¿Puedo usar Aranda 360 sin un antivirus?

A360 puede proteger su infraestructura informática de ataques ocasionados por virus. No obstante, esta solución es complementaria a su sistema de detección de firmas de amenazas informáticas. El antivirus puede eliminar cada uno de los rastros de un ataque de virus en una máquina que se encuentre infectada.

En la mayoría de los casos, también puede bloquear un virus conocido antes de que éste pueda tener cualquier efecto en la estación de trabajo.

Sin embargo, A360 bloquea varios tipos de ataques, así como operaciones peligrosas que un antivirus no es capaz de detener; dentro de ellos encontramos nuevos virus que no cuentan aún con firmas detectadas, ataques sigilosos, ataques a la red que toman ventaja de vulnerabilidades de ciertos protocolos, operaciones de usuario prohibidas por las políticas de la compañía, etc.

¿Puedo usar Aranda 360 sin un firewall personal?

Aranda 360 ENDPOINT SECURITY incorpora un firewall personal que controla la comunicación en la estación de trabajo; el uso de un firewall personal suplementario es por esta razón innecesario. Esta herramienta ofrece una solución completa y eficiente, mediante una protección más sólida que la que es ofrecida por un firewall personal.

En primer lugar, un firewall personal puede ser inhabilitado, o desinstalado durante un ataque. De otra parte, puede también ser malversado por aplicaciones dañinas que permiten establecer comunicación en la red de trabajo. Finalmente, un firewall es fundamentalmente estático, y por esta razón su eficiencia depende de las configuraciones preestablecidas por el administrador.

A360 está protegido de cualquier posible intento de inhabilitarlo o desinstalarlo. Preservando la integridad de los ejecutables, esta aplicación evita la creación de puertas de ingreso cubiertas, establecidas normalmente en programas que están autorizados para comunicarse con la red.

Además de ello, el firewall de A360 está unido a varios mecanismos de detección de intrusos y anomalías, los cuales bloquean instantáneamente cualquier comunicación que se considere peligrosa.

¿Cómo obtener más información acerca de Aranda 360? ¿Cómo puedo adquirir esta solución?

Contacte a nuestro equipo de ventas, comunicándose al mail info@arandasoft.com

Seguridad

¿De qué manera Aranda 360 protege mi PC de gusanos informáticos?

Un gusano informático es un tipo de virus que se propaga automáticamente a través de la red, sin requerir de ninguna acción por parte de los usuarios. Los gusanos informáticos usualmente explotan las debilidades más conocidas dentro del software de la red, tales como aquellas que existen en la recepción de correos electrónicos, las bases de datos o inclusive, el sistema operativo. A360 bloquea la propagación de gusanos mediante la implementación de los siguientes mecanismos: protección de la integridad de software en cada estación de trabajo, prevención de la inyección de códigos maliciosos, así como el impedimento del accionar de estos gusanos, aun antes de que se empiecen a propagar dentro de la red.

Además de ello, A360 monitorea el tráfico de la red para cada aplicación de una estación y detecta automáticamente cualquier actividad sospechosa. El firewall integrado de esta herramienta puede ser accionado para bloquear inmediatamente el tráfico ilícito, mediante la prevención, tanto de la corrupción de los ejecutables, como de la comunicación de la red. Sin duda alguna, A360 entrega una óptima protección contra gusanos informáticos.

¿Con qué mecanismos Aranda 360 protege de troyanos e intentos de tomar el control de la estación de trabajo?

Un gusano informático es un tipo de virus que se propaga automáticamente a través de la red, sin requerir de ninguna acción por parte de los usuarios. Los gusanos informáticos usualmente explotan las debilidades más conocidas dentro del software de la red, tales como aquellas que existen en la recepción de correos electrónicos, las bases de datos o inclusive, el sistema operativo.

¿De qué forma Aranda 360 protege de intentos de robo de información confidencial?

La estación de trabajo es el blanco principal de un número cada vez mayor de ataques, desarrollados con el fin de obtener y robar información confidencial: claves de ingreso, secretos industriales referidos a las actividades bancarias, entre otros. Cuando se enfrenta a este tipo de riesgo, el filtro del tráfico de red es ciertamente útil pero no siempre es suficiente, incluso si un firewall personal es instalado en la estación de trabajo.

Para asegurar una protección absoluta, esta aplicación implementa un firewall integrado que contiene mecanismos de protección específicos contra espionaje y captura de información almacenada en el computador: neutralización de keyloggers (captura de actividad de teclado), protección de zonas del sistema donde las claves de ingreso son guardadas, reglas de uso de dispositivos de almacenamiento removibles, limitación de acceso a archivos que son considerados como críticos, etc.

¿De qué manera Aranda 360 protege la estación de trabajo de ataques a la red?

A360 incluye un Sistema de Detección de Intrusos (SDI), que bloquea todos los ataques tan pronto como éstos tratan de afectar la estación. Cuando un ataque es dirigido hacia una vulnerabilidad aún desconocida, el sistema de protección de la herramienta toma el control y previene la ejecución de cualquier código malicioso.

¿El usuario es notificado cuando Aranda 360 bloquea una operación en la estación de trabajo? ¿La herramienta consulta al usuario para autorizar o prohibir acciones sospechosas?

A360 es una solución de defensa autónoma que funciona independientemente. Esta herramienta ha sido diseñada para nunca obstaculizar la actividad del usuario, ni interrumpirlo formulándole algún tipo de pregunta. No obstante, esta herramienta advierte al usuario cuando un comportamiento peligroso o una acción no autorizada es bloqueada. Esta notificación es presentada temporalmente en una pequeña ventana en la parte inferior de la pantalla. Este sistema de notificación puede ser desactivado si el usuario así lo determina.

¿Al usar Aranda 360 no debo instalar parches?

Un parche es la actualización de un software que remedia un error de un programa; los parches de seguridad bloquean ciertas debilidades identificadas que pueden ser aprovechadas durante un ataque. A360 protege sistemas no parchados de todos aquellos ataques que podrían tomar ventaja de aquellas vulnerabilidades.

Cuando las vulnerabilidades han sido identificadas, un ataque puede ocurrir mientras el parche no está aún disponible. Inclusive cuando el parche se encuentra ya instalado, desplegarlo en muchas estaciones de trabajo es una operación muy complicada. Por esta razón, una defensa proactiva es necesaria.

Los parches de seguridad son muy útiles y A360 no excluye de ninguna manera la importancia de su implementación. Sin embargo, esta aplicación es complementaria a los parches, debido a que protege al sistema durante periodos de vulnerabilidad, permitiendo que el usuario espere para que nuevos parches se encuentren disponibles y posteriormente, los pueda aprovechar de manera controlada y considerada.

¿Aranda 360 puede protegerse contra ataques?

A360 se encuentra totalmente protegido contra ataques diseñados para detener, desactivar, o desinstalar el producto. Esta herramienta siempre continuará operando, debido a que sus mecanismos principales están localizados al interior del núcleo del sistema operativo, haciéndolos inaccesibles a cualquier tipo de ataque.

Esta protección también aplica configuraciones de seguridad implementadas en la estación de trabajo, con el fin de mantener las políticas de seguridad bajo el control del administrador.

¿Un usuario puede desinstalar o detener Aranda 360?

El administrador de A360 puede autorizar o prohibir la desinstalación o desactivación de esta solución. Este hecho se evidencia inclusive cuando el usuario en cuestión, es el administrador de la estación de trabajo.

Políticas de Uso

¿Qué es una política de uso?

Una política de uso es un parámetro que regula la manera en que los empleados de una compañía deberían usar sus estaciones de trabajo. De esta manera, se refuerzan las políticas de seguridad de una organización, prohibiendo comportamientos peligrosos como por ejemplo, el uso de aplicaciones que son particularmente vulnerables a ataques.

Una política, así mismo puede prohibir cualquier comportamiento que sea considerado incompatible con un ambiente profesional particular, como la descarga de contenidos de multimedia.

¿Se puede prohibir el uso de dispositivos de almacenamiento removibles?

Simplicidad, discreción y una gran capacidad, son las características que hacen que un dispositivo de almacenamiento removible (USB, iPods, entre otros), sean el medio perfecto para robar información. Estos medios pueden también ser usados para introducir programas peligrosos, así como información prohibida en su red de trabajo, sin ser detectados por las defensas de seguridad de su estación.

A360 puede ser usado para bloquear el uso de USBs removibles, sin necesidad de afectar el acceso a otros periféricos que usan este tipo de conexión, como lo son el Mouse, la impresora, etc.

¿Es posible prohibir el uso de archivos específicos?

El acceso a Internet, así como el uso generalizado de portátiles, facilita la proliferación de comportamientos que pudieran ser considerados como perjudiciales a la compañía; dentro de ellos tenemos la descarga, almacenamiento y uso de archivos con propósitos no profesionales en la estación de trabajo.

A360 puede prevenir estos comportamientos, prohibiendo el acceso a archivos que no sean autorizados en las estaciones de los usuarios.

¿Es posible prohibir el uso de aplicaciones específicas?

Redes locales de alta velocidad, así como el acceso generalizado a Internet, motivan la instalación aleatoria de aplicaciones piratas y no profesionales. El control cercano de las aplicaciones instaladas en las estaciones de trabajo protege a la compañía de todo aquello que pueda ser considerado como un riesgo.

A360 le permite restringir al usuario instalar aplicaciones específicas, inclusive si este usuario corresponde al administrador de la estación de trabajo. Esta herramienta también le permite definir grupos de aplicaciones que deberían ser eliminados de los computadores de la compañía, tales como herramientas P2P y mensajería instantánea.

Distribución e Integración

¿Cómo se implementa Aranda 360?

La distribución de los agentes de A360 es un proceso simple y sencillo. Los agentes pueden ser distribuidos remotamente e instalados sin la intervención del usuario, promoviendo la gestión del software de A360. Cada agente puede también ser cargado directamente desde un servidor Web integrado en la solución. El servidor y la consola de manejo tienen sus propios wizards de instalación, cuyo proceso demora tan sólo unos minutos.

¿De que manera puede ser implementada una política de seguridad con Aranda 360?

Aranda 360 permite al administrador definir diversas políticas de seguridad, de acuerdo con las necesidades de los diferentes grupos de usuarios, así como con el tipo de riesgos a los que estos usuarios están expuestos.

Una política de seguridad es un conjunto de reglas que afectan el comportamiento del sistema, las aplicaciones y la red. Esta herramienta le permite adjuntar políticas a grupos de estaciones de trabajo, utilizando para ello, direcciones IP o en su defecto objetos del Directorio Activo. La distribución de políticas es llevada a cabo con un simple clic en la consola de manejo.

¿Aranda 360 es compatible con Windows XP SP2? ¿Aranda 360 es compatible con el firewall SP2?

A360 es compatible con Windows XP SP2. Si usted instala esta solución en Windows SP1 y está planeando actualizarlo a SP2, no será necesaria ninguna modificación del agente. A360 es técnicamente compatible con el firewall de Windows XP SP2.

No obstante, esta herramienta incorpora su propio firewall, el cual ofrece varias funcionalidades que no están disponibles en los firewalls de Windows, como por ejemplo, la integración de un (SDI), o el filtro de conexiones externas. En la práctica, es preferible desactivar el firewall de Windows cuando esta aplicación es utilizada.

¿Con qué antivirus se ha probado Aranda 360?

Aranda 360 ENDPOINT SECURITY ha sido probado y certificado con la mayoría de software de antivirus existentes en el mercado. Por ejemplo, Norton Antivirus 2005, McAfee Virus Scan, Trend Micro Office Scan, Kaspersky Anti-Virus, and Sophos Anti-Virus. Si su antivirus no aparece en esta lista, por favor no dude en enviar un mail a info@arandasoft.com, para confirmar si su compatibilidad con A360 ya ha sido probada.

Configuración y Administración

¿Cuánto tiempo toma configurar Aranda 360?

A360 puede ser implementada tan pronto como es instalada en la estación de trabajo, considerando reglas de seguridad que son predefinidas e incluidas en el producto.

Configurar esta aplicación, le permite incrementar el nivel de seguridad adicionando un control extra. Estos parámetros reflejarán sus propias políticas de seguridad.

Normalmente, definir un conjunto inicial de políticas, así como configurar parámetros apropiados para la herramienta, es un proceso que puede durar un par de días.

¿Qué conocimientos son indispensables para utilizar el producto?

El manejo de A360 es responsabilidad de la red de la compañía, el sistema o el administrador de seguridad. Para cumplir con este objetivo no es necesario tener competencias específicas; con la ayuda de los manuales de usuario, será posible manejar plenamente esta solución en unos minutos.

¿Existen algunos modelos de configuración disponibles?

Aranda 360 ENDPOINT SECURITY tiene incluidas varias plantillas de configuración, con diferentes grupos de reglas. Para cada política, usted puede escoger si incluir o no dichos parámetros.

Algunas de estas políticas de usuario comprenden reglas que impiden entre otros, la ejecución de aplicaciones prohibidas, como lo son la mensajería instantánea o el P2P.

Otras reglas pueden reforzar la seguridad de las estaciones de trabajo al restringir determinadas acciones de aplicaciones o servicios críticos de Windows, como lo son el buscador o el correo electrónico.

¿Por qué algunos productos no necesitan de configuraciones previas para proteger Pcs?

A diferencia de lo que sucede con Aranda 360 ENDPOINT SECURITY, algunos productos de seguridad para puntos finales no requieren de configuración.

Esto ocurre debido a que aquellos productos tienen en cuenta aspectos de seguridad muy limitados, por ejemplo, ataques específicamente referidos al desbordamiento de memoria. Este tipo de herramienta no necesita ningún tipo de parámetro, pero la protección ofrecida en estos casos, también es muy limitada.

Arquitectura

¿Cuáles son los requisitos de Aranda 360?

El agente de A360 protege PCs equipados con Windows 2000 SP4 o Windows XP Sp1 o Sp2. No existe un requerimiento específico de memoria de su CPU.

¿Cuáles son los componentes de la solución?

A360 está constituido por varios componentes de software: agentes, servidores, base de datos, y consola de manejo. La protección de cada estación de trabajo es llevada a cabo por parte del agente de la herramienta. Este agente se comunica con el servidor de despliegue, cuyo rol consiste en distribuir las políticas de seguridad a cada agente, así como reunir toda la información concerniente a la seguridad de la estación de trabajo. Esta información es guardada en una base de datos específica en el servidor de despliegue, a la cual se puede tener acceso por medio de la consola. Ésta activa los agentes de A360, define y distribuye las políticas de seguridad, y presenta la información que ha sido reunida por los agentes.

¿Cómo se comunican los componentes de la solución entre sí?

La comunicación entre los componentes de A360 es autenticada y encriptada, usando los certificados SSL v3 y X509 v3. La autenticación es mutua entre todos los componentes, con el fin de reforzar el nivel de seguridad de las soluciones. La frecuencia de la comunicación y el volumen de los datos transferidos, son controlados por el administrador.

¿Cuál es el tamaño del ejecutable de un agente?

Aproximadamente 7 MB de espacio en el disco son requeridos para instalar el agente de Aranda 360.

¿Es posible instalar el servidor en una máquina que es utilizada para otras tareas, o es necesario tener un servidor dedicado para esta aplicación?

A360 no requiere de un servidor dedicado. El requerimiento de recursos depende del número de agentes que están asociados con dicho servidor, el tamaño de las configuraciones, el volumen de los registros reunidos desde las estaciones de trabajo, y la frecuencia de comunicación entre los agentes y el mismo. Todos estos elementos pueden ser controlados en la consola de administración.

¿Es necesaria una base de datos? ¿Puede ser usada una base de datos ya existente?

Aranda 360 ENDPOINT SECURITY guarda la información que es recopilada desde las estaciones de trabajo en una base de datos relacional. Una base de datos (Motor de base de datos del Servidor SQL de Microsoft) se incluye con A360. Si usted ya tiene implementada una base de datos 2000 del servidor SQL y desea utilizarla para almacenar los datos de A360, puede especificarlo durante la instalación del producto, o registrar la base de datos en la consola de administración.

¿La instalación de los componentes de A360 puede ser organizada de acuerdo con las necesidades del administrador en una o más máquinas?

Los componentes de A360 son módulos de software independientes, los cuales pueden ser instalados según su preferencia. Por ejemplo, es perfectamente factible instalar cada servidor, consola y base de datos en una máquina diferente, ó en un único host definido con anterioridad.

Desempeño

¿Qué impacto tiene Aranda 360 en el desempeño de la estación de trabajo?

A360 tiene un consumo mínimo de recursos de la estación de trabajo, incluso bajo condiciones críticas como por ejemplo, cuando existen múltiples y simultáneas amenazas al sistema, esta solución utiliza tan sólo de un 2% a un 3% de la capacidad de la CPU.

¿Qué ancho de banda debería ser destinado para comunicarse con los agentes de Aranda 360? ¿Es posible gestionar y optimizar esta comunicación?

La comunicación entre los agentes de A360 y el servidor, permite tanto la aplicación de las políticas de seguridad a los agentes, como la recolección y consolidación de los registros de la estación.

A diferencia de los sistemas que están basados en actualización de firmas, la implementación de las políticas de seguridad para este caso, no es una operación obligatoria, debido a que esta herramienta no requiere de actualizaciones cuando una nueva amenaza aparece.

El tamaño promedio de una política de seguridad es de menos de 50 KB. La transmisión de este limitado volumen de datos usualmente no es un problema, inclusive en las redes más limitadas. El tipo y la cantidad de información que es subida en el servidor, es determinada por el administrador, quien para este fin, puede tener en cuenta la capacidad específica de la red. Finalmente, el administrador tiene la posibilidad de optimizar la comunicación entre los componentes de A360, distribuyéndolos sobre varios servidores, o configurando la frecuencia de conexión entre ellos.

¿Cómo escala Aranda 360? ¿Cuántas estaciones puede proteger?

Aranda 360 ENDPOINT SECURITY ha sido diseñado para proteger un número ilimitado de estaciones de trabajo virtualmente. Su capacidad para escalar resultados es garantizada por tres aspectos básicos: componentes de software especializados, una arquitectura de alta disponibilidad y su capacidad para optimizar el ancho de banda.

Esta solución está constituida por componentes modulares especializados, que pueden ser corridos en diferentes hosts, permitiendo una mejor distribución de la carga generada por las políticas de configuración y los datos de monitoreo (consola), protegiendo las estaciones de trabajo (agentes), enviando políticas y recolectando eventos desde las estaciones de trabajo (servidores) y finalmente, almacenando estos eventos (base de datos).

¿Aranda 360 tiene funcionalidades integradas para seguridad y generación de reportes?

Un alto nivel de disponibilidad es ofrecido a través de una arquitectura de tipo multi-servidor con un balance de carga y mecanismos de failover. Además de ello, nuevos servidores pueden ser agregados en cualquier momento para implementar el escalamiento en el sistema.

La escalabilidad también depende de los requerimientos de ancho de banda de la red, contrario a lo que ocurre con los productos basados en la detección de firmas de amenazas informáticas (que requieren de cargas frecuentes de archivos de firmas en cada estación de trabajo), el agente de A360 necesita ser actualizado únicamente cuando el administrador desee aplicar nuevas políticas.

Adicionalmente, con la consola de manejo el administrador puede definir claramente el volumen de datos que debe ser recolectado por las estaciones de trabajo.

Actualizaciones

¿Aranda 360 requiere de firmas para funcionar?

A360 está basado en una tecnología de comportamiento patentada. Una de las ventajas más importantes de esta tecnología es que no requiere de firmas para bloquear ataques conocidos o desconocidos en la estación de trabajo.

Para reforzar las capacidades de protección de A360, el producto también incluye un módulo de SDI (Sistema de Detección de Intrusos), el cual es usado para analizar el tráfico entrante a la red. El SDI de la aplicación es acoplado con un firewall basado en el kernel, que garantiza una capacidad de filtro instantánea en donde sea que se detecte tráfico sospechoso.

El (SDI) de Aranda 360 ENDPOINT SECURITY es la única parte del producto que hace uso de firmas de amenazas informáticas.

¿Existe alguna manera de verificar si un agente de A360 ha sido actualizado en la estación de trabajo?

Cualquier proceso de actualización es almacenado en el registro de la estación de trabajo. De igual manera, si una notificación de usuario es activada, un mensaje pop-up indicará que una nueva versión ha sido instalada.

Monitoreo

¿Qué información específica es registrada en la consola?

La información que considera la seguridad de la estación de trabajo, es almacenada en un archivo de registro: actividad del sistema, comportamiento de las aplicaciones, y comunicaciones de la red. Todos los eventos relevantes son almacenados en este registro, inclusive si no se implementó una acción de bloqueo. El tipo y el formato de la información que es cargada en la consola, puede ser consultado en la documentación técnica del producto.

¿La información de seguridad es enviada inmediatamente a la consola de administración?

Las alertas son enviadas a la consola con una frecuencia configurada por el administrador.

¿Aranda 360 tiene funcionalidades integradas para seguridad y generación de reportes?

Aranda 360 ENDPOINT SECURITY ofrece un completo monitoreo integrado y un módulo de reportes.

El monitoreo permite un análisis detallado de los datos de seguridad provenientes de las estaciones de trabajo. Este tipo de funciones, sumadas a la selección de múltiples criterios, facilitan el rápido manejo y acceso de la información requerida. Las herramientas de análisis integradas a la solución, junto con un generador de reportes gráficos, ofrecen al administrador un completo panorama de la seguridad real de las estaciones de trabajo.

¿Es posible generar alertas y acciones en las consolas de monitoreo de la red?

A360 se puede comunicar con los sistemas de monitoreo de la red mediante interfaces, utilizando un formato SMTP o un syslog. El administrador puede activar estas funciones desde la consola de manejo.

¿Los datos de seguridad pueden ser usados junto con otros análisis y herramientas de reporte, como por ejemplo, objetos de negocios o Crystal Reports?

La información que es cargada desde las estaciones de trabajo, es almacenada en la base de datos. Usted puede usar sus propias herramientas de análisis y reportes para consultar la base de datos de A360. No obstante, la consola de manejo de A360 ofrece su propio análisis y la capacidad de presentar reportes de forma gráfica y detallada a los usuarios.