



Bitdefender® ENTERPRISE

SECURITY FOR VIRTUALIZED ENVIRONMENTS

Guía del informador
(Multiplataforma) >>

Security for Virtualized Environments de Bitdefender

Guía del informador (Multiplataforma)

fecha de publicación 2012.12.19

Copyright© 2012 Bitdefender

Advertencia legal

Todos los derechos reservados. Ninguna parte de este libro puede ser reproducida o transmitida de forma alguna, ni por ningún medio, electrónico o mecánico, incluyendo fotocopia, grabación o mediante un sistema de almacenamiento y recuperación, sin la autorización previa por escrito de un representante de Bitdefender. La inclusión de citas breves en artículos sólo es posible con la mención de la fuente citada. El contenido no puede modificarse de forma alguna.

Advertencia y Renuncia de Responsabilidad. El presente producto y su documentación están protegidos por copyright. La información en este documento se provee "tal como está", sin garantía. Aunque se ha tomado toda precaución en la preparación de este documento, los autores no tendrán ninguna responsabilidad con ninguna persona o entidad con respecto a cualquier pérdida o daño causado o presuntamente causado directa o indirectamente por la información contenida en este trabajo.

Este documento contiene enlaces a sitios web de terceros que no están bajo el control de Bitdefender, por lo que Bitdefender no se hace responsable del contenido de cualquier sitio enlazado. Si usted accede a los sitios web de terceros listados en este documento, lo hará bajo su propia responsabilidad. Bitdefender proporciona estos enlaces sólo por conveniencia, y la inclusión del enlace no implica que Bitdefender apruebe o acepte ninguna responsabilidad por el contenido del sitio del tercero.

Marcas Registradas. En este documento pueden aparecer nombres de marcas registradas. Todas las marcas registradas y no registradas, en este documento, son propiedad exclusiva de sus respectivos propietarios, y respectivamente reconocidas.



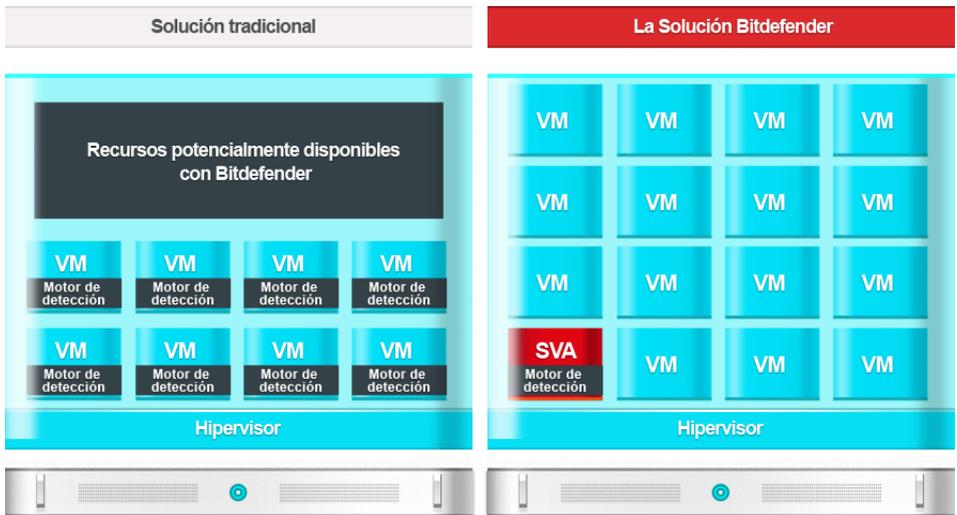
Tabla de contenidos

1. Acerca de Security for Virtualized Environments	1
2. Iniciando	4
2.1. Conectar a Security Console	4
2.2. Descripción general de Security Console	4
2.3. Directrices	5
2.4. Cambiar la contraseña de inicio de sesión predeterminada	5
2.5. Gestionar su cuenta	6
2.6. Trabajar con datos de la tabla	7
3. Panel de monitorización	8
3.1. Portlets de panel	8
3.2. Administrar Portlets	10
4. Usar informes	11
4.1. Tipos de informes disponibles	11
4.2. Creando Informes	13
4.3. Ver y administrar informes generados	14
4.3.1. Visualizando los Informes	15
4.3.2. Buscar detalles del informe	15
4.3.3. Guardar Informes	16
4.3.4. Imprimiendo los Informes	16
4.3.5. Enviar informes por correo	16
4.3.6. Eliminación automática de informes	16
4.3.7. Eliminar Informes	17
4.4. Administrar informes programados	17
4.4.1. Ver último informe generado	17
4.4.2. Renombrar informes programados	17
4.4.3. Editar informes programados	18
4.4.4. Eliminar informes programados	18
5. Registro de actividad del usuario	20
6. Obtener Ayuda	21
Glosario	22

1. Acerca de Security for Virtualized Environments

Las organizaciones hoy en día confían en las tecnologías de virtualización para incrementar el retorno de su inversión en infraestructuras de centros de datos. La consolidación de las cargas de trabajo de servidor y usuario final en infraestructuras compartidas ha conducido a la reducción de costes por deduplicación de recursos de hardware. La virtualización también proporciona ventajas operativas significativas mediante aprovisionamiento casi al instante a medida que las organizaciones crean y se apoyan en nubes públicas y privadas.

Para darse cuenta de todo el potencial de los centros de datos virtualizados, las organizaciones deben también ponerse como objetivo la consolidación de elementos de las propias cargas de trabajo, siendo la seguridad un elemento que debe estar presente en todas las cargas de trabajo. Para obtener tasas de consolidación y beneficios operacionales cada vez mayores, las organizaciones no deben sacrificar la seguridad mientras sus valiosas firmas cada vez están más amenazadas por atacantes aún más dedicados, sofisticados y especializados.



Bitdefender enfoque

Security for Virtualized Environments (SVE) es la primera solución de seguridad global para centros de datos virtualizados. SVE no sólo protege servidores y sistemas de usuario final

Windows, sino también sistemas Linux y Solaris. Integrado con VMware vShield y VMware vCenter, su arquitectura única también le permite defender sistemas que se ejecuten sobre cualquier tecnología de virtualización de sistemas. A medida que las organizaciones aumentan sus tasas de consolidación, la seguridad de Bitdefender que ha sido diseñada para, desde el primer día, proporcionar una seguridad fiable, proactiva y avanzada en entornos virtualizados se convierte en la piedra angular para construir y mejorar las estrategias de virtualización del centro de datos.

Cuando se instala en entornos VMware, SVE se beneficia de vShield Endpoint. No obstante, SVE no depende de la tecnología de virtualización; protege cualquier entorno basado en cualquier tecnología de virtualización.

Componentes

Security Virtual Appliance

Security for Virtualized Environments deduplica y centraliza buena parte de la funcionalidad en un único appliance virtual dedicado en cada host físico. Este appliance virtual de análisis de Linux reforzado se ocupa de las necesidades de análisis y mantenimiento (actualizaciones, mejoras, RAM, IOPS, etc.) de los clientes antimalware.

Security Console

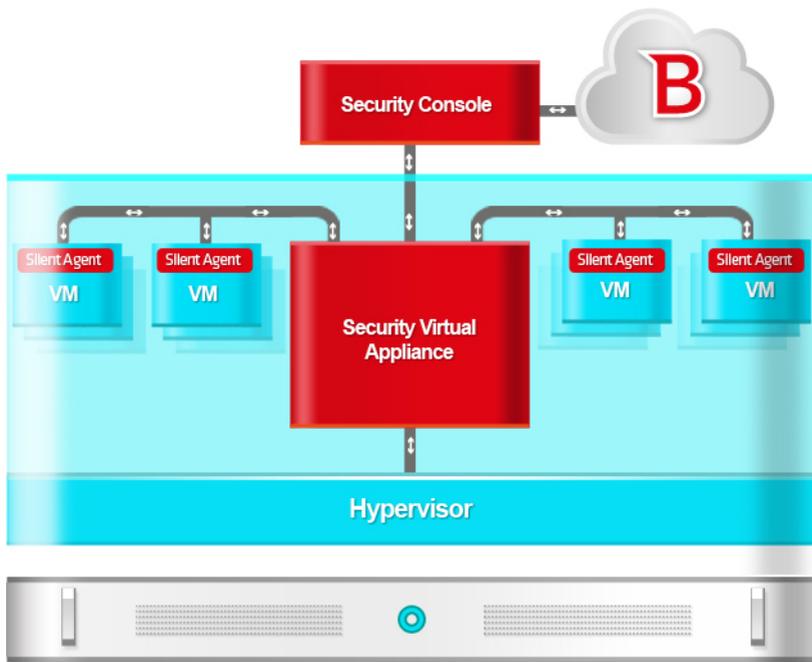
Security Console es una interfaz Web central utilizada para la implementación, configuración, monitorización, y generación de informes sobre el estado de seguridad de los centros de datos y los sistemas de usuario final. Basándose en la Bitdefender Gravity Architecture, una única Consola de seguridad y almacén de datos son fácilmente escalables horizontalmente desde las implementaciones más pequeñas hasta las más grandes.

Security Console se distribuye como un appliance virtual. El appliance Security Console también incluye el **Servidor de Actualizaciones**, componente que gestiona todas las tareas de actualización de productos y de firmas. El Servidor de Actualización es el único componente que necesita acceso a Internet para poder comunicarse con Bitdefender Cloud.

Silent Agent

Silent Agent es el componente en el lado del guest que facilita los análisis de memoria, al acceder o bajo demanda. Es una aplicación ligera, que a su vez tiene la función secundaria de mantener al corriente al usuario sobre el estado de seguridad local.

Silent Agent debe estar instalado en cada máquina virtual para que esté protegida (a diferencia de los entornos VMware donde Security for Virtualized Environments está integrado con vShield Endpoint). El kit de Silent Agent está disponible vía Security Console.



Componentes y operativa

2. Iniciando

Security for Virtualized Environments puede configurarse y administrarse usando la Security Console, una interfaz web central. La instalación, configuración y administración de tareas son realizadas por administradores.

Como usuario de una cuenta de informador, solamente puede monitorizar la protección de Security for Virtualized Environments y crear y visualizar informes de seguridad.

2.1. Conectar a Security Console

El acceso a Security Console se realiza a través de las cuentas de usuario. Recibirá su información de inicio de sesión por correo una vez que se haya creado su cuenta.

Para conectarse a Security Console:

1. Requisitos:
 - El appliance virtual de Security Console debe estar encendido, conectado a Internet y accesible desde cualquier equipo.
 - Internet Explorer 8+, Mozilla Firefox 4+, Google Chrome, Safari u Opera
 - Resolución de pantalla recomendada: 1024x768 o superior
2. Abra su navegador Web.
3. Vaya a la dirección IP del host de la consola (usando https).
4. Escriba la dirección de correo y contraseña de su cuenta.
5. Haga clic en **Inicio de sesión**.



Nota

Si ha olvidado su contraseña, utilice el enlace de recuperación de contraseña para recibir una nueva. Debe proporcionar la dirección de correo de su cuenta.

La primera vez que inicie sesión en la consola, se le solicitará que lea y confirme que está de acuerdo con los términos del servicio. Si no acepta estos términos, no podrá utilizar el servicio.

2.2. Descripción general de Security Console

Security Console está organizada para permitir el acceso fácil a todas las funciones.

Utilice la barra de menú en el área superior para navegar por la consola.

Panel de Control

Visualice tablas de fácil lectura que proporcionan información clave sobre seguridad referente a su red. Para más información, diríjase a [“Panel de monitorización”](#) (p. 8).

Informes

Obtenga informes de seguridad relativos a los equipos administrados. Para más información, diríjase a [“Usar informes”](#) (p. 11).

Log

Compruebe el registro de actividad del usuario. Para más información, diríjase a [“Registro de actividad del usuario”](#) (p. 20).

En la esquina superior derecha de la consola puede encontrar los siguientes enlaces:

- **Nombre de usuario.** Haga clic en su nombre de usuario para administrar la información de su cuenta y sus preferencias.
- **Ayuda y Soporte.** Haga clic en este enlace para encontrar información de soporte y ayuda.
- **Finalizar Sesión.** Haga clic en este enlace para cerrar la sesión de su cuenta.

2.3. Directrices

Aquí tiene algunas directrices para ayudarle a empezar:

1. [Cambie su contraseña predeterminada.](#)
2. Diríjase a la página **Panel de control** para ver información en tiempo real sobre la protección de Security for Virtualized Environments.
3. Vaya a la página **Informes > Nuevo informe** para crear los informes que necesite. Se recomienda crear informes programados para los tipos de informe que necesite normalmente. Para ver un informe generado, vaya a la página **Informes > Ver informes** y haga clic en el nombre del informe.

2.4. Cambiar la contraseña de inicio de sesión predeterminada

Se recomienda que cambie la contraseña de inicio de sesión predeterminada. También es aconsejable cambiar su contraseña de inicio de sesión periódicamente.

Para cambiar la contraseña de inicio de sesión:

1. Haga clic en su nombre de usuario en la esquina superior derecha de la consola.
2. Escriba una nueva contraseña en los campos correspondientes (en **Detalles de cuenta**).
3. Haga clic en **Enviar** para guardar los cambios.

2.5. Gestionar su cuenta

Para comprobar y cambiar sus detalles de cuenta y configuración:

1. Haga clic en su nombre de usuario en la esquina superior derecha de la consola.
2. Modifique o actualice sus detalles de cuenta en **Detalles de cuenta**.
 - **Nombre y apellidos.**
 - **Correo.** Esta es su dirección de correo de contacto e inicio de sesión. Los informes y notificaciones de seguridad importantes se envían a esta dirección. Las notificaciones de correo se envían automáticamente siempre que se detectan situaciones de riesgo importantes en la red.
 - **Funciones y grupo.** Estos campos representan su tipo de cuenta y el grupo de equipos que tiene a su cargo.
 - **Contraseña.** Para cambiar su contraseña de inicio de sesión, escriba una nueva en los campos correspondientes.
3. **¡Sólo cuenta de empresa!** Bajo **Configuración proxy**, seleccione **Usar proxy** si la máquina Security Console se conecta a Internet a través de un servidor proxy. Deben indicarse las siguientes opciones:
 - Dirección del servidor proxy.
 - Número de puerto usado por el servidor proxy.
 - Nombre de usuario reconocido por el proxy.
 - Contraseña válida para el nombre de usuario especificado anteriormente.
4. **¡Sólo cuenta de empresa!** Bajo **Configuración SMTP**, puede configurar Security Console para enviar informes por e-mail y notificaciones usando un servidor de correo externo en lugar del servidor de correo postfix incorporado. Si no especifica ninguna configuración, Security Console usa el servidor de correo incluido.
 - **IP/ Nombre del host.** Introduzca la dirección IP o el nombre del host del servidor de correo que va a enviar los e-mails.
 - **Puerto.** Introduzca el puerto utilizado para conectarse con el servidor de correo.
 - **Nombre de Usuario.** Si el servidor SMTP requiere autenticación, introduzca una dirección de e-mail / nombre de usuario reconocible.
 - **Contraseña.** Si el servidor SMTP requiere autenticación, introduzca la contraseña del usuario especificado anteriormente.
 - **Cifrado.** Si el servidor SMTP requiere una conexión encriptada, escoja el tipo apropiado en el menú (SSL o TLS).
 - **Desde el nombre.** Introduzca el nombre que quiere que aparezca en campo De del e-mail (el nombre del remitente).

- **Desde el e-mail.** Introduzca la dirección de e-mail que quiere que aparezca en el campo De del e-mail (dirección de e-mail del remitente).
5. Configure las opciones de cuenta según sus preferencias en **Configuración**.
- **Zona horaria.** Elija desde el menú la zona horaria de la cuenta. La consola mostrará la información de la hora de acuerdo con la zona horaria seleccionada.
 - **Idioma.** Elija desde el menú el idioma de visualización de la consola.
6. Haga clic en **Enviar** para guardar los cambios.

2.6. Trabajar con datos de la tabla

Las tablas se usan frecuentemente en la consola para organizar los datos en un formato más fácil de usar. Puede que esta información le sea útil:

- Las tablas pueden distribuirse en varias páginas (por omisión se muestran únicamente diez entradas por página). Para moverse por las páginas, use los botones de navegación en la parte inferior de la tabla. Para cambiar el número de entradas mostradas en una página, seleccione una opción desde el menú junto a los botones de navegación.
- Para encontrar fácilmente lo que está buscando, utilice los cuadros de búsqueda o las opciones de filtrado bajo los encabezados de columna.
- También puede hacer clic en los encabezados de la columna para ordenar la información por una columna específica. Haga clic en el encabezado de la columna nuevamente para cambiar el sentido de ordenación.

Para asegurarse de que se está mostrando la última información, haga clic en el botón  **Refrescar** en la esquina inferior izquierda de la tabla.

3. Panel de monitorización

Cada vez que se conecta a Security Console, se muestra la página **Panel** automáticamente. El panel de control es una página de estado que consiste en siete portlets que le proporcionan una rápida visión general sobre la seguridad de todas las máquinas virtuales protegidas.

Los portlets del panel muestran diversa información de seguridad utilizando tablas de fácil lectura, permitiendo por ello una identificación rápida de cualquier problema que pudiera requerir su atención. Cada portlet del panel incluye un informe detallado en segundo plano, accesible haciendo clic sobre el gráfico.

Algunos portlets ofrecen información de estado, mientras otros informan sobre los sucesos de la seguridad en el último periodo. Puede comprobar y configurar el periodo de informe de un portlet haciendo clic en el botón  de su barra de título.

3.1. Portlets de panel

El panel de control consiste en los siguientes portlets:

Estado de la Red

Le proporciona información detallada sobre el estado general de seguridad de la red. Los equipos se agrupan basándose en estos criterios:

- Los equipos no administrados no tienen instalada la protección Security for Virtualized Environments y su estado de seguridad no puede evaluarse. Los agentes de Security for Virtualized Environments instalados en máquinas virtuales protegidas detectan automáticamente los equipos no administrados. Pueden representar no solo máquinas virtuales, sino también equipos físicos (si están conectados a la red virtual).
- Los equipos offline normalmente tienen la protección Security for Virtualized Environments instalada, pero no hay actividad reciente de Silent Agent. El estado de seguridad de los equipos offline no puede evaluarse con precisión porque la información sobre su estado no es reciente.
- Los equipos protegidos tienen instalada la protección Security for Virtualized Environments y no se han detectado amenazas de seguridad.
- Los equipos vulnerables tienen instalada la protección de Security for Virtualized Environments, pero determinadas condiciones impiden la adecuada protección del sistema. Los detalles del informe le muestran qué aspectos de la seguridad necesitan abordarse.

Estado del equipo

Le proporciona diversas informaciones de estado relativas a los equipos en los que se ha instalado la protección Security for Virtualized Environments.

- Estado de actualización de protección
- Estado de protección antimalware
- Estado de la licencia
- Estado de actividad de la red (online/offline)

Puede aplicar filtros según aspectos de la seguridad y estado para encontrar la información que está buscando.

Equipos más infectados

Muestra los equipos más infectados en la red en un periodo de tiempo específico.

Malware más detectado

Le muestra las principales amenazas malware detectadas en la red en un periodo de tiempo específico.

Actividad de malware

Le ofrece detalles generales y por equipo sobre las amenazas de malware detectadas en la red en un periodo de tiempo específico. Puede ver:

- Número de detecciones (archivos que se han encontrado infectados con malware)
- Número de infecciones resueltas (archivos que han sido desinfectados o aislados con éxito en la carpeta de cuarentena)
- Número de infecciones bloqueadas (archivos que no pudieron desinfectarse pero se ha rechazado el acceso ellos; por ejemplo, un archivo infectado almacenado en algún formato comprimido propietario)

Estado malware de los equipos

Le ayuda a encontrar cuántos y cuáles de los equipos protegidos han sido afectados por malware en un periodo de tiempo específico y cómo se han tratado las amenazas. Los equipos se agrupan basándose en estos criterios:

- Equipos sin detecciones (no se ha detectado ninguna amenaza malware en el periodo de tiempo especificado)
- Equipos con malware solucionado (todos los archivos detectados han sido desinfectados correctamente o aislados en la carpeta de cuarentena local)
- Equipos con malware bloqueado (se ha rechazado el acceso a algunos de los archivos detectados)

Notificaciones

Este portlet, que aparece minimizado por omisión, le informa sobre los riesgos de seguridad existentes en el entorno virtualizado. Las notificaciones también se le envían por email.

3.2. Administrar Portlets

El panel de control es fácil de configurar basándose en las preferencias individuales.

Puede minimizar los portlets para centrarse en la información en la que está interesado. Cuando minimiza un portlet, se elimina del panel de control y su barra de título aparece en la parte inferior de la página. Los portlets restantes se dimensionan automáticamente para ajustarse a la pantalla. Todos los portlets minimizados pueden restaurarse en cualquier momento.

Para gestionar un portlet, utilice los botones de su barra de título:

-  La opción de refresco cargará datos para cada portlet.
-  Haga clic en este botón para configurar las opciones del portlet. Algunos portlets incluyen datos de un periodo de tiempo específico.
-  Minimice el portlet en la parte inferior de la página.
-  Restaure un portlet minimizado.

4. Usar informes

Security Console le permite crear y visualizar informes centralizados sobre el estado de seguridad de las máquinas virtuales. Los informes pueden usarse para múltiples propósitos, tales como:

- Monitorizar y asegurar el cumplimiento de las políticas de seguridad de la empresa.
- Comprobando y evaluando el estado de seguridad de la red virtual.
- Identificar los problemas de seguridad, amenazas y vulnerabilidades.
- Monitorizar los incidentes de seguridad y la actividad malware.
- Proporcionando una administración superior con datos de fácil interpretación sobre la seguridad de la MV.

Hay disponibles varios tipos de informes diferentes para que pueda conseguir fácilmente la información que necesita. La información se presenta a través de gráficos circulares de fácil comprensión, tablas y diagramas, permitiéndole comprobar rápidamente el estado de seguridad de la red virtual e identificar las incidencias de seguridad.

Los informes pueden consolidar información de toda la red virtual o únicamente de grupos MV específicos. De este modo, en un sólo informe puede encontrar la siguiente información:

- Información estadística referida a todas o grupos de máquinas virtuales protegidas.
- Información detallada para cada máquina virtual protegida.
- La lista de MVs que cumplen un criterio específico (por ejemplo, aquellas que tienen desactivada la protección antimalware).

Todos los informes generados están disponibles en Security Console durante un periodo predeterminado de 90 días, pero puede guardarlos en su equipo o enviarlos por correo. Los formatos disponibles incluyen Portable Document Format (PDF) y Comma-Separated Values (CSV).

4.1. Tipos de informes disponibles

Esta es la lista de tipos de informes disponibles:

Actualización

Muestra el estado de actualización de la protección de Security for Virtualized Environments instalada en los equipos seleccionados. Usando los filtros disponibles, puede descubrir fácilmente qué clientes se han actualizado o no, en un periodo de tiempo específico.

Estado del equipo

Le proporciona diversas informaciones de estado relativas a los equipos seleccionados en los que se ha instalado la protección Security for Virtualized Environments.

- Estado de actualización de protección
- Estado de la licencia
- Estado de actividad de la red (online/offline)
- Estado de protección antimalware

Puede aplicar filtros según aspectos de la seguridad y estado para encontrar la información que está buscando.

Actividad de malware

Le ofrece detalles generales y por equipo sobre las amenazas de malware detectadas en un periodo de tiempo específico en los equipos seleccionados. Puede ver:

- Número de detecciones (archivos que se han encontrado infectados con malware)
- Número de infecciones resueltas (archivos que han sido desinfectados o aislados con éxito en la carpeta de cuarentena)
- Número de infecciones bloqueadas (archivos que no pudieron desinfectarse pero se ha rechazado el acceso ellos; por ejemplo, un archivo infectado almacenado en algún formato comprimido propietario)

Estado del módulo de protección

Le informa del estado de la protección antimalware en los equipos seleccionados. El estado de protección puede habilitarse o deshabilitarse. Los detalles del informe también proporcionan información sobre el estado de actualización.

Puede aplicar filtros según estado para encontrar la información que está buscando.

Equipos más infectados

Muestra los equipos más infectados durante un periodo de tiempo específico entre los equipos seleccionados.

Malware más detectado

Le muestra las amenazas malware más detectadas en un periodo de tiempo específico en los equipos seleccionados.

Estado de la Red

Le proporciona información detallada sobre el estado general de seguridad de la red. Los equipos se agrupan basándose en estos criterios:

- Los equipos no administrados no tienen instalada la protección Security for Virtualized Environments y su estado de seguridad no puede evaluarse. Los agentes de Security for Virtualized Environments instalados en máquinas virtuales protegidas detectan automáticamente los equipos no administrados. Pueden representar no solo máquinas virtuales, sino también equipos físicos (si están conectados a la red virtual).
- Los equipos offline normalmente tienen la protección Security for Virtualized Environments instalada, pero no hay actividad reciente de Silent Agent. El estado

de seguridad de los equipos offline no puede evaluarse con precisión porque la información sobre su estado no es reciente.

- Los equipos protegidos tienen instalada la protección Security for Virtualized Environments y no se han detectado amenazas de seguridad.
- Los equipos vulnerables tienen instalada la protección de Security for Virtualized Environments, pero determinadas condiciones impiden la adecuada protección del sistema. Los detalles del informe le muestran qué aspectos de la seguridad necesitan abordarse.

Estado malware de los equipos

Le ayuda a encontrar cuántos y cuáles de los equipos seleccionados han sido afectados por malware en un periodo de tiempo específico y cómo se han tratado las amenazas. Los equipos se agrupan basándose en estos criterios:

- Equipos sin detecciones (no se ha detectado ninguna amenaza malware en el periodo de tiempo especificado)
- Equipos con malware solucionado (todos los archivos detectados han sido desinfectados correctamente o aislados en la carpeta de cuarentena local)
- Equipos con malware bloqueado (se ha rechazado el acceso a algunos de los archivos detectados)

Ejecutivo

Le permite exportar las gráficas desde los portlets del panel de control a un archivo PDF.

4.2. Creando Informes

Para crear un informe:

1. Vaya a la página **Informes > Nuevo informe**.



Nota

Si se encuentra en la página **Ver informes** o **Informes programados**, simplemente haga clic en el botón **Nuevo** ubicado encima de la tabla.

2. Seleccione el tipo de informe deseado desde el menú. Para más información, diríjase a [“Tipos de informes disponibles” \(p. 11\)](#).
3. Escriba un nombre descriptivo para el informe. Al elegir un nombre, tenga en cuenta el tipo de informe y objetivo, y posiblemente las opciones del informe.
4. Configure el objetivo del informe. Seleccione una de las opciones disponibles y haga clic en el enlace correspondiente para elegir el grupo o máquinas virtuales individuales que se incluirán en el informe.

5. Configure la recurrencia del informe (programación). Puede elegir crear el informe inmediatamente, diariamente, semanalmente (en un día específico de la semana) o mensualmente (en un día específico del mes).
6. Configure las opciones del informe.
 - a. Para la mayor parte de los tipos de informe, cuando crea un informe inmediato, debe especificar el periodo de generación de informes. El informe incluirá únicamente información sobre periodo de tiempo seleccionado.
 - b. Varios tipos de informes ofrecen opciones de filtrado para ayudarle a encontrar fácilmente la información en la que está interesado. Utilice las opciones de filtrado para obtener únicamente la información deseada. Por ejemplo, para un informe de **Estado de actualización** puede elegir ver sólo la lista de MVs protegidas que se han actualizado (o, por el contrario, las que no se han actualizado) en el período de tiempo seleccionado.



Nota

Cuando visualiza el informe en la consola, toda la información está disponible, independientemente de las opciones seleccionadas. Si de todas formas descarga o envía por correo el informe, se incluirá en el archivo PDF únicamente el resumen del informe y la información seleccionada. Los detalles completos del informe sólo estarán disponibles en formato CSV.

- c. Para recibir el informe por correo, seleccione la opción correspondiente.
7. Haga clic en **Generar** para crear el informe.
 - Si ha elegido crear un informe inmediato, se mostrará en la página [Ver informes](#). El tiempo requerido para crear los informes puede variar dependiendo del número de MVs administradas. Por favor, espere a que finalice la creación del informe. Una vez que se ha creado el informe, puede verlo haciendo clic sobre su nombre.
 - Si ha elegido crear un informe programado, se mostrará en la página [Informes programados](#).

4.3. Ver y administrar informes generados

Para ver y administrar los informes generados, vaya a la página **Informes > Ver informes**. Esta página se muestra automáticamente tras crear un informe inmediato.



Nota

Los informes programados pueden administrarse desde la página [Informes > Informes programados](#).

Puede ver los informes generados e información útil acerca de ellos:

- Nombre del informe y tipo.
- Cuando se generó el informe.

Para ordenar los informes por una columna específica, haga clic simplemente en el encabezado de esa columna. Haga clic nuevamente sobre el encabezado para cambiar el sentido de ordenación.

Cada informe se marca con uno de los siguientes iconos para indicarle si el informe está programado o no:

-  Indica un informe para una única vez.
-  Indica un informe programado.

Para asegurarse de que se está mostrando la última información, haga clic en el botón  **Refrescar** en la esquina inferior izquierda de la tabla.

4.3.1. Visualizando los Informes

Para ver un informe:

1. Vaya a la página **Informes > Ver informes**.
2. Haga clic en el nombre del informe que quiere ver. Para encontrar fácilmente el informe que está buscando, puede ordenar los informes por nombre, tipo u hora de creación.

Todos los informes consisten en una página Resumen y una página de Detalles.

- La página Resumen le ofrece datos estadísticos (gráficos circulares y diagramas) para todas las MVs o grupos objetivo. En la parte inferior de la página puede ver información general sobre el informe, como el período del informe (si es aplicable), objetivo del informe, etc.
- La página de Detalles le proporciona información detallada de cada MV administrada. En algunos informes, es posible que necesite hacer clic en el área del gráfico de tarta de la página Resumen para ver los detalles.

Use las pestañas de la esquina superior izquierda del informe para ver la página deseada.

4.3.2. Buscar detalles del informe

Los detalles del informe se muestran en una tabla que consiste en varias columnas que ofrecen variada información. La tabla puede distribuirse en varias páginas (por omisión se muestran únicamente 10 entradas por página). Para navegar por las páginas de detalle, use los botones en la parte inferior de la tabla.

Para encontrar fácilmente lo que está buscando, utilice los cuadros de búsqueda o las opciones de filtrado bajo los encabezados de columna.

Para ordenar los detalles del informe por una columna específica, haga clic simplemente en el encabezado de esa columna. Haga clic nuevamente sobre el encabezado para cambiar el sentido de ordenación.

4.3.3. Guardar Informes

Los informes generados están disponibles, de forma predeterminada, en Security Console durante 90 días. Pasado este periodo, se eliminan automáticamente.

Si necesita que los informes estén disponibles durante periodos de tiempo más largos, puede guardarlos en su equipo. El resumen del informe y la información del informe seleccionada estarán disponibles en formato PDF, mientras que los detalles del informe completo estarán disponibles en formato CSV.

Para guardar el informe que está visualizando en su equipo:

1. Haga clic en el botón **Exportar** en la esquina superior derecha de la página de informe. Aparecerá una ventana de descarga.
2. Descargue el archivo `.zip` en su equipo. Dependiendo de la configuración de su navegador, el archivo puede ser descargado automáticamente a una ubicación de descarga predeterminada.

4.3.4. Imprimiendo los Informes

Para imprimir un informe, primero debe guardarlo en su equipo.

4.3.5. Enviar informes por correo

Para enviar por correo el informe que está viendo:

1. Haga clic en el botón **Email** en la esquina superior derecha de la página de informe. Aparecerá una ventana.
2. Si lo desea puede cambiar el nombre del informe.
3. Introduzca las direcciones de correo de las personas a las que desea enviar el informe, separándolas por punto y coma (;).
4. Haga clic en **Enviar email**.

4.3.6. Eliminación automática de informes

Los informes generados están disponibles, de forma predeterminada, en Security Console durante 90 días. Pasado este periodo, se eliminan automáticamente.

Para modificar el periodo de eliminación automático para los informes generados:

1. Vaya a la página **Informes > Ver informes**.
2. Haga clic en el enlace en la parte inferior de la tabla.
3. Seleccione el nuevo período desde el menú.
4. Haga clic en **Aceptar**.

4.3.7. Eliminar Informes

Para eliminar un informe:

1. Vaya a la página **Informes > Ver informes**.
2. Seleccione el informe.
3. Haga clic en el botón **Eliminar** ubicado encima de la tabla.

4.4. Administrar informes programados

Cuando se crea un informe, puede elegir configurar una planificación basada en que el informe se generará automáticamente (a intervalos de tiempo regulares). Tales informes se denominan informes programados.

Los informes generados estarán disponibles en la página **Informes > Ver informes** durante un periodo predeterminado de 90 días. También se le enviarán por correo si ha seleccionado esta opción.

Para administrar informes programados, vaya a la página **Informes > Informes programados**. Puede ver todos los informes programados y la información útil acerca de ellos:

- Nombre del informe y tipo.
- Programación basada en la cual el informe se genera automáticamente.
- Cuando se generó el informe por última vez.

4.4.1. Ver último informe generado

Desde la página **Informes > Informes programados**, puede ver fácilmente el informe generado más recientemente haciendo clic en el enlace de la columna **Último informe generado**.

4.4.2. Renombrar informes programados

Los informes generados por un informe programado basan en él su nombre. Renombrar un informe programado no afecta a los informes generados anteriormente.

Para renombrar un informe programado:

1. Vaya a la página **Informes > Informes programados**.
2. Haga clic en el nombre del informe.
3. Cambie el nombre del informe en el campo correspondiente. Elija un nombre descriptivo para el informe para poder identificar fácilmente de qué se trata. Al elegir un nombre, tenga en cuenta el tipo de informe y objetivo, y posiblemente las opciones del informe.

4. Haga clic en **Enviar** para guardar los cambios.

4.4.3. Editar informes programados

Para cambiar la configuración de un informe programado:

1. Vaya a la página **Informes > Informes programados**.
2. Haga clic en el nombre del informe.
3. Cambiar los ajustes del informe según sea necesario. Puede cambiar lo siguiente:
 - **Nombre del informe.** Elija un nombre descriptivo para el informe para poder identificar fácilmente de qué se trata. Al elegir un nombre, tenga en cuenta el tipo de informe y objetivo, y posiblemente las opciones del informe. Los informes generados por un informe programado basan en él su nombre.
 - **Objetivo del informe.** La opción seleccionada indica el tipo de objetivo del informe actual (bien sean grupos o máquinas virtuales individuales). Haga clic en el enlace correspondiente para ver el objetivo del informe actual. Para cambiarlo, haga clic en cualquiera de los dos enlaces y seleccione los grupos o MVs que desee incluir en el informe.
 - **Recurrencia de informe (calendario).** Puede configurar el informe para que se genere de forma automática diariamente, semanalmente (en un día específico de la semana) o mensualmente (en un día específico del mes). Dependiendo del programa seleccionado, el informe incluirá sólo datos del último día, semana o mes, respectivamente.
 - **Opciones de informe.** Puede elegir recibir el informe por email. La mayoría de informes poseen opciones de filtrado para ayudarle a encontrar fácilmente la información en la que está interesado. Cuando visualiza el informe en la consola, toda la información está disponible, independientemente de las opciones seleccionadas. Si de todas formas descarga o envía por correo el informe, se incluirá en el archivo PDF únicamente el resumen del informe y la información seleccionada. Los detalles completos del informe sólo estarán disponibles en formato CSV.
4. Haga clic en **Enviar** para guardar los cambios.

4.4.4. Eliminar informes programados

Cuando ya no se necesita un informe programado, lo mejor es eliminarlo. Al eliminar un informe programado no se borrarán los informes que ha generado automáticamente hasta ese momento.

Para eliminar un informe programado:

1. Vaya a la página **Informes > Informes programados**.
2. Seleccione el informe.

3. Haga clic en el botón **Eliminar** ubicado encima de la tabla.

5. Registro de actividad del usuario

Security Console registra todas las operaciones y acciones ejecutadas por los usuarios. Los eventos registrados incluyen lo siguiente:

- Iniciar y cerrar sesión
- Crear, editar, renombrar, eliminar cuentas de usuario
- Crear, editar, renombrar, eliminar políticas
- Crear, editar, renombrar, eliminar informes
- Eliminar, restaurar archivos de cuarentena
- Eliminar o mover equipos entre grupos
- Crear, mover, renombrar, eliminar grupos

Para examinar los registros de actividad del usuario, vaya a la página **Log**.

Los eventos registrados se muestran en una tabla. Las columnas de la tabla le proporcionan información sobre los eventos listados:

- Nombre del usuario que realizó la acción.
- Tipo de cuenta de usuario.
- Acción que produjo el evento.
- Tipo de objeto de la consola afectado por la acción.
- Objeto específico afectado por la acción.
- Dirección IP desde la que se conecta el usuario.
- Hora en la que sucedió el evento.

Para encontrar fácilmente lo que está buscando, utilice los cuadros de búsqueda o las opciones de filtrado bajo los encabezados de columna. Para ordenar los eventos por una columna específica, haga clic simplemente en el encabezado de esa columna. Haga clic nuevamente sobre el encabezado para cambiar el sentido de ordenación.

Para ver información detallada sobre un evento, selecciónelo y compruebe la sección bajo la tabla.

Para asegurarse de que se está mostrando la última información, haga clic en el botón  **Refrescar** en la esquina inferior izquierda de la tabla.

6. Obtener Ayuda

Para cualquier problema o pregunta relativa a Security Console, contacte con un administrador.

Glosario

ActiveX

El ActiveX es un modelo para escribir programas de manera que otros programas y sistemas operativos puedan usarlos. La tecnología ActiveX se utiliza junto con Microsoft Internet Explorer para hacer páginas web interactivas que se vean y comporten como programas, y no como páginas estáticas. Con ActiveX, los usuarios pueden hacer o contestar preguntas, pulsar botones, interactuar de otras formas con una página web. Los controles ActiveX normalmente se escriben en Visual Basic.

ActiveX es notable por la ausencia absoluta de mandos de seguridad; los expertos de la seguridad computacional desapruaban el empleo de ActiveX en Internet.

Actualización

Una nueva versión de un producto de software o hardware, diseñada para reemplazar una versión anterior del mismo producto. Además, durante la instalación se verifica si en su ordenador existe una versión anterior; si no se encuentra ninguna, no se instalará la actualización.

Bitdefender tiene su propio módulo para realizar las actualizaciones, permitiéndole a usted buscar manualmente las actualizaciones o bien hacer una actualización automática del producto.

Adware

El Adware habitualmente se combina con aplicaciones que son gratuitas a cambio que el usuario acepte la instalación del componente adware. Puesto que las aplicaciones adware generalmente se instalan después que el usuario acepte los términos de licencia que declaran el propósito de la aplicación, no se comete ningún delito. Sin embargo, los pop-up de publicidad pueden resultar molestos, y en algunos casos afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar preocupación acerca de su privacidad a aquellos usuarios que no son plenamente conscientes de los términos de la licencia.

Sin embargo, los pop-up de publicidad pueden resultar molestos, y en algunos casos afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar problemas de privacidad a aquellos usuarios que no eran plenamente conscientes de los términos de la licencia.

Applet de Java

Es un programa de Java diseñado para funcionar solamente en una página web. Para usarlo tendría que especificar el nombre del applet y la dimensión (de ancho y de largo --- en pixels) que éste usará. Al acceder a una página web, el navegador descarga el

applet desde un servidor y lo abre en el ordenador del usuario (del cliente). Los applets difieren de las aplicaciones al ser gobernados por un protocolo de seguridad muy estricto.

Por ejemplo, aunque los applets se puedan ejecutar directamente en el ordenador del cliente, no pueden leer o escribir información en aquel ordenador. Además, los applets tienen restricciones en cuanto a leer y escribir información desde la misma área a la que pertenecen.

Appliance virtual

Una imagen de máquina virtual que contiene tanto un sistema operativo preconfigurado como una aplicación para facilitar la instalación y configuración de la aplicación en un entorno virtualizado.

Archivo Comprimido

Disco, cinta o directorio que contiene ficheros almacenados.

Fichero que contiene uno o varios ficheros en formato comprimido.

Archivo de informe

Es un archivo que lista las acciones realizadas. Bitdefender genera un archivo de informe (log) que contiene una lista de las rutas analizadas, las carpetas, el número de archivos y archivos comprimidos analizados, el número de archivos infectados y sospechosos que se han detectado.

Área de notificación del Sistema

Elemento introducido con el sistema Windows 95, la bandeja de sistema está ubicada en la barra de tareas de Windows (normalmente al lado del reloj) y contiene iconos en miniatura para acceder fácilmente a las funciones del sistema, como el fax, la impresora, el módem, el volumen etc. Al hacer doble clic o clic derecho en el icono correspondiente, verá y abrirá los detalles y los mandos de los programas.

Backdoor

Se trata de un agujero de seguridad dejado intencionalmente por los diseñadores o los administradores. El objetivo de estos agujeros no es siempre dañino; algunos sistemas operativos funcionan con unas cuentas privilegiadas, creadas para los técnicos de servicio u operadores de mantenimiento.

Cliente de mail

Un cliente de e-mail es una aplicación que permite enviar y recibir mensajes.

Cookie

En la industria del Internet, las cookies se describen como pequeños ficheros conteniendo información sobre los ordenadores individuales que se pueden analizar y usar por los publicistas para determinar los intereses y los gustos online de los usuarios respectivos. En este ambiente, la tecnología de las cookies se desarrolla con la intención

de construir reclamos y mensajes publicitarios correspondientes a los intereses declarados por usted. Es un arma de doble filo para mucha gente porque, por un lado, es más eficiente y pertinente que usted vea publicidades relacionadas con sus intereses. Por otro lado, implica seguir cada paso suyo y cada clic que usted haga. Por consiguiente, es normal que haya resultado un debate sobre la privacidad y mucha gente se sintió ofendida por la idea de ser vista como "número de SKU" (el código de barras ubicado en la parte posterior de los paquetes analizados a la salida de los supermercados). Aunque esta perspectiva pueda parecer extremista, en algunos casos es cierta.

Correo

Correo electrónico. Un servicio que envía mensajes a otros ordenadores mediante las redes locales o globales.

Descargar

Para copiar informaciones (por lo general un fichero entero) desde una fuente principal a un dispositivo periférico. El término se usa a menudo para describir el proceso de copiar un fichero desde un servicio online al ordenador personal. También se refiere al proceso de copiar ficheros desde un servidor de la red a un ordenador conectado a la red.

Elementos de Inicio

Todos los ficheros de esta carpeta se abren al iniciar el ordenador. Por ejemplo: una pantalla, un fichero audio, un calendario de tareas u otras aplicaciones pueden ser elementos de startup. Normalmente, se elige un alias del fichero para ubicar en esta carpeta y no directamente el fichero.

Eventos

Una acción o acontecimiento detectado por un programa. Los eventos pueden ser acciones, como por ejemplo hacer clic con el ratón o pulsar una tecla, o también pueden ser acontecimientos (agotar el espacio de memoria).

Explorador

Forma abreviada de Navegador de Web, aplicación de software empleada para ubicar y cargar las páginas web. Los dos navegadores más populares son Netscape Navigator y Microsoft Internet Explorer, sendos navegadores gráficos, lo cual significa que pueden mostrar tanto gráficos como textos. Además, la mayoría de los navegadores modernos incluyen información multimedia: sonido e imágenes, aunque requieran plugins para ciertos formatos.

Extensión de un archivo

La última parte del nombre de un fichero, que aparece después del punto e indica el tipo de información almacenada.

Hay varios sistemas operativos que utilizan extensiones de archivos (Por Ej. Unix, VMS, MS-DOS). Por lo general las extensiones tienen de uno a tres caracteres. Por ejemplo, "c" para archivos de código fuente en lenguaje C, "ps" para PostScript, "txt" para documentos de texto.

Falso positivo

Ocurre cuando un analizador identifica un fichero como infectado cuando éste no lo es.

Firma de virus

Es la secuencia binaria de un virus, utilizada por los antivirus para detectar y eliminar los virus.

Gusano

Es un programa que se propaga a través de la red, reproduciéndose mientras avanza. No se puede agregar a otros programas.

Heurístico

Es un método para identificar nuevos virus, que se basa en ciertas reglas y no en firmas específicas de los virus. La ventaja del análisis heurístico reside en la dificultad de engañarlo con una nueva versión de un virus ya existente. Sin embargo, ocasionalmente puede notificar sobre la existencia de unos códigos sospechosos en los programas normales, generando el "falso positivo".

Hypervisor

Un programa que permite ejecutar múltiples sistemas operativos en un solo equipo.

IP

Internet Protocol - Protocolo enrutable dentro del protocolo TCP/IP y que es responsable del direccionamiento IP, el enrutamiento y la fragmentación y reensamblado de los paquetes IP.

Línea de comando

En una interfaz con línea de comando, el usuario puede introducir comandos en el espacio provisto directamente en la pantalla, usando un lenguaje de comando.

Malware

Malware es el término genérico que define al software diseñado para causar daños - una contracción de 'malicious software'. Todavía no se usa de forma universal, pero su popularidad como términos general para definir virus, troyanos, gusanos y código móvil malicioso está creciendo.

Máquina virtual

Un entorno de software aislado que emula un equipo físico en el cual puede ejecutarse un sistema operativo y aplicaciones.

Memoria

Área de almacenamiento interno en un ordenador. El término memoria se refiere al almacenamiento de información en forma de virutas y la palabra almacenamiento se emplea para la memoria guardada en cintas o disquetes. Cada ordenador tiene una cierta cantidad de memoria física, generalmente denominada memoria principal o RAM.

No Heurístico

Este método de análisis se basa en firmas de virus específicas. La ventaja del análisis no heurístico es que no se le puede engañar por algo que parecería ser un virus. Por consiguiente, no genera alarmas falsas.

Phishing

Es el acto de enviar un e-mail a un usuario simulando pertenecer a una empresa existente, e intentar estafarlo solicitándole información privada con la que después se efectuará el robo. El e-mail conduce al usuario a visitar una página Web en la que se le solicita actualizar información personal, como contraseñas y números de tarjetas de crédito, seguridad social y números de cuentas corrientes, que en realidad ya posee la organización auténtica. La página Web, en cambio, es una réplica fraudulenta, creada sólo para robar la información de los usuarios.

Programas Empaquetados

Son ficheros en formato comprimido. Muchos sistemas operativos y varias aplicaciones contienen comandos que le permiten a usted empaquetar un fichero para que ocupe menos espacio en la memoria. Por ejemplo: tiene un fichero de texto conteniendo diez caracteres espacio consecutivos. Normalmente, para esto necesitaría diez bytes de almacenamiento.

Sin embargo, un programa que puede empaquetar ficheros podría reemplazar los caracteres mencionados por una serie a la que le sigue el número de espacios. En este caso, los diez espacios requieren dos bytes. Ésta es solamente una técnica para empaquetar programas o ficheros, hay muchas otras también.

Puerto

Interfaz en un ordenador a la que se puede conectar un dispositivo. Los ordenadores personales tienen distintos tipos de puertos. Hay varios puertos internos para conectar las unidades de disco, las pantallas, los teclados. Asimismo, los ordenadores personales tienen puertos externos para conectar módems, impresoras, ratones y otros dispositivos periféricos.

En las redes de tipo TCP/IP y UDP representa el punto final de una conexión lógica. El número de puerto indica el tipo del dicho puerto. Por ejemplo, el puerto 80 se usa para el tráfico http.

Rootkit

Un rootkit es un conjunto de herramientas de software que ofrecen acceso al sistema a nivel de administrador. El término empezó a usarse con los sistemas operativos UNIX

y se refería a las herramientas que proporcionaban permisos de administrador a los intrusos, permitiéndoles ocultar su presencia para no ser vistos por los administradores de sistema.

El papel principal de los rootkits es ocultar procesos, archivos, conexiones y logs. También pueden interceptar datos de terminales, conexiones de red o periféricos, si éstos incorporan el software apropiado.

Los rootkits no son maliciosos por naturaleza. Por ejemplo, los sistemas operativos y algunas aplicaciones esconden sus archivos críticos mediante rootkits. Sin embargo, normalmente se utilizan para esconder la presencia de malware o para encubrir la presencia de un intruso en el sistema. Cuando se combinan con malware, los rootkits representan una gran amenaza para la seguridad e integridad de su sistema. Pueden monitorizar el tráfico, crear puertas traseras en el sistema, alterar archivos o logs, y evitar su detección.

Ruta

Las direcciones exactas de un fichero en un ordenador, generalmente descritas mediante un sistema jerárquico: se empieza por el límite inferior, mostrando un listado que contiene la unidad de disco, el directorio, los subdirectorios, el fichero mismo, la extensión del fichero si tiene alguna. Esta suma de informaciones es una ruta completamente válida.

La ruta entre dos puntos, como por ejemplo el canal de comunicación entre dos ordenadores.

Script

Es otro término para macro o fichero batch y se constituye de una lista de comandos que se pueden ejecutar sin la intervención del usuario.

Sector de arranque

Un sector al principio de cada disco y que identifica la arquitectura del disco (tamaño del sector, tamaño del cluster, etc). Para los discos de inicio, el sector de arranque también incluye un programa para cargar el sistema operativo.

Sistema operativo del guest

Un sistema operativo aislado que funciona dentro de otro sistema operativo (el host) dentro de un sistema virtualizado.

Sistema operativo del host

Un sistema operativo dentro del cual otros sistemas operativos (los guests) se ejecutan por virtualización.

Spam

Correo basura o los posts basura en grupos de noticias, también denominado correo no solicitado.

Spyware

Se trata de cualquier software que, en secreto, recopile información del usuario a través de su conexión a Internet sin su consentimiento, generalmente con fines comerciales. Las aplicaciones Spyware son, generalmente, componentes ocultos de programas freeware o shareware que pueden descargarse por Internet; sin embargo, debe observarse que la gran mayoría de aplicaciones shareware y freeware no contienen spyware. Una vez instalado, el spyware monitoriza la actividad del usuario en Internet y, en segundo plano, envía esa información a una tercera persona. El spyware también puede recoger información acerca de las direcciones de correo, e incluso contraseñas y números de tarjetas de crédito.

El spyware es similar al Troyano en el hecho que los usuarios los instalan inconscientemente cuando instalan otra aplicación. Una forma habitual de infectarse con spyware es descargando, a través de programas de intercambio de ficheros, un determinado archivo que intercambia el nombre de los productos compartidos.

A parte de las cuestiones de ética y privacidad, el spyware roba al usuario recursos de memoria y ancho de banda mientras envía la información al creador del Spyware a través de la conexión de Internet del usuario. Puesto que el spyware utiliza memoria y recursos del sistema, las aplicaciones que se ejecutan en segundo plano pueden provocar errores del sistema o inestabilidad general del mismo.

TCP/IP

Transmission Control Protocol/Internet Protocol - Es una gama de protocolos de red, extremadamente utilizados en Internet para proporcionar comunicaciones en las redes interconectadas, que incluyen ordenadores con distintas arquitecturas de hardware y varios sistemas operativos. TCP/IP ofrece estándares para el modo de comunicación entre ordenadores y convenciones para las redes interconectadas.

Troyano

Es un programa destructivo disfrazado como aplicación benigna. A diferencia de los virus, los caballos troyanos no se multiplican; sin embargo pueden ser igual de peligrosos. Unos de los tipos más insidiosos de Troyano es un programa que pretende desinfectar su ordenador y que en realidad introduce virus.

El término tiene origen en la famosa obra "La Ilíada" de Homero, en la cual Grecia entrega un gigantesco caballo de madera a sus enemigos, los Troyanos, como supuesta oferta de paz. Pero una vez los Troyanos arrastraron el caballo hasta el interior de las murallas de la ciudad, los soldados Griegos salieron de un hueco del vientre del caballo y abrieron las puertas de las murallas, permitiendo la entrada de sus compatriotas y la conquista de Troya.

Unidad de disco

Es un dispositivo que lee la información y / o la escribe en un disco.

Una unidad de disco duro lee y escribe en los discos duros.

Una unidad de disquetera abre disquetes.

Las unidades de disco pueden ser internas (guardadas en el ordenador) o externas (guardadas en una caja separada conectada al ordenador).

Virus

Es un programa o una parte de un código cargado en su ordenador sin avisarle y en contra de su voluntad. La mayoría de los virus se pueden multiplicar. Todos los virus informáticos son artificiales, creados por una persona. Es muy simple producir un virus que se multiplique continuamente. Pero, aún así, sería muy peligroso porque dentro de poco tiempo estaría usando toda la memoria disponible y llevaría al bloqueo del sistema. Un tipo de virus todavía más peligroso es uno capaz de propagarse a través de redes y evitando los sistemas de seguridad.

Virus de boot

Es un virus que infecta el sector de arranque de un disco duro o disquete. Al intentar arrancar el sistema desde un disco infectado con un virus de boot, el virus quedará cargado en la memoria. A partir de ese momento, cada vez que intente arrancar el sistema, tendrá el virus activo en la memoria.

Virus de macro

Es un tipo de virus informático, que se encuentra codificado como un macro incluido en un documento. Muchas aplicaciones, como las de Microsoft Word o Excel, soportan fuertes lenguajes de macro.

Estas aplicaciones permiten introducir una macro en un documento y también que la macro se ejecute cada vez que se abra el documento.

Virus Polimórfico

Son virus que se modifican en cada fichero que infectan. Al no tener una secuencia binaria constante, son muy difíciles de identificar.