

BitDefender for File Servers

INICIO RÁPIDO



Cómo funciona?

BitDefender for File Servers es una solución desarrollada especialmente para servidores que funcionan bajo la plataforma Windows. Sus principales características cubren las necesidades principales de un servidor de intercambio de archivos, mientras que su propósito es el de reducir la carga que conlleva administrar una solución de software para servidores. Fácil de instalar y configurar, pero con un fuerte conjunto de funcionalidades, está destinado tanto a grandes como a pequeñas organizaciones.

Almacenar, compartir y distribuir información son las tareas principales de la gestión de información, pero estas fallarían sin un fácil acceso a la información, sin la integridad de la misma y sin un buen tiempo de actividad del sistema. BitDefender for File Servers aborda las cuestiones de la seguridad de los datos y la disponibilidad del sistema con:

Tecnologías antivirus avanzadas

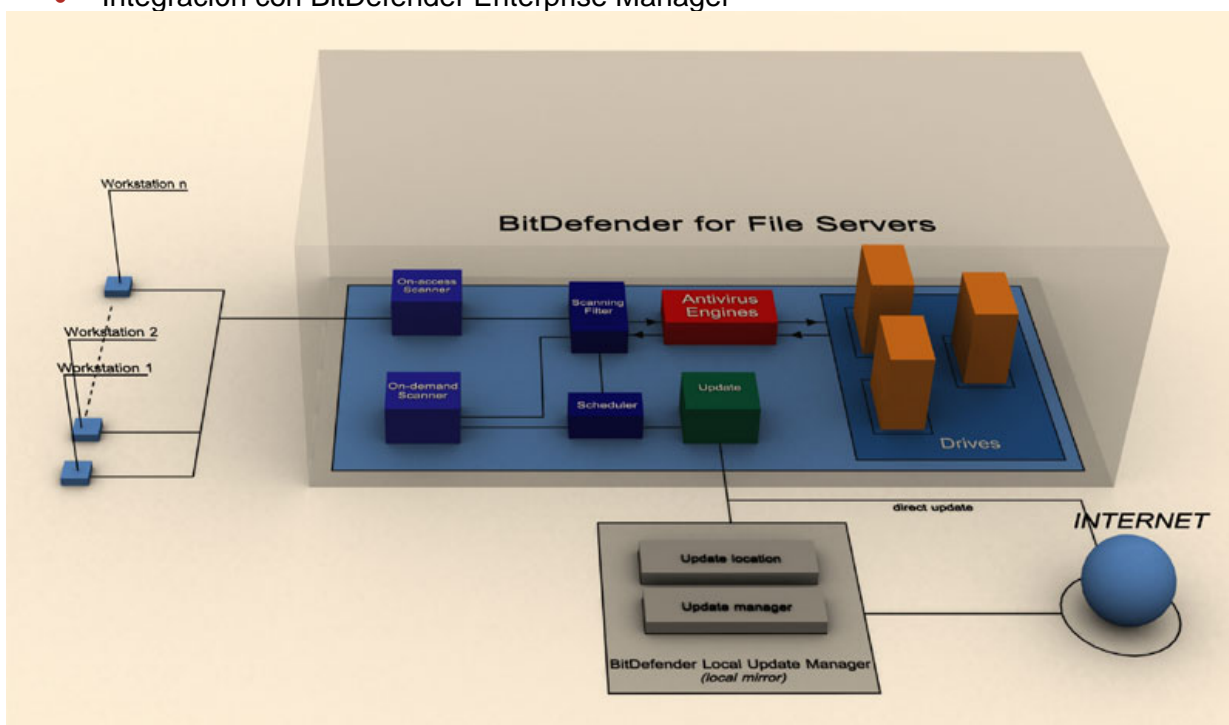
- Tecnología HiVE y motores certificados
- Análisis optimizados y análisis multihilo

Fuertes funcionalidades

- Análisis tanto al-acceder como bajo demanda
- Actualizaciones automáticas

Aumento de la Usabilidad

- Sistema de programación de tareas
- Sistema de registro de eventos, informes y alertas
- Integración con BitDefender Enterprise Manager



En el diagrama superior, se describen los principales procesos, el análisis antivirus y las actualizaciones.

Para mejorar su función como solución de seguridad destinada a servidores, **BitDefender for File Servers** ha sido desarrollada basándose en una arquitectura modular. Los módulos principales son:

- Analizador al-acceder
- Analizado bajo demanda
- Actualización
- Programador
- Filtro de Análisis
- Motores Antivirus

La protección en tiempo real

A medida que los archivos se escriben en el disco o se accede a ellos, el módulo **Analizador al-acceder** intercepta el evento e inicia el proceso de análisis.

Los pasos siguientes pueden describir el proceso de análisis:

1. El filtro de análisis comprueba el archivo. La extensión del archivo, el tamaño del archivo y la ruta del archivo se comprueban de forma secuencial para que el análisis coincida con la configuración del administrador. El resultado del Filtro de Análisis es ANALIZAR o NO ANALIZAR.
2. Si el resultado del Filtro de Análisis es ANALIZAR, el archivo es analizado por los Motores Antivirus. Primero se verifica el archivo a partir de la base de datos de firmas de virus. Si cualquier parte del archivo coincide con una firma, el archivo es identificado como infectado. Si no coincide con ninguna de las firmas, el archivo es comprobado con la tecnología HiVE. En caso de que el comportamiento del archivo se asemeje al comportamiento de software malintencionado, el archivo es identificado como sospechoso. El resultado del módulo de los motores Antivirus puede ser INFECTADO o LIMPIO.
3. Si el resultado del módulo de los Motores Antivirus es INFECTADO se realizará alguna de las siguientes acciones: desinfectar, eliminar, ignorar, mover en cuarentena. Si estas acciones fallan, se aplica la acción "Bloquear acceso". De esta forma el usuario no podrá ejecutar el código infectado.

La protección bajo demanda

Este tipo de protección es útil de cara al mantenimiento periódico, y para comprobar el estado del servidor después de un período de tiempo en el que la protección antivirus residente haya sido desactivada.

El módulo Antivirus puede ejecutarse haciendo clic en "Analizar ahora" en la interfaz de usuario o mediante una tarea programada de análisis bajo demanda. El proceso de análisis es el mismo que el detallado anteriormente, pero comprueba todos los archivos del disco en lugar de comprobar sólo los accedidos.

El proceso de actualización

El módulo Actualización realiza el proceso de actualización y su principal función es descargar los últimos archivos de BitDefender. Hay tres tipos de archivos disponibles:

- **Firmas antivirus.** Estos archivos se actualizan constantemente a medida que el Laboratorio BitDefender analiza nuevos virus cada día.
- **Motor antivirus.** Estos archivos se actualizan con la misma frecuencia que las firmas de virus. La tecnología HiVE, propiedad de BitDefender ha sido implementada en los motores antivirus.
- **Archivos de producto.** Los archivos de producto son distintos a las actualizaciones de firmas de virus, y su función es la de entregar soluciones de bugs y mejoras de funcionamiento del producto. Las actualizaciones del producto se descargan, pero no se instalan automáticamente. Tenga en cuenta que la instalación de actualizaciones de producto puede requerir un reinicio del sistema.

El proceso de actualización se realiza cada 3 horas, pero el intervalo de tiempo puede ser configurado igual que las tareas de actualización pueden programarse en cualquier momento.

La descarga de los archivos más recientes de BitDefender precisa de una ubicación de descarga aprobada por BitDefender. Por defecto el producto actualiza los archivos desde los sitios BitDefender, pero pueden crearse ubicaciones locales de descarga instalando **BitDefender Local Update Manager**. En el paquete de instalación para **BitDefender for File Servers** también se incluye **BitDefender Local Update Manager**. De esta forma, los productos **BitDefender for File Servers** pueden actualizarse desde una localización dentro de la misma red.

KEY FEATURES BENEFITS

HiVE	HIVE es la abreviación de Heuristics in Virtual Environment (análisis Heurístico en Entornos Virtuales); emula un ordenador-virtual-dentro-de-un-ordenador donde partes de software son ejecutadas para comprobar si se trata de software malintencionado (malware). Esta tecnología, propiedad de BitDefender, representa una nueva capa de seguridad que mantiene el sistema operativo a salvo de virus desconocidos al detectar partes potencialmente dañinas de código para las cuales todavía no han sido publicadas firmas. Así pues, es un suplemento a las usuales técnicas de firmas de virus y detección basada en el comportamiento, incrementando la efectividad global de su solución antivirus. HiVE es un componente del antivirus BitDefender que ha sido certificado por ICSA Labs, CheckMark, CheckVir, Virus Bulletin y TUV.
Optimización del Análisis	El analizador antivirus BitDefender marca, durante cada sesión, todos los archivos con permisos de “sólo lectura” que han sido analizados. El permiso “sólo lectura” asegura que el archivo no será modificado o infectado durante la respectiva sesión. Así pues, se crea una base de datos de los archivos analizados recientemente que han sido detectados como seguros. Si se realiza una actualización o si se detecta una infección en el sistema, la base de datos es reiniciada. Esta medida de seguridad garantiza que todos los archivos son re-analizados con las firmas antivirus más recientes.
Análisis Multihilo	El análisis multihilo utiliza un conocido método que simula la ejecución paralela de un programa (conocida como hilos de un programa). Se usan múltiples instancias de los motores con el fin de acortar el proceso de análisis.
Análisis al Acceder	El análisis al acceder proporciona una protección en tiempo real de los servidores de ficheros, analizando cada archivo al que se accede o es copiado al disco. Esta es la característica principal de una aplicación antivirus orientada a servidores y su función es la de mantener el servidor de ficheros libre de contenido malicioso.
Análisis bajo Demanda	El análisis bajo demanda es una poderosa herramienta especialmente diseñada para administradores. Su propósito es proporcionar una segunda línea de defensa contra el software malintencionado que pudiera infectar al servidor de ficheros. Recomendamos que analice el servidor de ficheros periódicamente con las firmas de virus más recientes, programando un análisis antivirus bajo demanda o realizando una acción de análisis manual.
Actualizaciones Automáticas	Actualizaciones de los productos y las firmas automatizadas, respaldadas por la tecnología HiVE, que minimizan la ventana de vulnerabilidad de su sistema. Las actualizaciones se descargan cada hora automáticamente desde los servidores de BitDefender o servidores alternativos certificados.

Programador de Tareas	En esta nueva versión se ha añadido la capacidad de programar tareas. El análisis bajo demanda y las tareas de actualización pueden programarse desde la interfaz del producto. Este sistema se relaciona con el módulo de Alertas para proporcionar notificaciones a administradores cuando un análisis bajo demanda o una actualización no ha podido realizarse.
Logs y Estadísticas	El sistema de monitorización también ha sido mejorado. Pueden crearse informes de la actividad del producto, y se incluye un módulo especial de estadísticas. De la misma forma, el sistema de alertas incluye nuevas características como alertas personalizables para varios tipos de eventos: actualizaciones de firmas de virus, actualizaciones de productos, análisis bajo demanda, virus detectados.
Interfaz Rediseñada	BitDefender for File Servers tiene una interfaz para el usuario basada en MMC que ofrece un entorno de trabajo amigable. El sistema de asistentes implementado en la interfaz mejora la utilidad del producto mientras que el sistema "snap-in" proporciona la actual funcionalidad en cuanto a la gestión.
Administración Centralizada	BitDefender for File Servers es totalmente compatible con BitDefender Enterprise Manager, ofreciendo a las compañías la posibilidad de administrar centralizadamente la protección antivirus y políticas de seguridad dentro de redes complejas. Instalación y configuración remotas y comprobaciones del estado de BitDefender for File Servers son tareas que pueden realizarse de forma centralizada desde una consola de administración en su red.

Requisitos del sistema:

Mínimo Procesador: Pentium II 300MHz

Mínimo 75 MB

Memoria Mínimo: 64 MB (128 MB recomendados para un rendimiento superior)

Sistemas operativos: Windows NT 4.0 SP6 + IE 5.5 +MMC v1.2

Windows 2000, Windows XP or Windows 2003 Server

Mejores prácticas

1. Una vez finalice el proceso de instalación, por favor, registre el producto. Debe acceder al apartado **Registrar**, seleccione el producto, escriba el número de licencia y haga clic en el botón **Aplicar**.
2. Active su Cuenta de Soporte. Para gestionar los comentarios, sugerencias o bugs que envíe a BitDefender, entre en el apartado **Información\Registro** y haga clic en **Registro online** del formulario del menú de Ayuda.
3. Configurar las actualizaciones. Entre en apartado **Configuración de Actualización** y configure las opciones de la actualización. Por defecto, BitDefender se actualizará automáticamente cada 3 horas. Haga clic en **Actualizar Ahora!** para actualizar inmediatamente los motores de análisis.

CONSEJO: Si **BitDefender for File Servers** se ha instalado en un equipo que no tiene acceso a Internet, configure **BitDefender Local Update Manager** para mantener las firmas de virus actualizadas.

4. Compruebe si hay nuevas **Actualizaciones de Producto**. Entre en el apartado **Actualización\Actualización de Producto** e instale las actualizaciones disponibles. Las actualizaciones de producto son distintas a las actualizaciones de firmas de virus, y su función es solucionar bugs y mejorar de funcionamiento del producto. Las actualizaciones del producto se descargan, pero no se instalan automáticamente. Tenga en cuenta que la instalación de actualizaciones de producto puede requerir un reinicio del sistema. Aconsejamos instalar las últimas versiones de las actualizaciones de producto.
5. Seleccione la acción a realizar al encontrar archivos infectados en el análisis al-acceder. Entre en el apartado **Antivirus/Analizador al-acceder** y seleccione la acción deseada: desinfectar, eliminar, mover a Cuarentena o ignorar (ninguna acción). Si selecciona desinfectar, puede elegir una segunda acción en caso que la desinfección falle.

CONSEJO: En caso que ambas acciones fallen, **BitDefender for File Servers** bloqueará el acceso a los archivos infectados para prevenir la infección del sistema.

6. Compruebe que BitDefender está funcionando con el test EICAR. La prueba consiste en crear un fichero usando un editor de texto, y guardarlo en formato estándar MSDOS ASCII con un tamaño 68 bytes de longitud. También puede ocupar 70 bytes si el editor de textos agrega CR/LF al final. El fichero debe contener únicamente la línea siguiente:
`X5O!P%@AP[4\PX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`. Guarde el fichero con cualquier nombre pero con la extensión COM, por ejemplo EICAR.COM, y envíelo por e-mail a un usuario que tenga su e-mail en el servidor protegido por BitDefender. BitDefender debe tratar este archivo como un archivo infectado.
7. Realice un análisis manual del servidor. Entre en el apartado **Antivirus\Analizador bajo demanda**, configure las opciones de análisis y haga clic en **Analizar ahora**.
8. Excluir archivos/carpetas del análisis al-acceder. Entre en el apartado **Antivirus\Analizador al-acceder** y seleccione los ficheros o carpetas deseados. Puede excluir del análisis tantas carpetas como quiera.

CONSEJO: Para mejorar el rendimiento, configure las opciones de análisis de extensiones seleccionando la casilla correspondiente a "Sólo programas", para que solo se analicen los archivos que pueden ejecutarse.

9. Configurar las alertas de BitDefender. Si se detecta un virus o se produce una situación inesperada, hay la posibilidad de enviar un mensaje de alerta por e-mail o por Net Send. A través de los apartados **Alertas por Mail** o **Alertas por Net Send** puede configurar BitDefender para que envíe estas notificaciones.