Bitdefender

Endpoint Security for Mac

GUÍA DE USUARIO

Endpoint Security for Mac
Guía de Usuario

fecha de publicación 2020.08.31

Advertencia legal

Bitdefender

Tabla de contenidos

Uso de la guía

1. Propósito y público al que va dirigida

Esta documentación se dirige a los usuarios finales de **Endpoint Security for Mac**, el software cliente Security for Endpoints instalado en equipos para protegerlos frente al malware y otras amenazas de Internet. La información aquí presentada debe ser fácilmente comprensible para cualquier persona que sepa trabajar en Macintosh.

Averiguará cómo configurar y usar Endpoint Security for Mac para protegerse contra virus y otro software malicioso. Aprenderá a sacarle el máximo partido a Bitdefender.

Le deseamos una útil y placentera lectura.

2. Cómo usar esta guía

Esta guía está organizada en diversos temas principales:

Iniciando (p. 1)
Comience con Endpoint Security for Mac y su interfaz de usuario.

Protección contra malware (p. 5)
Aprenda cómo utilizar Endpoint Security for Mac para proteger su equipo contra el software malicioso.

Preferencias de Configuración (p. 21)
Aprenda más sobre las preferencias de Endpoint Security for Mac.

Obtener Ayuda (p. 30)
Dónde consultar y dónde pedir ayuda si se produce una situación inesperada.

3. Convenciones utilizadas en esta guía

3.1. Convenciones Tipográficas

En esta guía se utilizan distintos estilos de texto con el fin de mejorar su lectura. En la siguiente tabla se indican su aspecto y significado.

Apariencia	Descripción
`ejemplo de sintaxis`	Ejemplos de sintaxis se muestran con letras `monospaced`.
http://www.bitdefender.es	Los enlaces URL le dirigen a alguna localización externa, en servidores http o ftp.
documentacion@bitdefender.com	Las direcciones de e-mail se incluyen en el texto como información de contacto.
Uso de la guía (p. v)	Este es un enlace interno, hacia alguna localización dentro del documento.
`nombre de archivo`	Los archivos y carpetas se muestran usando una fuente `monoespaciada`.
opción	Todas las opciones del producto se muestran utilizando caracteres en **negrita**.
palabra clave	La palabras o frase más importantes se destacan utilizando caracteres en **negrita**.

3.2. Admoniciones

Las advertencias son notas dentro del texto, marcadas gráficamente, que le facilitan información adicional relacionada con el párrafo que está leyendo.

Nota
La nota es una pequeña observación. Aunque puede omitirla, las notas pueden proporcionar información valiosa, como características específicas o enlaces hacia temas relacionados.

Importante
Este tipo de advertencia requiere su atención y no es recomendable omitirla. Normalmente proporciona información importante, aunque no extremadamente crítica.

Aviso
Se trata de información crítica que debería tratar con extrema cautela. No ocurrirá nada malo si sigue las indicaciones. Debería leer y entender estas notas, porque describen algo extremadamente arriesgado.

4. Petición de Comentarios

Le invitamos a ayudarnos a mejorar el manual. Hemos comprobado y verificado toda la información como mejor hemos sabido. Por favor, escríbanos para explicarnos cualquier tipo de defecto que encuentre en este manual o cómo podría mejorarse, y así ayudarnos a ofrecerle la mejor documentación posible.

Haganoslo saber mandando un e-mail a documentation@bitdefender.com. Por favor, escriba en Inglés todos los correos relacionados con la documentación, para poder procesarlos correctamente.

1. INICIANDO

Este capítulo incluye los siguientes temas:

1.1. Acerca de Endpoint Security for Mac

Endpoint Security for Mac es un programa de seguridad informática completamente automatizado, administrado remotamente por su administrador de red. Una vez instalado, le protege contra todo tipo de malware, incluyendo virus, spyware, troyanos, keyloggers, gusanos y adware. También puede utilizarse para hacer cumplir las políticas de uso de Internet y de equipos en su organización.

Esta aplicación detecta y elimina no solo malware de Mac, sino también malware de Windows, evitando por tanto que envíe accidentalmente archivos infectados a su familia, amigos y compañeros de trabajo que usen PCs.

1.2. Abrir Endpoint Security for Mac

Hay varias maneras de abrir Endpoint Security for Mac.

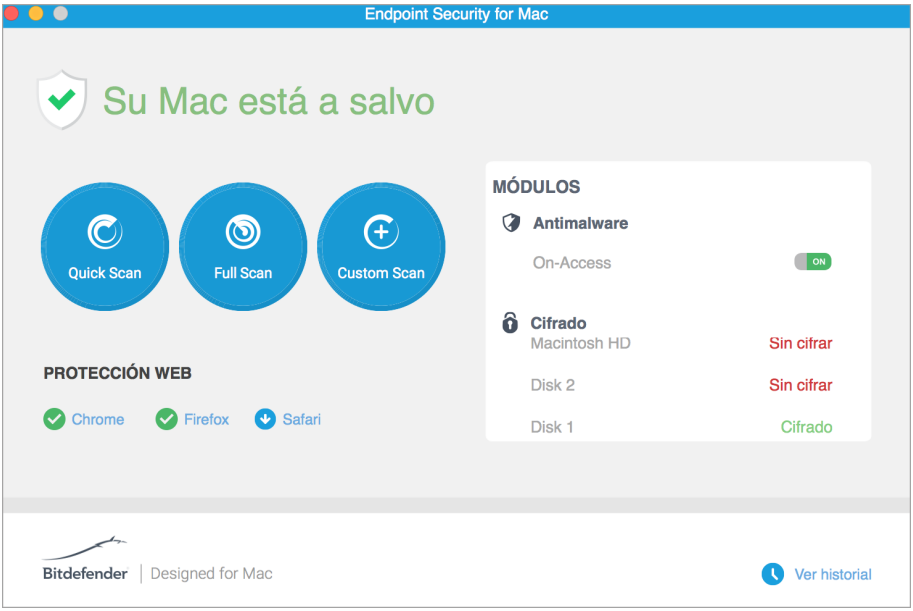
- Haga clic en el icono Endpoint Security for Mac en el Launchpad.
- Abra una ventana del Finder, acceda a **Aplicaciones** y haga doble clic en el icono **Endpoint Security for Mac**.
- También puede utilizar Spotlight para encontrar y abrir la aplicación.

Cuando se abre la aplicación, esta detecta automáticamente el idioma del sistema y le muestra la interfaz de usuario en su idioma.

Nota
Si el idioma del sistema no se encuentra entre los contemplados por Endpoint Security for Mac, la aplicación carga por defecto la interfaz en inglés.

1.3. Ventana Aplicación Principal

En la ventana principal de Aplicaciones puede llevar a cabo importantes acciones para mejorar la protección de su sistema. Puede comprobar el estado de seguridad de su equipo y proteger su navegación Web.



Ventana Aplicación Principal

El área de estado en la parte superior de la ventana le informa sobre el estado de seguridad del sistema mediante mensajes explícitos y ciertos colores:

- Verde: si Endpoint Security for Mac carece de avisos.
- Amarillo: si se ha detectado un problema de seguridad.
- Rojo: si la licencia ha caducado.

Bajo el área de estado, hay disponibles tres botones de análisis para ayudarle a analizar su Mac:

- **Quick Scan**: busca malware en las ubicaciones más vulnerables de su sistema (por ejemplo, las carpetas que contienen los documentos, descargas, descargas de correo electrónico y archivos temporales de cada usuario).

- **Full Scan (Análisis completo)**: realiza una comprobación exhaustiva en busca de malware en todo el sistema. Todos los dispositivos montados se analizarán también.
- **Análisis personalizado**: le ayuda a comprobar la existencia de malware en archivos, carpetas o volúmenes concretos.

Para más información, diríjase a Analizando Su Mac (p. 5).

Junto a los botones de análisis, la sección de Módulos le informa de lo siguiente:

- **Antimalware**: Le permite saber si el análisis on-access está activado o desactivado.
- **Control de contenido**: Le permite saber si los siguientes componentes están activados o desactivados.
  - Análisis tráfico
  - Lista negra de aplicaciones
  - Control de acceso Web
  - Antiphishing
- **Control de dispositivos**: Le informa de si el módulo está activado o desactivado.

> **Nota**
> Los módulos de Control de contenido y Control de dispositivos están disponibles a partir de OS X El Capitan (10.11). Estas capacidades se basan en una extensión del kernel de macOS. La instalación de extensiones del kernel requiere su aprobación en macOS High Sierra (10.13) y posteriores.

- **Cifrado**: Indica el estado del cifrado de cada disco (Cifrado, Cifrado en curso, Descifrado en curso, Sin cifrar, Bloqueado o En pausa) si se aplica una política de cifrado de GravityZone en su equipo.
- **EDR Sensor** - informs you if the EDR module is enabled (On) or disabled (Off).

Bajo los botones de análisis, hay disponible una opción más:

- **Protección Web** - filtra todo el tráfico Web y bloquea cualquier contenido malicioso para proteger su navegación en la Web. Para obtener más información, consulte Protección Web (p. 12).

Nota
La Protección web está disponible en OS X Mavericks (10.9) y OS X Yosemite (10.10). A partir de OS X El Capitan (10.11), el Control de contenido reemplaza esta característica.

En la parte inferior de la ventana, al hacer clic en el botón **Ver historial**, se abre un registro detallado de eventos relacionados con la actividad de Endpoint Security for Mac en su equipo. Para obtener información, consulte Historial (p. 21).

1.4. Icono Aplicación Dock

El icono de Endpoint Security for Mac puede verse en el Dock en cuanto abre la aplicación. El icono del Dock le proporciona una manera fácil para analizar archivos y carpetas en busca de malware. Simplemente arrastre y suelte el archivo o la carpeta en el icono del Dock y el análisis comenzará inmediatamente.

Icono del Dock

2. PROTECCIÓN CONTRA MALWARE

Este capítulo incluye los siguientes temas:

2.1. Mejores Prácticas

Para mantener su sistema libre de malware y evitar la infección accidental de otros sistemas, siga estas recomendaciones:

- Compruebe y repare regularmente las incidencias reportadas por Endpoint Security for Mac. Para información detallada, diríjase a Reparar Incidencias (p. 7).
- También debería seguir estas recomendaciones:
  - Acostúmbrese a analizar los archivos que descargue de una fuente de almacenamiento externa (como por ejemplo una memoria USB o un CD), especialmente cuando desconoce el origen de los mismos.
  - Si tiene un archivo DMG, móntelo y analice su contenido (los archivos del volumen/imagen montado).

2.2. Analizando Su Mac

El módulo de Análisis on-access monitoriza continuamente las aplicaciones que hay en su equipo, buscando acciones sintomáticas del malware, y evita que entre nuevo malware en su sistema. Su administrador de red controla el Análisis on-access mediante las políticas de seguridad.

También puede analizar su Mac o solo determinados archivos siempre que lo desee.

La forma más fácil de analizar un archivo, una carpeta o un disco es arrastrarlo y soltarlo sobre el icono del Dock. Aparecerá el asistente de análisis que le guiará durante este proceso.

Puede iniciar un análisis de la siguiente manera:

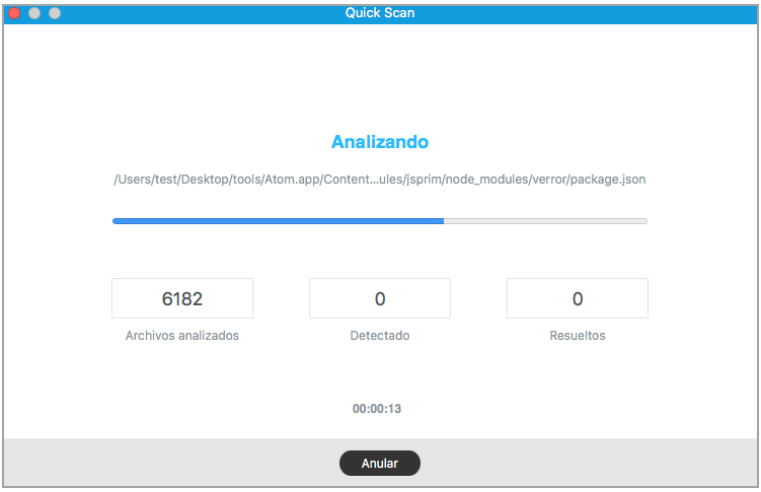
1. Abra Endpoint Security for Mac.
2. Haga clic en uno de los tres botones de análisis para iniciar el análisis deseado.
   - **Quick Scan**: busca malware en las ubicaciones más vulnerables de su sistema (por ejemplo, las carpetas que contienen los documentos, descargas, descargas de correo electrónico y archivos temporales de cada usuario).
   - **Full Scan (Análisis completo)**: realiza una comprobación exhaustiva en busca de malware en todo el sistema. Todos los dispositivos montados se analizarán también.

     Nota
     - Dependiendo del tamaño de su disco duro, analizar todo el sistema puede tardar bastante (hasta una hora o incluso más). Para mejorar el rendimiento, se recomienda no ejecutar esta tarea mientras se estén llevando a cabo otras tareas que consuman muchos recursos (como por ejemplo la edición de vídeo).
     - You can also run a quick scan or a full scan by using the **productConfigurationTool**Uso de la herramienta de línea de comandos (p. 23).

   - **Análisis personalizado**: le ayuda a comprobar la existencia de malware en archivos, carpetas o volúmenes concretos.

2.3. Asistente del Análisis

Cuando inicie una análisis, aparecerá el asistente de Análisis de Endpoint Security for Mac.



Análisis en Progreso

Puede ver información en tiempo real acerca del análisis, como el número de amenazas detectadas y la cantidad de problemas resueltos.

Espere a que Endpoint Security for Mac finalice su análisis.

Nota
El análisis puede llevar un tiempo, dependiendo de la complejidad del análisis.

2.4. Reparar Incidencias

Endpoint Security for Mac automáticamente detecta y le informa sobre una serie de incidencias que pueden afectar a la seguridad de su sistema y sus datos.

Los problemas detectados pueden referirse a:

- Las actualizaciones de producto y de nuevas firmas de malware no se han cargado desde los servidores de Bitdefender.
- Se han detectado amenazas para la seguridad en su sistema
- El módulo de análisis on-access está desactivado.
- La licencia ha caducado.

Solucionar los problemas indicados por Endpoint Security for Mac es un proceso rápido y fácil. De esta manera puede solventar a tiempo los riesgos para la seguridad.

Para comprobar y reparar las incidencias detectadas:

1. Abra Endpoint Security for Mac.
2. Compruebe el color del área de estado:
   - Verde: su Mac está a salvo.
   - Amarillo o rojo: su Mac tiene problemas. Para más información, siga los pasos que se indican a continuación.
3. Compruebe la descripción para más información.
4. Dependiendo del número y del tipo de los problemas detectados, puede que haya un botón disponible en el área de estado:
   - **Reparar incidencia**, si se encontró una sola. Haga clic en el botón para solucionar rápidamente el riesgo para la seguridad.
   - **Ver incidencias**, si se encontraron varios problemas. Haga clic en el botón para ver las incidencias. A continuación se abre una nueva ventana, en la que puede solucionar los problemas.

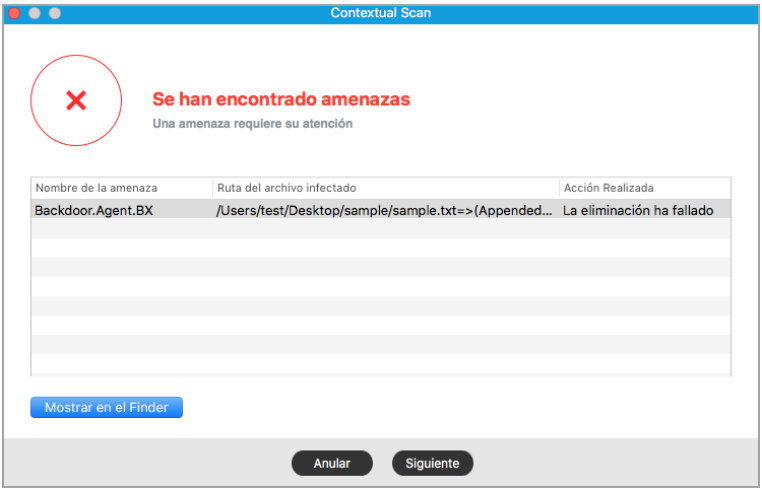
Si se ha detectado malware, la aplicación intenta automáticamente eliminarlo y reconstruir el archivo original. Esta operación se conoce como desinfección. Los archivos que no pueden desinfectarse son trasladados a la cuarentena para contener la infección.

Si el archivo no se puede desinfectar ni trasladar a la cuarentena, Endpoint Security for Mac le informa de este hecho para que pueda borrarlo manualmente.

Para eliminar infecciones manualmente:

- Haga clic en el botón **Mostrar en el Finder**.
- Seleccione el archivo y bórrelo de su sistema.

  Si el archivo pertenecía a una aplicación instalada, asegúrese de reparar la instalación de ese programa para que funcione correctamente.



Ventana de amenazas no solucionadas

Ciertos problemas pueden requerir que los solucione su administrador de red desde la consola de administración, como por ejemplo:

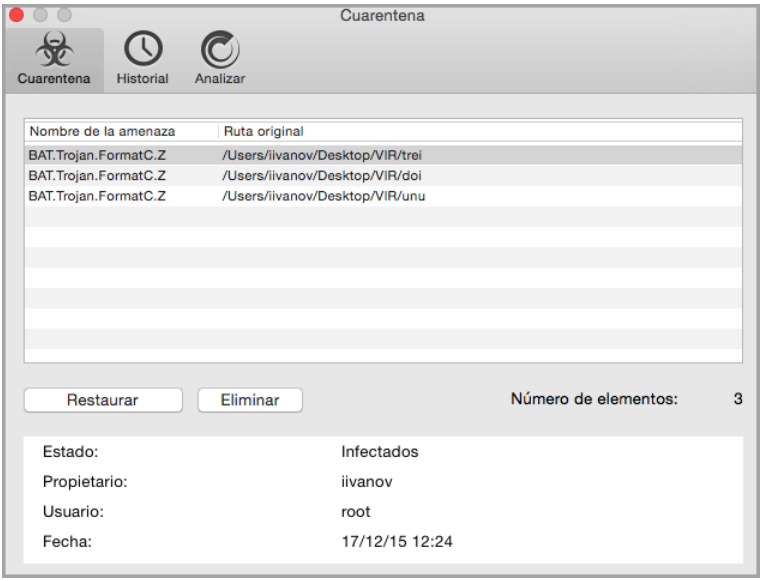
- Activar el módulo on-access mediante la política de seguridad.
- Renovar la licencia caducada.

2.5. Cuarentena

Endpoint Security for Mac le permite aislar los archivos infectados o sospechosos en una área segura, llamada cuarentena. Cuando una aplicación maliciosa está en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.

Para ver y gestionar los archivos en la cuarentena, abra la ventana de **Cuarentena**:

1. Haga clic con el botón derecho en el icono de Bitdefender en la barra de menús.
2. Elija **Preferencias** de la lista de opciones. Aparecerá una ventana.
3. Seleccione la pestaña **Ver cuarentena**.



Archivos trasladados a la cuarentena

El apartado Cuarentena muestra todos los archivos actualmente aislados en la carpeta Cuarentena.

Para borrar un archivo de la cuarentena, selecciónelo y haga clic en **Eliminar**. Si desea restaurar una archivo en cuarentena a su ubicación original, selecciónelo y haga clic en **Restaurar**.

2.6. Control de Contenidos

El módulo de Control de contenido le protege mientras navega por Internet contra ataques de phishing, intentos de fraude y contenidos web inapropiados. También incluye un amplio conjunto de controles de usuario que ayudan al administrador de la red a hacer cumplir las políticas de uso de los equipos y de Internet. Este módulo está disponible para Chrome, Firefox y Safari.

- **Análisis de tráfico**. Gracias al análisis del tráfico web en tiempo real, este componente evita la descarga de malware en el endpoint.

- **Lista negra de aplicaciones**. Este componente impide el acceso a las aplicaciones no autorizadas en su empresa. El administrador es el responsable de crear las reglas para las aplicaciones permitidas en la organización.
- **Control de acceso web**. Este componente le protege de acceder a sitios web peligrosos en función de las reglas definidas por el administrador.
- **Antiphishing**. Este componente bloquea automáticamente las páginas web de phishing conocidas para evitar que los usuarios puedan revelar, sin darse cuenta, información privada o confidencial a impostores online.

Nota
El Control de contenido está disponible a partir de OS X El Capitan (10.11). Esta funcionalidad se basa en una extensión del kernel de macOS. La instalación de extensiones del kernel requiere su aprobación en macOS High Sierra (10.13). El sistema le notifica que se ha bloqueado una extensión del sistema de Bitdefender y que puede permitirla desde las preferencias de **Seguridad y privacidad**. Este módulo no funcionará hasta que usted apruebe la extensión del sistema de Bitdefender y la interfaz de usuario de Endpoint Security for Mac mostrará un problema crítico que le solicitará su aprobación.

2.7. Control de dispositivos

El módulo de **Control de dispositivos** permite evitar la fuga de datos confidenciales y las infecciones de malware a través de dispositivos externos conectados a los endpoints. Para ello, aplica políticas con reglas de bloqueo a una amplia gama de tipos de dispositivos. El administrador es responsable de gestionar los permisos para los siguientes tipos de dispositivos:

- Dispositivos Bluetooth
- Dispositivos CDROM
- Dispositivos de imágenes
- Modems
- Windows Portable
- Impresoras
- Adaptadores de red
- Adaptadores de red inalámbrica
- Almacenamiento externo

Nota
El Control de dispositivos está disponible a partir de OS X El Capitan (10.11). Esta funcionalidad se basa en una extensión del kernel de macOS. La instalación de

extensiones del kernel requiere su aprobación en macOS High Sierra (10.13). El sistema le notifica que se ha bloqueado una extensión del sistema de Bitdefender y que puede permitirla desde las preferencias de **Seguridad y privacidad**. Este módulo no funcionará hasta que usted apruebe la extensión del sistema de Bitdefender y la interfaz de usuario de Endpoint Security for Mac mostrará un problema crítico que le solicitará su aprobación.

2.8. Protección Web

Endpoint Security for Mac utiliza las extensiones TrafficLight para proteger completamente su navegación Web. Las extensiones TrafficLight interceptan, procesan y filtran todo el tráfico Web, bloqueando cualquier contenido malicioso.

Las extensiones funcionan y se integran con los siguientes navegadores: Mozilla Firefox, Google Chrome y Safari.

Nota
Esta característica está disponible en OS X Mavericks (10.9) y OS X Yosemite (10.10). A partir de OS X El Capitan (10.11), el Control de contenido reemplaza a la Protección web.

Hay toda una serie de funciones disponibles para protegerle frente a todo tipo de amenazas que pueda encontrar mientras navega por la Web:

- Filtro de phishing avanzado - evita que acceda a sitios Web empleados para ataques de phishing.
- Filtro de malware - bloquea cualquier malware con el que entre en contacto mientras navega por Internet.
- Analizador de resultados de búsqueda - proporciona una advertencia anticipada sobre sitios Web peligrosos presentes en sus resultados de búsquedas.
- Filtro antifraude - proporciona protección contra sitios Web fraudulentos mientras navega por Internet.
- Notificación de seguimiento - detecta mecanismos de seguimiento en las páginas Web que visita para proteger su privacidad online.

Habilitación de extensiones TrafficLight

Para habilitar las extensiones TrafficLight, siga los pasos siguientes:

1. Abra Endpoint Security for Mac.

2. Haga clic en **Solucionar ahora** para abrir la ventana de la protección Web.
3. Endpoint Security for Mac detectará qué navegador tiene instalado en su sistema. Para instalar la extensión TrafficLight en el navegador que desee, haga clic en **Obtener extensión** en el panel correspondiente.
4. Será redirigido a esta ubicación online:

   http://bitdefender.com/solutions/trafficlight.html
5. Seleccione **Descarga gratuita**.
6. Siga los pasos para instalar la extensión TrafficLight para el navegador seleccionado.

Calificación de páginas y alertas

Dependiendo de la clasificación que TrafficLight otorgue a la página Web que esté viendo, mostrará en su área uno de los iconos siguientes:

 Esta es una página segura. Puede seguir trabajando.

 Esta página Web puede albergar contenidos peligrosos. Tenga cuidado si decide visitarla.

 Debe salir de la página Web inmediatamente. Como alternativa, puede escoger una de las opciones disponibles:

- Abandonar el sitio Web haciendo clic en **Llévame a un sitio seguro**.
- Dirigirse al sitio Web, a pesar de la advertencia, haciendo clic en **Estoy informado acerca de los riesgos, visitar la página de todos modos**.

2.9. Actualizaciones

Cada día se encuentran nuevas amenazas de malware. Por esta razón es muy importante mantener Endpoint Security for Mac actualizado con las últimas firmas de malware.

Cuando el **Análisis on-access** está activado, las firmas de malware y las actualizaciones de producto se descargan automáticamente en su sistema. Si el administrador de su red desactiva el módulo on-access mediante política, tendrá que solicitar manualmente la actualización de su aplicación Endpoint Security for Mac.

La actualización de firmas de malware se realiza al instante, reemplazándose progresivamente los archivos que hay que actualizar. De este modo, la actualización

no afecta al funcionamiento del producto y, al mismo tiempo, se evita cualquier riesgo.

2.9.1. Solicitando una Actualización

Puede solicitar una actualización manualmente en cualquier momento. La actualización por el usuario se recomienda antes de iniciar un análisis exhaustivo.

Se requiere conexión a Internet con el fin de comprobar las actualizaciones disponibles y descargarlas.

Para solicitar una actualización manual:

1. Abra Endpoint Security for Mac.
2. Haga clic en **Acciones** en la barra de menú.
3. Elija **Base de datos de virus**.

Puede ver el progreso de actualización y archivos descargados.

2.9.2. Obteniendo Actualizaciones a través de un Servidor Proxy

Endpoint Security for Mac puede actualizar solo a través de servidores proxy que no requiere autenticación. No tiene que configurar ninguna configuración del programa.

Si se conecta a Internet a través de un servidor proxy que requiere autenticación, debe cambiar a una conexión directa a Internet con el fin de obtener las actualizaciones de las firmas de malware.

2.9.3. Actualizar a una nueva versión

Ocasionalmente, lanzamos actualizaciones del producto para mejorar su funcionalidad. Estas actualizaciones podrían requerir un reinicio del sistema para dar paso a la instalación de nuevos archivos. De forma predeterminada, si una actualización precisa un reinicio del equipo, Endpoint Security for Mac seguirá funcionando con los archivos anteriores hasta que se reinicie el sistema. Así, el proceso de actualización no interferirá con su trabajo.

Cuando se complete una actualización del producto, una ventana emergente le informará de que debe reiniciar el sistema. Si no lee esta notificación, puede también hacer clic en **Reiniciar para actualizar** en la barra de menús o reiniciar manualmente el sistema.

3. USO DEL CIFRADO

El módulo de cifrado proporciona cifrado de disco completo en su Mac mediante las políticas aplicadas por su administrador de seguridad. El agente de seguridad utiliza FileVault para cifrar la unidad de arranque de Mac y la utilidad de línea de comandos diskutil para cifrar cualquier unidad que no sea de arranque. Las unidades extraíbles no se cifran.

Este capítulo incluye los siguientes temas:

- Cifrado de volúmenes
- Descifrado de volúmenes
- Cambio de la clave de recuperación
- Cambio de la contraseña de cifrado

3.1. Cifrado de volúmenes

Cuando se aplica una política de cifrado en su Mac:

- Para unidades de arranque:
  1. Una ventana le solicita que introduzca su nombre de usuario y contraseña del sistema.

  2. Haga clic en el botón **OK** para poner en marcha el proceso de cifrado.

     Si hace clic en la opción **Ahora no**, se pospone el proceso de cifrado, pero la ventana volverá a aparecer pasado un tiempo y seguirá haciéndolo mientras la política de cifrado continúe activa en el Mac.

3. Esto es lo que sucede después de cerrarse la ventana **Cifrar con FileVault**:
   - Si tiene un Mac con una versión del sistema operativo anterior a macOS Catalina (10.15), el proceso de cifrado comienza de inmediato.
   - Si tiene un Mac con macOS Catalina (10.15), Endpoint Security for Mac ("fdesetup") requerirá, en una ventana adicional, su aprobación para habilitar FileVault. Haga clic en el botón **Aceptar** para poner en marcha el cifrado. Si hace clic en **No permitir**, Endpoint Security for Mac no iniciará el cifrado y le pedirá su aprobación cada dos minutos.

   Nota
   En el caso de los sistemas de arranque dual, no se cifrará el otro volumen de arranque.

- Para unidades que no son de arranque:
  1. Una ventana le solicita que configure una contraseña específica para cifrar cada unidad. Dicha contraseña solo es necesaria para desbloquear una unidad concreta que no sea de arranque.
  2. Haga clic en el botón **Guardar**. El proceso de cifrado comienza de inmediato.

     Si hace clic en la opción **Descartar**, se pospone el proceso de cifrado. La ventana de diálogo aparecerá pasado un tiempo y seguirá haciéndolo mientras la política de cifrado continúe activa en el Mac.

Si el Mac tiene más de una unidad, las ventanas de diálogo para el cifrado de todas las unidades aparecerán al mismo tiempo.

3.2. Descifrado de volúmenes

Cuando se aplica una política de descifrado en su Mac:

- Para unidades de arranque:
  1. Una ventana de diálogo le solicita que introduzca su nombre de usuario y contraseña del sistema.
  2. Haga clic en el botón **ACEPTAR**. El proceso de descifrado comienza de inmediato.
- Para unidades que no son de arranque:
  1. Una ventana de diálogo le solicita que introduzca la contraseña de cifrado.
  2. Haga clic en el botón **Guardar**. El proceso de descifrado comienza de inmediato.

Si hace clic en la opción **Descartar**, se pospone el proceso de descifrado. La ventana de diálogo aparecerá pasado un tiempo y seguirá haciéndolo mientras la política de cifrado continúe activa en el Mac.

Si el Mac tiene más de una unidad, las ventanas de diálogo para el descifrado de todas las unidades aparecerán al mismo tiempo.

3.3. Cambio de la clave de recuperación

Una vez que se inicia el proceso de cifrado, Endpoint Security for Mac envía una clave de recuperación a la consola de administración del administrador de seguridad. La clave de recuperación le resultará útil a su administrador de seguridad en caso de que usted olvide sus credenciales de inicio de sesión o las contraseñas de cifrado y no pueda desbloquear las unidades o si el Mac tiene otro usuario que no pueda acceder a una de las unidades.

Puede cambiar la clave de recuperación de la unidad de arranque sin necesidad de cambiar sus credenciales de inicio de sesión.

Para cambiar la clave de recuperación de cifrado para la unidad de arranque:

1. Haga clic en la unidad de arranque cifrada en la ventana principal de Endpoint Security for Mac.
2. Haga clic en la opción **Cambiar la clave de recuperación**.
3. Introduzca su nombre de usuario y contraseña.
4. Haga clic en el botón **Guardar**.

La opción de cambiar la clave de recuperación solo está disponible si se aplica una política de cifrado a su Mac.

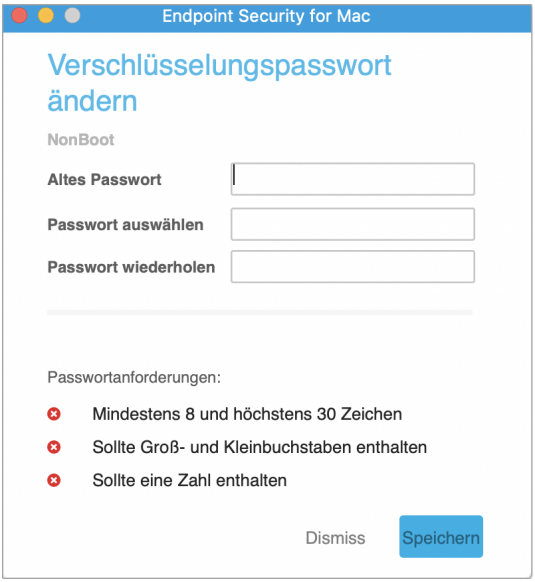
En caso de que cambie la contraseña del sistema, la unidad de arranque cifrada permanecerá como está, sin que se requiera ninguna acción por su parte.

3.4. Cambio de la contraseña de cifrado

Puede cambiar la contraseña de cifrado para unidades que no sean de arranque desde la interfaz de usuario de Endpoint Security for Mac. Tras cambiar la contraseña, Endpoint Security for Mac enviará una nueva clave de recuperación a la consola de administración del administrador de seguridad.

Cómo cambiar la contraseña de cifrado para una unidad que no sea de arranque:

1. Haga clic en el nombre del disco cifrado en la ventana principal de Endpoint Security for Mac.
2. Haga clic en la opción **Cambiar contraseña**.
3. En la ventana **Cambiar la contraseña de cifrado**, configure la nueva contraseña.
4. Haga clic en la opción **Guardar**.



La opción de cambiar la contraseña de cifrado solo está disponible si se aplica una política de cifrado a su Mac.

4. PREFERENCIAS DE CONFIGURACIÓN

Endpoint Security for Mac tiene un mínimo de opciones para que las configure el usuario, ya que es el administrador de la red quien lo gestiona a través de la política asignada.

Este capítulo incluye los siguientes temas:

- Preferencias de Acceso
- Cuarentena
- Historial
- Preferencias de análisis

4.1. Preferencias de Acceso

Para abrir la ventana de **Preferencias**:

1. Abra Endpoint Security for Mac.
2. Realice una de estas acciones:
   - Haga clic en Endpoint Security for Mac en el menú de la aplicación y seleccione **Preferencias**.
   - Haga clic con el botón derecho en el icono de Bitdefender en el menú de estado y seleccione **Preferencias**.
   - Presione el comando coma(,).
3. Haga clic en la pestaña de la característica que desee configurar. Estas se describen a continuación.

4.2. Cuarentena

La sección cuarentena muestra todos los archivos aislados actualmente en la carpeta cuarentena de su equipo.

Para borrar un archivo de la cuarentena, selecciónelo y haga clic en **Eliminar**. Si desea restaurar un archivo de la cuarentena a su ubicación original, selecciónelo y haga clic en **Restaurar**.

4.3. Historial

Endpoint Security for Mac mantiene un registro detallado de los eventos relativos a la actividad de la aplicación en su equipo. Siempre que sucede algo relevante

para la seguridad de su sistema o de sus datos, se añade un nuevo mensaje al historial de Endpoint Security for Mac. Los eventos son una herramienta muy importante para la supervisión y la gestión de la protección de su equipo. Por ejemplo, puede comprobar fácilmente si la actualización se realizó correctamente, si se encontró malware en su equipo, etc.

Cada vez que quiera eliminar el registro del historial, haga clic en el botón **Borrar historial**. El botón **Copiar** le da la posibilidad de copiar esta información en el portapapeles.

4.4. Preferencias de análisis

Esta ventana le permite elegir si Endpoint Security for Mac debe analizar también los archivos de copia de seguridad. La aplicación solo le informará de una amenaza existente, dado que OS X protege el disco de Time Machine e impide que Endpoint Security for Mac elimine cualquier archivo. Si posteriormente restaurase archivos infectados, Endpoint Security for Mac los detectaría automáticamente y adoptaría las medidas oportunas.

Por defecto, los archivos de copia de seguridad están excluidos del análisis. Quite la marca de la casilla de verificación **No analizar el disco de Time Machine** para analizar también esta ubicación.

5. USO DE LA HERRAMIENTA DE LÍNEA DE COMANDOS

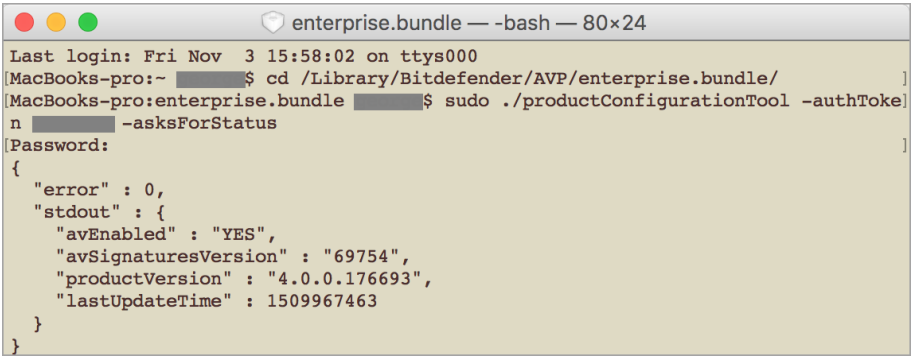
Endpoint Security for Mac le permite realizar ciertas tareas mediante el uso de una herramienta de línea de comandos llamada **productConfigurationTool**. Concretamente, puede recuperar información sobre el estado del producto y ejecutar análisis rápidos y completos del sistema.

Para utilizar **productConfigurationTool**:

1. Abra **Terminal** en su equipo.
2. Cambie el directorio de trabajo mediante el siguiente comando:

```
cd /Library/Bitdefender/AVP/enterprise.bundle/
```

3. Ejecute los comandos admitidos con privilegios de administrador (comando `sudo`).



Uso de productConfigurationTool en Terminal

Este capítulo aborda los siguientes temas relacionados con **productConfigurationTool**:

- Comandos compatibles
- El parámetro authToken
- Códigos de error

5.1. Comandos compatibles

La interfaz de **productConfigurationTool** admite los siguientes comandos:

`asksForStatus`

Obtiene información sobre lo siguiente:

- Estado del módulo antimalware (activado o desactivado).
- Versión de firmas antimalware.
- Versión del producto.
- Momento de la última actualización.

Cómo utilizarlo:

```
sudo ./productConfigurationTool -authToken [password]
     -asksForStatus
```

Ejemplo de salida en caso de éxito:

```
{
     "error" : 0,
     "stdout" : {
     "avEnabled" : "YES",
     "avSignaturesVersion" : "69440",
     "productVersion" : "4.0.0.175873",
     "lastUpdateTime" : 1507185205
     }
     }
```

Ejemplo de salida en caso de fallo:

```
"error" : 100
```

`asksForAScanToRun`

Inicia una tarea de análisis y proporciona, a su finalización, información sobre el proceso: total de elementos analizados, duración del análisis, ruta del registro y si se produjeron o no infecciones.

Este comando va seguido de un identificador predefinido para cada tipo de tarea de análisis:

- **Quick Scan** (ID: `da29f7c8-23b1-4974-8d11-209959ac694b`): Esta tarea está configurada para una seguridad básica y un bajo uso de los recursos. Los principales objetivos de análisis son los procesos en ejecución y algunas ubicaciones vulnerables. Solo se puede ejecutar simultáneamente una instancia de esta tarea.

  Cómo realizar un análisis rápido:

```
sudo ./productConfigurationTool -authToken
         [password] -asksForAScanToRun
         da29f7c8-23b1-4974-8d11-209959ac694b
```

- **Análisis completo** (ID: `dcf483c4-26d0-4e6f-ba28-6a53a00adae1`): Esta tarea está configurada para una protección máxima contra cualquier tipo de malware. Solo se puede ejecutar simultáneamente una instancia.

  Cómo realizar un análisis completo:

```
sudo ./productConfigurationTool -authToken
        [password] -asksForAScanToRun
        dcf483c4-26d0-4e6f-ba28-6a53a00adae1
```

Ejemplo de salida en caso de éxito después de ejecutar el comando `asksForAScanToRun`:

```
{
     "error" : 0,
     "stdout" : {
     "scanDuration" : 13,
     "logfilepath" : "\/Library\/Application Support\
        /Antivirus for Mac\/Logs\
        /da29f7c8-23b1-4974-8d11-209959ac694b.xml",
     "totalScanned" : 6158,
     "infection" : "NO"
     }
     }
```

Ejemplo de salida en caso de fallo:

```
"error" : 95
```

Nota

- No puede ejecutar un análisis personalizado utilizando **productConfigurationTool**.
- Algunas tareas de análisis pueden tardar mucho tiempo en llevarse a cabo. Por ejemplo, un análisis completo puede dilatarse más de veinte minutos.

5.2. El parámetro authToken

Este parámetro le ayuda a evitar el uso no autorizado de **productConfigurationTool**. Debe incluirse siempre que ejecute un comando.

Nota

Como medida temporal, el parámetro `authToken` requiere una contraseña que puede obtener contactando con el equipo de soporte corporativo de Bitdefender.

5.3. Códigos de error

La interfaz de **productConfigurationTool** puede devolver uno de los siguientes códigos de error:

Error	Descripción
100	Los parámetros de **productConfigurationTool no son correctos**.
99	La herramienta no se está ejecutando con privilegios de administrador.
98	No se ha encontrado `"/Library/Bitdefender/AVP/enterprise.bundle/epsdk.dylib"`. Actualice el producto.
97	Error al cargar las funciones de tipo `f_EPSDK_GetInstance` y `f_EPSDK_ReleaseInstance` de la biblioteca. Actualice el producto.
96	La respuesta `.json` carece de algunos de los campos que se esperaban o tiene un formato diferente al esperado. Actualice el producto.
95	Una determinada consulta requiere que los eventos obtengan todos los datos relevantes, pero no se han capturado todos los eventos. Actualice el producto.

Error	Descripción
	Si este error persiste, póngase en contacto con el equipo de soporte corporativo de Bitdefender.
94	No se ha encontrado `"/Library/Bitdefender/AVP/EndpointSecurityforMac.app/Contents/Info.plist"` o `"CFBundleVersion"` no se ha encontrado en el archivo `.plist`. Actualice el producto.
93	**productConfigurationTool** no es compatible con esta versión de Endpoint Security for Mac. Actualice el producto.
92	La contraseña de `authToken` suministrada no coincide con el valor esperado.
0	El comando se ha ejecutado correctamente.

6. PREGUNTAS FRECUENTES

El registro de análisis indica que todavía hay elementos sin resolver. ¿Cómo los elimino?

Los elementos sin resolver en el registro de análisis pueden ser:

- archivos de acceso restringido (xar, rar, etc.)

  Solución: Utilice la opción **Mostrar en el Finder** para encontrar el archivo y borrarlo manualmente. Asegúrese de vaciar la Papelera.

- buzones de correo de acceso restringido (Thunderbird, etc.)

  Solución: Utilice la aplicación para eliminar la entrada que contiene el archivo infectado.

- archivos pertenecientes a otro usuario

  Solución: Utilice la opción **Mostrar en el Finder** para encontrar el archivo y contactar con el propietario para averiguar si es seguro eliminar ese archivo. Si es seguro eliminar el archivo, bórrelo manualmente. Asegúrese de vaciar la Papelera.

> **Nota**
> Se entiende por archivos de acceso restringido aquellos que Endpoint Security for Mac solo puede abrir, pero no puede modificar.

¿Puedo actualizar Endpoint Security for Mac a través de un servidor proxy?

Endpoint Security for Mac se puede actualizar solo a través de servidores proxy que no requieran autenticación. No tiene que configurar ningún ajuste de programa.

Si se conecta a Internet a través de un servidor proxy que requiere autenticación, debe cambiar a una conexión directa a Internet con el fin de obtener las actualizaciones de las firmas de malware.

¿Cómo elimino las extensiones TrafficLight de mi navegador?

- Para eliminar las extensiones TrafficLight de Mozilla Firefox, siga los pasos siguientes:

  1. Abra su navegador Mozilla Firefox.
  2. Vaya a **Herramientas** y seleccione **Complementos**.
  3. Seleccione **Extensiones** en la columna izquierda.

4. Seleccione las extensiones y haga clic en **Eliminar**.
5. Reinicie el navegador para completar el proceso de eliminación.

- Para eliminar las extensiones TrafficLight de Google Chrome, siga los pasos siguientes:
  1. Abra su navegador Google Chrome.
  2. Haga clic en en la barra de herramientas del navegador.
  3. Vaya a **Herramientas** y seleccione **Extensiones**.
  4. Seleccione las extensiones y haga clic en **Eliminar**.
  5. Haga clic en **Eliminar de Chrome** para confirmar el proceso de eliminación.
- Para eliminar las extensiones TrafficLight de Safari, siga los pasos siguientes:
  1. Abra su navegador Safari.
  2. Haga clic en en la barra de herramientas del navegador y haga clic en **Preferencias**.
  3. Seleccione la pestaña **Extensiones** y localice en la lista la extensión **Bitdefender TrafficLight en Safari**.
  4. Seleccione la extensión y haga clic en **Desinstalar**.
  5. Haga clic en **Eliminar de Chrome** para confirmar el proceso de eliminación.

7. OBTENER AYUDA

Para cualquier problema o pregunta relativa a Endpoint Security for Mac, contacte con su administrador de red.

Abra la ventana **Acerca de Endpoint Security for Mac** para hallar información de contacto y del producto:

1. Abra Endpoint Security for Mac.
2. Haga clic en **Endpoint Security para Mac** en la barra de menú.
3. Escoja **Acerca de Endpoint Security for Mac**.

Tipos de Software Malicioso

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.

Gusano

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

Keylogger

Un keylogger es una aplicación que registra todo lo que escribe.

Los keyloggers no son maliciosos por naturaleza. Pueden utilizarse para propósitos legítimos, como la vigilancia de empleados o de la actividad de sus hijos. Sin embargo, son cada vez más utilizados por los cibercriminales con fines ilegales (por ejemplo, para recoger los datos privados, tales como credenciales de acceso y números de identificación).

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.

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.

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.

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 Polimórfico

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