Acronis

PRODUCTO #3
Advanced Security + EDR

Configuración de la protección antivirus y antimalware

Nota
En las máquinas Windows, la función de protección antimalware requiere la instalación del agente de protección antimalware y la función de filtrado de URL requiere la instalación del agente para el filtrado de URL. Estos agentes se instalan automáticamente en el caso de las cargas de trabajo protegidas si los módulos de **Protección antivirus y antimalware** o **Filtrado de URL** están habilitados en sus planes de protección.

Con la protección antimalware de Cyber Protection obtendrá los siguientes beneficios:

- Protección de calidad en todas las fases: proactivas, activas y reactivas.
- Cuatro tecnologías antimalware diferentes incluidas para proporcionar lo mejor de la protección de varias capas.
- Gestión de Microsoft Security Essentials y del antivirus Microsoft Defender.

  Nota
  La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Importante
El archivo de prueba EICAR se detecta solo cuando está habilitada la opción **Antimalware avanzado** en el plan de protección. Sin embargo, si no se detecta el archivo EICAR no afectará a las capacidades antimalware de Cyber Protection.

Sistemas operativos compatibles para la protección antivirus y antimalware

Las funciones de protección activa, antivirus y antimalware son compatibles con las plataformas siguientes.

Sistema operativo	Versión/distribución
Windows	Windows 7 Service Pack 1 y posteriores Windows Server 2008 R2 Service Pack 1 y posteriores

Sistema operativo	Versión/distribución
	Nota En Windows 7, debe instalar las siguientes actualizaciones de Microsoft antes de instalar el agente de protección. • Actualizaciones de seguridad ampliadas de Windows 7 (ESU) • KB4474419 • KB4490628 Consulte este artículo de la base de conocimientos para obtener más información sobre las actualizaciones requeridas.
Linux	Red Hat Linux 7.x, 8.x, 9.x CloudLinux 6.10, 7.x, 8.x CentOS 6.5 y versiones 6.x, 7.x y 8.x posteriores Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10 Debian 8.x, 9.x, 10,x, 11.x Oracle Linux 7.x, 8.x, 9.x SUSE Enterprise Linux 15.x openSUSE Leap 15.x
macOS	macOS 10.13.x y posterior

Funciones compatibles por plataforma

Nota
La protección antimalware para Linux y macOS está disponible con el paquete de antimalware avanzado.

Conjunto de características	Windows	Linux	macOS
Protección antivirus y antimalware			
Funcionalidad Active Protection integrada por completo	Sí	No	No
Protección contra malware en tiempo real	Sí	Sí, con el pack de antimalware avanzado	Sí, con el pack de antimalware avanzado
Protección contra malware en tiempo real avanzada con detección basada en firmas locales	Sí	Sí	Sí

Conjunto de características	Windows	Linux	macOS
Protección antivirus y antimalware			
Análisis estadístico para archivos ejecutables portátiles	Sí	No	Sí*
Análisis antimalware bajo demanda	Sí	Sí**	Sí
Protección de carpetas de red	Sí	Sí	No
Protección del servidor	Sí	No	No
Análisis de archivos del archivo comprimido	Sí	No	Sí
Análisis de unidades extraíbles	Sí	No	Sí
Análisis únicamente de archivos nuevos y cambiados	Sí	No	Sí
Exclusiones de archivos/carpetas	Sí	Sí	Sí***
Exclusiones de procesos	Sí	No	Sí
Motor de análisis de comportamiento	Sí	No	Sí
Prevención de vulnerabilidades	Sí	No	No
Cuarentena	Sí	Sí	Sí
Limpieza automática en cuarentena	Sí	Sí	Sí
Filtrado de URL (http/https)	Sí	No	No
Lista blanca corporativa	Sí	No	Sí
Gestión del firewall****	Sí	No	No
Gestión del antivirus Microsoft Defender*****	Sí	No	No
Gestión de Microsoft Security Essentials	Sí	No	No
Registro y gestión de la protección antivirus y antimalware mediante Windows Security Center	Sí	No	No
Para obtener más información sobre los sistemas operativos y sus versiones, consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 897).			

* En macOS, el análisis estadístico para archivos ejecutables portátiles solo se admite en los análisis programados.

** En Linux, las condiciones para un análisis bajo demanda no están admitidas.

*** En macOS, las exclusiones de archivos y carpetas solo se admiten cuando especifica los archivos y las carpetas que no se analizarán mediante la protección en tiempo real ni a través de análisis planificados.

**** La gestión del firewall es compatible con Windows 8 y versiones posteriores. Windows Server no es compatible.

***** La gestión del antivirus Windows Defender es compatible con Windows 8.1 y versiones posteriores.

Conjunto de características	Windows	Linux	macOS
Active Protection			
Detección inserciones de procesos	Sí	No	No
Recuperación automática de archivos afectados de la caché local	Sí	Sí	Sí
Autodefensa de las copias de seguridad de Acronis	Sí	No	No
Autodefensa de las copias de seguridad del software Acronis	Sí	No	Sí (Solo Active Protection y componentes antimalware)
Gestión de procesos de confianza/bloqueados	Sí	No	Sí
Exclusiones de procesos/carpetas	Sí	Sí	Sí
Detección de ransomware basada en el comportamiento de un proceso (basada en IA)	Sí	Sí	Sí
Detección del proceso de criptominería basada en el comportamiento de procesos	Sí	No	No
Protección de unidades externas (discos duros, unidades flash y tarjetas SD)	Sí	No	Sí
Protección de carpetas de red	Sí	Sí	Sí
Protección del servidor	Sí	No	No
Protección de Zoom, Cisco Webex, Citrix Workspace y Microsoft Teams	Sí	No	No
Para obtener más información sobre los sistemas operativos y sus versiones, consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 897).			

Protección antivirus y antimalware

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

El módulo **Antivirus y antimalware** protege sus máquinas Windows, Linux y macOS de todas las amenazas de malware recientes. Consulte la lista completa de funciones antimalware compatibles en "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 897).

La protección antimalware y antivirus es compatible con el centro de protección de Windows y viene registrada en él.

Características de la protección antimalware

- Detección de malware en archivos en los modos de protección en tiempo real y bajo demanda
- Detección de comportamientos maliciosos en los procesos (para Windows)
- Bloqueo de acceso a URL maliciosas (para Windows)
- Puesta en cuarentena de archivos peligrosos
- Inclusión de aplicaciones corporativas de confianza en la lista blanca

Tipos de análisis

Podrá configurar la protección antimalware y antivirus para que funcione de forma constante en segundo plano o a demanda.

Protección en tiempo real

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La protección en tiempo real comprueba todos los archivos que se van a ejecutar o abrir en una máquina para evitar las amenazas de malware.

La protección en tiempo real no funciona de forma paralela con otras soluciones antivirus que también utilizan funcionalidades en tiempo real para evitar posibles problemas de compatibilidad y rendimiento. El estado de otras soluciones antivirus instaladas se determinan mediante el Centro de seguridad de Windows. Si el equipo Windows ya está protegido por otra solución antivirus, la protección en tiempo real se apaga de forma automática.

Para habilitar la protección en tiempo real, deshabilite o desinstale la otra solución antivirus. La protección en tiempo real puede reemplazar la protección en tiempo real de Microsoft Defender de forma automática.

Nota
En máquinas que ejecutan sistemas operativos de Windows Server, Microsoft Defender no se apagará de forma automática cuando se habilite la protección en tiempo real. Los administradores deben apagar Microsoft Defender de forma manual para evitar posibles problemas de compatibilidad.

Puede escoger uno de los siguientes modos de análisis:

- La detección **En acceso inteligente** es aquella en la que el programa antimalware se ejecuta en segundo plano, y analiza de forma activa y constante su equipo en busca de virus y otras amenazas maliciosas. Además, se lleva a cabo siempre que el sistema esté encendido. En ambos casos, el malware se detectará cuando se ejecute un archivo y durante las operaciones con el mismo, por ejemplo, al abrirlo para su lectura o modificación.
- La detección **en ejecución** significa que los archivos ejecutables solo se escanean en el momento de su ejecución para garantizar que estén limpios y que no causarán ningún daño al equipo o a los datos. No se detectará la copia de un archivo infectado.

Análisis planificado

El análisis antimalware se lleva a cabo según una planificación.

Puede escoger uno de los siguientes modos de análisis.

- **Análisis rápido**: solo comprueba los archivos del sistema de carga de trabajo.
- **Análisis completo**: comprueba todos los archivos de su carga de trabajo.
- **Análisis personalizado**: comprueba los archivos y las carpetas que añadió el administrador al plan de protección.

Una vez que finalice el análisis antimalware, podrá ver los detalles sobre las cargas de trabajo que se vieron afectadas por amenazas en el widget **Supervisión** > **Información general** > Elementos afectados recientemente.

Configuración de los ajustes de la protección antivirus y antimalware

En esta sección se describen las funciones que puede configurar en el módulo **Protección antivirus y antimalware** de un plan de protección. Para obtener más información sobre cómo crear un plan de protección, consulte "Creación de un plan de protección" (p. 230).

Se pueden configurar las siguientes funciones en el módulo de protección antivirus y antimalware para un plan de protección:

- "Active Protection" (p. 903)
- "Antimalware avanzado" (p. 904)

- "Protección de carpetas de red" (p. 904)
- "Protección del servidor" (p. 905)
- "Autoprotección" (p. 906)
- "Detección del proceso de criptominería" (p. 907)
- "Configuración de cuarentena" (p. 908)
- "Motor de comportamiento" (p. 908)
- "Prevención de vulnerabilidades" (p. 909)
- "Protección en tiempo real" (p. 911)
- "Planificar análisis" (p. 912)
- "Exclusiones de protección" (p. 915)

Nota
No todos los sistemas operativos admiten las funciones de protección antivirus y antimalware. Para obtener más información sobre los sistemas operativos y las funciones compatibles, consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 897). Algunas funciones requieren una licencia específica para estar disponibles en su plan de protección.

Active Protection

Active Protection protege su sistema del software malicioso conocido como ransomware, el cual cifra los archivos y pide un rescate para obtener la clave de cifrado.

Configuración predeterminada: **Habilitado**.

Nota
Debe instalarse un agente de protección en el equipo protegido. Para obtener más información sobre los sistemas operativos y las funciones compatibles, consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 897).

Pasos para configurar Active Protection

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Active Protection**.
3. En la sección **Acción sobre la detección**, seleccione una de las opciones disponibles:

   Configuración predeterminada: **Revertir usando la caché**

   - **Solo notificar**: el software genera una alerta sobre el proceso sospechoso de actividad de ransomware.
   - **Detener el proceso**: el software genera una alerta y detiene el proceso sospechoso de actividad de ransomware.

- **Revertir usando la caché**: el software genera una alerta, detiene el proceso y revierte los cambios de los archivos usando la caché de servicios.

4. Haga clic en **Listo** para aplicar las opciones seleccionadas a su plan de protección.

Antimalware avanzado

Este motor utiliza una base de datos mejorada de firmas de virus para mejorar la eficiencia de la detección antimalware tanto en los análisis rápidos como completos.

Importante
Esta función solo está disponible si tiene el paquete de protección Advanced Security habilitado. Para obtener más información, consulte https://www.acronis.com/es-es/products/cloud/cyber-protect/security/

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Pasos para configurar el antimalware avanzado

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. En la sección **Antimalware avanzado**, utilice el conmutador para habilitar el motor basado en firmas locales.

Nota
La protección antivirus y antimalware para macOS y Linux también requiere el motor basado en firmas locales. Para Windows, la protección antivirus y antimalware está disponible con o sin este motor.

Protección de carpetas de red

La función **Protección de carpetas de red** define si la protección antivirus y antimalware protege las carpetas de red que están asignadas como unidades locales. Esta protección se aplica a carpetas compartidas por protocolos SMB o NFS.

Pasos para configurar la protección de carpetas de red

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Protección de carpetas de red**.
3. Añada los archivos en los que quiera hacer la copia de seguridad de las carpetas de red:
   - Por ejemplo, si la carga de trabajo es Windows, en el campo **Windows**, introduzca la ruta al archivo de Windows en el que quiera hacer la copia de seguridad de las carpetas de red. Valor predeterminado: C:\ProgramData\Acronis\Restored Network Files.

- Por ejemplo, si la carga de trabajo es macOS, en el campo **macOS**, introduzca la ruta a los archivos de macOS en los que quiera hacer la copia de seguridad de las carpetas de red. Valor predeterminado: /Library/Application Support/Acronis/Restored Network Files/.

Nota
Introduzca la ruta a una carpeta local. No se admiten carpetas de red, ni siquiera las de unidades asignadas, como destino de copias de seguridad para las carpetas de red.

4. Haga clic en **Listo** para aplicar las opciones seleccionadas a su plan de protección.

Protección del servidor

Esta función define si Active Protection protege las carpetas de la red que comparte de conexiones entrantes externas de otros servidores de la red que puedan suponer una amenaza.

Configuración predeterminada: **Apagado**.

Nota
La protección del servidor no es compatible con Linux.

Pasos para establecer conexiones de confianza

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Protección del servidor**.
3. Utilice el conmutador **Protección del servidor** para habilitarla.
4. Seleccione la pestaña **De confianza**.
5. En el campo **Conexiones de confianza**, haga clic en **Añadir** para definir las conexiones que podrán modificar datos.
6. En el campo **Nombre del equipo/Cuenta**, escriba el nombre del ordenador y la cuenta del equipo donde está instalado el agente de protección. Por ejemplo, `MyComputer\TestUser`.
7. En el campo **Nombre del servidor**, escriba el nombre del servidor del equipo que tiene permitido conectarse a este con el agente de protección.
8. Haga clic en la marca de verificación de la derecha para guardar la definición de la conexión.
9. Haga clic en **Listo**.

Pasos para establecer conexiones bloqueadas

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Protección del servidor**.
3. Utilice el conmutador **Protección del servidor** para habilitarla.
4. Seleccione la pestaña **Bloqueadas**.

5. En el campo **Conexiones bloqueadas**, haga clic en **Añadir** para definir las conexiones que no podrán modificar datos.
6. En el campo **Nombre del equipo/Cuenta**, escriba el nombre del ordenador y la cuenta del equipo donde está instalado el agente de protección. Por ejemplo, `MyComputer\TestUser`.
7. En el campo **Nombre del servidor**, escriba el nombre del servidor del equipo que tiene permitido conectarse a este con el agente de protección.
8. Seleccione la casilla de verificación de la derecha para guardar la definición de la conexión.
9. Haga clic en **Listo**.

Autoprotección

La autoprotección evita los cambios no autorizados en los procesos propios del software, los archivos de registro, los archivos ejecutables y de configuración, y las copias de seguridad que se encuentran en las carpetas locales.

Los administradores pueden habilitar **Autoprotección**, sin habilitar **Active Protection**.

Configuración predeterminada: **Activado**.

Nota
La autoprotección no es compatible con Linux.

Pasos para habilitar la autoprotección

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Autoprotección**.
3. Utilice el conmutador **Autoprotección** para habilitarla.

Para habilitar la Protección con contraseña

1. Una vez que se haya habilitado la función **Autoprotección**, puede marcar el conmutador de la opción **Protección con contraseña** para habilitarla.
2. Haga clic en **Generar nueva contraseña** para generar una contraseña que le permite modificar o eliminar agentes locales.
3. Haga clic en **Copiar** y péguela en un lugar seguro, ya que se le solicitará cuando quiera modificar la lista de componentes localmente.

   Importante
   La contraseña no estará disponible cuando cierre la ventana. Para aplicar esta contraseña a los dispositivos, debe guardar la configuración del plan de protección.

4. Haga clic en **Cerrar**.

La **protección con contraseña** evita que un software o usuario no autorizado desinstale el agente para Windows o modifique sus componentes. Estas acciones solo se pueden realizar con una contraseña provista por un administrador.

Las siguientes acciones nunca requieren contraseña:

- Actualizar la instalación mediante la ejecución local del programa de instalación.
- Actualizar la instalación mediante el uso de la consola de Cyber Protect
- Reparar la instalación.

Configuración predeterminada: **Deshabilitado**

Para obtener más información acerca de cómo habilitar la **protección con contraseña**, consulte Evitar la desinstalación o modificación de agentes no autorizadas.

Detección del proceso de criptominería

El malware de criptominería afecta al rendimiento de aplicaciones de utilidad, aumenta el importe de las facturas de electricidad, puede hacer que el sistema se bloquee e, incluso, dañar el hardware debido a su explotación. La función **Detección del proceso de criptominería** protege los dispositivos del malware de criptominería para impedir el uso no autorizado de los recursos del equipo.

Los administradores pueden habilitar **Detección del proceso de criptominería**, sin habilitar **Active Protection**. Configuración predeterminada: **Habilitado**.

Nota
La detección del proceso de criptominería no es compatible con Linux.

Pasos para configurar la protección de carpetas de red

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Detección del proceso de criptominería**.
3. Utilice el conmutador **Detectar procesos de criptominería** para habilitar o deshabilitar la función.
4. Seleccione qué se debe hacer con los procesos sospechosos de actividad de criptominería:

   Configuración predeterminada: **Detener el proceso**

   - **Solo notificar**: el software genera una alerta.
   - **Detener el proceso**: el software genera una alerta y detiene el proceso.
5. Haga clic en **Listo** para aplicar las opciones seleccionadas a su plan de protección.

Configuración de cuarentena

La carpeta Cuarentena sirve para aislar los archivos sospechosos (posiblemente infectados) o potencialmente peligrosos.

Pasos para configurar Cuarentena

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Cuarentena**.
3. En el campo **Eliminar archivos en cuarentena después de**, puede definir el periodo en días tras el que se eliminarán los archivos que están puestos en cuarentena.
   Configuración predeterminada: **30 días**
4. Haga clic en **Listo**.

Para obtener más información sobre esta función, consulte Cuarentena.

Motor de comportamiento

La función **Motor de comportamiento** protege un sistema contra el malware aplicando un método heurístico de comportamiento para identificar procesos maliciosos.

Configuración predeterminada: **Habilitado**.

Nota
El motor de comportamiento no es compatible con Linux.

Pasos para configurar la protección de carpetas de red

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Motor de comportamiento**.
3. Utilice el conmutador **Motor de comportamiento** para habilitar o deshabilitar la función.
4. En la sección **Acción sobre la detección**, seleccione la acción que el software deberá realizar al detectar una actividad de malware:
   Configuración predeterminada: **Cuarentena**
   - **Solo notificar**: el software genera una alerta sobre el proceso sospechoso de actividad de malware.
   - **Detener el proceso**: el software genera una alerta y detiene el proceso sospechoso de actividad de malware.
   - **Cuarentena**: el software genera una alerta, detiene el proceso y traslada los archivos ejecutables a la carpeta de cuarentena.
5. Haga clic en **Listo** para aplicar las opciones seleccionadas a su plan de protección.

Prevención de vulnerabilidades

Importante
Esta función solo está disponible si tiene el paquete de protección Advanced Security habilitado. Para obtener más información, consulte https://www.acronis.com/es-es/products/cloud/cyber-protect/security/

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La prevención de vulnerabilidades detecta e impide que los procesos infectados se expandan y se aprovechen de las vulnerabilidades de software de los sistemas. Cuando se detecta una vulnerabilidad de seguridad, el software puede generar una alerta y detener el proceso sospechoso de actividad de vulnerabilidades.

La prevención de vulnerabilidades solo está disponible con agentes de versiones 12.5.23130 (21.08, lanzada en agosto de 2020) o posteriores.

Configuración predeterminada: **Habilitado** para planes de protección creados recientemente, y **Deshabilitado** para planes de protección existentes, creados con versiones de agente anteriores.

Nota
La prevención de vulnerabilidades no es compatible con Linux.

Puede seleccionar lo que debe hacer el programa cuando se detecte una vulnerabilidad y los métodos de prevención de vulnerabilidades que aplica el programa.

Pasos para configurar la prevención de vulnerabilidades

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Prevención de vulnerabilidades**.
3. En la sección **Acción sobre la detección**, seleccione una de las opciones disponibles:

   Configuración predeterminada: **Detener el proceso**

   - **Solo notificar**
     El software generará una alerta sobre el proceso sospechoso de actividades de vulnerabilidades.
   - **Detener el proceso**
     El software generará una alerta y detendrá el proceso sospechoso de actividades de vulnerabilidades.
4. En la sección **Técnicas de prevención de vulnerabilidades habilitadas**, seleccione de las opciones disponibles las que quiera aplicar:
   Configuración predeterminada: **Todos los métodos están habilitados**

- **Protección de memoria**

  Detecta e impide la modificación sospechosa de los derechos de ejecución de las páginas de memoria. Los procesos maliciosos aplican estas modificaciones en las propiedades de las páginas para permitir la ejecución de códigos de shell desde áreas de memoria no ejecutables, como las pilas o los montones.
- **Protección de la programación orientada al retorno (ROP)**

  Detecta y previene intentos de uso de la técnica de vulnerabilidad ROP.
- **Protección de escalada de privilegios**

  Detecta y evita los intentos de elevación de privilegios que ejecuta un código o una aplicación no autorizados. La escalada de privilegios la utilizan los códigos maliciosos para obtener el acceso completo del equipo atacado y luego llevar a cabo tareas esenciales y sensibles. Un código no autorizado no puede acceder a los recursos críticos del sistema ni modificar la configuración del sistema.
- **Protección de inyección de código**

  Detecta y previene la inyección de código malicioso en los procesos remotos. La inyección de código sirve para ocultar las intenciones maliciosas de una aplicación detrás de procesos limpios o benignos con el objetivo de evadir la detección por parte de los productos antimalware.

5. Haga clic en **Listo** para aplicar las opciones seleccionadas a su plan de protección.

Nota

Los procesos que aparecen como procesos de confianza en la lista de exclusiones no se examinarán para buscar vulnerabilidades.

Permitir que procesos específicos modifiquen las copias de seguridad

La configuración **Permitir que procesos específicos modifiquen las copias de seguridad** solo está disponible si está habilitada la configuración **Autoprotección**.

Se aplica a los archivos cuyas extensiones son .tibx, .tib o .tia y que se encuentran en carpetas locales.

Con esta configuración, puede especificar los procesos que se siguen para modificar los archivos incluidos en la copia de seguridad, aunque estén protegidos por la autoprotección. Esto es útil, por ejemplo, si elimina archivos de copia de seguridad o los traslada a una ubicación diferente con una secuencia de comandos.

Si esta configuración está deshabilitada, solo los procesos firmados por el proveedor del software de la copia de seguridad pueden modificar los archivos incluidos en ella. Así, el software puede aplicar reglas de retención y eliminar copias de seguridad cuando un usuario lo solicite desde la interfaz web. Otros procesos no podrán llevar a cabo modificaciones en ellas, sin importar si son sospechosos o no.

Si esta configuración está habilitada, puede permitir que otros procesos modifiquen las copias de seguridad. Especifique la ruta completa al ejecutable del proceso, empezando por la letra de unidad de disco.

Configuración predeterminada: **Deshabilitado**.

Protección en tiempo real

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La **Protección en tiempo real** comprueba constantemente el sistema informático para detectar virus y otras amenazas maliciosas durante todo el tiempo que el sistema esté encendido, a menos que el usuario lo detenga.

Configuración predeterminada: **Habilitado**.

Importante
Esta función solo está disponible si tiene el paquete de protección Advanced Security habilitado. Para obtener más información, consulte https://www.acronis.com/es-es/products/cloud/cyber-protect/security/

Pasos para configurar la protección en tiempo real

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Protección en tiempo real**.
3. En la lista desplegable **Acción sobre la detección**, seleccione una de las opciones disponibles:

   Configuración predeterminada: **Cuarentena**

   - **Solo notificar**

     El software genera una alerta sobre el proceso sospechoso de actividad de ransomware.

   - **Bloquear y notificar**

     El software bloquea el proceso y genera una alerta del proceso sospechoso de actividades de malware.

   - **Cuarentena**
4. El software genera una alerta, detiene el proceso y traslada el archivo ejecutable a la carpeta de cuarentena.
5. En la sección **Modo de análisis**, seleccione la acción que el software deberá realizar al detectar un virus u otra amenaza maliciosa:

   Configuración predeterminada: **En acceso inteligente**

- **En acceso inteligente**: supervisa todas las actividades del sistema y analiza automáticamente los archivos cuando se accede a ellos para su lectura o escritura, o cuando se inicia un programa.
- **En ejecución**: escanea de forma automática solo los archivos ejecutables cuando se inician para garantizar que estén limpios y que no causarán ningún daño al equipo o a los datos.

6. Haga clic en **Listo**.

Planificar análisis

El análisis bajo demanda comprueba el sistema de su equipo en busca de virus según la planificación especificada. Un análisis completo comprueba todos los archivos de su equipo, mientras que un análisis rápido solo comprueba los archivos de sistema del equipo.

Pasos para configurar Planificar análisis

Configuración predeterminada:

- **Análisis personalizado** está deshabilitado.
- Se ha programado el escaneado **Rápido** y **Completo**.

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Planificar análisis**.
3. Utilice el conmutador para habilitar el tipo de análisis que quiera aplicar al equipo.

Tipos de análisis disponibles:

- **Completo**: tarda mucho tiempo en terminar en comparación con el análisis rápido porque se comprueban todos los archivos.
- **Rápido**: solo comprueba las zonas habituales en las que suele residir el malware en el equipo.
- **Personalizado**: comprueba los archivos y las carpetas que seleccionó el administrador para el plan Protección.

> **Nota**
> Puede planificar los tres análisis, **Rápido**, **Completo** y **Personalizado**, dentro de un único plan de protección.

Pasos para configurar el análisis personalizado

- Utilice el conmutador **Análisis personalizado** para habilitar o deshabilitar este tipo de análisis.
- En la lista desplegable **Acción sobre la detección**, seleccione una de las opciones disponibles:

Configuración predeterminada: **Cuarentena**

Cuarentena

El software genera una alerta y traslada el archivo ejecutable a la carpeta de cuarentena.

Solo notificar

El software genera una alerta del proceso sospechoso de ser malware.

Campo	Descripción
Planificar la ejecución de tareas con los siguientes eventos	Esta configuración define cuándo se ejecutará la tarea. Los valores disponibles son los siguientes: • **Planificar por hora**: esta es la configuración predeterminada. La tarea se ejecutará según la hora especificada. • **Cuando el usuario inicia sesión en el sistema**: de forma predeterminada, la tarea se iniciará cuando cualquier usuario inicie sesión. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea. • **Cuando el usuario cierra sesión en el sistema**: de forma predeterminada, la tarea se iniciará cuando cualquier usuario cierre sesión. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea. **Nota** La tarea no se ejecutará al apagarse el sistema. Apagar y cerrar sesión son dos acciones diferentes de la configuración de la programación. • **Al iniciarse el sistema**: la tarea se ejecutará cuando el sistema operativo se inicie. • **Al apagarse el sistema**: la tarea se ejecutará cuando el sistema operativo se apague.
Tipo de planificación	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora**. Los valores disponibles son los siguientes: • **Mensual**: seleccione los meses y las semanas o días del mes en los que se ejecutará la tarea. • **Diariamente**: esta es la configuración predeterminada. Seleccione los días de la semana en los que se ejecutará la tarea. • **Cada hora**: seleccione los días de la semana, el número de repeticiones y el intervalo de tiempo en los que se ejecutará la tarea.
Iniciar a las	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora** Seleccione la hora exacta a la que se ejecutará la tarea.
Ejecutar dentro de un intervalo de fechas	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora**. Establezca un rango en el que la planificación configurada sea efectiva.

Campo	Descripción
Especifique una cuenta de usuario cuyo inicio de sesión en el sistema operativo iniciará una tarea	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Cuando el usuario inicia sesión en el sistema**. Los valores disponibles son los siguientes: • **Cualquier usuario**: utilice esta opción si quiere que se inicie la tarea cuando cualquier usuario inicie sesión. • **El siguiente usuario**: utilice esta opción si quiere que se inicie la tarea solo cuando un usuario específico inicie sesión.
Especifique una cuenta de usuario que al cerrar sesión en el sistema operativo iniciará una tarea	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Cuando el usuario cierra sesión en el sistema**. Los valores disponibles son los siguientes: • **Cualquier usuario**: utilice esta opción si quiere que se inicie la tarea cuando cualquier usuario cierre sesión. • **El siguiente usuario**: utilice esta opción si quiere que se inicie la tarea solo cuando un usuario específico cierre sesión.
Condiciones de inicio	Defina todas las condiciones que se deben cumplir de forma simultánea para que se ejecute la tarea. Las condiciones de inicio para el análisis antimalware son similares a las de inicio del **Módulo de copia de seguridad** que se describen en "Condiciones de inicio". Puede definir las siguientes condiciones de inicio adicionales: • **Distribuir las horas de inicio de la tarea en un período de tiempo**: esta opción le permite establecer el plazo de tiempo de la tarea para evitar cuellos de botella en la red. Puede especificar el retraso en horas o minutos. Por ejemplo, si la hora de inicio predeterminada son las 10:00 y el retraso es de 60 minutos, la tarea empezará entre las 10:00 y las 11:00. • **Si el equipo está apagado, ejecutar las tareas perdidas al iniciar el equipo** • **Evitar el modo de suspensión o hibernación durante la ejecución de una tarea**: esta opción solo se aplica en equipos que ejecuten Windows. • **Si no se cumplen las condiciones de inicio, ejecutar la tarea de todos modos después de**: especifique el periodo tras el que se ejecutará la tarea, sin importar el resto de las condiciones de inicio. **Nota** En Linux, las condiciones de inicio no están admitidas.

- Selecciona la casilla de verificación **Analizar únicamente archivos nuevos y modificados** si desea analizar solo los archivos que se hayan creado recientemente y los que se hayan modificado.

Configuración predeterminada: **Habilitado**

- Se mostrarán dos opciones adicionales para **Análisis personalizado** únicamente si se selecciona **Análisis completo**:

1. **Analizar archivos del archivo comprimido**

   Configuración predeterminada: **Habilitado**.

   Máxima profundidad de recursión

   Configuración predeterminada: **16**

   Número de niveles de archivos incrustados que se pueden analizar. Por ejemplo, documento MIME > archivo zip > archivo comprimido de Office > contenido del documento.

   Tamaño máx.

   Configuración predeterminada: **100**

   Tamaño máximo de los archivos de un archivo comprimido que se vaya a escanear.

2. **Analizar unidades extraíbles**

Configuración predeterminada: **Deshabilitado**

- **Unidades de red asignadas (remotas)**
- **Dispositivos de almacenamiento USB** (como memorias y discos duros externos)
- **CD/DVD**

Nota
El análisis de unidades extraíbles no es compatible con Linux.

Exclusiones de protección

Las exclusiones de protección le permiten eliminar falsos positivos cuando un programa de confianza se considera ransomware o malware. Puede definir los elementos de confianza y los bloqueados. Para ello, añádalos a la lista de exclusiones de protección.

En la lista de elementos de confianza, puede añadir archivos, procesos y carpetas para que el sistema los considere seguros y evitar que los detecte en el futuro.

En la lista de elementos bloqueados, puede añadir procesos y hash. Esta opción garantiza que se bloquean esos procesos y su carga de trabajo estará a salvo.

Elemento de exclusión de protección	Bloqueado	De confianza
Hash	Cuando se añada un hash a la lista de bloqueados, el sistema detendrá el proceso, según el hash proporcionado. Por ejemplo, cuando añade este hash MD5, 938c2cc0dcc05f2b68c4287040cfcf71, se bloquea el proceso asociado a dicho hash.	Cuando se añada un hash a la lista de confianza, el sistema sabrá qué procesos debe ignorar mediante la supervisión, según el hash proporcionado. Por ejemplo, cuando añade este hash MD5, 938c2cc0dcc05f2b68c4287040cfcf71, el proceso asociado a este hash se considera de confianza y se excluye de la supervisión.
Proceso	Cuando se añada un proceso a la lista de bloqueados, el sistema sabrá que debe supervisar esos procesos, y los procesos se bloquearán siempre. Por ejemplo, si añade esta ruta C:\Users\user1\application\nppInstaller.exe a la lista de bloqueados, se bloqueará este proceso específico y, cuando intente abrirlo, no podrá iniciarse.	Cuando se añada un proceso a la lista de confianza, el sistema sabrá que debe excluir esos procesos de la supervisión. **Nota** Los procesos firmados por Microsoft siempre son de confianza. Por ejemplo, si añade la ruta C:\Users\user1\application\nppInstaller.exe, este proceso específico se excluirá de la supervisión y el antivirus no interferirá con dicho proceso.
Archivo/carpeta		Cuando se añada un archivo o una carpeta a la lista de confianza, el sistema sabrá que dichos archivos o carpetas se considerarán siempre seguros y no es necesario analizarlos o supervisarlos.

Pasos para especificar los elementos que siempre serán de confianza

1. Abra el plan de protección.
2. Expanda el módulo **Protección antivirus y antimalware**.
3. Seleccione la opción **Exclusiones**.
   Se mostrará la ventana **Exclusiones de protección**.
4. En la sección **Elementos de confianza**, haga clic en **Añadir** para seleccionar entre las opciones disponibles:

- Para añadir archivos, carpetas o procesos a los elementos de confianza, seleccione la opción **Archivo/carpeta/proceso**. Se mostrará la ventana **Añadir archivo/carpeta/proceso**.
  - En el campo **Archivo/proceso/carpeta**, escriba la ruta para cada proceso, carpeta o archivo en una nueva línea. En la sección **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos de confianza.
  - Seleccione la casilla de verificación **Añadir como archivo/carpeta** para añadir el archivo o carpeta a los elementos de confianza.
    Ejemplos de descripciones de carpetas: D:\carpeta\, /inicio/Carpeta/carpeta2, F:\
  - Seleccione la casilla de verificación **Añadir como proceso** para añadir el proceso a los elementos de confianza. Los procesos seleccionados se excluirán de la supervisión.

    Nota
    Especifique la ruta completa al ejecutable del proceso, empezando por la letra de unidad de disco. Por ejemplo, `C:\Windows\Temp\er76s7sdkh.exe`.

    Nota
    Se admiten rutas de red local. Por ejemplo, \\localhost\folderpath\file.exe

- Seleccione la opción **Hash** para añadir hash MD5 a la lista de elementos de confianza. Se mostrará la ventana **Añadir hash**.
  - Aquí puede insertar los hash MD5 en líneas separadas para que se incluyan como de confianza en la lista de exclusiones de protección. En función de estos hash, Cyber Protection excluirá los procesos descritos por los hash MD5 de la supervisión.

Configuración predeterminada: no se define ninguna exclusión de forma predeterminada.

Pasos para especificar los elementos que siempre se bloquearán

1. Abra el plan de protección.
2. Expanda el módulo **Protección antivirus y antimalware**.
3. Seleccione la opción **Exclusiones de protección**. Se mostrará la ventana **Exclusiones de protección**.

   En la sección **Elementos bloqueados**, haga clic en **Añadir** para seleccionar entre las opciones disponibles:
- Para bloquear procesos, seleccione la opción **Proceso**. Se mostrará la ventana **Añadir proceso**.
  - En el campo **Proceso**, escriba la ruta de cada proceso en una nueva línea. En el campo **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos bloqueados.

  Nota
  Estos procesos no podrán iniciarse mientras Active Protection esté habilitado en el equipo.

- Para bloquear hash, seleccione la opción **Hash**. Se mostrará la ventana **Añadir hash**.
  - En el campo **Hash**, escriba el hash de cada proceso en una nueva línea. En el campo **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos bloqueados.

Configuración predeterminada: no se define ninguna exclusión de forma predeterminada.

Comodines

Para especificar carpetas, puede utilizar los caracteres comodín * y ?. El asterisco (*) sustituye a cero o más caracteres. La interrogación (?) sustituye exactamente a un carácter. No se pueden usar variables de entorno, como `%AppData%`.

Puede usar un comodín (*) para añadir elementos a las listas de exclusión.

- Los comodines se pueden usar en medio o al final de la descripción.

Ejemplos de comodines aceptados en descripciones:

C:*.pdf

D:\carpetas\archivo.*

C:\Users*\AppData\Roaming

- No se pueden utilizar caracteres comodín al principio de la descripción.

Ejemplos de comodines que no se aceptan en descripciones:

*.docx

*:\carpeta\

Variables

También puede usar variables para añadir elementos a las listas de exclusiones de protección, con las siguientes limitaciones:

- Para Windows, solo se admiten las variables del SISTEMA. No se admiten las variables específicas del usuario, por ejemplo, %USERNAME% o %APPDATA%. No se admiten variables con {username}. Para obtener más información, consulte https://ss64.com/nt/syntax-variables.html.
- Para macOS, no se admiten las variables de entorno.
- Para Linux, no se admiten las variables de entorno.

Ejemplos de formatos compatibles:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Descripción

Puede usar el campo **Descripción** para introducir notas sobre las exclusiones añadidas en la lista de exclusiones de protección. A continuación, puede ver algunas sugerencias de notas que puede añadir:

- Motivo y objetivo de la exclusión.
- Nombre del archivo actual de una exclusión hash.
- La fecha y la hora.

Si se añaden varios elementos en una única entrada, solo podrá haber 1 comentario para todos los elementos.

Active Protection en la edición Cyber Backup Standard

En las edición de Cyber Backup Standard, Active Protection es un módulo independiente del plan de protección. Por lo tanto, se puede configurar de forma independiente y aplicar a distintos dispositivos o grupos de dispositivos.

Para todas las demás ediciones del servicio de ciberprotección, Active Protection es parte del módulo **Antivirus y antimalware** del plan de protección.

Configuración predeterminada: **Habilitado**.

Nota
Debe instalarse un agente de protección en el equipo protegido. Para obtener más información sobre los sistemas operativos y las funciones compatibles, consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 897).

Cómo funciona

Active Protection controla los procesos que se ejecutan en el equipo protegido. Si el proceso de un tercero intenta cifrar algún archivo o minar criptomonedas, Active Protection genera una alerta y lleva a cabo otras acciones, según se especifica en el plan de protección.

Además, Active Protection evita los cambios no autorizados en los procesos propios del software de copia de seguridad, los archivos de registro, los archivos ejecutables y de configuración y las copias de seguridad que se encuentran en las carpetas locales.

Para identificar los procesos maliciosos, Active Protection utiliza la heurística basada en el comportamiento. Active Protection compara la cadena de acciones realizadas por un proceso con las cadenas de eventos registradas en la base de datos de patrones de conducta maliciosos. Este enfoque permite a Active Protection detectar malware nuevo identificando su comportamiento típico.

Configuración de Active Protection en Cyber Backup Standard

En la edición Cyber Backup Standard, podrá configurar las siguientes funciones de Active Protection:

- Acción sobre la detección
- Autoprotección
- Protección de carpetas de red
- Protección del servidor
- Detección del proceso de criptominería
- Exclusiones

Nota
Active Protection para Linux es compatible con las opciones de configuración siguientes: Acción sobre la detección, protección de carpetas de red y exclusiones. La protección de carpetas de red siempre está activa y no es configurable.

Acción sobre la detección

En la sección **Acción sobre la detección**, seleccione una de las opciones disponibles:

- **Solo notificar**
  El software generará una alerta sobre el proceso sospechoso de actividad de ransomware.
- **Detener el proceso**
  El software generará una alerta y detendrá el proceso sospechoso de actividad de ransomware.
- **Revertir usando la caché**
  El software generará una alerta, detendrá el proceso y revertirá los cambios de los archivos usando la caché de servicios.

Configuración predeterminada: **Revertir usando la caché**.

La autoprotección evita los cambios no autorizados en los procesos propios del software, los archivos de registro, los archivos ejecutables y de configuración, y las copias de seguridad que se encuentran en las carpetas locales.

Los administradores pueden habilitar **Autoprotección**, sin habilitar **Active Protection**.

Configuración predeterminada: **Activado**.

Nota
La autoprotección no es compatible con Linux.

Pasos para habilitar la autoprotección

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.

2. Haga clic en **Autoprotección**.
3. Utilice el conmutador **Autoprotección** para habilitarla.

Para habilitar la Protección con contraseña

1. Una vez que se haya habilitado la función **Autoprotección**, puede marcar el conmutador de la opción **Protección con contraseña** para habilitarla.
2. Haga clic en **Generar nueva contraseña** para generar una contraseña que le permite modificar o eliminar agentes locales.
3. Haga clic en **Copiar** y péguela en un lugar seguro, ya que se le solicitará cuando quiera modificar la lista de componentes localmente.

   Importante
   La contraseña no estará disponible cuando cierre la ventana. Para aplicar esta contraseña a los dispositivos, debe guardar la configuración del plan de protección.

4. Haga clic en **Cerrar**.

La **protección con contraseña** evita que un software o usuario no autorizado desinstale el agente para Windows o modifique sus componentes. Estas acciones solo se pueden realizar con una contraseña provista por un administrador.

Las siguientes acciones nunca requieren contraseña:

- Actualizar la instalación mediante la ejecución local del programa de instalación.
- Actualizar la instalación mediante el uso de la consola de Cyber Protect
- Reparar la instalación.

Configuración predeterminada: **Deshabilitado**

Para obtener más información acerca de cómo habilitar la **protección con contraseña**, consulte Evitar la desinstalación o modificación de agentes no autorizadas.

Protección de carpetas de red

La configuración **Proteger carpetas de red asignadas como dispositivos locales** define si Active Protection protege las carpetas de la red que están asignadas como dispositivos locales de los procesos maliciosos locales.

Esta configuración se aplica a carpetas compartidas por protocolos SMB o NFS.

Si un archivo se encontraba al principio en un dispositivo asignado, no se puede guardar en la ubicación original cuando se extraiga de la caché mediante la acción **Revertir usando la caché**. En su lugar, se guardará en la carpeta especificada en esta configuración. La carpeta predeterminada es `C:\ProgramData\Acronis\Restored Network Files` para Windows y `Library/Application Support/Acronis/Restored Network Files/` para macOS. Si esta carpeta no existe, se creará. Si quiere

cambiar la ruta, especifique una carpeta local. No se admiten carpetas de red, ni siquiera las de dispositivos asignados.

Configuración predeterminada: **Activado**.

Esta función define si Active Protection protege las carpetas de la red que comparte de conexiones entrantes externas de otros servidores de la red que puedan suponer una amenaza.

Configuración predeterminada: **Apagado**.

Nota
La protección del servidor no es compatible con Linux.

Pasos para establecer conexiones de confianza

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Protección del servidor**.
3. Utilice el conmutador **Protección del servidor** para habilitarla.
4. Seleccione la pestaña **De confianza**.
5. En el campo **Conexiones de confianza**, haga clic en **Añadir** para definir las conexiones que podrán modificar datos.
6. En el campo **Nombre del equipo/Cuenta**, escriba el nombre del ordenador y la cuenta del equipo donde está instalado el agente de protección. Por ejemplo, `MyComputer\TestUser`.
7. En el campo **Nombre del servidor**, escriba el nombre del servidor del equipo que tiene permitido conectarse a este con el agente de protección.
8. Haga clic en la marca de verificación de la derecha para guardar la definición de la conexión.
9. Haga clic en **Listo**.

Pasos para establecer conexiones bloqueadas

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Protección del servidor**.
3. Utilice el conmutador **Protección del servidor** para habilitarla.
4. Seleccione la pestaña **Bloqueadas**.
5. En el campo **Conexiones bloqueadas**, haga clic en **Añadir** para definir las conexiones que no podrán modificar datos.
6. En el campo **Nombre del equipo/Cuenta**, escriba el nombre del ordenador y la cuenta del equipo donde está instalado el agente de protección. Por ejemplo, `MyComputer\TestUser`.
7. En el campo **Nombre del servidor**, escriba el nombre del servidor del equipo que tiene permitido conectarse a este con el agente de protección.

8. Seleccione la casilla de verificación de la derecha para guardar la definición de la conexión.
9. Haga clic en **Listo**.

El malware de criptominería afecta al rendimiento de aplicaciones de utilidad, aumenta el importe de las facturas de electricidad, puede hacer que el sistema se bloquee e, incluso, dañar el hardware debido a su explotación. La función **Detección del proceso de criptominería** protege los dispositivos del malware de criptominería para impedir el uso no autorizado de los recursos del equipo.

Los administradores pueden habilitar **Detección del proceso de criptominería**, sin habilitar **Active Protection**. Configuración predeterminada: **Habilitado**.

Nota
La detección del proceso de criptominería no es compatible con Linux.

Pasos para configurar la protección de carpetas de red

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Detección del proceso de criptominería**.
3. Utilice el conmutador **Detectar procesos de criptominería** para habilitar o deshabilitar la función.
4. Seleccione qué se debe hacer con los procesos sospechosos de actividad de criptominería:

   Configuración predeterminada: **Detener el proceso**

   - **Solo notificar**: el software genera una alerta.
   - **Detener el proceso**: el software genera una alerta y detiene el proceso.
5. Haga clic en **Listo** para aplicar las opciones seleccionadas a su plan de protección.

Las exclusiones de protección le permiten eliminar falsos positivos cuando un programa de confianza se considera ransomware o malware. Puede definir los elementos de confianza y los bloqueados. Para ello, añádalos a la lista de exclusiones de protección.

En la lista de elementos de confianza, puede añadir archivos, procesos y carpetas para que el sistema los considere seguros y evitar que los detecte en el futuro.

En la lista de elementos bloqueados, puede añadir procesos y hash. Esta opción garantiza que se bloquean esos procesos y su carga de trabajo estará a salvo.

Elemento de exclusión de protección	Bloqueado	De confianza
Hash	Cuando se añada un hash a la lista de bloqueados, el sistema detendrá el proceso, según el hash proporcionado. Por ejemplo, cuando añade este hash MD5, 938c2cc0dcc05f2b68c4287040cfcf71, se bloquea el proceso asociado a dicho hash.	Cuando se añada un hash a la lista de confianza, el sistema sabrá qué procesos debe ignorar mediante la supervisión, según el hash proporcionado. Por ejemplo, cuando añade este hash MD5, 938c2cc0dcc05f2b68c4287040cfcf71, el proceso asociado a este hash se considera de confianza y se excluye de la supervisión.
Proceso	Cuando se añada un proceso a la lista de bloqueados, el sistema sabrá que debe supervisar esos procesos, y los procesos se bloquearán siempre. Por ejemplo, si añade esta ruta C:\Users\user1\application\nppInstaller.exe a la lista de bloqueados, se bloqueará este proceso específico y, cuando intente abrirlo, no podrá iniciarse.	Cuando se añada un proceso a la lista de confianza, el sistema sabrá que debe excluir esos procesos de la supervisión. **Nota** Los procesos firmados por Microsoft siempre son de confianza. Por ejemplo, si añade la ruta C:\Users\user1\application\nppInstaller.exe, este proceso específico se excluirá de la supervisión y el antivirus no interferirá con dicho proceso.
Archivo/carpeta		Cuando se añada un archivo o una carpeta a la lista de confianza, el sistema sabrá que dichos archivos o carpetas se considerarán siempre seguros y no es necesario analizarlos o supervisarlos.

Pasos para especificar los elementos que siempre serán de confianza

1. Abra el plan de protección.
2. Expanda el módulo **Protección antivirus y antimalware**.
3. Seleccione la opción **Exclusiones**.
   Se mostrará la ventana **Exclusiones de protección**.
4. En la sección **Elementos de confianza**, haga clic en **Añadir** para seleccionar entre las opciones disponibles:

- Para añadir archivos, carpetas o procesos a los elementos de confianza, seleccione la opción **Archivo/carpeta/proceso**. Se mostrará la ventana **Añadir archivo/carpeta/proceso**.
  - En el campo **Archivo/proceso/carpeta**, escriba la ruta para cada proceso, carpeta o archivo en una nueva línea. En la sección **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos de confianza.
  - Seleccione la casilla de verificación **Añadir como archivo/carpeta** para añadir el archivo o carpeta a los elementos de confianza.
    Ejemplos de descripciones de carpetas: D:\carpeta\, /inicio/Carpeta/carpeta2, F:\
  - Seleccione la casilla de verificación **Añadir como proceso** para añadir el proceso a los elementos de confianza. Los procesos seleccionados se excluirán de la supervisión.

    Nota
    Especifique la ruta completa al ejecutable del proceso, empezando por la letra de unidad de disco. Por ejemplo, `C:\Windows\Temp\er76s7sdkh.exe`.

    Nota
    Se admiten rutas de red local. Por ejemplo, \\localhost\folderpath\file.exe

- Seleccione la opción **Hash** para añadir hash MD5 a la lista de elementos de confianza. Se mostrará la ventana **Añadir hash**.
  - Aquí puede insertar los hash MD5 en líneas separadas para que se incluyan como de confianza en la lista de exclusiones de protección. En función de estos hash, Cyber Protection excluirá los procesos descritos por los hash MD5 de la supervisión.

Configuración predeterminada: no se define ninguna exclusión de forma predeterminada.

Pasos para especificar los elementos que siempre se bloquearán

1. Abra el plan de protección.
2. Expanda el módulo **Protección antivirus y antimalware**.
3. Seleccione la opción **Exclusiones de protección**. Se mostrará la ventana **Exclusiones de protección**.

   En la sección **Elementos bloqueados**, haga clic en **Añadir** para seleccionar entre las opciones disponibles:
- Para bloquear procesos, seleccione la opción **Proceso**. Se mostrará la ventana **Añadir proceso**.
  - En el campo **Proceso**, escriba la ruta de cada proceso en una nueva línea. En el campo **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos bloqueados.

  Nota
  Estos procesos no podrán iniciarse mientras Active Protection esté habilitado en el equipo.

- Para bloquear hash, seleccione la opción **Hash**. Se mostrará la ventana **Añadir hash**.
  - En el campo **Hash**, escriba el hash de cada proceso en una nueva línea. En el campo **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos bloqueados.

Configuración predeterminada: no se define ninguna exclusión de forma predeterminada.

Comodines

Para especificar carpetas, puede utilizar los caracteres comodín * y ?. El asterisco (*) sustituye a cero o más caracteres. La interrogación (?) sustituye exactamente a un carácter. No se pueden usar variables de entorno, como `%AppData%`.

Puede usar un comodín (*) para añadir elementos a las listas de exclusión.

- Los comodines se pueden usar en medio o al final de la descripción.

Ejemplos de comodines aceptados en descripciones:

C:*.pdf

D:\carpetas\archivo.*

C:\Users*\AppData\Roaming

- No se pueden utilizar caracteres comodín al principio de la descripción.

Ejemplos de comodines que no se aceptan en descripciones:

*.docx

*:\carpeta\

Variables

También puede usar variables para añadir elementos a las listas de exclusiones de protección, con las siguientes limitaciones:

- Para Windows, solo se admiten las variables del SISTEMA. No se admiten las variables específicas del usuario, por ejemplo, %USERNAME% o %APPDATA%. No se admiten variables con {username}. Para obtener más información, consulte https://ss64.com/nt/syntax-variables.html.
- Para macOS, no se admiten las variables de entorno.
- Para Linux, no se admiten las variables de entorno.

Ejemplos de formatos compatibles:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Descripción

Puede usar el campo **Descripción** para introducir notas sobre las exclusiones añadidas en la lista de exclusiones de protección. A continuación, puede ver algunas sugerencias de notas que puede añadir:

- Motivo y objetivo de la exclusión.
- Nombre del archivo actual de una exclusión hash.
- La fecha y la hora.

Si se añaden varios elementos en una única entrada, solo podrá haber 1 comentario para todos los elementos.

Filtrado de URL

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

El malware lo suelen distribuir sitios infectados o maliciosos mediante el método de infección conocido como Drive-by download.

La funcionalidad Filtrado de URL que le permite proteger los equipos de amenazas como el malware o suplantación de identidad que procedan Internet. Puede proteger su organización si bloquea el acceso del usuario a los sitios web en los que pueda haber contenido malicioso.

El filtrado de URL también puede controlar el uso de los sitios web para que cumplan con las regulaciones externas y las directivas internas de la empresa. Puede configurar el acceso a los sitios web en función de su categoría relacionada. En estos momentos, el filtrado de URL admite 44 categorías de sitio web y permite gestionar el acceso a ellas.

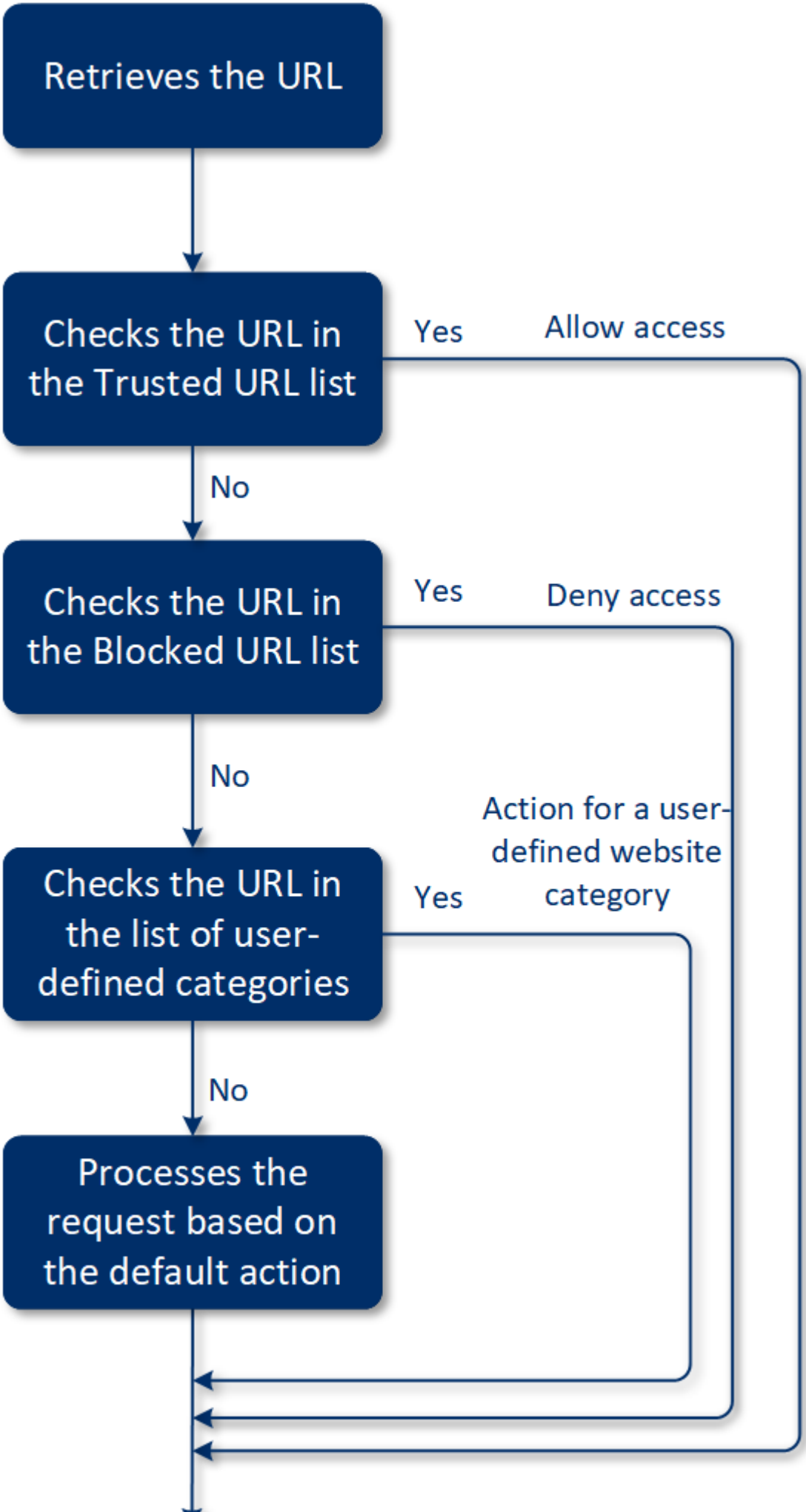
Actualmente las conexiones HTTP/HTTPS de los equipos Windows las comprueba el agente de protección.

La característica Filtrado de URL necesita conectarse a Internet para funcionar.

Nota
Para evitar posibles problemas de compatibilidad con compilaciones 15.0.26692 (lanzamiento C21.03 HF1) de agentes de protección y anteriores, la función del filtrado de URL se deshabilitará de forma automática si se detecta otra solución antivirus o si el servicio del Centro de seguridad de Windows no está presente en el sistema.
Para agentes de protección posteriores, los problemas de compatibilidad se resuelven para que el filtrado de URL esté siempre habilitado según la directiva.

Cómo funciona

Un usuario introduce el enlace de un URL en un navegador. El interceptor obtiene el enlace y lo envía al agente de protección. El agente obtiene la URL, la analiza y comprueba el veredicto. El interceptor redirige a un usuario a la página con el mensaje con distintas acciones para que continúe manualmente a la página solicitada.

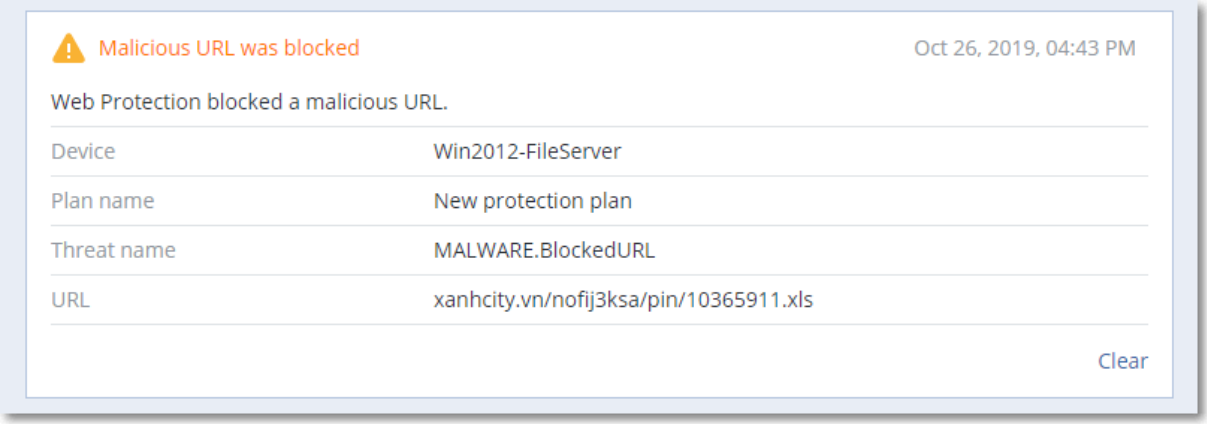

Retrieves the URL
Checks the URL in the Trusted URL list
Yes
Allow access
No
Checks the URL in the Blocked URL list
Yes
Deny access
No
Checks the URL in the list of user-defined categories
Yes
Action for a user-defined website category
No
Processes the request based on the default action

Flujo de trabajo de la configuración del filtrado de URL

Normalmente, la configuración del filtrado de URL está formada por los siguientes pasos:

1. Cree un plan de protección con el módulo **Filtrado de URL** habilitado.
2. Especifique los ajustes del filtrado de URL (consulte la información que aparece a continuación).
3. Asigne el plan de protección a los equipos.

Para comprobar qué direcciones URL se han bloqueado, vaya a **Supervisión** > **Alertas**.



Ajustes del filtrado de URL

Para el módulo de filtrado de URL se pueden establecer los siguientes ajustes:

Acceso a sitio web malicioso

Especifique qué acción se llevará a cabo cuando un usuario abra un sitio web malicioso:

- **Solo notificar**: el software genera una alerta sobre el proceso sospechoso de actividad de ransomware.
- **Bloquear**: bloquear el acceso al sitio web malicioso. El usuario no podrá acceder al sitio web y se generará una alerta advertencia.
- **Preguntar siempre al usuario**: preguntar al usuario si quiere continuar y acceder al sitio web o volver atrás.

Categorías que se pueden filtrar

Hay 44 categorías de sitio web cuyo acceso puede configurar:

- **Permitir**: permite el acceso a los sitios web relacionados con la categoría seleccionada.
- **Rechazar**: deniega el acceso a los sitios web relacionados con la categoría seleccionada.

De manera predeterminada, todas las categorías están permitidas.

Mostrar todas las notificaciones de las URL bloqueadas por categorías: si esta opción está habilitada, recibirá organizadas por categorías todas las notificaciones que se muestran en la bandeja de URL bloqueadas. Si un sitio web tiene varios subdominios, el sistema también genera notificaciones para ellos, por lo que el número de notificaciones puede ser muy elevado.

En la tabla siguiente puede encontrar la descripción de las categorías:

	Categoría del sitio web	Descripción
1	**Publicidad**	En esta categoría se incluyen aquellos dominios cuyo objetivo principal es ofrecer anuncios.
2	**Tableros de mensajes**	En esta categoría se incluyen los foros, los grupos de discusión y los sitios web de pregunta-respuesta. Esta categoría no cubre las secciones específicas de los sitios web empresariales donde los clientes hacen preguntas.
3	**Sitios web personales**	En esta categoría se incluyen los sitios web personales y todos los tipos de blogs: individuales, de varias personas e incluso de empresas. Un blog es un diario publicado en la World Wide Web. Consta de entradas (“publicaciones”) que normalmente se muestran en orden cronológico inverso, de modo que las más recientes aparecen primero.
4	**Sitios web empresariales/corporativos**	Esta categoría es amplia porque abarca los sitios web corporativos que no suelen pertenecer a ninguna otra categoría.
5	**Software**	En esta categoría se incluyen aquellos sitios web en los que se ofrece software, normalmente de código abierto, gratuito o shareware. También puede cubrir algunas tiendas de software en línea.
6	**Medicamentos**	En esta categoría se incluyen los sitios web relacionados con los medicamentos, el alcohol o los cigarros en los que se habla del uso o la venta de medicamentos (legales) o parafernalia médica, alcohol o productos con tabaco. Tenga en cuenta que las drogas ilegales quedan cubiertas en la categoría Drogas.
7	**Formación**	En esta categoría se incluyen aquellos sitios web que pertenecen a instituciones educativas oficiales, incluidos aquellos que no pertenecen al dominio .edu. También incluye los sitios web educativos, como las enciclopedias.
8	**Entretenimiento**	En esta categoría se incluyen aquellos sitios web que proporcionan información relacionada con actividades artísticas y museos, además de sitios web en los que se analiza o puntúa contenido como películas, música o arte.
9	**Uso compartido de archivos**	Esta categoría cubre los sitios web de compartición de archivos,

		donde un usuario puede cargar archivos y compartirlos con otros. También cubre los sitios web para compartir torrents, así como los rastreadores de torrents.
10	**Finanzas**	Esta categoría incluye todos los sitios web propiedad de bancos que proporcionan acceso en línea. También cubre algunas unidades de crédito y otras instituciones financieras. Sin embargo, las entidades bancarias locales podrían no estar cubiertas.
11	**Apuestas**	En esta categoría se incluyen los sitios web de apuestas. Son los del tipo "casino en línea " o "lotería en línea", que normalmente requieren un pago anticipado para que el usuario pueda apostar dinero en juegos de azar en línea como la ruleta, el póquer, el blackjack, etcétera. Algunos son legítimos, lo que significa que existe una posibilidad de ganar: otros son fraudulentos y no existe dicha posibilidad. También detecta los sitios web de "consejos y trucos para apostar", donde se describen modos de ganar dinero con los sitios web de juegos de azar y loterías en línea.
12	**Juegos**	En esta categoría se incluyen los sitios web que ofrecen juegos en línea, normalmente basados en applets Adobe Flash o Java. Para la detección, no importa si el juego es gratuito o si requiere una suscripción, pero los sitios web de estilo casino se integran en la categoría Apuestas. Esta categoría no cubre lo siguiente: • Sitios web oficiales de empresas que desarrollan videojuegos (salvo que produzcan juegos en línea) • Sitios web donde se conversa sobre juegos • Sitios web donde se pueden descargar juegos que no son en línea (algunos de los cuales se cubren en la categoría Ilegal) • Juegos que requieren que el usuario descargue y ejecute un archivo ejecutable, como World of Warcraft; es posible prevenirlos de distintas formas, como un cortafuegos
13	**Gobierno**	En esta categoría se incluyen los sitios web del Gobierno, incluidas las instituciones oficiales, las embajadas y los ministerios.
14	**Hackeo**	En esta categoría se incluyen los sitios web que proporcionan herramientas de hackeo, artículos y plataformas de discusión para los hackers. También cubre los sitios web que ofrecen "exploits" para plataformas comunes que facilitan el hackeo de cuentas de Facebook o Gmail.
15	**Actividades ilegales**	Esta categoría es amplia e incluye todo lo relacionado con el odio, la violencia y el racismo, y está pensada para bloquear las

		siguientes categorías de sitio web: • Sitios web pertenecientes a organizaciones terroristas • Sitios web con contenido racista o xenófobo • Sitios web donde se habla de deportes violentos, o que promueven la violencia
16	**Salud y bienestar**	En esta categoría se incluyen aquellos sitios web que están asociados a instituciones médicas, sitios web relacionados con la prevención de enfermedades y su tratamiento, y sitios web que ofrecen información o productos para perder peso, dietas, esteroides, anabolizantes y productos para estimular la hormona del crecimiento, así como aquellos sitios web que proporcionan información sobre cirugía plástica.
17	**Aficiones**	En esta categoría se incluyen aquellos sitios web que ofrecen recursos sobre actividades normalmente de ocio, como el coleccionismo, las manualidades y el ciclismo.
18	**Alojamiento web**	En esta categoría se incluyen los sitios web gratuitos y comerciales que alojan servicios con los que los usuarios y las organizaciones privadas pueden crear únicas páginas web.
19	**Descargas ilegales**	En esta categoría se incluyen los sitios web relacionados con la piratería de software, como los siguientes: • Sitios web de rastreadores P2P (BitTorrent, emule, DC++) conocidos por ayudar a distribuir contenido con derechos de autor sin el consentimiento de los poseedores de estos derechos • Sitios web y tableros de discusión de warez (software comercial pirateado) • Sitios web que proporcionan a los usuarios cracks, generadores de claves y números de serie para facilitar el uso ilegal del software Algunos de estos sitios web también pueden detectarse como pornografía o alcohol/tabaco, ya que a menudo utilizan publicidad de esta clase para obtener ingresos.
20	**Mensajería instantánea**	En esta categoría se incluyen los sitios web para chatear y de mensajería instantánea con los que los usuarios pueden hablar en tiempo real. También detecta yahoo.com y gmail.com, pues ambos contienen un servicio integrado de mensajería instantánea.
21	**Empleo**	En esta categoría se incluyen los sitios web que ofrecen bolsas de empleo, anuncios clasificados relacionados con el empleo y oportunidades de trabajo, además de agregadores de esos servicios. No cubre las agencias de reclutamiento ni las páginas

		de "empleos" en los sitios web oficiales de las empresas.
22	**Contenido para adultos**	En esta categoría se incluye el contenido que el creador de un sitio web ha etiquetado como dirigido a un público adulto. Cubre una amplia gama de sitios web, desde el libro Kama Sutra y las páginas de educación sexual hasta la pornografía más explícita.
23	**Drogas**	En esta categoría se incluyen los sitios web en los que se comparte información sobre drogas ilegales y recreativas. Esta categoría también cubre los sitios web sobre el desarrollo y cultivo de drogas.
24	**Noticias**	En esta categoría se incluyen los sitios web que ofrecen noticias en vídeo y texto. Intenta cubrir los sitios web de noticias tanto globales como locales, aunque algunos sitios web locales de pequeño tamaño pueden no quedar incluidos.
25	**Citas en línea**	En esta categoría se incluyen los sitios web de citas en línea, de pago y gratuitos, en los que los usuarios pueden buscar a otras personas según ciertos criterios. También pueden publicar sus perfiles para permitir que otras personas los busquen. Este categoría incluye los sitios web de citas tanto de pago como gratuitos. Como la mayoría de las redes sociales populares pueden utilizarse como sitios de citas en línea, determinados sitios populares, como Facebook, también se detectan dentro de esta categoría. Le recomendamos que utilice esta categoría con la categoría Redes sociales.
26	**Pagos en línea**	En esta categoría se incluyen los sitios web que ofrecen pagos o transferencias de dinero en línea. Detecta sitios web de pago populares como PayPal o Moneybookers. También detecta de forma heurística las páginas web que, en sitios de otra naturaleza, solicitan información de tarjetas de crédito, lo que permite detectar tiendas en línea ocultas, desconocidas o ilegales.
27	**Uso compartido de fotos**	En esta categoría se incluyen los sitios web para compartir fotos cuyo objetivo principal es que los usuarios suban y compartan imágenes.
28	**Tiendas en línea**	En esta categoría se incluyen las tiendas en línea conocidas. Un sitio web se considera una tienda en línea si vende en línea bienes o servicios.
29	**Pornografía**	En esta categoría se incluyen los sitios web en los que hay contenido erótico y pornografía. Incluye tanto los sitios gratuitos como los de pago. Cubre los sitios web que ofrecen imágenes,

		historias y vídeos, y también detecta contenido pornográfico en sitios web con contenidos mixtos.
30	**Portales**	En esta categoría se incluyen los sitios web que reúnen información de varios recursos y dominios, y que normalmente ofrecen funciones como motores de búsqueda, correo electrónico, noticias e información sobre entretenimiento.
31	**Radio**	En esta categoría se incluyen los sitios web que ofrecen servicios de reproducción de música en Internet, desde emisoras de radio en línea hasta sitios web que proporcionan contenido de audio bajo demanda, ya sea de pago o gratuito.
32	**Religión**	En esta categoría se incluyen los sitios web que promueven la religión o las sectas religiosas. También cubre los foros de discusión relacionados con una o más religiones.
33	**Motores de búsqueda**	En esta categoría se incluyen los sitios web de motores de búsqueda, como Google, Yahoo y Bing.
34	**Redes sociales**	En esta categoría se incluyen los sitios web de redes sociales, como MySpace.com, Facebook.com, Bebo.com, etc. Sin embargo, las redes sociales especializadas, como YouTube.com, se encuadran en la categoría Vídeo/Foto.
35	**Deportes**	En esta categoría se incluyen los sitios web que ofrecen información, noticias y tutoriales deportivos.
36	**Suicidio**	En esta categoría se incluyen los sitios web que promueven, ofrecen o defienden el suicidio. No cubre las clínicas de prevención del suicidio.
37	**Prensa amarilla**	Esta categoría se ha diseñado principalmente para los sitios web de porno suave y cotilleo sobre famosos. Muchos sitios web de noticias sensacionalistas pueden tener subcategorías aquí integradas. La detección de esta categoría también se basa en un mecanismo heurístico.
38	**Pérdida de tiempo**	En esta categoría se incluyen aquellos sitios web en los que las personas suelen pasar mucho tiempo. Pueden incluirse sitios web de otras categorías, como las redes sociales o el entretenimiento.
39	**Viajes**	En esta categoría se incluyen aquellos sitios web que ofrecen ofertas de viajes y equipamiento para viajar, además de reseñas y puntuaciones sobre destinos de viajes.
40	**Vídeos**	En esta categoría se incluyen aquellos sitios web en los que se alojan vídeos o fotos, ya sean subidos por los usuarios u ofrecidos por distintos proveedores de contenidos. Se incluyen sitios web como YouTube, Metacafe o Google Video, y sitios de

		fotos como Picasa o Flickr. También detecta vídeos incrustados en otros sitios web o blogs.
41	**Dibujos animados violentos**	En esta categoría se incluyen aquellos sitios web en los que se habla, se comparten y se proporcionan dibujos animados violentos o manga que pueden ser inapropiados para menores por su violencia, lenguaje explícito o contenido sexual. Esta categoría no cubre los sitios web que ofrecen dibujos animados generalistas como "Tom y Jerry".
42	**Armas**	En esta categoría se incluyen los sitios web de venta, intercambio, fabricación o uso de armas. También cubre los recursos de caza y el uso de armas BB y de aire comprimido, así como las armas cuerpo a cuerpo.
43	**Correo electrónico**	En esta categoría se incluyen aquellos sitios web que proporcionan funcionalidades de correo electrónico en forma de aplicación web.
44	**Proxy web**	En esta categoría se incluyen aquellos sitios web que ofrecen servicios de proxy web. Se trata de sitios web del tipo “navegador dentro de un navegador” en los que el usuario abre una página web, introduce la URL solicitada en un formulario y hace clic en “Enviar”. A continuación, el sitio de proxy web descarga la página y la muestra dentro del navegador del usuario. Estas son las razones por las que se detectan estos sitios (y por las que podría ser necesario bloquearlos): • Para navegar de forma anónima. Como las solicitudes al servidor web de destino se realizan desde el servidor web del proxy, solo la dirección IP de dicho servidor es visible. Si el administrador del servidor de destino rastrea al usuario, el rastro termina en el proxy web, que puede o no mantener registros que permitan localizar al usuario original. • Para falsificar la ubicación. La dirección IP de los usuarios se utiliza a menudo para segmentar los servicios según la ubicación de origen (algunos sitios gubernamentales solo están disponibles desde direcciones IP locales); el uso de estos servicios puede ayudar al usuario a camuflar su auténtica ubicación. • Para acceder a contenido prohibido. Si se utiliza un simple filtro de URL, solo se verán las URL del proxy web y no los servidores reales que el usuario visita. • Para evitar la supervisión de las empresas. Una directiva de empresa puede requerir que se supervise el uso que los empleados hacen de Internet. Como se accede a todo el contenido a través de un proxy web, un usuario podría evadir

		esta supervisión, que no obtendrá información correcta. Como el SDK analiza la página HTML (si se proporciona) y no solo las URL, en algunas categorías, el SDK podrá seguir detectando el contenido. Sin embargo, con el simple uso del SDK no pueden evitarse algunas de las razones.

Exclusiones de URL

Las direcciones URL que se sabe que son seguras se pueden añadir a la lista de dominios de confianza. Las direcciones URL que suponen una amenaza se pueden añadir a la lista de dominios bloqueadas.

Pasos para especificar las URL que siempre serán de confianza o bloqueadas

1. En el módulo filtrado de URL de un plan de protección, haga clic en **Exclusiones de URL**.
   Se mostrará la ventana **Exclusiones de URL**.
   Se mostrarán las siguientes opciones:

Elementos de confianza: haga clic en **Añadir** para seleccionar entre las opciones disponibles:

- **Dominio**: si selecciona esta opción, se abrirá la ventana **Añadir dominio**.
  - En el campo **Dominio**, escriba cada dominio en una nueva línea. En el campo **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos de confianza.
- **Procesos**: si selecciona esta opción, se mostrará la ventana **Añadir proceso**.
  - En el campo **Proceso**, escriba la ruta de cada proceso en una nueva línea. En la sección **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos de confianza.

Elementos bloqueados: haga clic en **Añadir**. Se mostrará la ventana **Añadir dominio**.

En el campo **Dominio**, escriba cada dominio en una nueva línea. En el campo **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos bloqueados.

Nota
Se admiten rutas de red local. Por ejemplo, \\localhost\folderpath\file.exe.

Descripción

Puede usar el campo **Descripción** para introducir notas sobre las exclusiones añadidas en la lista de exclusiones de URL. A continuación, puede ver algunas sugerencias de notas que puede añadir:

- Motivo y objetivo de la exclusión.
- La fecha y la hora.

Si se añaden varios elementos en una única entrada, solo podrá haber 1 comentario para todos los elementos.

Antivirus Microsoft Defender y Microsoft Security Essentials

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Antivirus Microsoft Defender

El antivirus Microsoft Defender es un componente antimalware integrado de Microsoft Windows que se empezó a ofrecer en Windows 8.

Con el módulo Antivirus Microsoft Defender (WDA), puede configurar la directiva de seguridad del antivirus Microsoft Defender y realizar un seguimiento de su estado a través de la consola de Cyber Protect.

Este módulo se aplica a cargas de trabajo en las que esté instalado el Antivirus de Microsoft Defender.

Microsoft Security Essentials

Microsoft Security Essentials es un componente antimalware integrado de Microsoft Windows que se empezó a ofrecer con Windows en versiones anteriores a la 8.

Con el módulo Antivirus Microsoft Security Essentials, puede configurar la directiva de seguridad de Microsoft Security Essentials y realizar un seguimiento de su estado a través de la consola de Cyber Protect.

Este módulo se aplica a cargas de trabajo en las que esté instalado Microsoft Security Essentials.

La configuración de Microsoft Security Essentials es similar a la del antivirus Microsoft Defender, pero no puede configurar la protección en tiempo real ni definir las exclusiones con la consola de Cyber Protect.

Planificar análisis

Especifique la planificación para el análisis planificado.

Modo de análisis:

- **Full**: comprobación completa de todos los archivos y las carpetas, además de los elementos analizados en el análisis rápido. Para su ejecución se necesitan más recursos del equipo que los empleados para el análisis rápido.
- **Rápido**: comprobación rápida de los procesos y las carpetas de la memoria en los que se suele encontrar malware. Para su ejecución, se requieren menos recursos del equipo.

Defina el día de la semana y la hora en que se llevará a cabo el análisis.

Análisis rápido diario: sirve para definir el momento en que tendrá lugar el análisis diario rápido.

Puede establecer las siguientes opciones en función de sus necesidades:

Iniciar el análisis planificado cuando el equipo está encendido, pero no en uso

Buscar las definiciones de virus y software espía más recientes antes de ejecutar un análisis planificado

Limitar el uso de la CPU durante el análisis a

Para obtener más información sobre la configuración del antivirus Microsoft Defender, consulte https://docs.microsoft.com/es-es/mem/configmgr/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings

Acciones predeterminadas

Defina las acciones predeterminadas que se van a llevar a cabo para las amenazas detectadas con distintos niveles de gravedad:

- **Limpiar**: limpiar el malware detectado en una carga de trabajo.
- **Cuarentena**: poner en cuarentena el malware detectado en la carpeta Cuarentena, pero no eliminarlo.
- **Eliminar**: eliminar el malware detectado de una carga de trabajo.
- **Permitir**: no eliminar ni poner en cuarentena el malware detectado.
- **Definido por el usuario**: se pedirá a un usuario que especifique la acción que se va llevar a cabo con el malware detectado.
- **Sin acción**: no se llevará a cabo ninguna acción.
- **Bloquear**: bloquear el malware detectado.

Para obtener más información sobre la configuración de las acciones por defecto del antivirus Microsoft Defender, consulte https://docs.microsoft.com/es-es/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings

Protección en tiempo real

Habilite la **Protección en tiempo real** para detectar malware e impedir que se instale o se ejecute en las cargas de trabajo.

Analizar todas las descargas: si esta opción está seleccionada, se analizan todos los adjuntos y archivos descargados.

Habilitar supervisión del comportamiento: si esta opción está seleccionada, se habilitará la supervisión del comportamiento.

Analizar archivos de red: si esta opción está seleccionada, se analizarán los archivos de red.

Permitir análisis completo de los dispositivos de red asignados: si esta opción está seleccionada, se analizarán por completo los dispositivos de red asignados.

Permitir análisis del correo electrónico: si esta opción está habilitada, el motor analizará los archivos del correo y de los buzones de correo en función de su formato específico con el fin de analizar los archivos adjuntos y el cuerpo de los correos.

Para obtener más información sobre la configuración de la protección en tiempo real del antivirus Microsoft Defender, consulte https://docs.microsoft.com/es-es/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings

Avanzado

Especifique la configuración de análisis avanzado:

- **Analizar archivos del archivo comprimido**: incluye archivos comprimidos como archivos .zip o .rar en el análisis.
- **Analizar unidades extraíbles**: analiza unidades extraíbles durante los análisis completos.
- **Crear un punto de restauración del sistema**: hay ocasiones en las que una entrada de registro o un archivo importante se elimina como "falso positivo". Con esta opción podrá restaurar el sistema desde un punto de recuperación.
- **Eliminar archivos en cuarentena después de**: define el periodo tras el que se eliminarán los archivos que están puestos en cuarentena.
- **Enviar muestras de archivos automáticamente cuando se requiere un análisis más detallado:**
  - **Indicar siempre**: se le pedirá su confirmación antes de enviar un archivo.
  - **Enviar muestras seguras automáticamente**: se enviarán automáticamente la mayoría de las muestras, excepto los archivos que puedan contener información personal. Esos archivos requerirán una confirmación adicional.
  - **Enviar todas las muestras automáticamente**: se enviarán todas las muestras automáticamente.
- **Deshabilitar interfaz del antivirus Windows Defender**: si se selecciona esta opción, no estará disponible la interfaz de usuario del antivirus Windows defender para un usuario. Puede gestionar las directivas del antivirus Windows Defender a través de la consola de Cyber Protect.
- **MAPS (Microsoft Active Protection Service)**: comunidad en línea que la ayuda a decidir cómo responder a posibles amenazas.
  - **No quiero unirme a MAPS**: no se enviará ninguna información a Microsoft sobre el software que se haya detectado.
  - **Afiliación básica**: se enviará información básica a Microsoft sobre el software que se haya detectado.
  - **Afiliación avanzada**: se enviará información más detallada a Microsoft sobre el software que se haya detectado.

  Para obtener más información, consulte https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/ (en inglés).

Para obtener más información sobre la configuración avanzada del antivirus Microsoft Defender, consulte https://docs.microsoft.com/es-es/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings

Exclusiones

Puede definir que se excluyan del análisis los siguientes archivos y carpetas:

- **Procesos**: cuando añade un proceso, cualquier archivo en que el proceso lea o escriba quedará excluido del análisis. Tiene que definir una ruta completa al archivo ejecutable del proceso.
- **Archivos y carpetas**: los archivos y las carpetas especificados excederán del análisis. Tiene que definir una ruta completa a una carpeta o un archivo, o bien definir la extensión del archivo.

Para obtener más información sobre la configuración de exclusiones del antivirus Microsoft Defender, consulte https://docs.microsoft.com/es-es/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings

Gestión de firewall

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La gestión de firewall le permite ajustar fácilmente la configuración del firewall en las cargas de trabajo protegidas.

Esta funcionalidad en Cyber Protect se proporciona a través de un componente integrado del Firewall de Microsoft Defender de Microsoft Windows. El Firewall de Microsoft Defender bloquea el tráfico de red no autorizado que entra o sale en las cargas de trabajo.

Esta gestión de firewall se aplica a cargas de trabajo en las que esté instalado el Firewall de Microsoft Defender.

Sistemas operativos Windows compatibles

Los siguientes sistemas operativos Windows son compatibles para la gestión de firewall:

Windows

- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server no es compatible.

Habilitar y deshabilitar la gestión de firewall

Puede habilitar la gestión de firewall al crear un plan de protección. Puede cambiar un plan de protección existente para habilitar o deshabilitar la gestión de firewall.

Pasos para habilitar o deshabilitar la gestión de firewall

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Realice uno de los siguientes procedimientos para abrir el panel del plan de protección:
   - Si va a crear un nuevo plan de protección, seleccione un equipo para proteger, haga clic en **Proteger** y, a continuación, haga clic en **Crear plan**.
   - Si va a cambiar un plan de protección existente, seleccione un equipo protegido, haga clic en **Proteger**, haga clic en el icono de puntos suspensivos (...) junto al nombre del plan de protección y, a continuación, haga clic en **Editar**.
3. En el panel del plan de protección, vaya al área de **gestión de firewall** y habilite o deshabilite la **gestión de firewall**.
4. Realice uno de los siguientes procedimientos para aplicar los cambios:
   - Para crear un plan de protección, haga clic en **Crear**.
   - Para editar un plan de protección, haga clic en **Guardar**.

El **estado del firewall de Microsoft Defender** en el área de **gestión de firewall** del panel del plan de protección aparece como **activado** o **desactivado**, en función de si ha habilitado o deshabilitado la gestión de firewall.

También puede acceder al plan de protección desde la pestaña Administración. Sin embargo, esta opción no está disponible en todas las ediciones del servicio Cyber Protection.

Cuarentena

`Cuarentena` es una carpeta especial y aislada en el disco duro de un dispositivo protegido. Si la protección antivirus y antimalware detecta algún archivo sospechoso, se mueve a esta carpeta para evitar la propagación de amenazas.

En la pestaña **Cuarentena** de la consola Cyber Protection puede revisar los archivos sospechosos y potencialmente peligrosos de todos los dispositivos protegidos y decidir si eliminarlos o restaurarlos.

Nota
Los archivos que estén en cuarentena se borran automáticamente si el dispositivo se ha eliminado del entorno.

¿Cómo llegan los archivos a la carpeta de cuarentena?

1. En el plan de protección, seleccione **Cuarentena** como la acción predeterminada para los archivos infectados o sospechosos.
   Para obtener más información sobre cómo crear un plan de protección, consulte "Creación de un plan de protección" (p. 230).
2. Mientras se realiza el análisis, el módulo de protección antivirus y antimalware detecta los archivos malintencionados y los mueve a la carpeta segura de `Cuarentena`.
3. El módulo actualiza la lista de cuarentena para añadir información sobre los archivos que se movieron a esta carpeta de cuarentena.

Nota
Los archivos se borran automáticamente de la carpeta `Cuarentena` cuando pasa el periodo de tiempo definido en el parámetro **Eliminar archivos en cuarentena después de** del plan de protección. Consulte "Configuración de cuarentena" (p. 908).

Gestión de los archivos que están en cuarentena

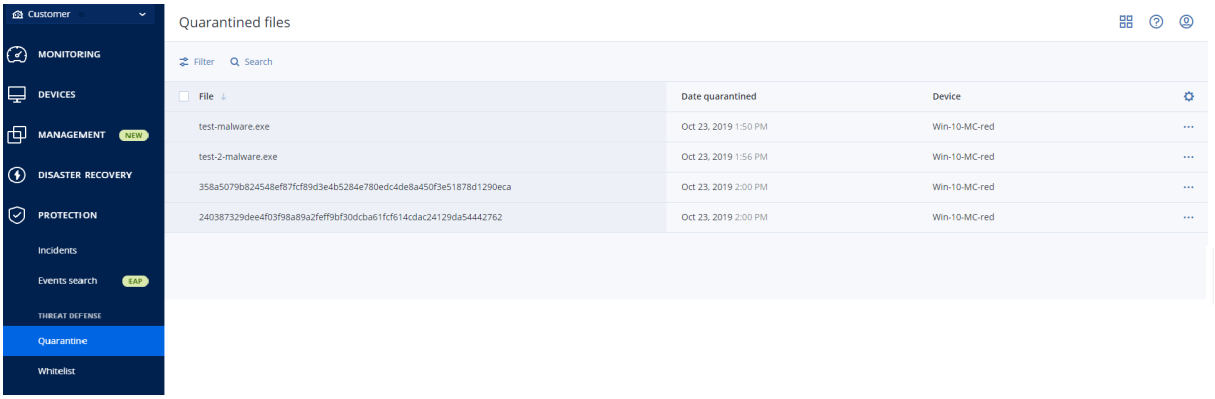
Para gestionar los archivos en cuarentena, vaya a **Protección** > **Cuarentena**. La lista de archivos en cuarentena de todos los dispositivos protegidos contiene la siguiente información.

Nombre	Descripción
Archivo	El nombre del archivo en cuarentena.
Fecha de puesta en cuarentena	Fecha y hora en que el archivo se puso en cuarentena.
Dispositivo	Dispositivo en que se encuentra el archivo infectado.
Nombre de la amenaza	El nombre de la amenaza.
Plan de protección	El plan de protección según el cual el archivo sospechoso se puso en cuarentena.

Puede llevar a cabo las siguientes acciones en los archivos en cuarentena:

- **Eliminar**: Eliminar permanentemente un archivo en cuarentena de todos los equipos. Puede eliminar todos los archivos con el mismo hash de archivo. Puede restaurar todos los archivos con el mismo hash de archivo. Agrupe los archivos por hash, seleccione los que necesite y después, elimínelos.
- **Restaurar**: Restaurar un archivo en cuarentena a su ubicación original sin ninguna modificación. Si ya hay un archivo con el mismo nombre en la ubicación original, se sobrescribirá con el archivo restaurado.

Nota
El archivo restaurado se añadirá a la lista de permitidos y se omitirá cuando se realicen otros análisis antimalware.



Ubicación de la carpeta Cuarentena en los equipos

A continuación, se muestra una lista de ubicaciones predeterminadas para los archivos en cuarentena por sistema operativo.

- Para equipos Windows: `%programdata%\Acronis\NGMP\quarantine`
- Para equipos Mac: `/Library/Application Support/Acronis/NGMP/quarantine`
- Para equipos Linux: `/var/lib/Acronis/NGMP/quarantine`

El almacenamiento para poner los archivos en cuarentena se encuentra en la protección de autodefensa del proveedor de servicios.

Carpeta personalizada de autoservicio bajo demanda

Puede seleccionar carpetas personalizadas de la carga de trabajo y analizarlas directamente desde el menú contextual.

Para acceder a la opción Análisis con Cyber Protect de menú contextual

Para las cargas de trabajo con protección antivirus y antimalware habilitada en el plan de protección, haga clic con el botón derecho en la carpeta o carpetas en las que quiera realizar el análisis.

Nota
Esta opción solo está disponible para los administradores de la carga de trabajo.

Lista blanca corporativa

Alguna solución antivirus podría identificar aplicaciones específicas corporativas legítimas como sospechosas. Para evitar esos falsos positivos, las aplicaciones de confianza se añaden de forma

manual a la lista blanca, y eso supone perder bastante tiempo.

Nota
La lista blanca corporativa no afecta a los análisis antimalware de las copias de seguridad.

Cyber Protection puede automatizar este proceso: el módulo de protección antivirus y antimalware analiza las copias de seguridad y los datos, de modo que dichas aplicaciones pasan a la lista blanca, por lo que se evitan las detecciones de falsos positivos. Además, la lista blanca de toda la empresa mejora el rendimiento del análisis antimalware.

La lista blanca se crea para cada cliente basándose en sus datos.

La lista blanca se puede activar y desactivar. Cuando está desactivada, sus archivos añadidos se ocultan temporalmente.

Nota
Solo las cuentas con rol de administrador (por ejemplo, administrador de Cyber Protection; administrador de la empresa; administrador de un partner que opera en nombre del administrador de una empresa; administrador de la unidad) pueden configurar y gestionar la lista blanca. Esta función no está disponible para una cuenta de administrador de solo lectura ni para una cuenta de usuario.

Inclusión automática de aplicaciones en la lista blanca

1. Ejecutar un análisis en la nube de las copias de seguridad en al menos dos equipos. Para hacerlo, utilice los planes de análisis de copia de seguridad.
2. En la configuración de las listas blancas, habilite el conmutador **Generación automática de listas blancas**.

Inclusión manual de aplicaciones en la lista blanca

Cuando el conmutador **Generación automática de listas blancas** esté deshabilitado, podrá añadir archivos a la lista blanca de forma manual.

1. En la consola de Cyber Protect, vaya a **Protección Antimalware** > **Lista blanca**.
2. Haga clic en **Añadir archivo**.
3. Especifique la ruta del archivo y haga clic en **Añadir**.

Añadir archivos en cuarentena a la lista blanca

Puede añadir archivos en cuarentena a la lista blanca.

1. En la consola de Cyber Protect, vaya a **Protección Antimalware** > **Cuarentena**.
2. Seleccione un archivo en cuarentena y haga clic en **Añadir a la lista blanca**.

Configuración de la lista blanca

Cuando habilite el conmutador **Generación automática de listas blancas**, debe especificar uno de los siguientes niveles de protección heurística:

- **Bajo**
  Las aplicaciones empresariales se añadirán a la lista blanca solo después de un tiempo significativo y varias comprobaciones. Tales aplicaciones ofrecen mayor confianza. Sin embargo, este enfoque aumenta la posibilidad de que se detecten falsos positivos. Los criterios para considerar que un archivo está limpio y es de confianza son muy elevados.
- **Predeterminado**
  : las aplicaciones empresariales se añadirán a la lista blanca en función del nivel de protección recomendado para reducir la detección de posibles falsos positivos. Los criterios para considerar que un archivo está limpio y es de confianza son intermedios.
- **Alto**
  : las aplicaciones empresariales se añadirán a la lista blanca más rápido para reducir la detección de posibles falsos positivos. Sin embargo, así no se garantiza que el software esté limpio y más adelante podría reconocerse como sospechoso o malware. Los criterios para considerar que un archivo está limpio y es de confianza son bajos.

Visualización de detalles sobre elementos de la lista blanca

Puede hacer clic en un elemento para ver más información sobre este y analizarlo en línea.

Si tiene dudas sobre un elemento que añadió, puede comprobarlo en el analizador de VirusTotal. Al hacer clic en **Comprobar en VirusTotal**, el sitio analiza archivos y URL sospechosos para detectar tipos de malware mediante el hash del archivo del elemento que añadió. Puede ver el hash en la cadena **Hash del archivo (MD5)**.

El valor **Equipos** representa el número de equipos en los que se ha encontrado ese hash durante el análisis de copias de seguridad. Este valor se completa solo si un elemento proviene del análisis de copias de seguridad o de la cuarentena. El campo se queda vacío si se ha añadido el archivo manualmente a la lista blanca.