Dell Threat Defense

Guía de instalación y del administrador

Con la tecnología de Cylance

v17.11.06

06-11-2017

Contenido

DESCRIPCIÓN GENERAL 6
Funcionamiento 6
Acerca de esta guía 6
CONSOLA 7
Inicio de sesión 7
Política de dispositivo 7
Acciones de archivo 7
Configuración de protección 8
Registros de agentes 10
Prácticas recomendadas sobre políticas 10
Zonas 11
Propiedades de zona 12
Regla de zona 12
Lista de dispositivos de zonas 14
Prácticas recomendadas de administración de zonas 15
Administración de usuarios 16
Red relacionada 17
Servidor de seguridad 17
Proxy 18
Dispositivos 18
Administración de dispositivos 18
Amenazas y actividades 19
Dispositivos duplicados 20
Actualización del agente 21
Panel 22
Protección: amenazas 23
Tipo de archivo 23
Puntuación de Cylance 24
Visualización de la información de amenazas 24
Solución de amenazas 26
Solución de amenazas en un dispositivo específico 27
Solución de amenazas globalmente 27
Protección: control de la secuencia de comandos 27
Lista global 28

Lista segura por certificado ... 29
Perfil ... 30
Mi cuenta ... 30
Registro de auditoría ... 30
Configuración ... 31
APLICACIÓN ... 31
Threat Defense Agent ... 31
Agente de Windows ... 31
Requisitos del sistema ... 31
Instalación del agente: Windows ... 32
Parámetros de instalación de Windows ... 32
Instalación del agente de Windows mediante Wyse Device Manager (WDM) ... 33
Cuarentena mediante la línea de comandos ... 35
Desinstalación del agente ... 36
Agente macOS ... 37
Requisitos del sistema ... 37
Instalación del agente: macOS ... 37
Parámetros de instalación de macOS ... 38
Instalación del agente ... 39
Desinstalación del agente ... 39
Servicio de agente ... 40
Menú Agente ... 41
Habilitación de las opciones avanzadas de la interfaz de usuario del agente ... 41
Máquinas virtuales ... 42
Deinstalación protegida por contraseña ... 42
Para crear una contraseña de desinstalación ... 43
Integraciones ... 43
Syslog/SIEM ... 43
Autenticación personalizada ... 45
Informe de datos de amenazas ... 45
SOLUCIÓN DE PROBLEMAS ... 46
Compatibilidad ... 46
Parámetros de instalación ... 46
Problemas de rendimiento ... 46
Problemas de actualización, estado y conectividad ... 47
Cómo habilitar el registro de depuración ... 47

Incompatibilidades de control de la secuencia de comandos 47
APÉNDICE A: GLOSARIO 48
APÉNDICE B: ADMINISTRACIÓN DE EXCEPCIONES 49
Archivos 49
Secuencias de comandos 49
Certificados 49
APÉNDICE C: PERMISOS DE USUARIO 49
APÉNDICE D: FILTRO DE ESCRITURA BASADO EN ARCHIVOS 51

DESCRIPCIÓN GENERAL

Dell Threat Defense, con tecnología de Cylance, detecta y bloquea malware antes de que afecte a un dispositivo. Cylance utiliza un enfoque matemático para la identificación de malware, mediante técnicas de aprendizaje automático en lugar de firmas reactivas, sistemas de confianza o espacios aislados. Este enfoque convierte el nuevo malware, los virus, bots y variantes futuras en inútiles. Threat Defense analiza ejecuciones de archivo con potencial malware en el sistema operativo.

Esta guía explica el uso de la consola Threat Defense, la instalación de Threat Defense Agent y la forma de configurar ambos.

Funcionamiento

Threat Defense se compone de un pequeño agente, instalado en cada host, que se comunica con la consola basada en la nube. El agente detecta e impide el malware en el host utilizando modelos matemáticos probados, no requiere conectividad continua de la nube ni actualizaciones continuas de firma, y funciona en redes abiertas y aisladas. A medida que evoluciona el panorama de amenazas, lo hace Threat Defense. Formándose constantemente en enormes conjuntos de datos del mundo real, Threat Defense permanece un paso por delante de los atacantes.

- **Amenaza**: cuando una amenaza se descarga en el dispositivo o existe un intento de explotación.
- **Detección de amenazas**: cómo identifica Threat Defense Agent las amenazas.
    - **Escaneado de procesos**: escanea procesos que se ejecutan en el dispositivo.
    - **Control de ejecución:** solo analiza procesos en ejecución. Esto incluye todos los archivos que se ejecutan al inicio, que están establecidos para su ejecución automática y que el usuario ejecuta de forma manual.
- **Análisis**: cómo se identifican los archivos como maliciosos o seguros.
    - **Búsqueda de puntuaciones de amenazas en la nube**: el modelo matemático de la nube que se utiliza para puntuar archivos.
    - **Local**: el modelo matemático incluido con el agente. Permite el análisis cuando el dispositivo no está conectado a Internet.
- **Acción**: lo que el agente hace al identificarse un archivo como amenaza.
    - **Global**: comprueba la configuración de políticas, incluida la *cuarentena global* y las *listas seguras*.
    - **Local**: comprueba manualmente la existencia de archivos *en cuarentena* o *exentos*.

Acerca de esta guía

Dell recomienda que los usuarios se familiaricen con la consola basada en la nube antes de instalar el agente en los extremos. Entender la forma en que se administran los extremos facilita la protección y el mantenimiento de los mismos. Este flujo de trabajo es una recomendación. Los usuarios pueden enfocar la implementación en sus entornos de la forma que tenga sentido para ellos.

Ejemplo: las zonas ayudan a agrupar dispositivos de la organización. Por ejemplo, configure una zona con una regla de zona que automáticamente agregue nuevos dispositivos a una zona en función de criterios seleccionados (como, por ejemplo, sistema operativo, nombre de dispositivo o nombre de dominio).

Nota: Las instrucciones para instalar el agente vienen tras obtener información sobre políticas y zonas. Los usuarios pueden empezar con la instalación del agente, si fuera necesario.

CONSOLA

La consola de Threat Defense es un sitio web en el que se inicia sesión para ver la información sobre amenazas de la organización. La consola facilita la organización de los dispositivos en grupos (zonas), la configuración de las acciones que tomar al detectar amenazas en un dispositivo (política), y la descarga de los archivos de instalación (agente).

La consola de Threat Defense es compatible con los siguientes idiomas.

Francés	Alemán	Italiano	Japonés
Portugués (Portugal)	Coreano	Español	Portugués (Brasil)

Tabla 1: Idiomas compatibles con la consola de Threat Defense

Inicio de sesión

Tras activar su cuenta, recibirá un correo electrónico con su información de inicio de sesión para la consola de Threat Defense. Haga clic en el enlace del correo electrónico para ir a la página de inicio de sesión o ir a:

- América del Norte: http://dellthreatdefense.com
- Europa: http://dellthreatdefense-eu.cylance.com

Política de dispositivo

Una política define cómo el agente administra el malware que detecta. Por ejemplo, ponga el malware automáticamente *en cuarentena* o ignórelo si se encuentra en una carpeta específica. Todos los dispositivos deben estar en una política y solo se puede aplicar una política a un dispositivo. Al restringir un dispositivo a una única política se eliminan las características en conflicto (como, por ejemplo, el bloqueo de un archivo cuando debiera estar permitido para dicho dispositivo). El dispositivo se coloca en la política predeterminada si no se asigna ninguna política.

Solo se habilita el Control de ejecución para la política predeterminada, que analiza procesos solo cuando se ejecutan. De esta manera se proporciona protección básica al dispositivo, no se interrumpen las operaciones en el dispositivo y se proporciona tiempo para probar las características de la política antes de implementar la política en el entorno de producción.

Para agregar una política

1. Inicie sesión en la consola (http://dellthreatdefense.com) como administrador. Solo los administradores pueden crear políticas.
2. Seleccione **Configuración > Política de dispositivos**.
3. Haga clic en **Agregar nueva política**.
4. Escriba un nombre de política y seleccione las opciones de políticas.
5. Haga clic en **Crear**.

Acciones de archivo

CONFIGURACIÓN > Política de dispositivo > [seleccione una política] > Acciones de archivos

Acciones de archivo ofrece diferentes opciones para procesar los archivos detectados por Threat Defense como *no seguros* o *a*nómalos.

Consejo: Para obtener más información sobre la clasificación de archivos *no seguros* o anómalos, consulte la sección Protección: amenazas.

Cuarentena automática con control de ejecución

Esta función pone *en cuarentena* o bloquea el archivo *no seguro* o a*nómalo*, e impide que se ejecute. Al poner un archivo *en cuarentena*, se traslada de su ubicación original al directorio de *cuarentena* **`C:\ProgramData\Cylance\Desktop\q`**.

Cierto malware está diseñado para colocar otros archivos en determinados directorios. Este malware sigue intentándolo hasta que el archivo se coloca con éxito. Threat Defense modifica el archivo colocado para que no se ejecute y hacer que este tipo de malware deje de colocar continuamente el archivo eliminado.

Consejo: Dell recomienda encarecidamente que se pruebe la función de *cuarentena automática* en un número reducido de dispositivos antes de aplicarla al entorno de producción. Los resultados de la prueba deben observarse para garantizar que no se bloqueen aplicaciones críticas para el negocio durante la ejecución.

Carga automática

Dell recomienda que los usuarios activen la carga automática para los archivos tanto *no seguros* como *anómalos*. Threat Defense carga automáticamente cualquier archivo *no seguro* o a*nómalo* detectado a la nube Cylance Infinity para realizar un análisis más profundo del archivo y proporcionar detalles adicionales.

Threat Defense solo carga y analiza archivos Portable Executable (ejecutables portátiles, PE) desconocidos. Si el mismo archivo desconocido se detecta en varios dispositivos de la organización, Threat Defense carga un archivo solo para el análisis, no un archivo por dispositivo.

Lista segura de políticas

Agregue archivos que se consideren seguros, a nivel de política. El agente no aplicará las acciones de amenazas a los archivos de esta lista.

Para obtener más información acerca de la administración de excepciones de archivos (*en cuarentena* o *seguros*), en los diferentes niveles (*Local, Política o Global*), consulte Apéndice B: administración de excepciones.

1. Inicie sesión en la consola (http://dellthreatdefense.com) como administrador. Solo los administradores pueden crear políticas.
2. Seleccione **Configuración > Política de dispositivos**.
3. Agregue una política nueva o edite una existente.
4. Haga clic en **Agregar archivo** en *Lista segura de p*olíticas.
5. Introduzca la información del **SHA256**. Opcionalmente, incluya el MD5 y el nombre de archivo, si los conoce.
6. Seleccione una **categoría** para ayudar a identificar lo que hace este archivo.
7. Introduzca un motivo para agregar este archivo a la *lista segura de políticas*.
8. Haga clic en **Enviar**.

Configuración de protección

`CONFIGURACIÓN > Política de dispositivo > [seleccione una política] > Configuración de protección`

Control de ejecución

Threat Defense siempre vigila la ejecución de procesos maliciosos y alerta cuando se intenta ejecutar cualquier archivo *no seguro* o a*nómalo.*

Evitar la interrupción del servicio desde el dispositivo

Si se selecciona, el servicio Threat Defense está protegido contra el apagado tanto de forma manual como mediante otro proceso.

Copiar muestras de malware

Permite especificar un recurso compartido de red en el que copiar muestras de malware. De este modo, los usuarios pueden realizar su propio análisis de los archivos que Threat Defense considere *no seguros* o *a*nómalos.

- Admite recursos compartidos de red CIFS/SMB.
- Especifique una ubicación del recurso compartido de red. Ejemplo: `c:\test`.
- Todos los archivos que reúnen los criterios se copian en el recurso compartido de red, incluidos los duplicados. No se realiza ninguna prueba de unicidad.
- Los archivos no están comprimidos.
- Los archivos no están protegidos mediante contraseña.

AVISO: LOS ARCHIVOS NO ESTÁN PROTEGIDOS MEDIANTE CONTRASEÑA. SE DEBE TENER CUIDADO DE NO EJECUTAR DE FORMA ACCIDENTAL EL ARCHIVO MALICIOSO.

Control de la secuencia de comandos

El control de la secuencia de comandos protege a los dispositivos bloqueando la ejecución de secuencias de comandos maliciosas de Active Script y PowerShell.

1. Inicie sesión en la consola (http://dellthreatdefense.com).
2. Seleccione **Configuración > Política de dispositivos**.
3. Seleccione una política y haga clic en **Configuración de protección**.
4. Marque la casilla de verificación para habilitar el **Control de la secuencia de comandos**.
    a. **Alerta**: supervise las secuencias de comandos que se ejecutan en el entorno. Recomendado para la implementación inicial.
    b. **Bloquear:** solo permite que se ejecuten secuencias de comandos desde carpetas específicas. Utilícese después de probar en modo de alerta.
    c. **Aprobar los scripts en estas carpetas (y subcarpetas)**: las exclusiones de carpetas de secuencias de comandos deben especificar la ruta de acceso relativa de la carpeta.
    d. **Bloquear el uso de la consola PowerShell**: bloquea la consola de PowerShell para que no se inicie. Esta acción ofrece seguridad adicional frente al uso de la entrada de una línea de PowerShell.

    Nota: Si la secuencia inicia la consola PowerShell y el control de la secuencia de comandos está configurado para bloquear la consola PowerShell, el script fallará. Se recomienda que los usuarios cambien sus secuencias de comandos para invocar las secuencias de comandos de PowerShell, no la consola de PowerShell.
5. Haga clic en **Guardar**.

Registros de agentes

CONFIGURACIÓN > Política de dispositivo > [seleccione una política] > Registros del agente

Habilite Registros del agente en la consola para cargar los archivos de registro y permitir la visualización en la consola.

1. Inicie sesión en la consola (http://dellthreatdefense.com).
2. Seleccione **Configuración > Política de dispositivos**.
3. Seleccione una política y haga clic en **Registros del agente**. Asegúrese de que el dispositivo seleccionado para los archivos de registro se asigne a esta política.
4. Seleccione **Habilitar carga automática de archivos de registro** y, a continuación, haga clic en **Guardar**.
5. Haga clic en la pestaña **Dispositivos** y seleccione un dispositivo.
6. Haga clic en **Registros del agente**. Aparecen los archivos de registro.
7. Haga clic en un archivo de registro. El nombre del archivo de registro es la fecha del registro.

Prácticas recomendadas sobre políticas

Cuando se crean políticas por primera vez, Dell recomienda implementar características de políticas mediante un enfoque por fases para garantizar que el rendimiento y las operaciones no se vean afectados. Cree nuevas políticas con más características habilitadas como la comprensión de cómo funciona Threat Defense en el entorno.

1. Al crear las políticas iniciales, active solamente **Carga automática**.
    a. El agente utiliza el control de ejecución y el supervisor de procesos para analizar únicamente procesos en ejecución.

       Esto incluye todos los archivos que se ejecutan al inicio, que están establecidos para su ejecución automática y que el usuario ejecuta de forma manual.

       El agente solo envía alertas a la consola. Ningún archivo está bloqueado o *en cuarentena*.

    b. Compruebe en la consola si hay alertas de amenazas.

       El objetivo es encontrar aplicaciones o procesos que deban ejecutarse en el extremo y se consideren una amenaza (*anómalos* o *no seguros*).

       Configurar una política o establecer una configuración de la consola para *permitir* que estos se ejecuten cuando se dé el caso (por ejemplo, *excluir* carpetas en una política, *eximir* los archivos para ese dispositivo o agregar los archivos a la *lista segura*).

    c. Utilice esta política inicial durante un día para permitir que las aplicaciones y los procesos que se utilizan normalmente en el dispositivo se ejecuten y se analicen.

IMPORTANTE: Puede que haya aplicaciones y procesos que se ejecuten periódicamente en un dispositivo (por ejemplo, una vez al mes) que se consideren una amenaza. Le corresponde al usuario decidir si desea ejecutarlos durante esta política inicial o recordar supervisar el dispositivo cuando se ejecuten según lo programado.

2. En Configuración de protección, habilite **Eliminar los procesos en ejecución no seguros**, una vez se haya completado el control de ejecución y la supervisión de procesos.

   Eliminar procesos en ejecución no seguros y sus subprocesos elimina los procesos (y subprocesos), con independencia del estado, cuando se detecta una amenaza (EXE o MSI).

3. En Acciones de archivo, active la **Cuarentena automática**.

   La *cuarentena automática* traslada todos los archivos malintencionados a la carpeta de *cuarentena*.

4. En Configuración de protección, active **Control de la secuencia de comandos**.

   Control de la secuencia de comandos protege a los usuarios de las secuencias de comandos maliciosas que se ejecutan en su dispositivo.

   Los usuarios pueden aprobar la ejecución de secuencias de comandos para carpetas específicas.

   La carpeta Control de la secuencia de comandos debe especificar una ruta de acceso relativa para la carpeta (por ejemplo, **`\Cases\ScriptsAllowed`**).

Zonas

Una zona es la forma de organizar y administrar dispositivos. Por ejemplo, los dispositivos pueden dividirse en función de su geografía o función. Si hay un grupo de dispositivos críticos, se pueden agrupar juntos y asignarse una alta prioridad a la zona. Además, las políticas se aplican en el nivel Zona, así que los dispositivos se pueden agrupar en una zona en función de la política aplicada a dichos dispositivos.

Una organización tiene una zona predeterminada (Fuera de zona) a la que solo pueden acceder los administradores. Los nuevos dispositivos se asignan a Fuera de zona, a menos que existan reglas de zona que automáticamente asignen los dispositivos a zonas.

Se pueden asignar administradores y usuarios de zonas a las zonas, permitiéndoles ver cómo está configurada esa zona. Esto también permite a los administradores y usuarios de zonas acceder a los dispositivos de los que son responsables. Debe crearse al menos una zona que permite a cualquiera con un rol de usuario o administrador de zona verla.

Un dispositivo puede pertenecer a varias zonas, pero solo puede aplicarse una política a un dispositivo. Permitir varias zonas ofrece cierta flexibilidad a la manera de agrupar dispositivos. Al restringir un dispositivo a una única política, se eliminan las características en conflicto (como, por ejemplo, el bloqueo de un archivo cuando debiera estar *permitido* para dicho dispositivo).

Podría haber dispositivos existentes en varias zonas por las siguientes razones:

- El dispositivo se ha agregado manualmente a varias zonas
- El dispositivo cumple con las reglas de más de una zona
- El dispositivo ya reside en una zona y cumple así con las reglas de otra zona

Consulte las prácticas recomendadas en la utilización de zonas, en Prácticas recomendadas de administración de zonas.

Para agregar una zona

1. Inicie sesión en la consola (http://dellthreatdefense.com) como administrador. Solo los administradores pueden crear zonas.
2. Haga clic en **Zonas**.
3. Haga clic en **Agregar nueva zona**.
4. Escriba un nombre de zona, seleccione una política y seleccione un valor. Una zona debe tener una política asociada. El valor es la prioridad para la zona.
5. Haga clic en **Guardar**.

Para agregar dispositivos a una zona

1. Inicie sesión en la consola (http://dellthreatdefense.com) con una cuenta de administrador o administrador de zonas.
2. Haga clic en **Zonas**.
3. Haga clic en una zona de la *Lista de zonas*. Los dispositivos actuales de esa zona se muestran en la *Lista de dispositivos de zonas* en la parte inferior de la página.
4. Haga clic en **Agregar dispositivos a una zona** Aparecerá una lista de dispositivos.
5. Seleccione cada dispositivo que desea agregar a la zona y haga clic en **Guardar**. También puede seleccionar **Aplicar política de zona a los dispositivos seleccionados**. Al agregar un dispositivo a una zona no se aplica automáticamente la política de zona porque una zona puede estar siendo utilizada para organizar dispositivos, y no para administrar la política de dichos dispositivos.

Para eliminar una zona

1. Inicie sesión en la consola (http://dellthreatdefense.com) como administrador. Solo los administradores pueden eliminar zonas.
2. Haga clic en **Zonas**.
3. Marque las casillas de verificación para las zonas que desea eliminar.
4. Haga clic en **Quitar**.
5. Haga clic en **Sí** en el mensaje de confirmación de eliminación de la zona seleccionada.

Propiedades de zona

Las propiedades de zona se pueden editar según sea necesario.

Acerca de la prioridad de zona

A las zonas se les pueden asignar diferentes niveles de prioridad (baja, normal o alta) que clasifiquen la importancia o criticalidad de los dispositivos de dicha zona. En las diversas áreas del panel, los dispositivos se distribuyen por prioridad para ayudar a identificar qué dispositivos necesitan atención inmediata.

La prioridad se puede establecer al crear una zona o editar la zona para cambiar el valor de prioridad.

Para editar las propiedades de zona

1. Inicie sesión en la consola (http://dellthreatdefense.com) como administrador o administrador de zonas.
2. Haga clic en **Zonas**.
3. Haga clic en una zona de la *Lista de zonas*.
4. Introduzca un nuevo nombre en el campo **Nombre** para cambiar el nombre de zona.
5. Seleccione una opción diferente en el menú desplegable **Política** para cambiar la política.
6. Seleccione un valor **bajo**, **normal** o **alto**.
7. Haga clic en **Guardar**.

Regla de zona

Los dispositivos se pueden asignar automáticamente a una zona en función de determinados criterios. Esta automatización es ventajosa cuando se trata de agregar numerosos dispositivos a las zonas. Cuando se agregan nuevos dispositivos que coinciden con una regla de zona, tales dispositivos se asignan automáticamente a esa zona. Si la opción **Aplicar ahora a todos los dispositivos existentes** está seleccionada, todos los dispositivos existentes que coincidan con la regla se agregarán a esa zona.

Nota: Las reglas de zona agregan automáticamente dispositivos a una zona pero no pueden eliminarlos. Si cambia la dirección IP o el nombre de host del dispositivo, el dispositivo no se eliminará de una zona. Los dispositivos deben eliminarse manualmente de una zona.

No existe ninguna opción para aplicar la política de zona a dispositivos agregados a la zona como resultado de la coincidencia con la regla de zona. Esto significa que la política existente del dispositivo se reemplaza por la política de zona especificada. La aplicación automática de una política en función de la regla de zona debe utilizarse con precaución. Si no se administra correctamente, podría asignarse un dispositivo a una política errónea porque el dispositivo coincidiese con una regla de zona.

Vea la página Detalles del dispositivo en la consola para ver qué política se aplica a un dispositivo.

Para agregar una regla de zona

1. Inicie sesión en la consola (http://dellthreatdefense.com) como administrador o administrador de zonas.
2. Haga clic en **Zonas** y seleccione una zona de la *Lista de zonas*.
3. Haga clic en **Crear regla** en Regla de zona.
4. Especifique los criterios para la zona seleccionada. Haga clic en el signo más para agregar más condiciones. Haga clic en el signo menos para eliminar una condición.
5. Haga clic en **Guardar**.

Criterios de reglas de zona

- **Cuando se agrega un nuevo dispositivo a la organización**: cualquier nuevo dispositivo agregado a la organización que coincida con la regla de zona se agrega a la zona.
- **Cuando cambia algún atributo de un dispositivo**: cuando cambian atributos de un dispositivo existente y luego coinciden con la regla de zona, el dispositivo existente se agrega a la zona.
- **Dirección IPv4 en el rango**: introduzca un rango de direcciones IPv4.
- **Nombre del dispositivo**:
    - Empieza por: los nombres de dispositivo deben empezar así.
    - Contiene: los nombres de dispositivo deben contener esta cadena, pero puede estar en cualquier lugar del nombre.
    - Finaliza por: los nombres de dispositivo deben finalizar así.
- **Sistema operativo**:
    - Es: el sistema operativo debe ser el sistema seleccionado.
    - No es: el sistema operativo no debe ser el sistema seleccionado. Por ejemplo, si la única regla de zona indica que el sistema operativo no debe ser Windows 8, entonces todos los sistemas operativos, incluidos los de dispositivos no Windows, se agregarán a esta zona.
- **Nombre de dominio**:
    - Empieza por: el nombre de dominio debe empezar así.
    - Contiene: el nombre de dominio debe contener esta cadena, pero puede estar en cualquier lugar del nombre.
    - Finaliza por: el nombre de dominio debe finalizar así.

- **Nombre distintivo**:
    - Empieza por: el nombre distintivo debe empezar así.
    - Contiene: el nombre distintivo debe contener esta cadena, pero puede estar en cualquier lugar del nombre.
    - Finaliza por: el nombre distintivo debe finalizar así.
- **Miembro de (LDAP)**:
    - Es: el miembro de (grupo) debe coincidir con esto.
    - Contiene: el miembro de (grupo) debe contener esto.
- **Se cumplen las siguientes condiciones**:
    - Todas: todas las condiciones de la regla de zona deben coincidir para agregar el dispositivo.
    - Cualquiera: al menos una regla de zona debe coincidir para agregar el dispositivo.
- **Aplicación de la política de zona**:
    - No aplicar: no aplicar la política de zona a medida que se agregan dispositivos a la zona.
    - Aplicar: aplicar la política de zona a medida que se agregan dispositivos a la zona.

      Aviso: La aplicación automática de la política de zona puede afectar de forma negativa a algunos dispositivos de la red. Aplique automáticamente la Política de zona *solo* si está seguro de que la Regla de zona *solo* busca los dispositivos que *deben* tener esta Política de zona específica.
- **Aplicar ahora a todos los dispositivos existentes**: aplica la regla de zona a todos los dispositivos de la organización. Esto no se aplica a la política de zona.

Acerca de nombres distinguidos (DN)

Algunas cosas que deben saberse sobre los nombres distinguidos (DN) al utilizarlos en reglas de zona.

- No se permiten comodines, pero la condición "Contiene" permite lograr resultados parecidos.
- Los errores y las excepciones de DN relacionadas con el agente se capturan en los archivos de registro.
- Si el agente encuentra información de DN en el dispositivo, esa información se envía automáticamente a la consola.
- Al agregar información de DN, debe estar correctamente formateada, de la siguiente forma.
    - Ejemplo: CN=JDoe,OU=Sales,DC=dell,DC=COM
    - Ejemplo: OU=Demo,OU=SEngineering,OU=Sales

Lista de dispositivos de zonas

La *Lista de dispositivos de zonas* muestra todos los dispositivos asignados a esta zona. Los dispositivos pueden pertenecer a varias zonas. Utilice **Exportar** para descargar un archivo CSV con información relacionada con todos los dispositivos de la *Lista de dispositivos* de zonas.

Nota: Si no existe permiso para ver una zona, y sin embargo se hace clic en el enlace Zona de la columna Zonas, aparecerá una página Recurso no encontrado.

Prácticas recomendadas de administración de zonas

La mejor manera de enfocar las zonas es como etiquetas donde cualquier dispositivo puede pertenecer a varias zonas (o tener varias etiquetas). Aunque no existen restricciones en el número de zonas que se pueden crear, las prácticas recomendadas identifican tres pertenencias a zona diferentes entre pruebas, política y granularidad de rol de usuario dentro de la organización.

Estas tres zonas se componen de:

- Administración de actualizaciones
- Administración de políticas
- Administración del acceso basado en roles

Organización de zonas para la administración de actualizaciones

Un uso común de las zonas es ayudar a administrar las actualizaciones del agente. Threat Defense admite la última versión del agente y la versión anterior. Esto permite a las empresas admitir períodos de congelación de cambios, y realizar pruebas rigurosas de las nuevas versiones del agente.

Existen tres tipos de zona sugeridas que se utilizan para dirigir y especificar las fases de prueba y producción del agente:

- **Actualizar zona: grupo de pruebas.** Estas zonas deben tener dispositivos de prueba que representen correctamente los dispositivos (y el software utilizado en estos dispositivos) de la organización. Esto permite probar el agente más reciente y garantiza que su implementación en los dispositivos de producción no interfiera con los procesos empresariales.
- **Actualizar zona: grupo piloto.** Esta zona se puede utilizar como zona de prueba secundaria o como zona de producción secundaria. Como zona de prueba secundaria, esto permitiría probar nuevos agentes en un grupo más grande de dispositivos antes de implementar en producción. Como zona de producción secundaria, esto permitiría dos versiones de agente diferentes, pero entonces debe administrar dos zonas de producción diferentes.
- **Actualizar zona**: **producción.** La mayoría de los dispositivos deben estar en zonas asignadas a producción.

Nota: Para actualizar el agente a la zona de producción, consulte Actualización del agente.

Agregar una zona de prueba o piloto

1. Inicie sesión en la consola (http://dellthreatdefense.com) con una cuenta de administrador o administrador de zonas.
2. Seleccione **Configuración > Actualización del agente**.
3. Para zonas de prueba o piloto:
    a. Haga clic en **Seleccionar zonas de prueba** o **Seleccionar zonas piloto**.
    b. Haga clic en una zona.

    Si la zona de producción está configurada en **Actualización automática**, las zonas de prueba y piloto no estarán disponibles. Cambie la actualización automática de la zona de producción a cualquier otra para habilitar las zonas de prueba o piloto.
4. Haga clic en **Seleccionar la versión**.
5. Seleccione una versión del agente que aplicar a la zona de prueba o piloto.
6. Haga clic en **Aplicar**.

Organización de zonas para la administración de políticas

Otro conjunto de zonas que crear ayuda a aplicar diferentes políticas a distintos tipos de extremos. Tenga en cuenta los siguientes ejemplos:

- Zona de política – Estaciones de trabajo
- Zona de política – Estaciones de trabajo – Exclusiones
- Zona de política – Servidores
- Zona de política – Servidores – Exclusiones
- Zona de política – Ejecutivos – Protección alta

Dell sugiere aplicar una política de forma predeterminada a todos los dispositivos de esta zona de política en cada una de estas zonas. Tenga cuidado de no colocar un dispositivo en varias zonas de política, ya que puede crear un conflicto sobre qué política se aplica. Recuerde también que el motor de reglas de zona puede ayudar a organizar automáticamente estos hosts en función de la IP, el nombre de host, el sistema operativo y el dominio.

Organización de zonas para la administración del acceso basado en roles

El acceso basado en roles se utiliza para limitar el acceso del usuario de la consola a un subconjunto de dispositivos de cuya administración son responsables. Esto podría incluir separación por rango IP, nombres de host, sistema operativo o dominio. Plantéese agrupaciones por ubicación geográfica, tipo o ambas cosas.

Ejemplo:

- Zona RBAC – Escritorios – Europa
- Zona RBAC – Servidores – Asia
- Zona RBAC – Alfombra roja (Ejecutivos)

Utilizando los ejemplos anteriores, podría asignarse un administrador de zonas a Zona *RBAC - Equipos de sobremesa - Europa*, y solo tendría acceso a los dispositivos de esa zona. Si el usuario del administrador de zonas ha intentado ver las otras zonas, se recibiría un mensaje de error indicando que no tiene permiso para verlas. Aunque un dispositivo pueda estar en varias zonas, y el administrador de zonas pueda ver dicho dispositivo, si ha intentado ver las otras zonas con las que el dispositivo está asociado, no podría, y vería el mensaje de error.

En otras partes de la consola, como el panel, el administrador de zonas para la *Zona RBAC - Equipos de sobremesa - Europa*, estaría limitado también a las amenazas y otra información relacionada con la zona o el dispositivo asignado a esa zona.

Las mismas restricciones se aplican a usuarios asignados a una zona.

Administración de usuarios

Los administradores tienen permisos globales y pueden agregar o eliminar usuarios, asignar usuarios a zonas (como usuario o administrador de zonas), agregar o eliminar dispositivos, crear políticas y crear zonas. Los administradores también pueden eliminar usuarios, dispositivos, políticas y zonas de forma permanente de la consola.

Los usuarios y administradores de zonas solo tienen acceso y privilegios relacionados con la zona que se les asigna. Esto se aplica a los dispositivos asignados a la zona, a las amenazas detectadas en dichos dispositivos, y a la información del panel.

Para obtener una lista completa de los permisos que posee cada usuario, consulte Apéndice C: permisos de usuario.

Para agregar usuarios

1. Inicie sesión en la consola (http://dellthreatdefense.com) como administrador. Solo los administradores pueden crear usuarios.
2. Seleccione **Configuración > Administración de usuarios**.
3. Introduzca la dirección de correo electrónico del usuario.
4. Seleccione un rol en el menú desplegable Rol.
5. Al agregar un administrador de zonas o usuario, seleccione una zona para asignarlo.
6. Haga clic en **Agregar**. Se envía un correo electrónico al usuario con un enlace para crear una contraseña.

Para cambiar roles de usuario

1. Inicie sesión en la consola (http://dellthreatdefense.com) como administrador. Solo los administradores pueden crear usuarios.
2. Seleccione **Configuración > Administración de usuarios**.
3. Haga clic en un usuario. Aparecerá la página Detalles del usuario.
4. Seleccione un rol y haga clic en **Guardar**.

Para eliminar usuarios

1. Inicie sesión en la consola (http://dellthreatdefense.com) como administrador. Solo los administradores pueden crear usuarios.
2. Seleccione **Configuración > Administración de usuarios**.
3. Marque la casilla de verificación para el usuario o los usuarios que desea eliminar.
4. Haga clic en **Quitar**.
5. Haga clic en **Sí** en el mensaje de confirmación de eliminación.

Red relacionada

Configure la red para permitir que Threat Defense Agent se comunique con la consola a través de Internet. Esta sección cubre la configuración del servidor de seguridad y las configuraciones de proxy.

Servidor de seguridad

No es necesario ningún software local para administrar dispositivos. Los Threat Defense Agents se adminsitran mediante la consola e informan a la consola (interfaz de usuario basada en nube). El puerto 443 (HTTPS) se utiliza para la comunicación y debe estar abierto en el servidor de seguridad para que los agentes puedan comunicarse con la consola. La consola se aloja en servicios web de Amazon (AWS) y no tiene ninguna dirección IP fija. Asegúrese de que los agentes puedan comunicarse con los siguientes sitios:

- login.cylance.com
- data.cylance.com
- my.cylance.com
- update.cylance.com
- api2.cylance.com
- download.cylance.com

Si no, permita el tráfico HTTPS en *.cylance.com.

Proxy

La compatibilidad de proxy para Threat Defense se configura a través de una entrada de registro. Cuando está configurado un proxy, el agente utiliza la dirección IP y el puerto de la entrada de registro para todas las comunicaciones externas a los servidores de la consola.

1. Acceda al registro.

   Nota: Puede que se exijan privilegios elevados o ser responsable del registro, dependiendo de cómo se haya instalado el agente (Modo protegido habilitado o no).

2. En el editor del registro, vaya a **`HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`**.
3. Cree un nuevo valor de cadena (REG_SZ):
   - Nombre del valor = ProxyServer
   - Datos del valor = configuración de proxy (por ejemplo, http://123.45.67.89:8080)

El agente intenta utilizar las credenciales del usuario que actualmente haya iniciado sesión para comunicarse con Internet en entornos autenticados. Si está configurado un servidor proxy autenticado y un usuario no ha iniciado sesión en el dispositivo, el agente no podrá autenticar el proxy y no podrá comunicarse con la consola. En este caso puede:

- Configurar el proxy y agregar una regla para permitir todo el tráfico a *.cylance.com.
- O utilizar una política de proxy diferente, que permita el acceso de proxy no autorizado a los hosts de Cylance (*.cylance.com).

Al hacer esto, si ningún usuario inicia sesión en el dispositivo, el agente no necesitará autenticarse y debería poder conectarse con la nube y comunicarse con la consola.

Dispositivos

Una vez el agente esté instalado en un extremo, estará disponible como dispositivo en la consola. Comience administrando dispositivos mediante la asignación de políticas (para hacer frente a las *amenazas* identificadas) y grupos de dispositivos (utilizando las *Zonas*), y llevando a cabo acciones manualmente en cada dispositivo (*En cuarentena* y *Eximir*).

Administración de dispositivos

Los dispositivos son equipos con un Threat Defense Agent. Administre los dispositivos desde la consola.

1. Inicie sesión en la consola (http://dellthreatdefense.com) como administrador. Solo los administradores pueden administrar dispositivos.
2. Haga clic en **Dispositivos**.
3. Marque una casilla de verificación para permitir las siguientes acciones:
   - **Exportar**: crea y descarga un archivo CSV. El archivo contiene información del dispositivo (nombre, estado y política) de todos los dispositivos de la organización.
   - **Eliminar**: elimina dispositivos seleccionados de la *Lista de dispositivos*. Esta acción no desinstala el agente del dispositivo.
   - **Asignar política**: permite la asignación de los dispositivos seleccionados a una política.
   - **Agregar a zonas**: permite agregar los dispositivos seleccionados a una zona o a zonas.

4. Haga clic en un dispositivo para mostrar la página Detalles de dispositivo.
    - **Información del dispositivo:** muestra información como el nombre de host, la versión del agente y la versión del sistema operativo.
    - **Propiedades del dispositivo:** permite cambiar el nombre de dispositivo, la política, las zonas y el nivel de registro.
    - **Amenazas y actividades:** muestra la información sobre amenazas y otras actividades relacionadas con el dispositivo.
5. Haga clic en **Agregar nuevo dispositivo** para mostrar un cuadro de diálogo con un token de instalación y enlaces para descargar el instalador del agente.
6. En la columna Zonas, haga clic en un nombre de zona para ver la página Detalles de zona.

Amenazas y actividades

Muestra la información sobre amenazas y otras actividades relacionadas con el dispositivo seleccionado.

Amenazas

Muestra todas las amenazas detectadas en el dispositivo. De manera predeterminada, las amenazas se agrupan por estado (*insegura*, *anormal*, *en cuarentena* y *exenta*).

- **Exportar**: crea y descarga un archivo CSV que contiene información para todas las amenazas detectadas en el dispositivo seleccionado. La información sobre amenazas incluye información como el nombre, la ruta de acceso al archivo, la puntuación de Cylance y el estado.
- **En cuarentena**: pone *en cuarentena* las amenazas seleccionadas. Se trata de una *cuarentena local*, lo que significa que esta amenaza solo está *en cuarentena* en este dispositivo. Para poner una *amenaza en cuarentena* en todos los dispositivos de la organización, asegúrese de que la casilla **Además, aislar esta amenaza cada vez que se encuentre en cualquier dispositivo** (*Cuarentena global*) está marcada cuando un archivo se encuentra *en cuarentena*.
- **Eximir**: cambia el estado de las amenazas seleccionadas a *exentas*. Los archivos *exentos* se pueden ejecutar. Se trata de una *exención local*, por lo que este archivo solo se permite en este dispositivo. Para permitir este archivo en todos los dispositivos en la organización, marque la casilla ***Además, marcar como seguro en todos los dispositivos*** (*Lista segura*) al *eximir* un archivo.

Intentos de explotación

Muestra todos los intentos de explotación del dispositivo. Incluye información sobre el nombre de proceso, identificación, tipo y acción realizada.

Registros de agentes

Muestra los archivos de registro cargados por el agente en el dispositivo. El nombre del archivo de registro es la fecha del registro.

Para ver los archivos de registro del agente:

1. Cargue el archivo de registro actual de un único dispositivo.
    a. Haga clic en Dispositivos > Registros del agente.
    b. Haga clic en **Cargar archivo de registro actual**. Esto podría llevarle algunos minutos, dependiendo del tamaño del archivo de registro.

O bien

1. Configuración de la política:
   a. Haga clic en Configuración > Política de dispositivo > [seleccione una política] > Registros del agente.
   b. Haga clic en Habilitar carga automática de archivos de registro.
   c. Haga clic en **Guardar**.

Para ver los registros detallados, cambie el nivel de registro del agente antes de cargar ningún archivo.

1. En la consola: **Dispositivos > [haga clic en un dispositivo]**, seleccione **Detallado** en el menú desplegable Nivel de registro del agente y, a continuación, haga clic en **Guardar**. Una vez cargados los archivos de registro detallados, Dell recomienda volver a cambiar el nivel de registro del agente a *Información*.
2. En el dispositivo, cierre la interfaz de usuario de Threat Defense (haga clic con el botón derecho en el icono de Threat Defense de la bandeja del sistema y, a continuación, en **Salir**).

O bien

1. Abra la línea de comandos como administrador. Introduzca la siguiente línea de comandos y, a continuación, pulse **Intro**.

   ```
   cd C:\Program Files\Cylance\Desktop
   ```

2. Introduzca la siguiente línea de comandos y, a continuación, pulse **Intro**.

   ```
   Dell.ThreatDefense.exe –a
   ```

3. El icono de Threat Defense aparece en la bandeja del sistema. Haga clic con el botón derecho, seleccione **Registro** y, a continuación, haga clic en **Todos** (igual que Detallado en la consola).

O (para macOS)

1. Salga de la interfaz de usuario actualmente en ejecución.
2. Ejecute el siguiente comando desde el terminal.

   ```
   sudo /Applications/Cylance/CylanceUI.app/Contents/MacOS/CylanceUI -a
   ```

3. Haga clic con el botón derecho del mouse en la interfaz de usuario nueva cuando se abra. Seleccione **Registro > Todos**.

Control de la secuencia de comandos

Muestra todas las actividades importantes del Control de la secuencia de comandos, como las secuencias de comandos rechazadas.

Dispositivos duplicados

Cuando Threat Defense Agent se instala por primera vez en un dispositivo, se crea un identificador único que la consola utiliza para identificar y referenciar dicho dispositivo. No obstante, determinados eventos como el uso de una imagen de máquina virtual para crear varios sistemas puede hacer que se genere un segundo identificador para el mismo dispositivo. Seleccione el dispositivo y, a continuación, haga clic en **Eliminar** si se muestra una entrada duplicada en la página Dispositivos de la consola.

Para ayudar en la identificación de tales dispositivos, utilice la característica de ordenación de columnas de la página Dispositivo para ordenar y comparar los dispositivos, normalmente por nombre de dispositivo. De forma alternativa, la *Lista de dispositivos* puede exportarse como un archivo .CSV y, a continuación, visualizarse en Microsoft Excel u otro programa similar con funciones avanzadas de ordenación/organización.

Ejemplo de uso de Microsoft Excel

1. Abra el archivo CSV del dispositivo en Microsoft Excel.
2. Seleccione la columna de nombre de dispositivo.
3. En la pestaña Inicio, seleccione Formateo condicional > Resaltar reglas de celda > Valores duplicados.
4. Asegúrese de que **Duplicado** está seleccionado y, a continuación, seleccione una opción de resaltar.
5. Haga clic en **Aceptar**. Los elementos duplicados se resaltan.

Nota: El comando Eliminar solo elimina el dispositivo de la página Dispositivo. No emite un comando de desinstalación para Threat Defense Agent. El agente debe desintalarse en el extremo.

Actualización del agente

El mantenimiento y la administración de los Threat Defense Agents no comporta complicaciones. Los agentes descargan automáticamente las actualizaciones desde la consola, y la consola la mantiene Cylance.

El agente se pone en contacto con la consola cada 1-2 minutos. La consola informa sobre el estado actual del agente (*en línea* o *sin conexión*, *no seguro* o *protegido*), la versión, el sistema operativo y el estado de amenaza.

Threat Defense lanza actualizaciones del agente mensualmente. Estas actualizaciones pueden incluir revisiones de configuración, nuevos módulos y cambios de programa. Cuando hay disponible una actualización de agente (según lo notifica la consola en Configuración > Actualizaciones del agente), el agente automáticamente descarga y aplica la actualización. Para controlar el tráfico de red durante las actualizaciones del agente, todas las organizaciones están configuradas para albergar un máximo de 1000 actualizaciones de dispositivo simultáneamente. Los usuarios también pueden desactivar la función de actualización automática si lo prefieren.

Nota: El máximo número de dispositivos para la actualización simultánea puede ser modificado por Dell Support.

Actualización basada en zonas

La actualización basada en zonas permite que una organización evalúe un nuevo agente en un subconjunto de dispositivos antes de implementarlo en todo el entorno (producción). Uno o más zonas actuales se pueden agregar temporalmente a una de las dos zonas de prueba (prueba y piloto) que pueden utilizar un agente diferente del de producción.

Para configurar actualizaciones basadas en zonas:

1. Inicie sesión en la consola (http://dellthreatdefense.com) utilizando una cuenta de administrador.
2. Seleccione **Configuración > Actualización del agente**. Aparecen las últimas tres versiones del agente.

   Si la zona de producción está configurada en **Actualización automática**, las zonas de prueba y piloto no estarán disponibles. Cambie la actualización automática de la zona de producción a cualquier otra para habilitar las zonas de prueba o piloto.
3. Seleccione una versión del agente específica en la lista desplegable Producción.
4. Para producción, seleccione también Actualización automática o No actualizar.
   a. La **Actualización automática** permite actualizar automáticamente todos los dispositivos de producción a la versión más reciente de la *Lista de versiones del agente compatibles*.
   b. **No actualizar** prohíbe la actualización del agente en todos los dispositivos de producción.
5. Para la zona de prueba, elija una o más zonas de la lista desplegable Zona y, a continuación, seleccione una versión del agente específica en la lista desplegable de versiones.
6. Si lo desea, repita el paso 5 para la zona piloto.

Nota: Cuando se agrega un dispositivo a una zona que forma parte de la zona de prueba o piloto, el dispositivo comienza a utilizar la versión del agente de la zona de prueba o piloto. Si un dispositivo pertenece a más de una zona y una de esas zonas pertenece a la zona de prueba o piloto, la versión del agente de la zona de prueba o piloto tiene precedencia.

Para desencadenar una actualización de agente

Para desencadenar una actualización de agente antes del siguiente intervalo de horas:

1. Haga clic con el botón derecho en el icono de Threat Defense Agent de la bandeja del sistema, y seleccione **Buscar actualizaciones**.
2. Reinicie el servicio de Threat Defense. Esto lo fuerza a comunicarse de inmediato con la consola.

O bien

- Las actualizaciones se pueden iniciar desde la línea de comandos. Ejecute el siguiente comando desde el directorio de Cylance:

  ```
  Dell.ThreatDefense.exe – update
  ```

Panel

La página Panel aparece una vez registrado en la consola de Threat Defense. El panel ofrece una descripción general de las amenazas del entorno y proporciona acceso a diferente información de la consola desde una página.

Estadísticas de amenazas

Las estadísticas de amenazas proporcionan el número de amenazas encontradas en la organización en las *Últimas 24 horas* y en *Total*. Haga clic en una *Estadística de amenazas* para ir a la página Protección y mostrar la lista de amenazas relacionadas con esa estadística.

- **Amenazas en ejecución**: archivos identificados como amenazas que se ejecutan actualmente en dispositivos de la organización.
- **Amenazas de ejecución automática**: amenazas configuradas para ejecutarse de forma automática.
- **Amenazas en cuarentena**: amenazas puestas *en cuarentena* en las últimas 24 horas y en total.
- **Exclusivas de Cylance**: amenazas identificadas por Cylance pero no por otros antivirus.

Porcentajes de protección

Muestra porcentajes para Threat Protection y Protección de dispositivos.

- **Protección frente a amenazas**: el porcentaje de amenazas con las que se ha realizado una acción (Cuarentena, Cuarentena global, Exentas y Listas seguras).
- **Protección del dispositivo**: el porcentaje de dispositivos asociados con una política que tiene habilitada la cuarentena automática.

Amenazas por prioridad

Muestra el número total de amenazas que requieren una acción (*En cuarentena*, *Cuarentena global*, *Eximir* y *Listas seguras*). Las amenazas se agrupan por prioridad (alta, media y baja). Este descripción general muestra el número total de amenazas que requieren una acción, divide dicho total por prioridad, ofrece un total de porcentajes y a cuántos dispositivos afecta.

Las amenazas aparecen por prioridad en la esquina inferior izquierda de la página Panel. Se especifica el número total de amenazas de una organización agrupadas por sus clasificaciones de prioridad.

Se clasifica una amenaza como de nivel Bajo, Medio o Alto según cuántos de los siguientes atributos presente:

- El archivo tiene una puntuación de Cylance superior a 80.
- El archivo se está ejecutando.
- El archivo se ha ejecutado anteriormente.
- El archivo está establecido en ejecución automática.
- La prioridad de la zona donde se ha encontrado la amenaza.

Esta clasificación ayuda a los administradores a determinar qué amenazas y dispositivos abordar primero. Haga clic en la amenaza o en Número de dispositivo para ver la amenaza y Detalles del dispositivo.

Eventos de amenazas

Muestra un gráfico de líneas con el número de amenazas descubiertas en los últimos 30 días. Las líneas están codificados por color para distinguir entre archivos *no seguro*s, *anómalos*, *en cuarentena*, *exentos* y *borrados*.

- Pase el puntero del mouse sobre un punto del gráfico para ver los detalles.
- Haga clic en los colores de la leyenda para ver o ocultar dicha línea.

Clasificaciones de amenazas

Muestra un mapa de calor de los tipos de amenazas detectadas en la organización, como por ejemplo, virus o malware. Haga clic en un elemento del mapa de calor para ir a la página Protección y mostrar una lista de amenazas de dicho tipo.

Listas de cinco principales

Muestra listas de las cinco amenazas principales detectadas en la mayoría de los dispositivos, los cinco dispositivos principales con la mayoría de amenazas y las cinco zonas principales con la mayoría de amenazas en la organización. Haga clic en un elemento de la lista para obtener más detalles.

Las primeras cinco listas del panel resaltan las amenazas *no seguras* en la organización para las que no se ha emprendido ninguna acción, como *En cuarentena* o *Exentas*. La mayoría de las veces estas listas deberían estar vacías. Aunque las amenazas *anómalas* también requieren una acción, las cinco listas principales pretenden llamar su atención sobre las amenazas críticas.

Protección: amenazas

Threat Defense puede hacer más que simplemente clasificar los archivos como *no seguros* o *anómalo*s. Puede ofrecer detalles sobre las características estáticas y dinámicas de los archivos. Permite a los administradores no solo bloquear amenazas, sino también comprender su comportamiento para mitigarlas o responder mejor a estas.

Tipo de archivo

No seguro: archivo con una puntuación que va de 60 a 100. Un archivo *no seguro* es aquel en el que el motor de Threat Defense encuentra atributos que presentan un gran parecido con el malware.

Anómalo: archivo con una puntuación que va de 1 a 59. Un archivo anómalo tiene algunos atributos de malware pero menos que un archivo *no seguro*, por lo que es menos probable que sea malware.

Nota: Ocasionalmente, un archivo puede clasificarse como *no seguro* o *anómalo*, aunque la puntuación que se muestra no coincida con el intervalo para la clasificación. Esto podría deberse a nuevos hallazgos o más análisis de archivos después de la detección inicial. En cuanto a análisis más actualizados, habilite Carga automática en la política de dispositivos.

Puntuación de Cylance

Se asigna una puntuación de Cylance a cada archivo considerado *anómalo* o *no seguro*. La puntuación representa el nivel de confianza para considerar el archivo como malware. Cuanto mayor sea el número, mayor será la confianza.

Visualización de la información de amenazas

La pestaña Protección de la consola muestra información detallada sobre amenazas, los dispositivos en los que se han detectado las amenazas y las acciones realizadas en dichos dispositivos para esas amenazas.

Nota: La *Lista de amenazas* en la pestaña Protección dispone de columnas que se pueden configurar. Haga clic en la flecha hacia abajo de cualquier columna para acceder al menú y, a continuación, mostrar/ocultar los diversos detalles de las amenazas. El menú incluye un submenú de filtrado.

Para ver los detalles de las amenazas

1. Inicie sesión en la consola (http://dellthreatdefense.com).
2. Haga clic en la pestaña **Protección** para ver una lista de las amenazas de la organización.
3. Utilice el filtro de la barra del menú de la izquierda para filtrar por prioridad (alta, media y baja) y estado (*En cuarentena*, *Exentas*, *No seguras* o *Anómalas*).

   Nota: Los números que aparecen en rojo en el panel izquierdo indican amenazas destacadas que no están *en cuarentena* ni *exentas*. Filtre dichos elementos para ver una lista de los archivos que deben examinarse.
4. Para agregar columnas y que se pueda ver información adicional sobre amenazas, haga clic en la fecha hacia abajo situada junto a uno de los nombres de columna y seleccione un nombre de columna.
5. Para ver información adicional sobre una amenaza específica, haga clic en el enlace de nombre de amenaza (los detalles aparecen en una nueva página) o haga clic en cualquier sitio de la fila de la amenaza (los detalles aparecen en la parte inferior de la página). Ambas vistas muestran el mismo contenido pero tienen distintos estilos de presentación. Entre los detalles se incluyen una descripción general de los metadatos del archivo, una lista de dispositivos con la amenaza e informes de evidencias.
   a. Metadatos de archivos
      - Clasificación [asignada por el equipo Advanced Threat and Alert Management (Administración avanzada de amenazas y alertas, ATAM) de Cylance]
      - Puntuación de Cylance (nivel de confianza)
      - Convicción de la industria AV (enlaces a VirusTotal.com para su comparación con otros proveedores)
      - Encontrado por primera vez, Encontrado por última vez
      - SHA256
      - MD5
      - Información de archivo (autor, descripción, versión, etc.)
      - Detalles de firma

b. Dispositivos

La *Lista de dispositivos/zonas* para una amenaza puede filtrarse por estado de amenaza (*No segura*, *En cuarentena*, *Exenta*, *Anómala*). Haga clic en los enlaces de filtro del estado para que se muestren los dispositivos con la amenaza en ese estado.

- *No seguro*: el archivo se ha clasificado como *no seguro* pero no se ha realizado ninguna acción.
- *En cuarentena*: el archivo ya se encontraba *en cuarentena* debido a una configuración de la política.
- *Exento*: el administrador *eximió* el archivo o lo incluyó en una *lista blanca*.
- *Anómalo*: el archivo se ha clasificado como *an*ómalo pero no se ha realizado ninguna acción.

c. Informes de evidencia

- **Indicadores de amenazas**: observaciones sobre un archivo que el motor de Cylance Infinity ha analizado. Estos indicadores ayudan a comprender el motivo de la clasificación de un archivo y ofrecen datos del comportamiento y los atributos de un archivo. Los indicadores de amenazas se agrupan en categorías que ayudan en el contexto.
- **Datos detallados de la amenaza:** datos detallados de la amenaza proporciona un resumen exhaustivo de las características estáticas y dinámicas de un archivo, incluidos los detalles estructurales del archivo y los metadatos del archivo adicionales, además de comportamientos dinámicos como archivos descartados, claves de registro creadas o modificadas, así como las URL con las que ha intentado establecer comunicación.

Para ver los indicadores de amenazas:

1. Inicie sesión en la consola (http://dellthreatdefense.com).
2. Haga clic en **Protección**, en el menú superior, para ver una lista de amenazas (o haga clic en **Dispositivos** y seleccione un dispositivo).
3. Haga clic en el nombre de alguna amenaza. Aparecerá la página Detalles de amenaza.
4. Haga clic en **Informes de evidencia**.

Categorías de indicadores de amenazas:

Cada categoría representa un área que se ha visto con frecuencia en software malicioso y que se basa en un profundo análisis de más de 100 millones de binarios. El informe Indicadores de amenazas indica cuántas de esas categorías estaban presentes en el archivo.

Anomalías

El archivo tiene elementos que son incoherentes o anómalos de alguna forma. Con frecuencia, son incoherencias en la estructura del archivo.

Recopilación

El archivo muestra evidencias de recopilación de datos. Esto puede incluir la enumeración de configuración del dispositivo o la recopilación de información confidencial.

Pérdida de datos

El archivo muestra evidencias de exfiltración de datos. Esto puede incluir conexiones de red salientes, evidencia de actuar como navegador, u otras comunicaciones de red.

Engaño
El archivo muestra evidencias de intentos de engañar. El engaño puede estar en forma de secciones ocultas, inclusión de código para evitar la detección, o indicaciones de etiquetado incorrecto en metadatos u otras secciones.

Destrucción
El archivo muestra evidencias de capacidades destructivas. La destrucción puede incluir la capacidad de eliminar recursos del dispositivo como archivos y directorios.

Varios
Todos los demás indicadores que no entran en otras categorías.

Nota: Ocasionalmente, las secciones Indicadores de amenazas y Datos detallados de amenazas no tienen resultados o no están disponibles. Esto ocurre cuando el archivo no se ha cargado. El registro de depuración puede proporcionar información acerca de por qué no se ha cargado el archivo.

Solución de amenazas

El tipo de acción que debe llevarse a cabo en algunas amenazas puede depender del usuario asignado a un dispositivo. Las acciones aplicadas a amenazas pueden aplicarse a nivel de dispositivo o a nivel global. A continuación se presentan diferentes acciones que se pueden realizar frente a amenazas o archivos detectados:

- ***En cuarentena***: poner un archivo específico *en cuarentena* para evitar su ejecución en el dispositivo.

  Nota: Puede poner en cuarentena una amenaza mediante la línea de comandos en un dispositivo. Esta se encuentra disponible solo con Windows Agent. Consulte Cuarentena mediante la línea de comandos para obtener más información.

- ***Cuarentena global***: poner un archivo *en cuarentena global* para impedir que el archivo se ejecute en cualquier dispositivo de la organización.

  Nota: Al poner un archivo *en cuarentena*, se traslada de su ubicación original al directorio de *cuarentena* (`C:\ProgramData\Cylance\Desktop\q`).

- ***Eximir***: *eximir* un archivo específico para permitir que se ejecute en un dispositivo concreto.

- ***Seguridad global***: *Lista de Seguridad Global* un archivo para permitir que ese archivo se ejecute en cualquier dispositivo en toda la organización.

  Nota: Ocasionalmente, Threat Defense puede poner *en cuarentena* o informar sobre un archivo seguro (por ejemplo, si las características de ese archivo se parecen en gran medida a las de archivos maliciosos). La *exención* del archivo o su inclusión en la *lista segura global* puede resultar útil en estos casos.

- ***Cargar archivo***: cargue manualmente un archivo en Cylance Infinity para su análisis. Si está habilitada la opción de carga automática, se cargarán automáticamente los nuevos archivos (los que no hayan sido analizados por Cylance) en Cylance Infinity. Si el archivo está en Cylance Infinity, el botón Cargar archivo no estará disponible (inactivo).

- ***Descargar archivo***: descargue un archivo para sus propios fines de prueba. Esta característica debe estar habilitada para la organización. El usuario debe ser administrador. La amenaza debe detectarse con la versión del agente 1320 o superior.

  Nota: El archivo debe estar disponible en Cylance Infinity y los tres hashes (SHA256, SHA1 y MD5) deben coincidir entre Cylance Infinity y el agente. Si no, el botón Descargar archivo no estará disponible.

Solución de amenazas en un dispositivo específico

1. Inicie sesión en la consola (http://dellthreatdefense.com) como administrador o administrador de zonas.
2. Haga clic en la pestaña **Dispositivos**.
3. Busque y seleccione el dispositivo.
4. Si no, puede que esté disponible un enlace al dispositivo en la pestaña Protección si aparece con una amenaza asociada.
5. Todas las amenazas de ese dispositivo aparecerán en la parte inferior de la página. Seleccione poner *En cuarentena* o *Eximir* el archivo de amenaza en ese dispositivo.

Solución de amenazas globalmente

Los archivos agregados a la *Lista en cuarentena global* o *Lista segura global* se encuentran bien *en cuarentena* o bien están *permitidos* en todos los dispositivos de todas las zonas.

1. Inicie sesión en la consola (http://dellthreatdefense.com) como administrador.
2. Haga clic en **Configuración** > **Lista global**.
3. Haga clic en Cuarentena global o Seguro.
4. Haga clic en **Agregar archivo**.
5. Agregue el SHA256 del archivo (necesario), el MD5, el nombre del archivo y el motivo por el que se ha colocado en la *Lista global*.
6. Haga clic en **Enviar**.

Protección: control de la secuencia de comandos

Threat Defense ofrece detalles sobre las secuencias de comandos de Active y PowerShell que se han bloqueado o están bajo alerta. Con Control de la secuencia de comandos habilitado, los resultados aparecen en la pestaña Control de la secuencia de la página Protección. Esta proporciona detalles sobre la secuencia de comandos y los dispositivos afectados.

Para ver los resultados del control de la secuencia de comandos

1. Inicie sesión en la consola (http://dellthreatdefense.com) como administrador.
2. Haga clic en Protección.
3. Haga clic en Control de la secuencia de comandos.
4. Seleccione una secuencia de comandos de la tabla. Esto actualiza la tabla Detalles con una lista de los dispositivos afectados.

Descripciones de columnas de Control de la secuencia de comandos

- **Nombre del archivo**: el nombre de la secuencia de comandos.
- **Intérprete**: la característica de control de la secuencia de comandos que ha identificado la secuencia de comandos.
- **Última encontrada**: la fecha y la hora en la que se ejecutó la secuencia de comandos por última vez.
- **Tipo de unidad**: el tipo de unidad en la que se ha encontrado la secuencia de comandos (ejemplo: unidad de disco duro interna).

- **SHA256**: el hash SHA 256 de la secuencia de comandos.
- **N.º de dispositivos**: el número de dispositivos afectados por esta secuencia de comandos.
- **Alerta**: el número de veces que la secuencia de comandos ha estado bajo alerta. Podría ser varias veces para el mismo dispositivo.
- **Bloquear:** el número de veces que se ha bloqueado la secuencia de comandos. Podría ser varias veces para el mismo dispositivo.

Descripciones de columnas de detalles

- **Nombre del dispositivo**: el nombre del dispositivo afectado por la secuencia de comandos. Haga clic en el nombre de dispositivo para ir a la página Detalles de dispositivo.
- **Estado**: el estado del dispositivo (en línea o fuera de línea).
- **Versión del agente**: el número de versión del agente actualmente instalado en el dispositivo.
- **Ruta de acceso a archivo**: la ruta de acceso de archivo desde la que se ha ejecutado la secuencia de comandos.
- **Cuando**: la fecha y hora en que se ha ejecutado la secuencia de comandos.
- **Nombre de usuario**: el nombre del usuario registrado al ejecutarse la secuencia de comandos.
- **Acción**: la acción realizada en la secuencia de comandos (Alerta o Bloquear).

Lista global

La *Lista global* permite marcar un archivo para ponerlo en *cuarentena* o para *permitir* su ejecución en todos los dispositivos de la organización.

- **Cuarentena global:** todos los agentes de la organización ponen *en cuarentena* cualquier archivo de la *Lista en cuarentena global* detectado en el dispositivo.
- **Seguro:** todos los agentes en la organización *permiten* cualquier archivo de la *Lista segura* detectado en el dispositivo.
- **No asignado:** cualquier amenaza identificada en la organización que no se haya asignado a la *Lista de cuarentena global* o la *Lista segura*.

Cambiar estado de amenaza

Para cambiar un estado de amenaza (*Cuarentena global*, *Segura* o *Sin asignar*):

1. Inicie sesión en la consola (http://dellthreatdefense.com) como administrador.
2. Seleccione **Configuración > Lista global**.
3. Seleccione la lista actual a la que se ha asignado la amenaza. Por ejemplo, haga clic en Sin asignar para cambiar una amenaza no asignada a *Segura* o a *Cuarentena global.*
4. Marque las casillas de verificación de las amenazas que desee cambiar y haga clic en un botón de estado.
    a. Seguro: mueve los archivos a la *Lista segura*.
    b. Cuarentena global: mueve los archivos a la *Lista de cuarentena global.*
    c. Eliminar de la lista: mueve los archivos a la *Lista sin asignar*.

Agregar un archivo

Agregue un archivo a la *Lista de cuarentena global* o la *Lista segura* de forma manual. La información del hash SHA256 para el archivo que se ha agregado es necesaria.

1. Inicie sesión en la consola (http://dellthreatdefense.com) como administrador.
2. Seleccione **Configuración > Lista global**.
3. Seleccione la lista a la que desea agregar el archivo (*Lista de cuarentena global* o *Lista segura*).
4. Haga clic en **Agregar archivo**.
5. Introduzca la información del hash SHA256. Opcionalmente, introduzca la información del nombre de archivo y el MD5.
6. Escriba un motivo para agregar este archivo.
7. Haga clic en **Enviar**.

Lista segura por certificado

Los clientes pueden incluir archivos en la *Lista segura* mediante certificado firmado, que permite la ejecución sin interrupciones de cualquier software personalizado y debidamente firmado.

Nota: Esta característica funciona actualmente únicamente con sistemas operativos Windows.

- Esta función permite a los clientes establecer una *Lista blanca/Lista segura* mediante certificado firmado, que se identifica por la huella digital SHA1 del certificado.
- La información de certificado la extrae la consola (Sellado de tiempo, Asunto, Emisor y Huella digital). El certificado no se ha cargado o guardado en la consola.
- El sellado de tiempo del certificado representa cuándo se creó el certificado.
- La consola no comprueba si el certificado está vigente o ha caducado.
- Si el certificado cambia (por ejemplo, se renueva o es nuevo), debería agregarse a la *Lista segura* en la consola.

1. Agregue los detalles del certificado al repositorio de certificados.
    a. Identifique la huella digital del certificado para el Portable Executable (ejecutable portátil, PE) firmado.
    b. Seleccione **Configuración > Certificados**.
    c. Haga clic en **Agregar certificado**.
    d. Haga clic en **Examinar los certificados para agregar** o arrastre y suelte el certificado en la casilla.
    e. Si busca los certificados, aparece la ventana Abrir para permitir la selección de los certificados.
    f. Opcionalmente, agregue notas sobre este certificado.
    g. Haga clic en **Enviar**. El emisor, el asunto, la huella digital y las notas (si se han introducido) se agregan al repositorio.
2. Agregue el certificado a la *Lista segura*.
    a. Seleccione **Configuración > Lista global**.
    b. Haga clic en la pestaña **Segura**.
    c. Haga clic en **Certificados**.

d. Haga clic en **Agregar certificado**.

e. Seleccione un certificado de la *Lista segura.* Opcionalmente, seleccione una categoría y agregue un motivo para agregar este certificado.

f. Haga clic en **Enviar**.

Visualización de huellas digitales de una amenaza

En la pestaña Protección, Detalles de amenaza muestra ahora la huella digital del certificado. En la pantalla, seleccione **Agregar certificado** para agregar el certificado al repositorio.

Privilegios

Agregar certificado es una función disponible solo para administradores. Si el certificado ya se ha agregado al repositorio de certificados, la consola mostrará **Ir a certificado**. Los certificados son solo de lectura para los administradores de zonas, que ven la opción **Ir a certificado**.

Perfil

El menú de perfil (esquina superior derecha) permite la administración de su cuenta, que se vean los registros de auditoría de la consola y acceder a la Ayuda del producto.

Mi cuenta

Cambie su contraseña y la configuración de notificación por correo electrónico en la página Mi cuenta.

1. Inicie sesión en la consola (http://dellthreatdefense.com).
2. Haga clic en el menú de perfil en la esquina superior derecha y seleccione **M**i cuenta.
3. Para cambiar su contraseña:
    a. Haga clic en Cambiar contraseña.
    b. Introduzca su contraseña antigua.
    c. Introduzca la nueva contraseña y vuelva a hacerlo para confirmarla.
    d. Haga clic en Actualizar.
4. Marque o desmarque la casilla de verificación para habilitar o deshabilitar las notificaciones por correo electrónico. La marcación o desmarcación de la casilla de verificación se guarda automáticamente. Las notificaciones por correo electrónico solo están disponibles para administradores.

Registro de auditoría

Lista desplegable de iconos de usuario (esquina superior derecha de la consola)

El registro de auditoría contiene información sobre las siguientes acciones realizadas desde la consola:

- Inicio de sesión (Correcto, Error)
- Política (Agregar, Editar, Eliminar)
- Dispositivo (Editar, Eliminar)
- Amenaza (Cuarentena, Exenta, Cuarentena global, Lista segura)
- Usuario (Agregar, Editar, Eliminar)
- Actualización del agente (Editar)

Puede consultarse el registro de auditoría desde la consola; navegue hasta la lista de perfiles desplegable en la parte superior derecha de la consola y seleccione **Registro de auditoría**. Los registros de auditoría están disponibles solo para administradores.

Configuración

La página Configuración muestra las pestañas Aplicación, Administración de usuarios, Política de dispositivos, Lista global y Actualización del agente. El elemento de menú Configuración solo está disponible para administradores.

APLICACIÓN

Threat Defense Agent

Los dispositivos se agregan a la organización instalando Threat Defense Agent en cada extremo. Una vez conectado a la consola, aplique la política (para administrar las amenazas identificadas) y organice los dispositivos en función de sus necesidades organizativas.

Threat Defense Agent está diseñado para utilizar una cantidad mínima de recursos del sistema. El agente trata los archivos y procesos que ejecuta como prioridad ya que estos eventos podrían ser maliciosos. Los archivos que simplemente estén en el disco (en almacenamiento pero no en ejecución) tienen una prioridad más baja porque aunque podrían ser maliciosos, no suponen una amenaza inmediata.

Agente de Windows

Requisitos del sistema

Dell recomienda que el hardware de extremo (CPU, GPU, etc.) cumpla con, o supere, los requisitos recomendados para el sistema operativo de destino. Las excepciones se anotan a continuación (RAM, espacio de unidad de disco duro disponible y requisitos adicionales de software).

Sistemas operativos	• Windows 7 (32 bits o 64 bits) • Windows Embedded Standard 7 *(32 bits)* y Windows Embedded Standard 7 Pro *(64 bits)* • Windows 8 y 8.1 (32 bits y 64 bits)* • Windows 10 (32 bits y 64 bits)** • Windows Server 2008 y 2008 R2 (32 bits y 64 bits)*** • Windows Server 2012 y 2012 R2 (64 bits)*** • Windows Server 2016: Standard, Data Center y Essentials***
RAM	• 2 GB
Espacio de unidad de disco duro disponible	• 300 MB
Requisitos/software adicionales	• .NET Framework 3.5 (SP1) o superior (solo Windows) • Navegador de Internet • Acceso a Internet para iniciar sesión, acceder al instalador, y registrar el producto • Derechos de administrador local para instalar el software
Otros requisitos	• TLS 1.2 es compatible con el agente 1422 o superior y requiere .NET Framework 4.5 o superior

Tabla 2: Requisitos del sistema para Windows

**No admitido: Windows 8.1 RT
**La actualización Windows 10 Anniversary Update requiere el agente 1402 o posterior.
***No admitido: Server Core (2008 y 2012) y Minimal Server (2012).
****Requiere el agente 1412 o posterior.

Para descargar el archivo de instalación

1. Inicie sesión en la consola (http://dellthreatdefense.com).
2. Seleccione **Configuración > Aplicaciones**.
3. Copie el **token de instalación**.

   La señal de instalación es una cadena de caracteres generada aleatoriamente que permite que el agente informe a su cuenta asignada de la consola. La señal de instalación es necesaria durante la instalación, en el asistente para la instalación o como valor de parámetro de instalación.
4. Descargue el instalador.
   a. Seleccione el sistema operativo.
   b. Seleccione el tipo de archivo que descargar.

      Para Windows, Dell recomienda utilizar el archivo MSI de instalación del agente.

Consejo: Si está configurada una regla de zona, los dispositivos se pueden asignar automáticamente a una zona si el dispositivo coincide con los criterios de regla de zona.

Instalación del agente: Windows

Asegúrese de que se cumplen todos los requisitos previos antes de instalar Threat Defense. Ver Requisitos del sistema.

1. Haga doble clic en DellThreatDefenseSetup.exe (o MSI) para iniciar la instalación.
2. Haga clic en **Instalar** en la ventana de configuración de Threat Defense.
3. Introduzca la señal de instalación proporcionada por el arrendatario de Threat Defense. Haga clic en **Siguiente**.

   Nota: Póngase en contacto con el administrador de Threat Defense o consulte el artículo de KB Cómo administrar Threat Defense cuando el token de instalación no se encuentra disponible.
4. Cambie opcionalmente la carpeta de destino de Threat Defense.

   Haga clic en **Aceptar** para comenzar la instalación.
5. Haga clic en **Finalizar** para completar la instalación. Marque la casilla de verificación para iniciar Threat Defense.

Parámetros de instalación de Windows

El agente se puede instalar interactivamente o no interactivamente a través de GPO, Microsoft System Center Configuration Manager (normalmente conocido como SCCM), y MSIEXEC. Los MSI se pueden personalizar con parámetros integrados (que aparecen a continuación) o los parámetros se pueden proporcionar desde la línea de comandos.

Propiedad	Valor	Descripción
PIDKEY	<Señal de instalación>	Entrada automática de la señal de instalación
LAUNCHAPP	0 o 1	0: el icono de la bandeja del sistema y la carpeta del menú de inicio están ocultos durante el tiempo de ejecución 1: el icono de la bandeja del sistema y la carpeta del menú de inicio no están ocultos durante la ejecución (valor predeterminado)
SELFPROTECTIONLEVEL	1 o 2	1: solo los administradores locales pueden realizar cambios en el registro y los servicios 2: solo el administrador del sistema puede realizar cambios en el registro y los servicios (valor predeterminado)
APPFOLDER	<Carpeta de instalación de destino>	Especifica el directorio de instalación del agente La ubicación predeterminada es C:\Program Files\Cylance\Desktop
VenueZone	"Nombre_zona"	Requiere la versión de agente 1382 o superior •Agregue dispositivos a una zona. •Si la zona no existe, la zona se crea utilizando el nombre proporcionado. •Sustituya nombre_zona por el nombre de una zona existente o una zona que desee crear. **Aviso**: Agregar espacios antes o después del nombre de zona creará una nueva zona.

Tabla 3: Parámetros de instalación para Windows

El siguiente ejemplo de línea de comandos muestra cómo ejecutar la herramienta de instalación de Microsoft Windows (MSIEXEC) pasándole los parámetros de instalación PIDKEY, APPFOLDER y LAUNCHAPP:

```
msiexec /i DellThreatDefenseSetup_x64.msi /qn PIDKEY=<INSTALLATION TOKEN>
LAUNCHAPP=0 /L*v C:\temp\install.log
```

La instalación es silenciosa y el registro de instalación se guarda en `C:\temp`. Cuando el agente está en ejecución, el icono de la bandeja del sistema y la carpeta Threat Defense del menú de inicio están ocultos. Encontrará información adicional sobre los diferentes conmutadores de línea de comandos aceptados por MSIEXEC en KB 227091.

Instalación del agente de Windows mediante Wyse Device Manager (WDM)

Esta sección explica cómo crear e instalar una secuencia de comandos, cómo crear un paquete RSP para WDM, y cómo agregar el paquete a WDM para instalarlo en varios clientes finos de manera simultánea sin interacción del usuario.

Cree una secuencia de comandos de archivo por lotes que realizará la instalación de la línea de comandos de Threat Defense. WDM ejecuta esta secuencia de comandos durante la implementación.

1. Abra el Bloc de notas. Utilice los parámetros de línea de comandos anteriores y escriba el siguiente comando para ejecutar la instalación, sustituyendo **<INSTALLATION TOKEN>** por el token que se le ha proporcionado.
   msiexec /i C:\TDx86\DellThreatDefense_x86.msi PIDKEY=<INSTALLATION TOKEN> /q

   C:\TDx86 se utiliza para nuestro directorio, ya que esta carpeta se copia a esta ubicación en el cliente ligero durante la instalación.

2. Guarde el archivo con una extensión .bat en la carpeta TDx86. Por ejemplo, **TDx86_Install.bat**.

   Cree un paquete RSP con el que se podrá instalar la aplicación Threat Defense Agent en varios clientes ligeros a la vez, sin la interacción del usuario.

3. Abra Scriptbuilder en un equipo que tenga instalado WDM.
4. Escriba un nombre de paquete y una descripción del paquete.
   - Seleccione Otros paquetes en Categoría de paquete.
   - Seleccione Windows Embedded Standard 7 en Sistema operativo.
5. Agregue comandos de la secuencia de comandos para comprobar que los sistemas de destino son WES7 o WES7p.
   - Seleccione Confirmar sistema operativo (CO) en Comando de secuencia de comandos
   - Para el valor del sistema operativo del dispositivo, introduzca el sistema operativo adecuado.
6. Utilice las flechas dobles para agregar elemento.
7. Pulse **Aceptar** cuando se le solicite.
8. Agregue comando para bloquear el cliente fino e impedir la interacción del usuario.
   - Seleccione **Comando de script > Bloqueo de usuarios (LU)**. No es necesario ningún valor. Sin embargo, en este ejemplo se ha introducido el **valor Sí**, de modo que la pantalla de presentación se elimina si el instalador no puede terminar o se produce un error.
9. Agregue comando para copiar archivos en el cliente fino.
   - Seleccione Comando de script **Copia X (XC)**.
   - Para el valor del **Directorio de repositorio**, agregue ***** al final del **<regroot>** existente.
   - Como valor del **Directorio del dispositivo**, introduzca la ruta de acceso a los archivos que desea copiar en los clientes ligeros de destino. En este ejemplo, se utiliza el nombre de paquete.
10. Agregue comando para ejecutar la secuencia de comandos de instalación .bat.
    - Seleccione **Ejecutar comando de script > Ejecutar en el dispositivo (EX)**.
    - Como valor de Nombre de archivo del dispositivo, escriba la ruta de acceso **C:\TDx86\TDx86_install.bat**. La carpeta TDx86 se copia desde nuestro comando XC anterior.
    - Agregue **+** como valor de Ejecución sincrónica. De esta forma se indica a WDM que espere hasta que haya finalizado la ejecución del archivo para continuar.
11. Agregue comando para eliminar archivos copiados desde el cliente fino.
    - Agregue el comando de script **Eliminar árbol (DT)**.

12. Agregue comandos para deshabilitar el bloqueo.
    - Agregue el comando de script **Finalizar bloqueo (EL**).
13. A la hora de revisar, el paquete de secuencia de comandos debe parecerse a lo siguiente.
    - Si implementa Threat Defense en sistemas WES7P, actualice la sección del sistema operativo a WES7P. De lo contrario, el paquete no podrá instalarse.
14. Guarde el paquete.
    - Haga clic en **Guardar** y navegue hasta la ubicación de la carpeta **TDx86**. Si ha seguido estas instrucciones, la carpeta se encontrará en el escritorio.
15. Cierre Scriptbuilder.
16. Ejecute **WyseDeviceManager** para agregar el paquete a WDM.
17. Acceda a **WyseDeviceManager > Administrador de paquetes > Otros paquetes**.
18. Seleccione **Acción > Nueva > Paquete** en la barra de menús.
19. Seleccione **Registrar un paquete desde un archivo de script (.RSP)** y haga clic en **Siguiente**.
20. Vaya a la ubicación del archivo RSP creado en el paso anterior y haga clic en **Siguiente.**
21. Asegúrese de que está seleccionada la opción **Activo** y haga clic en **Siguiente.**
22. Haga clic en **Siguiente** una vez que WDM esté listo para registrar el paquete.
23. Haga clic en **Terminar** cuando el paquete se registre correctamente.
24. El paquete será visible en **Otros paquetes**.
25. Compruebe el contenido del paquete:
    - Abra el Explorador de archivos y acceda a **C:\inetpub\ftproot\Rapport**. Localice la carpeta **TDx86**.
    - Abra la carpeta TDx86 y compruebe que la carpeta incluye el instalador y el archivo .bat.

Ahora dispone de un paquete en WDM que puede implementar Threat Defense en varios clientes finos de WES7 sin interacción del usuario.

Cuarentena mediante la línea de comandos

Puede poner en cuarentena un archivo mediante la línea de comandos en un dispositivo. Esto requiere conocer el hash SHA256 para la amenaza.

Nota: Esta función es solo para Windows y requiere el agente 1432 o superior.

1. En el dispositivo de Windows, abra la línea de comandos. Ejemplo: En el menú Inicio, busque cmd.exe.
2. Invoque Dell.ThreatDefense.exe e incluya el argumento **-q: <hash>**, donde <hash> es el hash SHA256 para el archivo. Esta solicitará al Agent que envíe el archivo a la carpeta de cuarentena.

   Ejemplo de línea de comandos (con Dell Threat Defense instalado en la ubicación predeterminada):

   ```
   "C:\Program Files\Cylance\Desktop\Dell.ThreatDefense.exe" -q:
   14233d4875e148c370a6bbe40fccabccdbfa194dac9e8bd41b0eadcf2351f941
   ```

Desinstalación del agente

Para desinstalar el agente en un sistema Windows, utilice la función Agregar o quitar programas o utilice la línea de comandos.

La desinstalación del agente no elimina el dispositivo de la consola. Debe eliminar manualmente el dispositivo de la consola.

Antes de intentar desinstalar el agente:

- Si la opción **Requiere contraseña para desinstalar el Agente** está activada, asegúrese de tener la contraseña para desinstalar.
- Si la opción **Prevenir el apagado del servicio del dispositivo** está activada, deshabilítela en la política o aplique una política diferente de los dispositivos de los cuales desea desinstalar el agente.

Desinstalación con Agregar o quitar programas

1. Seleccione **Inicio > Panel de control**.
2. Haga clic en **Desinstalar un programa**. Si tiene seleccionado Iconos en lugar de Categorías, haga clic en Programas y características.
3. Seleccione **Dell Threat Defense** y haga clic en **Desinstalar**.

Con la línea de comandos

1. Abra el símbolo del sistema como administrador.
2. Use los siguientes comandos, según el paquete de instalación que utilizó para instalar el agente.
    a. DellThreatDefense_x64.msi
        i. Desinstalación estándar: msiexec /uninstall DellThreatDefense_x64.msi
        ii. Windows Installer: msiexec /x DellThreatDefense_x64.msi
    b. DellThreatDefense_x86.msi
        i. Desinstalación estándar: msiexec /uninstall DellThreatDefense_x86.msi
        ii. Windows Installer: msiexec /x DellThreatDefense_x86.msi
3. Los siguientes comandos son opcionales:
    a. Para una desinstalación silenciosa: /quiet
    b. Para una desinstalación silenciosa y oculta: /qn
    c. Para la desinstalación de protección con contraseña UNINSTALLKEY=<contraseña>
    d. Para desinstalar el archivo de registro: /Lxv* <ruta de acceso>
        i. Esto crea un archivo de registro en la ruta de acceso designada (<ruta de acceso>), que incluye el nombre del archivo.
        ii. Ejemplo: C:\Temp\Uninstall.log

Agente macOS

Requisitos del sistema

Dell recomienda que el hardware de extremo (CPU, GPU, etc.) cumpla con, o supere, los requisitos recomendados para el sistema operativo de destino. Las excepciones se anotan a continuación (RAM, espacio de unidad de disco duro disponible y requisitos adicionales de software).

Sistemas operativos	• Mac OS X 10.9 • Mac OS X 10.10 • Mac OS X 10.11 • macOS 10.12* • macOS 10.13**
RAM	• 2 GB
Espacio de unidad de disco duro disponible	• 300 MB

Tabla 4: Requisitos del sistema macOS

*Requiere el agente 1412 o posterior.
** Requiere el agente 1452 o posterior.

Para descargar el archivo de instalación

1. Inicie sesión en la consola (http://dellthreatdefense.com).
2. Seleccione **Configuración > Aplicaciones**.
3. Copie el **token de instalación**.

   La señal de instalación es una cadena de caracteres generada aleatoriamente que permite que el agente informe a su cuenta asignada de la consola. La señal de instalación es necesaria durante la instalación, en el asistente para la instalación o como valor de parámetro de instalación.
4. Descargue el instalador.
   a. Seleccione el sistema operativo.
   b. Seleccione el tipo de archivo que descargar.

Consejo: Si está configurada una regla de zona, los dispositivos se pueden asignar automáticamente a una zona si el dispositivo coincide con los criterios de regla de zona.

Instalación del agente: macOS

Asegúrese de que se cumplen todos los requisitos previos antes de instalar Threat Defense. Consulte los Requisitos del sistema.

Nota: El agente de macOS tendrá la marca Dell en una futura versión.

1. Haga doble clic en **`DellThreatDefense.dmg`** para montar el instalador.
2. Haga doble clic en el icono de *proteger* en la interfaz de usuario de PROTECT para comenzar la instalación.
3. Haga clic en **Continuar** para verificar que el sistema operativo y el hardware cumplen los requisitos.
4. En la pantalla de introducción, haga clic en **Continuar**.
5. Introduzca la señal de instalación proporcionada por el arrendatario de Threat Defense. Haga clic en **Continuar**.

Nota: Póngase en contacto con el administrador de Threat Defense o consulte el artículo de KB Cómo administrar Threat Defense cuando el token de instalación no se encuentra disponible.

6. Cambie opcionalmente la ubicación de instalación de Threat Defense.

   Haga clic en **Instalar** para comenzar la instalación.

7. Introduzca el nombre de usuario y la contraseña del administrador. Haga clic en **Instalar software**.

8. En la pantalla de resumen, haga clic en **Cerrar**.

Parámetros de instalación de macOS

Threat Defense Agent se puede instalar mediante opciones de línea de mandatos en Terminal. El siguiente ejemplo utiliza el instalador de PKG. Para DMG, simplemente cambie la extensión de archivo del comando.

Nota: Asegúrese de que los extremos de destino cumplan los requisitos del sistema y que la persona que instala el software tenga las credenciales adecuadas para instalar software.

Propiedad	Valor	Descripción
InstallToken		Señal de instalación disponible en la consola.
NoCylanceUI		El icono de Agent no debe aparecer al inicio. El valor predeterminado es Visible.
SelfProtectionLevel	0 o 1	1: solo los administradores locales pueden realizar cambios en el registro y los servicios. 2: solo el administrador del sistema puede realizar cambios en el registro y los servicios (valor predeterminado).
LogLevel	0, 1, 2 o 3	0: Error – Solo se registran mensajes de error. 1: Aviso – Se registran mensajes de error y de aviso. 2: Información (valor predeterminado) – Se registran mensajes de error, de aviso y de información. Esto puede ofrecer algunos detalles durante la solución de problemas. 3: Detallado – Se registran todos los mensajes. Durante la solución de problemas, este es el nivel de registro recomendado. No obstante, los tamaños de archivo de registro detallado pueden crecer mucho. Dell recomienda activar Detallado durante la solución de problemas y, a continuación, cambiar de nuevo a Información una vez haya finalizado aquella.
VenueZone	"nombre_zona"	Requiere la versión de agente 1382 o superior •Agregue dispositivos a una zona. •Si la zona no existe, la zona se crea utilizando el nombre proporcionado. •Sustituya nombre_zona por el nombre de una zona existente o una zona que desee crear. **Aviso**: Agregar espacios antes o después del nombre de zona creará una nueva zona.

Tabla 5: Parámetros de instalación para macOS

Instalación del agente

Instalación sin la señal de instalación

```
sudo installer –pkg DellThreatDefense.pkg –target/
```

Instalación con la señal de instalación

```
echo [install_token] > cyagent_install_token

sudo installer –pkg DellThreatDefense.pkg –target/
```

Nota: Sustituya **[install_token]** por el token de instalación. El comando eco genera un archivo de texto **cyagent_install_token** con una opción de instalación por línea. El archivo debe estar en la misma carpeta que el paquete de instalación. Tenga cuidado con las extensiones de archivo, el ejemplo anterior muestra el archivo cyagent_install_token sin extensión. Las configuraciones predeterminadas en macOS tienen las extensiones ocultas. Al editar manualmente este archivo con un editor de texto es posible que se añada automáticamente una extensión de archivo que será necesario eliminar.

Parámetros de instalación opcionales

Escriba lo siguiente en el terminal para crear un archivo (**cyagent_install_token**) que utilice el instalador para aplicar las opciones introducidas. Cada parámetro debe estar en su propia línea. El archivo debe estar en la misma carpeta que el paquete de instalación.

A continuación se muestra un ejemplo. Todos los parámetros no son necesarios en el archivo. Terminal incluye todo lo contenido entre comillas simples en el archivo. Asegúrese de presionar Intro/Retorno después de cada parámetro para mantener cada parámetro en su propia línea del archivo.

También se puede utilizar un editor de texto para crear el archivo que incluya cada parámetro (en su propia línea). El archivo debe estar en la misma carpeta que el paquete de instalación.

Ejemplo:

```
echo 'InstallToken

NoCylanceUI

SelfProtectionLevel=2

LogLevel=2'> cyagent_install_token

sudo installer –pkg DellThreatDefense.pkg –target/
```

Desinstalación del agente

Sin contraseña

```
sudo /Applications/Cylance/Uninstall\
DellThreatDefense.app/Contents/MacOS/Uninstall\ DellThreatDefense
```

Con contraseña

```
sudo /Applications/Cylance/Uninstall\
DellThreatDefense.app/Contents/MacOS/Uninstall\ DellThreatDefense --
password=thisismypassword
```

Nota: Sustituya **thisismypassword** por la contraseña de desinstalación creada en la consola.

Servicio de agente

Iniciar servicio

```
sudo launchctl load
/Library/launchdaemons/com.cylance.agent_service.plist
```

Detener servicio

```
sudo launchctl unload
/Library/launchdaemons/com.cylance.agent_service.plist
```

Comprobación de la instalación

Revise los siguientes archivos para comprobar la instalación correcta del agente.

1. Se ha creado la carpeta Programa.
    - Valor predeterminado de Windows: **`C:\Program Files\Cylance\Desktop`**
    - macOS predeterminado: **`/Applications/DellThreatDefense/`**
2. El icono de Threat Defense es visible en la bandeja del sistema del dispositivo de destino.

    Esto no se aplica si se utiliza el parámetro LAUNCHAPP=0 (Windows) o NoCylanceUI (macOS).
3. Hay una carpeta Threat Defense en el menú Inicio\Todos los programas del dispositivo de destino.

    Esto no se aplica si se utiliza el parámetro LAUNCHAPP=0 (Windows) o NoCylanceUI (macOS).
4. El servicio Threat Defense se ha agregado y está en ejecución. Debería haber un servicio Threat Defense que aparezca en ejecución en el panel Servicios de Windows del dispositivo de destino.
5. El proceso Dell.ThreatDefense.exe está en ejecución. Debería haber un proceso Dell.ThreatDefense.exe mostrado en la pestaña Procesos del Administrador de tareas de Windows del dispositivo de destino.
6. El dispositivo está informando a la consola. Inicie sesión en la consola y haga clic en la pestaña Dispositivos; el dispositivo de destino debería aparecer y mostrarse en la lista en el estado En línea.

Interfaz de usuario del agente

La interfaz de usuario del agente está habilitada de forma predeterminada. Haga clic en el icono del agente de la bandeja del sistema para verlo. Si no, el agente se puede instalar para que su icono esté oculto en la bandeja del sistema.

Pestaña Amenazas

Muestra todas las amenazas detectadas en el dispositivo y la acción llevada a cabo. *No seguro* significa que no se ha emprendido ninguna acción ante la amenaza. *En cuarentena* significa que la amenaza se ha modificado (para evitar la ejecución del archivo) y se ha movido a la carpeta *En cuarentena*. *Exento* significa que el administrador considera el archivo seguro y *Permitido* que se puede ejecutar en el dispositivo.

Pestaña Eventos

Muestra los eventos de amenazas que se han producido en el dispositivo.

Pestaña Secuencias de comandos

Muestra las secuencias de comandos maliciosas que se han ejecutado en el dispositivo y cualquier acción realizada en la secuencia de comandos.

Menú Agente

El menú Agente proporciona acceso a la ayuda y actualizaciones para Threat Defense. También se proporciona acceso a la interfaz de usuario avanzada que ofrece más opciones de menú.

Menú Agente

El menú Agente permite a los usuarios realizar algunas acciones en el dispositivo. Haga clic con el botón derecho en el icono del agente para ver el menú.

- **Buscar actualizaciones**: el agente busca e instala las actualizaciones disponibles. Las actualizaciones están restringidas a la versión del agente permitida para la zona a la que pertenece el dispositivo.
- **Comprobar si existen actualizaciones de políticas:** El agente comprueba si hay disponible una actualización de la política. Puede ser cambios en la política existente o una política diferente que se aplicará al agente.

  Nota: Consulte si la actualización de la política es compatible en la versión 1422 (o superior) para Windows y la versión 1432 (o superior) para Mac OS.
- **Acerca de**: muestra un diálogo con la versión del agente, el nombre de la política asignada al dispositivo, la última hora en que el agente buscó una actualización, y la señal de instalación utilizada durante la instalación.
- **Salir**: cierra el icono del agente en la bandeja del sistema. De esta forma no se desactiva ningún servicio de Threat Defense.
- **Opciones > Mostrar notificaciones**: seleccione esta opción para mostrar nuevos eventos como notificaciones.

Habilitación de las opciones avanzadas de la interfaz de usuario del agente

Threat Defense Agent ofrece algunas opciones avanzadas a través de la interfaz de usuario para proporcionar características en dispositivos sin conectividad a la consola. CylanceSVC.exe debe estar ejecutándose cuando se habiliten las opciones avanzadas.

Windows

1. Si el icono del agente está visible en la bandeja del sistema, haga clic con el botón derecho en el icono y seleccione **Salir**.
2. Inicie el símbolo del sistema y escriba el siguiente comando. Presione Intro cuando haya terminado.

   ```
   cd C:\Program Files\Cylance\desktop
   ```

   Si la aplicación se ha instalado en una ubicación diferente, navegue hasta dicha ubicación en el símbolo del sistema.
3. Escriba el siguiente comando y presione Intro cuando haya terminado.

   ```
   Dell.ThreatDefense.exe –a
   ```

   El icono del agente aparece en la bandeja del sistema.
4. Haga clic con el botón derecho en el icono. Se muestran las opciones *Registro*, *Ejecutar una detección* y *Administración de amenazas*.

macOS

1. Si el icono del agente está visible en el menú superior, haga clic con el botón derecho en el icono y seleccione **Salir**.
2. Abra el terminal y ejecute
    a. Sudo /Applications/DellThreatDefense/DellThreatDefense.app/Contents/MacOS/DellThreatDefenseUI –a

    Nota: Esta es la ruta de acceso de instalación predeterminada para Dell Threat Defense. Es posible que deba editar la ruta para adaptarla a su entorno, según corresponda.
3. La interfaz de usuario del agente aparece ahora con opciones adicionales.

Registro

Seleccione el nivel de información de registro que recopilar del agente. El valor predeterminado es Información. Dell recomienda establecer el nivel de registro en Todo (Detallado) durante la solución de problemas. Una vez completada la solución de problemas, vuelva a cambiar a Información (el registro de toda la información puede generar archivos de registro muy grandes).

Ejecución de una detección

Permite a los usuarios especificar una carpeta para buscar amenazas.

1. Seleccione **Ejecutar una detección > Especificar la carpeta**.
2. Seleccione una carpeta para analizar y haga clic en **Aceptar**. Las amenazas detectadas aparecerán en la interfaz de usuario del agente.

Administración de amenazas

Permite a los usuarios eliminar los archivos *en cuarentena* en el dispositivo.

1. Seleccione **Administración de amenazas > Eliminar en cuarentena**.
2. Haga clic en **Aceptar** para confirmar.

Máquinas virtuales

Existen algunas recomendaciones cuando se utiliza Threat Defense Agent en una imagen de máquina virtual.

Al crear una imagen de máquina virtual que utilizar como plantilla, desconecte la configuración de red de máquina virtual antes de instalar el agente. Esto impide que el agente se comunique con la consola y configure los detalles del dispositivo. Impide que haya dispositivos duplicados en la consola.

Deinstalación protegida por contraseña

CONFIGURACIÓN > Aplicación

Los administradores pueden requerir una contraseña para deinstalar el agente. Al desinstalar el agente con una contraseña:

- Si el instalador MSI se ha utilizado para la instalación, realice la desinstalación a través de MSI o mediante el Panel de control.

- Si se ha utilizado el instalador EXE para realizar la instalación, utilice EXE para la desinstalación. El uso del panel de control no funciona si se ha utilizado el instalador de EXE y se necesita una contraseña para realizar la desinstalación.
- Si realiza la desinstalación mediante la línea de comandos, agregue la cadena de desinstalación: **`UNINSTALLKEY = [MyUninstallPassword]`**.

Para crear una contraseña de desinstalación

1. Inicie sesión en la consola (http://dellthreatdefense.com) utilizando una cuenta de administrador.
2. Seleccione **Configuración > Aplicaciones**.
3. Marque la casilla **Solicitar contraseña para desinstalar el agente**.
4. Escriba una contraseña.
5. Haga clic en **Guardar**.

Integraciones

La consola de Threat Defense ofrece integración con programas de terceros.

Syslog/SIEM

Threat Defense puede integrarse con el software de Security Information Event Management (SIEM) mediante la característica Syslog. Los eventos de Syslog persisten al mismo tiempo que los eventos del agente persisten en la consola.

Para obtener las direcciones IP más recientes para mensajes de Syslog, póngase en contacto con Dell Support.

Tipos de eventos

Registro de auditoría

Seleccione esta opción para enviar el registro de auditoría de las acciones de usuario realizadas en la consola (sitio web) al servidor de Syslog. Los eventos del registro de auditoría siempre aparecen en la pantalla Registro de auditoría, aunque esta opción no está seleccionada.

Mensaje de ejemplo para un registro de auditoría enviado a Syslog

Dispositivos

Seleccione esta opción para enviar eventos de dispositivo al servidor de Syslog.

- Cuando se registre un nuevo dispositivo, se recibirán dos mensajes para este evento: Registro y SystemSecurity.

  Mensaje de ejemplo para evento de dispositivo registrado

- Cuando se elimina un dispositivo.

  Mensaje de ejemplo para evento de dispositivo eliminado

- Cuando se cambia la política, la zona, el nombre o el nivel de registro de un dispositivo.

  Mensaje de ejemplo para evento de dispositivo actualizado

Amenazas
Seleccione esta opción para registrar las amenazas recién detectadas o los cambios observados para cualquier amenaza existente, o para iniciar sesión en el servidor de Syslog. Los cambios incluyen una amenaza que va a *eliminarse*, ponerse *en cuarentena*, *eximirse* o *ejecutarse*.

Existen cinco tipos de eventos de amenaza:

- **threat_found**: se ha encontrado una nueva amenaza en un estado *No seguro*.
- **threat_removed**: se ha *eliminado* una amenaza existente.
- **threat_quarantined**: se ha encontrado una nueva amenaza en el estado *En cuarentena*.
- **threat_waived**: se ha encontrado una nueva amenaza en el estado *Exento*.
- **threat_changed**: El comportamiento de una amenaza existente ha cambiado (ejemplos: Puntuación, Cuarentena, Estado, Estado en ejecución).
- **threat_cleared**: una amenaza exenta, agregada a la lista segura o eliminada de la cuarentena en un dispositivo.

Mensaje de ejemplo de evento de amenaza

Clasificaciones de amenazas
Miles de amenazas se clasifican cada día como Malware o como Potentially Unwanted Programs (Programas potencialmente no deseados - PUP). Si esta opción está seleccionada, estará suscrito a las notificaciones cuando se produzcan tales eventos.

Mensaje de ejemplo de clasificación de amenazas

Security Information and Event Management (Información de seguridad y administración de eventos - SIEM)
Especifica el tipo de servidor de Syslog o SIEM al que deben enviarse los eventos.

Protocolo
Debe coincidir con lo que se ha configurado en el servidor de Syslog. Las opciones son UDP o TCP. UDP no se recomienda normalmente porque no garantiza la entrega de los mensajes. Dell recomienda TCP (valor predeterminado).

TLS/SSL
Solo disponible si el protocolo especificado es TCP. TLS/SSL garantiza que el mensaje de Syslog se cifre en tránsito desde Threat Defense al servidor de Syslog. Dell recomienda a los clientes seleccionar esta opción. Asegúrese de que el servidor de Syslog escuche los mensajes de TLS/SSL.

IP/Dominio
Especifica la dirección IP o el nombre de dominio completo del servidor de Syslog que el cliente ha configurado. Consulte con sus expertos en red interna para asegurarse de que los valores del dominio y el servidor de seguridad estén bien configurados.

Puerto
Especifica el número de puerto de los dispositivos que el servidor de Syslog escucha en busca de mensajes. Debe ser un número entre 1 y 65535. Los valores habituales son: 512 para UDP, 1235 o 1468 para TCP y 6514 para TCP protegido (ejemplo: TCP con TLS/SSL habilitado).

Gravedad
Especifica la gravedad de los mensajes que deben aparecer en el servidor de Syslog. Se trata de un campo subjetivo, y puede establecerse en cualquier nivel preferido. El valor de la gravedad no cambia los mensajes que se reenvían a Syslog.

Recurso
Especifica el tipo de aplicación que registra el mensaje. El valor predeterminado es Interno (o Syslog). Se utiliza para categorizar los mensajes cuando los recibe el servidor de Syslog.

Prueba de la conexión
Haga clic en **Probar conexión** para probar la configuración de IP/dominio, puerto y protocolo. Si se introducen valores válidos, tras un par de segundos aparecerá una confirmación de que son *correctos*.

Autenticación personalizada

Utilice proveedores de identidad (IdP) externos para iniciar sesión en la consola. Esto requiere configurar los valores con su IdP para obtener un certificado X.509 y una URL para comprobar su inicio de sesión de IdP. La autenticación personalizada funciona con Microsoft SAML 2.0. Se ha confirmado que esta característica funciona con OneLogin, OKTA, Microsoft Azure y PingOne. Esta característica también ofrece una configuración personalizada y debe funcionar con otros proveedores de identidad que sigan Microsoft SAML 2.0.

Nota: La autenticación personalizada no admite Active Directory Federation Services (Servicios de federación de Active Directory - ADFS).

- **Autenticación sólida**: proporciona acceso de autenticación multifactor.
- **Inicio de sesión único**: proporciona acceso de sesión único (SSO).

  Nota: Una selección de Autenticación sólida o Inicio de sesión único no afecta a los valores de autenticación personalizada porque todos los valores de configuración los administra el proveedor de identidad (IdP).
- **Permitir inicio de sesión con contraseña**: seleccione esta opción para permitir el inicio de sesión directamente en la consola, mediante SSO. Esto permite pruebas de configuración de SSO sin bloqueo de la consola. Una vez haya iniciado sesión correctamente en la consola mediante SSO, Dell recomienda deshabilitar esta característica.
- **Proveedor:** seleccione el proveedor de servicios para la autenticación personalizada.
- **Certificado X.509**: introduzca la información de certificación X.509.
- **Dirección URL de inicio de sesión**: introduzca la URL para la autenticación personalizada.

Informe de datos de amenazas

Una hoja de cálculo que contiene la siguiente información sobre la organización:

- **Amenazas**: muestra todas las amenazas detectadas en la organización. Esta información incluye el nombre y el estado del archivo (*No seguro*, *Anómalo*, *Ex*ento y *En cuarentena*).
- **Dispositivos**: muestra todos los dispositivos de la organización que tienen instalado Threat Defense Agent. Esta información incluye Nombre de dispositivo, Versión del sistema operativo, Versión del agente y Política aplicada.
- **Indicadores de amenazas**: muestra cada amenaza y las características de amenazas asociadas.

- **Borrado**: muestra todos los archivos que se han borrado de su organización. Esta información incluye los archivos *exentos*, agregados a la *lista segura* o *eliminados* de la carpeta *En cuarentena* de un dispositivo.
- **Eventos**: muestra todos los eventos relacionados con el gráfico Eventos de amenazas en el panel, de los últimos 30 días. Esta información incluye Hash de archivo, Nombre de dispositivo, Ruta de acceso a archivo, y Fecha del evento ocurrido.

Cuando esta característica está habilitada, se actualiza el informe automáticamente a la 1:00 AM Hora estándar del Pacífico (PST). Haga clic en **Regenerar informe** para generar manualmente una actualización.

El informe de datos de amenazas proporciona un URL y una señal que se pueden utilizar para descargar el informe sin requerir un inicio de sesión en la consola. También se puede eliminar o volver a generar una señal, si fuera necesario, que permite el control sobre quién tiene acceso al informe.

SOLUCIÓN DE PROBLEMAS

Esta sección proporciona una lista de preguntas que responder y archivos que recopilar cuando se solucionan problemas con Threat Defense. Esta información permite a Dell Support ayudarle a resolver problemas.

Esta sección también contiene algunos problemas comunes y soluciones sugeridas.

Compatibilidad

Parámetros de instalación

- ¿Cuál es el método de instalación? Proporcione los parámetros utilizados.
  - Ejemplo – Windows: utilice LAUCHAPP=0 al realizar la instalación desde la línea de comandos para ocultar el icono del agente y la carpeta del menú Inicio durante la ejecución.
  - Ejemplo: macOS: utilice SelfProtectionLevel=1 al realizar la instalación desde la línea de comandos para deshabilitar la protección automática en el agente.
- ¿Qué pasos de la instalación pueden comprobarse?
  - Ejemplo – Windows: ¿se ha utilizado el instalador MSI o EXE?
  - Ejemplo – Cualquier sistema operativo: ¿se utilizaron opciones de línea de comandos? Por ejemplo, el modo silencioso o ninguna interfaz de usuario del agente.
- Habilite el registro detallado para la instalación.

Problemas de rendimiento

- Realice una captura de pantalla del Administrador de tareas (Windows) o el Monitor de actividad (macOS) que muestre los procesos de Threat Defense y el consumo de memoria.
- Capture un volcado del proceso de Threat Defense.
- Recopile registros de errores.
- Recopile la salida de información del sistema durante el problema.
  - Para Windows: msinfo32 o winmsd
  - Para macOS: Información del sistema
- Recopile los registros de eventos (Windows) o la información de la consola (macOS) relevantes.

Problemas de actualización, estado y conectividad

- Asegúrese de que el puerto 443 esté abierto en el servidor de seguridad y que el dispositivo pueda resolver y conectarse con sitios de Cylance.com.
- ¿Aparece el dispositivo en la lista de la página Dispositivos de la consola? ¿Está en línea o fuera de línea? ¿Cuál fue la hora de la última conexión?
- ¿Está utilizando el dispositivo un proxy para conectarse a Internet? ¿Se han configurado las credenciales correctamente en el proxy?
- Reinicie el servicio de Threat Defense para que intente conectarse a la consola.
- Recopile registros de errores.
- Recopile la salida de información del sistema durante el problema.
    - Para Windows: msinfo32 o winmsd
    - Para macOS: Información del sistema

Cómo habilitar el registro de depuración

De manera predeterminada, Threat Defense guarda los archivos de registro en **`C:\Program Files\Cylance\Desktop\log`**. Para fines de solución de problemas, Threat Defense se puede configurar para que produzca más registros detallados.

Incompatibilidades de control de la secuencia de comandos

Problema:

Cuando el control de secuencias de comandos está habilitado en algunos dispositivos, puede producir conflictos con otro software que se ejecute en dichos dispositivos. Este conflicto se suele deber a que el agente se introduce en determinados procesos que están siendo llamados por otro software.

Solución:

Dependiendo del software, este problema se puede resolver agregando exclusiones de proceso específicas a la política de dispositivos de la consola. Otra opción es habilitar el modo de compatibilidad (clave de registro) en cada dispositivo que se vea afectado. No obstante, si las exclusiones no son efectivas, Dell recomienda deshabilitar el control de secuencias de control de la política de dispositivo que afecta a los dispositivos y restaurar las funciones normales del dispositivo.

Nota: Esta solución de modo de compatibilidad es para la versión del agente 1370. A partir del agente 1382 y en versiones superiores, el proceso de inyección se ha actualizado para ofrecer compatibilidad con otros productos.

Modo de compatibilidad

Agregue la siguiente clave de registro para habilitar el Modo de compatibilidad:

1. Si utiliza el Editor de registro, vaya a **`HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`**.
2. Haga clic con el botón derecho en **Escritorio**, haga clic en **Permisos**, asuma la propiedad y otórguese **Control completo**. Haga clic en **Aceptar**.
3. Haga clic con el botón derecho del ratón en **Escritorio** y, a continuación, seleccione **Nuevo > Valor binario**.

4. Nombre del archivo **CompatibilityMode**.
5. Abra la configuración de registro y cambie el valor a **01**.
6. Haga clic en **Aceptar** y, a continuación, cierre el Editor de registro.
7. Puede que sea necesario reiniciar el dispositivo.

Opciones de la línea de comandos

Uso de Psexec:

```
psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE
\Cylance\Desktop /v CompatibilityMode /t REG_BINARY /d 01
```

Para ejecutar un comando en varios dispositivos, utilice **`Invoke-Command cmdlet`**:

```
$servers = "testComp1","testComp2","textComp3"

$credential = Get-Credential -Credential {UserName}\administrator

Invoke-Command -ComputerName $servers -Credential $credential -
ScriptBlock {New-Item -Path HKCU:\Software\Cylance\Desktop -Name
CompatibilityMode -Type REG_BINARY -Value 01}
```

APÉNDICE A: GLOSARIO

Anómalo	Un archivo sospechoso con una puntuación más baja (de 1 a 59) con menos probabilidades de ser malware
Administrador	Administrador arrendatario de Threat Defense
Agente	Host de extremo de Threat Defense que se comunica con la consola
Registro de auditoría	Registro que registra las acciones realizadas desde la consola de Threat Defense
Cuarentena automática	Evite automáticamente la ejecución de todos los archivos *no seguros* o *anómalos*
Carga automática	Cargue automáticamente cualquier archivo ejecutable portátil desconocido, detectado como *no seguro* o *an*ómalo, a la nube de Cylance Infinity para su análisis
Consola	Interfaz de usuario de administración de Threat Defense
Política de dispositivo	La política de Threat Defense que puede configurar el administrador de la organización y que define la forma en que se administran las amenazas en todos los dispositivos
Cuarentena global	Impide la ejecución de un archivo globalmente (en todos los dispositivos de una organización)
Lista segura global	Permite la ejecución de un archivo globalmente (en todos los dispositivos de una organización)
Infinity	El modelo matemático utilizado para puntuar archivos
Organización	Una cuenta de arrendatario que utiliza el servicio Threat Defense
En cuarentena	Impide la ejecución de un archivo localmente (en un dispositivo específico)
Amenazas	Archivos potencialmente maliciosos detectados por Threat Defense, clasificados como *no seguro*s o *an*ómalos
No seguro	Un archivo sospechoso con una alta puntuación (60 – 100) que probablemente sea malware
Eximir	Permite la ejecución de un archivo localmente (en un dispositivo específico)

Zona	Una forma de organizar y agrupar dispositivos de una organización en función de la prioridad, la funcionalidad, etc.
Regla de zona	Característica que permite la automatización de la asignación de dispositivos a zonas específicas en función de las direcciones IP, el sistema operativo y los nombres de dispositivo

APÉNDICE B: ADMINISTRACIÓN DE EXCEPCIONES

Hay momentos en que los usuarios deben poner *en cuarentena* o *permitir* (*eximir*) un archivo de forma manual. Threat Defense proporciona formas de manejar las excepciones para cada dispositivo (*Local*), para un grupo de dispositivos (*Política*) o para toda la organización (*Global*).

Archivos

Local: pone *en cuarentena* o *exim*e (*Lista segura*) un archivo en el dispositivo. Resulta útil para *bloquear* o *permitir* un archivo temporalmente hasta que haya tiempo de analizarlo. *Eximir* un archivo en un dispositivo también resulta útil si dicho dispositivo es el único dispositivo en el que se puede *ejecutar* el archivo. Dell recomienda el uso de *Política* o *Global* si esta acción debe realizarse en varios dispositivos.

Política: coloca un archivo en la *Lista segura* para todos los dispositivos asignados a una política. Útil para permitir un archivo para un grupo de dispositivos (por ejemplo, permitir que los dispositivos de TI ejecuten herramientas que podrían utilizarse con fines maliciosos, como PsExec). No está disponible la opción para poner un archivo *en cuarentena* a nivel de Política.

Global: pone *en cuarentena* o en la *lista segura* un archivo para la organización. Pone *en cuarentena* un archivo malicioso conocido en la organización. Pone en la *Lista segura* un archivo que es seguro y se utiliza en la organización, pero que el agente marca como malicioso.

Secuencias de comandos

Política: el control de secuencia de comandos permite aprobar la ejecución de secuencias de comandos desde una carpeta asignada. Permitir la ejecución de secuencias de comandos para una carpeta también permite secuencias de comandos en subcarpetas.

Certificados

Global: agregue certificados a la consola y, a continuación, a la *Lista segura* global. Esto permite que las aplicaciones firmadas por este certificado se ejecuten en la organización.

Para agregar un certificado, seleccione **Configuración > Certificados** y, a continuación, haga clic en **Agregar certificado**.

Para agregar el certificado a la ***Lista segura global***, seleccione **Configuración > Lista global**, seleccione la pestaña **Segura**, seleccione la pestaña **Certificados** y, a continuación, haga clic en **Agregar certificado**.

APÉNDICE C: PERMISOS DE USUARIO

Las acciones que pueden realizar los usuarios depende del permiso de usuario (rol) que se les haya asignado. En general, los administradores pueden realizar acciones en cualquier sitio de la organización. Los usuarios y administradores de zonas están restringidos a las zonas que les han sido asignadas. Esta restricción incluye solo poder acceder a dispositivos de una zona, y solo ver datos de amenazas relacionados con dichos dispositivos. Si un administrador de zonas o usuario no puede ver un dispositivo o una amenaza, existen probabilidades de que el dispositivo no pertenezca a las zonas que le han sido asignadas.

	USUARIO	ADMINISTRADOR DE ZONAS	ADMIN
Actualización del agente			
Ver/Editar			X
Registro de auditoría			
Ver			X
Dispositivos			
Agregar dispositivos: global			X
Agregar dispositivos a una zona			X
Eliminar dispositivos: global			X
Eliminar dispositivos de una zona		X	X
Editar nombre de dispositivo		X	X
Zonas			
Crear zona			X
Eliminar zona			X
Editar nombre de zona – Cualquiera			X
Editar nombre de zona asignada		X	X
Política			
Crear política: global			X
Crear política para una zona			X
Agregar política: global			X
Agregar política a una zona		X	X
Eliminar política: global			X
Eliminar política de una zona		X	X
Amenazas			
Poner en cuarentena archivos: global			X
Poner en cuarentena archivos de una zona	X	X	X
Eximir archivos: global			X
Eximir archivos de una zona	X	X	X
Cuarentena global/segura			X
Configuración			
Generar o eliminar señal de instalación			X
Generar o eliminar URL de invitación			X
Copiar señal de instalación	X	X	X
Copiar URL de invitación			X
Administración de usuarios			
Asignar usuarios a cualquier zona			X
Asignar usuarios a zona administrada		X	X
Asignar administrador de zonas: global			X
Asignar administrador de zonas a zonas administradas		X	X
Eliminar usuarios de la consola			X
Eliminar usuarios de zona: global			X
Eliminar usuarios de zona administrada		X	X

APÉNDICE D: FILTRO DE ESCRITURA BASADO EN ARCHIVOS

Dell Threat Defense Agent puede instalarse en un sistema con Windows Embedded Standard 7 (cliente ligero). En los dispositivos integrados, la escritura en el almacenamiento del sistema podría no estar permitida. En este caso, puede que el sistema utilice un filtro de escritura basado en archivos (FBWF) que desvíe todas las escrituras en el almacenamiento del sistema a la memoria caché del sistema. Esto podría provocar que el agente pierda los cambios cada vez que el sistema se reinicie.

Si utiliza el agente en un sistema integrado, siga este procedimiento:

1. Antes de instalar el agente, desactive FBWF mediante el comando: `Fbwfmgr /disable`.
2. Reinicie el sistema. De este modo permitirá que la desactivación de FBWF surta efecto.
3. Instale Dell Threat Defense Agent.
4. Después de instalar el agente, vuelva a habilitar FBWF utilizando el comando: `Fbwfmgr /enable`.
5. Reinicie el sistema. De este modo, la activación FBWF surtirá efecto.
6. En FBWF, excluya las siguientes carpetas:
    a. C:\Program Files\Cylance\Desktop: al excluir esta carpeta, las actualizaciones del agente se mantienen tras el reinicio del sistema.
7. Utilice el siguiente comando para excluir la carpeta del escritorio: `fbwfmgr /addexclusion C: "\Program Files\Cylance\Desktop\"`
    a. El sistema asume que va a instalar en el directorio predeterminado. Cambie la exclusión a la carpeta en la que ha instalado el agente.
8. Si tiene pensado para almacenar las amenazas en el equipo para realizar pruebas con el agente, asegúrese de que también excluye la ubicación de almacenamiento de FBWF (`C:\Samples`, por ejemplo).