Dell Endpoint Security Suite Enterprise

Advanced Threat Prevention Quick Start Guide v3.9

January 2024
Rev. A01

DELL Technologies

Notas, precauciones y advertencias

NOTA: NOTE indica información importante que lo ayuda a hacer un mejor uso de su producto.

PRECAUCIÓN: CAUTION indica la posibilidad de daños en el hardware o la pérdida de datos y le informa cómo evitar el problema.

AVISO: WARNING indica la posibilidad de daños en la propiedad, lesiones personales o la muerte.

Contents

1

Introduction

Before you perform tasks explained in this guide, the following components must be installed:

- Endpoint Security Suite Enterprise - refer to *Endpoint Security Suite Enterprise Advanced Installation Guide* or *Endpoint Security Suite Enterprise Basic Installation Guide*
- Security Management Server or Security Management Server Virtual Server - refer to *Security Management Server Installation and Migration Guide* or *Security Management Server Virtual Server Quick Start and Installation Guide*

This guide explains basic administration of Advanced Threat Prevention and should be used with *AdminHelp*, available in the Management Console.

Comuníquese con el equipo de Dell ProSupport for Software

Llame al 877-459-7304, extensión 4310039 para obtener soporte telefónico sobre su producto Dell 24 horas al día, 7 días a la semana.

De manera adicional, puede obtener soporte en línea para los productos Dell en dell.com/support. El soporte en línea incluye controladores, manuales, recomendaciones técnicas, P+F y posibles problemas.

Tenga su Código de servicio rápido o Etiqueta de servicio a mano cuando realice la llamada para asegúrese de ayudarnos a conectarle rápidamente con el experto técnico adecuado.

Para obtener los números de teléfono fuera de los Estados Unidos, consulte Números de teléfono internacionales de Dell ProSupport for Software.

2

Introducción

En este capítulo se detallan los pasos recomendados para comenzar a administrar Advanced Threat Prevention.

Los pasos recomendados para empezar a administrar Advanced Threat Prevention incluyen las siguientes fases:

- Aprovisionar un inquilino para Advanced Threat Prevention
  - Es necesario para implementar Advanced Threat Prevention
  - Las licencias de Advanced Threat Prevention deben estar presentes en el Dell Server
- Configuración de actualización automática del agente Advanced Threat Prevention
  - Inscribirse para recibir las actualizaciones automáticas de Advanced Threat Prevention (opcional)
  - Las actualizaciones se efectúan mensualmente
- Asignar o modificar roles de administrador
  - Aprovisionar o recuperar el servicio de Advanced Threat Prevention
  - Realizar copias de seguridad y descargar certificados existentes de Advanced Threat Prevention
  - Ver, modificar y confirmar las políticas
- Configurar notificaciones
  - Establecer las notificaciones por correo electrónico o mediante el tablero para recibir alertas de Advanced Threat Prevention (opcional)
  - Personalizar las notificaciones según las necesidades de su empresa

Aprovisionamiento de un inquilino

Debe aprovisionar un inquilino en Dell Server antes de que se active la aplicación de las políticas de Advanced Threat Prevention.

Requisitos previos

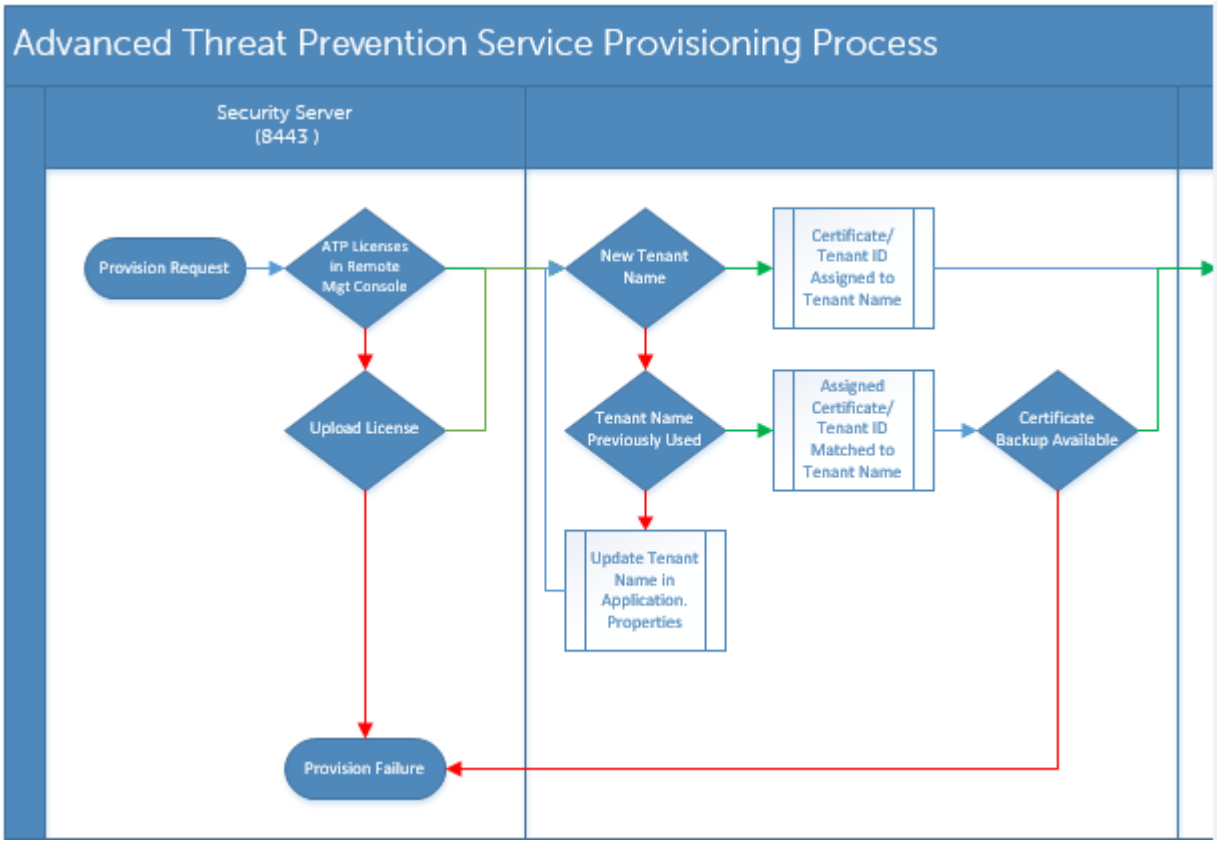
- Lo debe llevar a cabo el administrador con el rol de administrador del sistema.
- Debe tener conexión a Internet para el aprovisionamiento en Dell Server.
- Debe tener conexión a Internet en el cliente para mostrar la integración del servicio en línea de Advanced Threat Prevention en la consola de administración.
- El aprovisionamiento se basa en una señal generada a partir de un certificado durante el proceso de aprovisionamiento.
- Las licencias de Advanced Threat Prevention deben estar presentes en Dell Server.

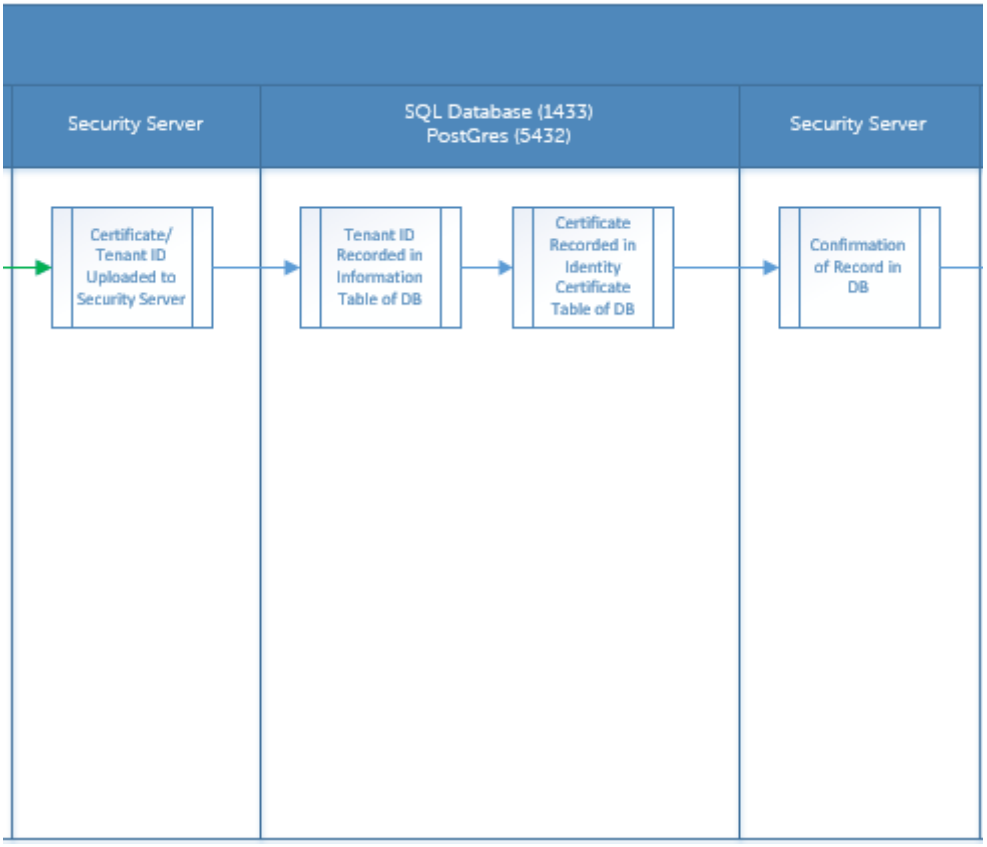
Aprovisionamiento de un inquilino

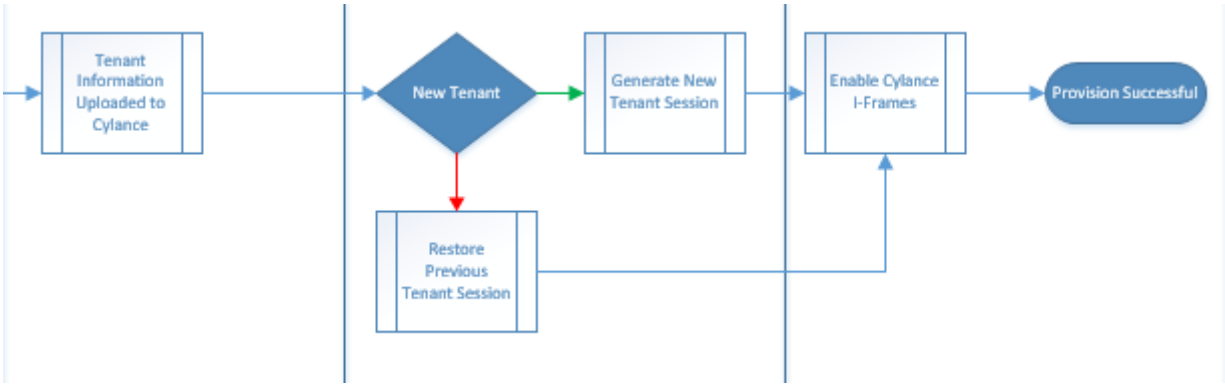
1. Como administrador de Dell, inicie sesión en la Consola de administración.
2. En el panel izquierdo de la consola de administración, haga clic en **Administración > Administración de servicios**.
3. Haga clic en **Configurar servicio Advanced Threat Protection**. Importe sus licencias Advanced Threat Prevention si se produce un error en este punto.
4. La configuración guiada inicia una vez que se han importado las licencias. Haga clic en **Siguiente** para empezar.
5. Lea y acepte el EULA y haga clic en **Siguiente**.
6. Proporcione las credenciales de identificación a Dell Server para aprovisionar el inquilino. Haga clic en **Siguiente**. *No se permite aprovisionar un inquilino existente con marca Cylance.*
7. Descargue el certificado. Esto es necesario para poder llevar a cabo una recuperación si se produce algún problema con Dell Server. No se realiza automáticamente una copia de seguridad de este certificado. Realice una copia de seguridad del certificado en una ubicación segura de otro equipo. Seleccione la casilla de verificación para confirmar que se realizó una copia de seguridad del certificado y haga clic en **Siguiente**.
8. La configuración ha terminado. Haga clic en **Aceptar**.

Comunicación de agentes y aprovisionamiento

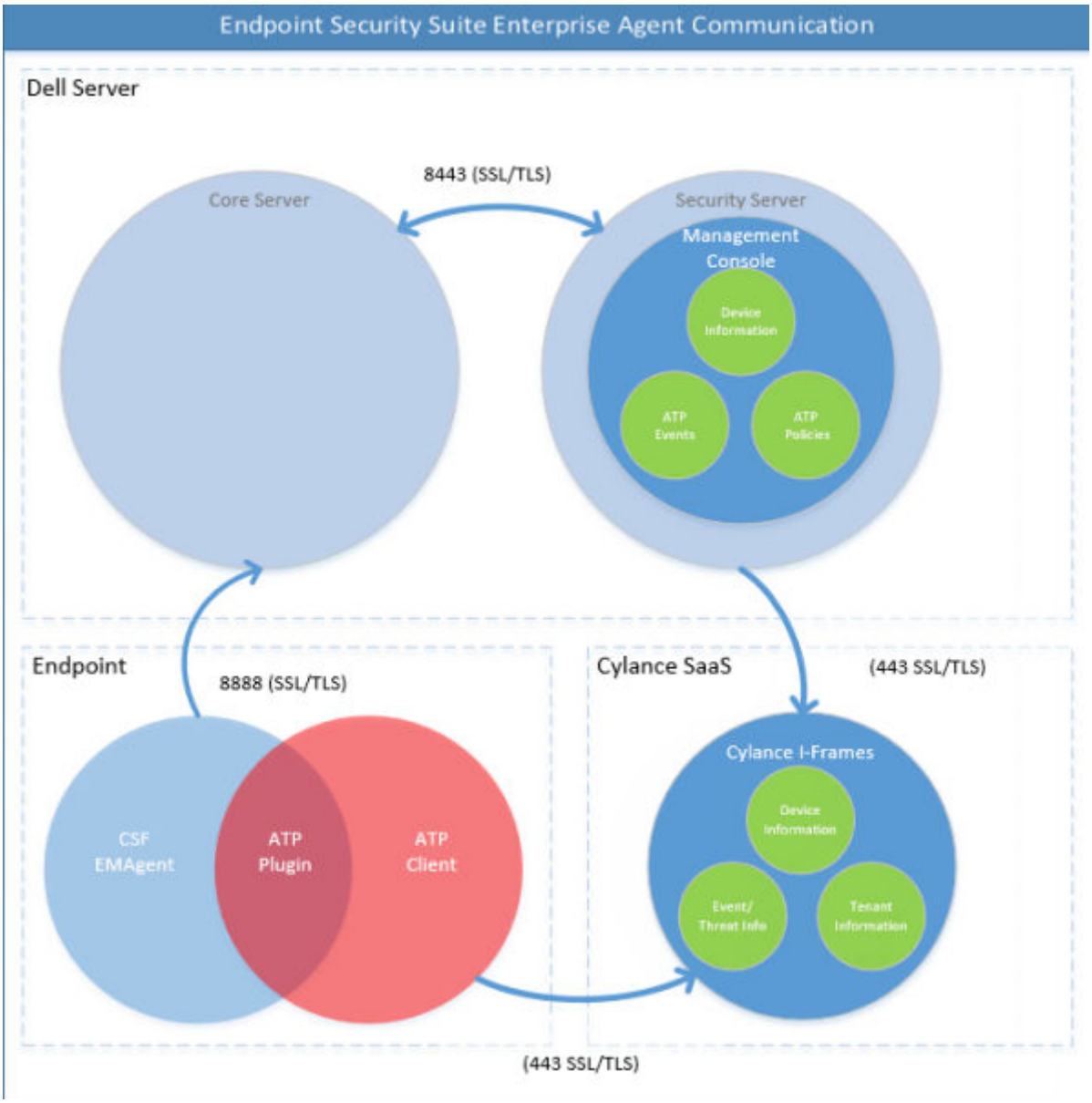
Los siguientes diagramas muestran el proceso de aprovisionamiento del servicio de Advanced Threat Prevention.



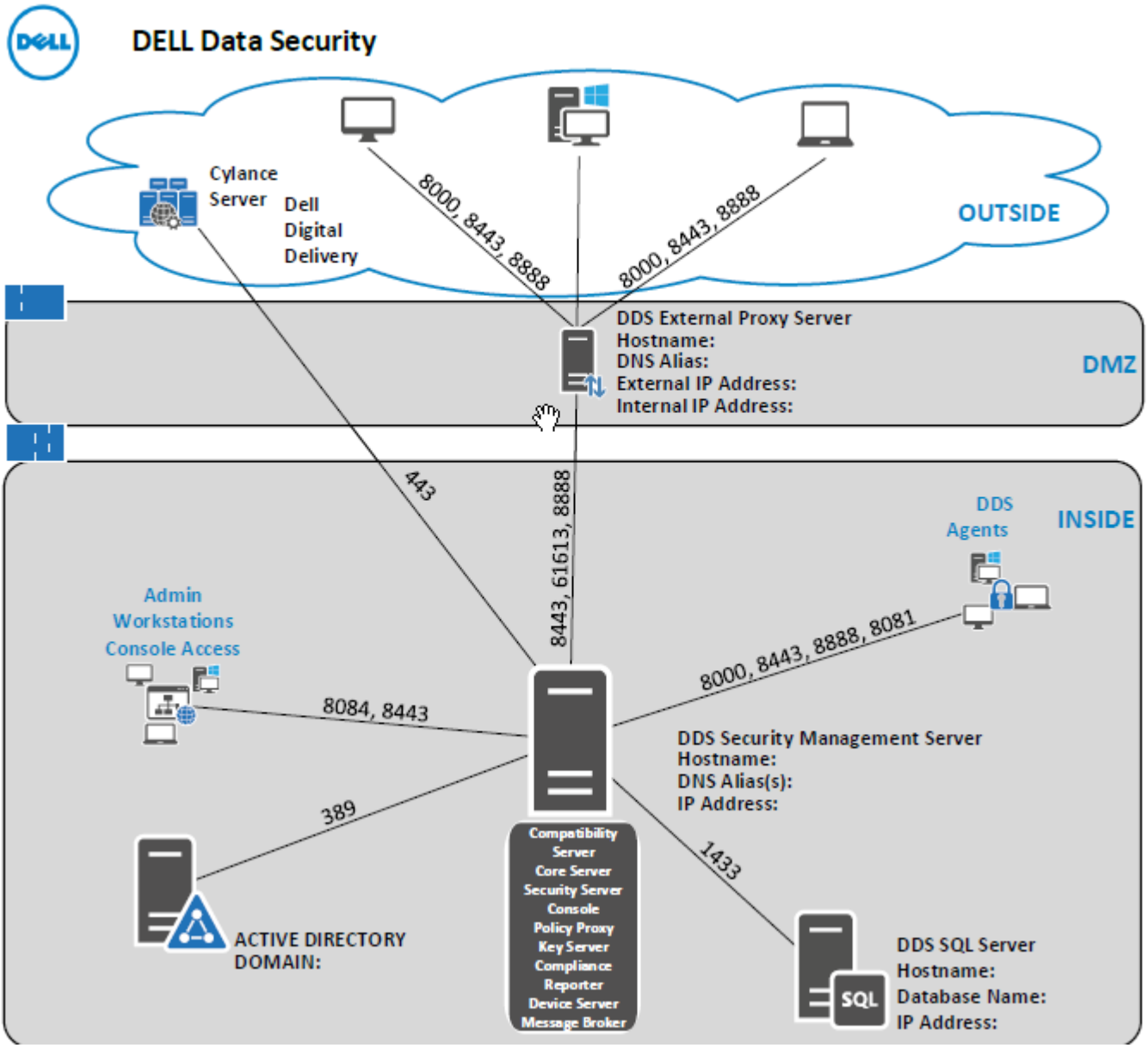




El siguiente diagrama muestra el proceso de comunicación de agentes de Advanced Threat Prevention.



El siguiente diagrama ilustra la arquitectura y la comunicación del servidor Dell.



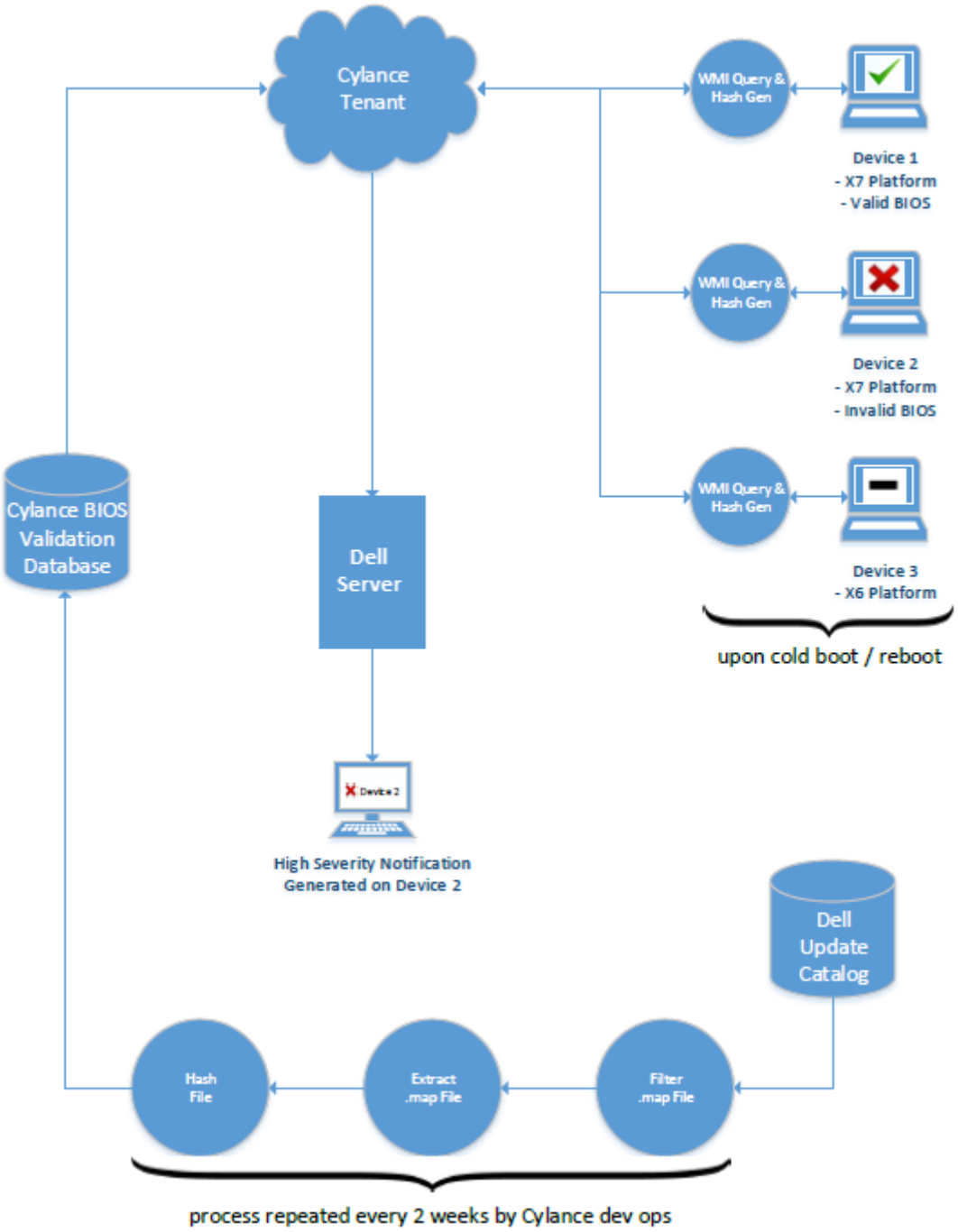
Activar la verificación de la integridad de la imagen del BIOS

La política de verificación de la integridad de la imagen del BIOS está activada de forma predeterminada cuando el conmutador principal para Advanced Threat Prevention está activado.

Para obtener una descripción general del proceso de verificación de la integridad de la imagen del BIOS, consulte Proceso de verificación de la integridad de la imagen del BIOS.

Proceso de verificación

El siguiente diagrama muestra el proceso de verificación de la imagen del BIOS.



Si la política *Habilitar la garantía de BIOS* se selecciona en la consola de administración, el grupo de usuarios de Cylance valida un hash del BIOS en computadoras de terminales para asegurarse de que el BIOS no ha sido modificado desde la versión de fábrica de Dell, que es un posible vector de ataque. Si se detecta una amenaza, se pasa una notificación al Dell Server y el administrador de TI recibe un mensaje de alerta en la Remote Management Console. Para obtener una descripción general del proceso, consulte Proceso de verificación de la integridad de la imagen del BIOS.

NOTA: Con esta función, no se puede usar una imagen de fábrica personalizada, ya que BIOS se ha modificado.

Modelos de equipos de Dell compatibles con la verificación de la integridad de la imagen del BIOS	
• Latitude 3470 • Latitude 3570 • Latitude 7275 • Latitude 7370	• OptiPlex 5040 • OptiPlex 7040 • OptiPlex 7440 • Estación de trabajo Precision 3510

Modelos de equipos de Dell compatibles con la verificación de la integridad de la imagen del BIOS		
• Latitude E5270 • Latitude E5470 • Latitude E5570 • Latitude E7270 • Latitude E7470 • Latitude Rugged 5414 • Latitude Rugged 7214 Extreme • Latitude Rugged 7414 • OptiPlex 3040 • OptiPlex 3240	• Estación de trabajo Precision 5510 • Estación de trabajo Precision 3620 • Estación de trabajo Precision 7510 • Estación de trabajo Precision 7710 • Estación de trabajo Precision T3420 • Venue 10 pro 5056 • Venue Pro 5855 • Venue XPS 12 9250 • XPS 13 9350 • XPS 9550	

Configuración de actualización automática del agente Advanced Threat Prevention

En la consola de administración, puede inscribirse para recibir actualizaciones automáticas del agente Advanced Threat Prevention. La inscripción para recibir las actualizaciones automáticas del agente permite a los clientes descargar y aplicar automáticamente las actualizaciones desde el servicio de Advanced Threat Prevention. Las actualizaciones se efectúan mensualmente.

NOTA:

Las actualizaciones automáticas del agente son compatibles con Dell Server v9.4.1 o posterior.

Cómo recibir actualizaciones automáticas del agente

Para inscribirse y recibir actualizaciones automáticas del agente:

1. En el panel izquierdo de la consola de administración, haga clic en **Administración** > **Administración de servicios**.
2. En la pestaña *Amenazas avanzadas*, en *Actualización automática del agente*, haga clic en **Activar** y, a continuación, en **Guardar preferencias**.

   Es posible que se tarde unos minutos en rellenar la información y mostrar las actualizaciones automáticas.

Cómo dejar de recibir actualizaciones automáticas del agente

Para dejar de recibir actualizaciones automáticas del agente:

1. En el panel izquierdo de la consola de administración, haga clic en **Administración** > **Administración de servicios**.
2. En la pestaña *Amenazas avanzadas*, en *Actualización automática del agente*, haga clic en **Desactivar** y, a continuación, en **Guardar preferencias**.

Asignar o modificar roles de administrador

Ver o modificar los privilegios de administrador existentes desde la página Administradores en la consola de administración.

Roles de administrador

El inicio de sesión de administrador se integra en Active Directory para simplificar el proceso de control de los administradores y aprovechar la infraestructura de autenticación de usuarios existente. Los administradores reciben funciones que definen el nivel de acceso que se otorga a cada administrador. Por ejemplo, algunos administradores solo tienen permiso para implementar una recuperación asistida por soporte técnico, mientras que otros tienen acceso completo para modificar las políticas de seguridad. Es posible asignar roles de administrador a grupos de Active Directory para poder modificar con facilidad el nivel de acceso de administrador de los usuarios con una simple modificación en la pertenencia del grupo de AD. Los usuarios que no pertenecen al dominio pueden recibir permisos de acceso solo para elaboración de informes mediante Compliance Reporter.

Se requiere la función de administrador del sistema para realizar las siguientes tareas:

- Aprovisionar o recuperar el servicio de Advanced Threat Prevention
- Inscribirse para recibir las actualizaciones automáticas de Advanced Threat Prevention
- Establecer las notificaciones por correo electrónico o mediante el tablero para recibir alertas de Advanced Threat Prevention

- Realizar copias de seguridad y descargar certificados existentes de Advanced Threat Prevention

NOTA: Se requiere el rol de administrador de seguridad para ver, modificar o confirmar políticas.

Para ver o modificar los privilegios de administrador existentes, siga estos pasos:

1. En el panel izquierdo, haga clic en **Poblaciones> Administradores**.
2. Busque o seleccione la fila que muestra el nombre de usuario del administrador correspondiente para mostrar detalles del usuario.
3. Consulte o modifique roles de administrador en el panel de la derecha.
4. Haga clic en **Guardar**.

NOTA: Dell recomienda asignar funciones de administrador en el nivel de grupo en lugar de en el nivel de usuario.

Para ver, asignar o modificar funciones de administrador en el nivel de grupo, siga estos pasos:

1. En el panel izquierdo, haga clic en **Poblaciones > Grupos de usuarios**.
2. Busque o seleccione un nombre de grupo y, a continuación, seleccione la pestaña **Admin**. Aparece la página Detalles del grupo de usuarios.
3. Seleccione o anule la selección de funciones de administrador asignados al grupo.
4. Haga clic en **Guardar**.

Si quita un grupo con privilegios administrativos y después vuelve a agregar el grupo, sigue siendo un grupo de administrador.

Para ver, asignar o modificar roles de administrador en el nivel de usuarios, siga estos pasos:

1. En el panel izquierdo, haga clic en **Poblaciones > Usuarios**.
2. Busque o seleccione un nombre de usuario y, a continuación, la pestaña Admin.
3. Seleccione o anule la selección de funciones de administrador asignados al usuario.
4. Haga clic en **Guardar**.

Roles de administrador: asigne o modifique roles para el usuario y haga clic en **Guardar**.

Funciones de grupo heredadas: una lista de solo lectura de roles que el usuario heredó de un grupo. Para modificar los roles, haga clic en la pestaña **Grupos de usuarios** de ese usuario y seleccione el nombre de grupo.

Funciones designadas: delegue derechos de administrador a un usuario.

Configurar notificaciones

En la Remote Management Console, se puede inscribir para recibir notificaciones. La lista Notificaciones proporciona un resumen configurable de noticias, alertas y eventos para mostrar en el Panel o para enviarse como notificaciones de correo electrónico.

Tipos de notificaciones

Puede seleccionar los tipos de notificación para incluir en la lista. Las notificaciones de los demás tipos permanecen ocultas. Notificaciones de **Protección frente a amenazas** y **Eventos de amenazas avanzadas** relacionadas con las Advanced Threat Prevention.

Los tipos son:

- **Actualización**: novedades de las próximas actualizaciones del producto. Para visualizar y recibir actualizaciones de productos, debe subscribirse para recibirlas. Seleccione **Administración de servicios > Notificaciones del producto**, haga clic en **Activado** y, a continuación, en **Guardar preferencias**.
- **Config.**: novedades sobre los cambios de configuración.
- **Base de conocimientos**: resúmenes y vínculos a artículos de la base de conocimientos con información técnica detallada, como por ejemplo soluciones provisionales y métodos de configuración.
- **Anuncio**: novedades de las próximas versiones y los nuevos productos.
- **Licencia**: alertas para cuando la disponibilidad de la licencia del volumen sea baja o cuando se haya superado el recuento de licencias de acceso del cliente.
- **Threat Protection**: una alerta de amenaza de Advanced Threat Prevention.
- **Evento de amenaza avanzado**: un evento detectado por Advanced Threat Prevention. El resumen contiene una lista de eventos de tipo Crítico, Grave, Leve, Aviso o Información, con vínculos a información más detallada.
- **Evento de amenaza**: un evento detectado por Threat Protection.
- **Certificado**: notificación de caducidad del certificado.
- **Excepciones del servidor Dell**: un problema de comunicación del servidor Dell está afectando las entregas de las siguientes notificaciones: Threat Protection, actualización, configuración, base de conocimientos y anuncio.

Después de seleccionar uno o más tipos, haga clic en el espacio neutral situado sobre la lista desplegable para aplicar las selecciones.

Seleccione **Borrar elementos seleccionados** para restablecer las selecciones de esta lista.

Niveles de prioridad

NOTA: Los niveles de prioridad de notificación no están relacionados con los niveles de prioridad mostrados en el tablero que no sea el del área de notificaciones.

Las prioridades son Crítica, Alta, Media y Baja. Estos niveles de prioridad están relacionados entre sí dentro de un tipo de notificación.

Puede seleccionar los niveles de prioridad de las notificaciones para incluir en el área de notificaciones del tablero o de las listas de notificaciones por correo electrónico. Las notificaciones de los niveles de prioridad restantes no están incluidas en el tablero ni en las listas de notificaciones de correo electrónico.

Seleccione **Borrar elementos seleccionados** para restablecer las selecciones de esta lista. Aparecerán todas las notificaciones (a menos que se hayan filtrado en otro sitio).

3

Políticas

En este capítulo se detalla la administración de políticas de Advanced Threat Prevention.

- Habilitar Advanced Threat Prevention
- Configuración de la política recomendada
- Confirmar modificaciones de la política

Para ver una lista con todas las políticas de Advanced Threat Prevention y sus correspondientes descripciones, consulte *AdminHelp*, disponible en la consola de administración.

Habilitar Advanced Threat Prevention

La política de Advanced Threat Prevention se **apaga** de manera predeterminada y se debe **encender** para las políticas activadas de Advanced Threat Prevention. Las políticas de Advanced Threat Prevention se aplican en los niveles de empresa, grupos de extremos y extremos.

Para activar la política de Advanced Threat Prevention a nivel de empresa, siga estos pasos:

1. En el panel izquierdo, haga clic en **Poblaciones > Empresa**.
2. Haga clic en **Threat Prevention**.
3. Cambie el conmutador maestro Advanced Threat Prevention de **Apagado** a **Encendido**.

Para activar la política de Advanced Threat Prevention a nivel de grupos de extremos, siga estos pasos:

1. En el panel izquierdo, haga clic en **Poblaciones > Grupo de extremos**.
2. Haga clic en **Threat Prevention**.
3. Cambie el conmutador maestro Advanced Threat Prevention de **Apagado** a **Encendido**.

Para activar la política de Advanced Threat Prevention a nivel de extremos, siga estos pasos:

1. En el panel izquierdo, haga clic en **Poblaciones > Extremos**.
2. Haga clic en **Threat Prevention**.
3. Cambie el conmutador maestro Advanced Threat Prevention de **Apagado** a **Encendido**.

Configuración de la política recomendada

- Para obtener la lista más reciente de la configuración de la política recomendada, consulte el siguiente artículo de la base de conocimientos: SLN301562.

Confirmar modificaciones de la política

Para confirmar las políticas que se modificaron y guardaron:

1. En el panel izquierdo de la consola de administración, haga clic en **Administración > Confirmar**.
2. En Comentarios, ingrese una descripción del cambio.
3. Haga clic en **Confirmar políticas**.

Una política se confirma o publica cuando un administrador hace clic en **Confirmar políticas**. Se muestra la siguiente información:

- Cambios pendientes en las políticas: número de cambios en las políticas listos para confirmar.
- Fecha confirmada: hora y fecha en que se confirmaron las políticas.
- Cambiado por: nombre de usuario del administrador que llevó a cabo la confirmación de la política.
- Comentario: comentarios que se agregaron cuando se confirmaron las políticas.
- Versión: número de veces que se ha guardado la política desde la última confirmación de la política, más la versión anterior.

4

Amenazas

En este capítulo se explica cómo identificar y administrar las amenazas que se hayan encontrado en un entorno empresarial después de la instalación de Advanced Threat Prevention.

- Identificar una amenaza
  - Ver eventos de amenazas
  - Actualizaciones de puntuación de Cylance y del modelo de amenazas
  - Ver datos detallados de la amenaza
- Administrar una amenaza
  - Exportar datos sobre amenazas a formato CSV
  - Administrar la lista de cuarentena global

Identificar una amenaza

Notificaciones por correo electrónico y panel

Si configuró las notificaciones por correo electrónico para Threat Protection y eventos de amenazas avanzadas, se notifica al administrador por correo electrónico de los eventos y las amenazas de Advanced Threat Prevention.

El resumen de notificaciones del tablero en la consola de administración muestra las amenazas y los eventos de Advanced Threat Prevention, como tipos de notificaciones de eventos de protección contra amenazas y eventos de amenazas avanzadas.

- Tipo de Threat Protection: alerta de amenaza de Advanced Threat Prevention.
- Tipo de evento de amenaza avanzada: evento detectado por Advanced Threat Prevention. Un evento no necesariamente es una amenaza.

En la siguiente tabla, se detallan las etiquetas de amenazas, la gravedad y la información de la amenaza.

Etiqueta	Gravedad	Detalle
Amenaza encontrada	Crítico	Indica que en un dispositivo se identificó un ejecutable portátil (PE), pero que no se bloqueó ni se puso en cuarentena en el terminal, lo cual indica una amenaza activa en el sistema.
Amenaza bloqueada	Aviso	Indica que en un dispositivo se identificó un ejecutable portátil y se bloqueó su ejecución. Esta amenaza no se puso en cuarentena específicamente y es probable que se deba a que no se activó la política de cuarentena automática o que el archivo está en una ubicación en la que no se puede escribir en este con la cuenta del SISTEMA local (recurso compartido de red, dispositivo USB que se desconectó, etc.).
Amenaza eliminada	Aviso	Indica que en un dispositivo se identificó un ejecutable portátil (PE) y el proceso se eliminó, ya que se detectó en ejecución activa. Esto no permite indicar que el archivo se puso en cuarentena también, ya que el PE se podría haber ejecutado desde otra ubicación. Se recomienda buscar otro evento relacionado con este terminal y el ejecutable para validar que la amenaza se contuvo correctamente.
Trasgresión bloqueada de la memoria	Aviso	Indica que se intentó ejecutar un archivo ejecutable o un script, pero que estaba en infracción con la política de protección de la memoria o de control de scripts. Luego, se bloqueó la ejecución del archivo ejecutable o del script. Normalmente, esto indica que la política descrita de protección de la memoria o de control de scripts se estableció en Bloquear.

Etiqueta	Gravedad	Detalle
Transgresión eliminada de la memoria	Aviso	Indica que se detectó un archivo ejecutable o un script que estaba activamente en ejecución y en trasgresión con la política de protección de la memoria o de control de scripts. Luego, se eliminó el archivo ejecutable o el script. Normalmente, esto indica que la política descrita de protección de la memoria o de control de scripts se estableció en Eliminar.
Trasgresión de la memoria	Aviso	Indica que se encontró un archivo ejecutable o un script que estaba en trasgresión con la política de protección de la memoria o de control de scripts. No se tomó ninguna acción contra el archivo ejecutable o el script, probablemente debido a que la política se estableció en Permitir.
Amenaza borrada	Información	Indica que un ejecutable portátil (PE) que anteriormente estaba marcado y que se consideraba una amenaza, se borró del terminal. Esto podría indicar que el PE se borró de la cuarentena o de la ubicación inicial. Esto es común con los PE que se detectaron inicialmente en medios extraíbles (USB, CD-ROM, etc.)
Amenaza en cuarentena	Información	Indica que se determinó que un portable ejecutable (PE) es una amenaza potencial y, luego, se puso correctamente en cuarentena. Esto indica que la política para poner amenazas automáticamente en cuarentena basadas en la clasificación Anormal (puntuación de Cylance de 0 a 60) o Insegura (puntuación de Cylance de 60 a 100) está activa.
Amenaza eximida	Información	Indica que un portable ejecutable (PE) que se determinó que es una amenaza potencial, se eximió según la lista segura global o mediante una exención local. Esto también puede indicar que el hash SHA256 se agregó a las políticas "Eximir" o "Lista segura global" dentro de Dell Security Management Server.
Cambio de puntaje de amenaza	Información	Indica cuando cambia la puntuación de Cylance de un ejecutable portátil (PE). Por lo general, esto sucede debido al puntaje en dos pasos que realiza Cylance. Puede que el análisis del motor de puntuación local de la amenaza no coincida con el análisis del motor en la nube de Cylance. En estos casos, debido a los datos adicionales que tiene el motor en la nube de Cylance, se utiliza el puntaje que se deriva del motor en la nube de Cylance. Esto también puede indicar que una actualización de Cylance inició un nuevo análisis de los archivos que anteriormente se consideraron amenazas y que se calculó una puntuación nueva que determinó que este PE ya no se considere una amenaza.
Cambio de estado de protección	Información	Indica que se cambió cualquier estado de protección del terminal. Esto se activa cuando el agente de Dell Encryption Management se vuelve a conectar a los servicios de Cylance a través de los complementos de Cylance. Esto suele activarse cuando se reinicia un terminal, ya que hay un breve período en que puede que CSF no se haya conectado a los complementos de Cylance durante el arranque.

Haga clic en una notificación para obtener más detalles. En el resumen se incluyen vínculos a un detalle adicional de los eventos o amenazas.

Pestaña Amenazas avanzadas

En la pestaña Amenazas avanzadas proporciona una visualización dinámica de información detallada sobre eventos para toda la empresa, incluida una lista de los dispositivos en los que se han producido eventos y las acciones emprendidas en estos dispositivos para dichos eventos.

Para acceder a la pestaña Amenazas avanzadas de Enterprise, siga estos pasos:

1. En el panel izquierdo, haga clic en **Poblaciones > Empresa**.

2. Seleccione la pestaña **Amenazas avanzadas**.

La información sobre eventos, dispositivos y acciones se organiza en las siguientes pestañas:

- **Protección**: muestra los archivos y las secuencias posiblemente perjudiciales y los detalles respectivos, incluidos los dispositivos en los que se encuentran los archivos y las secuencias de comandos.
- **Agentes:** proporciona información acerca de los dispositivos que ejecutan el cliente de Advanced Threat Prevention, así como la opción para exportar la información o quitar dispositivos de la lista.
- **Lista global**: muestra los archivos en Cuarentena global y en Lista de seguridad y ofrece la opción de mover archivos a estas listas.
- **Opciones**: permite integrarse con el software de Security Information Event Management (SIEM).
- **Certificado**: permite cargar certificados. Tras la carga, los certificados se mostrarán en la pestaña Lista global y se pueden poner en la lista Segura.

Las tablas de las pestañas se pueden organizar de la siguiente manera:

- Agregar o quitar columnas de la tabla: haga clic en la flecha situada junto a cualquier encabezado de columna, seleccione **Columnas** y seleccione las columnas que desea ver. Desactive la casilla de verificación de las columnas que desea ocultar.
- Ordenar los datos: haga clic en un encabezado de columna.
- Agrupar por columna: arrastre el encabezado de la columna hacia arriba hasta que se vuelva de color verde.

Pestaña Eventos de amenazas avanzados

La pestaña Eventos de amenaza avanzados muestra información sobre eventos para toda la empresa basándose en la información disponible en el Dell Server.

La pestaña muestra si el servicio Advanced Threat Prevention está aprovisionado y si las licencias están disponibles.

Para exportar datos desde la pestaña de eventos de amenazas avanzadas, haga clic en el botón **Exportar** y seleccione el formato de archivo **Excel** o **CSV**.

NOTA: Los archivos de Excel se limitan a 65.000 filas. CSV no tiene límite de tamaño.

Actualizaciones de puntuación de Cylance y del modelo de amenazas

Se asigna una puntuación de Cylance a cada archivo que se considere 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.

El modelo predictivo de amenazas que se utiliza para proteger los dispositivos recibe actualizaciones periódicas para mejorar las tasas de detección.

Dos columnas de la página Protección en la consola de administración muestran cómo un nuevo modelo de amenazas puede afectar a su organización. Visualice y compare las columnas Estado de producción y Estado nuevo para ver los archivos de los dispositivos que pueden verse afectados por un cambio de modelo.

Para ver las columnas Estado de producción y Estado nuevo:

1. En el panel izquierdo, haga clic en **Poblaciones > Empresa**.
2. Seleccione la pestaña **Amenazas avanzadas**.
3. Haga clic en la pestaña **Protección**.
4. Haga clic en la flecha hacia abajo en un encabezado de columna de la tabla.
5. Coloque el puntero sobre **Columnas**.
6. Seleccione las columnas **Estado de producción** y **Estado nuevo**.

Estado de producción: estado del modelo actual (Seguro, Anómalo o No seguro) para el archivo.

Estado nuevo: estado del modelo del archivo en el nuevo modelo.

Por ejemplo, un archivo que se considera Seguro en el modelo actual podría cambiar a No seguro en el nuevo modelo. Si su organización necesita ese archivo, puede agregarlo a la lista Seguro. Un archivo que nunca se haya visto o que no haya sido puntuado por el modelo actual, el nuevo modelo podría considerarlo No seguro. Si su organización necesita ese archivo, puede agregarlo a la lista Seguro.

Solo se muestran los archivos que se encuentran en el dispositivo de su organización y que tienen un cambio en la puntuación de Cylance. Algunos archivos pueden sufrir un cambio en la puntuación, pero aún así mantienen su estado actual. Por ejemplo, si la puntuación de Cylance de un archivo va de 10 a 20, el estado del archivo puede permanecer como Anómalo y el archivo se muestra en la lista actualizada de modelos (si este archivo existe en los dispositivos de su organización).

Comparar modelo actual con modelo nuevo

Puede revisar las diferencias entre el modelo actual y el nuevo modelo.

Debería tener en cuenta dos escenarios:

Estado de producción = Seguro, Estado nuevo = Anómalo o No seguro

- Su empresa considera el archivo como Seguro
- Su organización ha definido Anómalo o No seguro en Cuarentena automática

En las situaciones descritas anteriormente, la recomendación es incluir en la lista de seguridad los archivos que desea permitir en su organización.

Identificar clasificaciones

Para identificar las clasificaciones que pueden influir en su organización, Dell recomienda el siguiente enfoque:

1. Aplicar un filtro a la columna Estado nuevo para mostrar todos los archivos con los estados Seguro, Anómalo y Cuarentena.
2. Aplicar un filtro a la columna Estado de producción para mostrar todos los archivos con el estado Seguro.
3. Aplicar un filtro a la columna Clasificación para mostrar solo las amenazas locales de confianza.

Confianza: Cylance ha analizado los archivos locales y son seguros. Incluya estos elementos en la lista de seguridad tras su revisión. Si tiene muchos archivos en la lista filtrada, es posible que deba darle prioridad con más atributos. Por ejemplo, agregue un filtro a la columna Detectado por para revisar las amenazas halladas por Control de ejecución. Estas amenazas fueron consideradas como tal cuando un usuario intentó ejecutar una aplicación y necesitó atención más urgente que los archivos inactivos condenados por Detección de amenazas en segundo plano o Monitor de archivos.

La información para la comparación de modelos proviene de la base de datos, no de sus dispositivos. Así que no se hace un nuevo análisis para la comparación de modelos. No obstante, cuando un nuevo modelo está disponible y se instala el Agent correcto, se efectúa un nuevo análisis en la organización y se aplican los cambios del modelo.

Consulte *AdminHelp* para obtener más información.

Ver eventos de protección Web y del servidor de seguridad

Las amenazas se categorizan como malware/vulnerabilidad de la seguridad, filtro web, servidor de seguridad o eventos sin clasificar. La lista de eventos de amenaza puede clasificarse por cualquiera de encabezados de columna. Puede ver eventos de amenaza para la empresa completa o para un extremo específico. Para ver eventos de amenaza de un terminal específico, en la pestaña Eventos de amenaza de empresa, seleccione el dispositivo en la columna Id. del dispositivo.

Para ver eventos de amenaza en la empresa, siga estos pasos:

1. En el panel izquierdo, haga clic en **Poblaciones > Empresa**.
2. Haga clic en la pestaña **Eventos de amenaza**.
3. Seleccione el nivel de gravedad deseado y el período de tiempo para el que se mostrarán eventos.

Para ver amenazas en un extremo específico, siga estos pasos:

1. En el panel izquierdo, haga clic en **Poblaciones > Extremos**.
2. Busque o seleccione un nombre de host y haga clic en la pestaña **Eventos de amenaza**.

Administrar una amenaza

Puede poner en cuarentena, hacer una lista de seguridad, omitir y exportar amenazas.

Realizar las siguientes acciones a nivel empresarial:

- Exportar una amenaza o secuencia de comandos que desencadenó una alerta
- Poner en cuarentena una amenaza
- Hacer una lista de seguridad de una amenaza
- Editar manualmente la lista global

Para administrar una amenaza identificada a nivel empresarial:

1. En el panel izquierdo, haga clic en **Poblaciones > Empresa**.
2. Seleccione la pestaña **Amenazas avanzadas**.
3. Seleccione Protection.

En la tabla de control de secuencias de comandos, puede exportar una secuencia de comandos que se muestra en la tabla como una posible amenaza.

Administrar amenazas avanzadas de Enterprise

La pestaña Protección proporciona información acerca de los archivos y secuencias de comandos que son potencialmente peligrosos.

Tabla de amenazas

En la tabla de amenazas, puede exportar, poner en cuarentena o hacer una lista de seguridad de amenazas. También puede agregar manualmente una amenaza a la lista de cuarentena global.

En la tabla se enumeran todos los eventos que se han encontrado en la organización. Un evento también puede ser una amenaza pero no lo es necesariamente.

Para ver información adicional sobre una amenaza específica, haga clic en el vínculo del nombre de amenaza para ver los detalles en una nueva página o haga clic en cualquier sitio de la fila de la amenaza para ver los detalles en la parte inferior de la página.

Para ver más información sobre las amenazas de la tabla, haga clic en la flecha desplegable en un encabezado de columna para seleccionar y agregar columnas. Las columnas muestran los metadatos relacionados con el archivo, como clasificaciones, puntuación de Cylance (nivel de confianza), convicción de la industria de AV (vínculos a VirusTotal.com para su comparación con otros proveedores), fecha de primera detección, SHA256, MD5, información del archivo (autor, descripción, versión) y detalles de la firma.

Comandos

- **Exportar**: exporte los datos de la amenaza a un archivo .CSV. Seleccione las filas que desea exportar y haga clic en **Exportar**.
- **Cuarentena global**: agregue un archivo a la lista de cuarentena global. La amenaza se pone permanentemente en cuarentena en todos los dispositivos.
- **Seguro**: agregue un archivo a la lista de seguridad. El archivo se trata permanentemente como seguro en todos los dispositivos.

  NOTA: En ocasiones, es posible que se informe de un “buen” archivo como no seguro (esto podría suceder si las características de este archivo coinciden en gran medida con las de los archivos maliciosos). La exención o la inclusión del archivo en la lista de seguridad puede ser útil en estos casos.

- **Editar lista global**: agregue o elimine archivos de la lista de cuarentena global.
- **Omitir**: agregue un archivo a la lista de omitidos en una computadora. Este archivo se puede ejecutar en la computadora.

Administrar amenazas avanzadas de Endpoint

Para administrar una amenaza identificada en una computadora específica:

1. En el panel izquierdo, haga clic en **Poblaciones > Empresa**.
2. Seleccione la pestaña **Amenazas avanzadas**.
3. Seleccione Agentes.
4. Seleccione un nombre específico de agente y seleccione el comando adecuado: **Exportar, poner en cuarentena** u **omitir** una amenaza.

5

Modo desconectado

El modo desconectado permite que un Dell Server gestione extremos de Advanced Threat Prevention sin conexión de cliente a Internet ni a una red externa. El modo desconectado también permite que el Dell Server administre sin conexión a Internet ni a un servicio de Advanced Threat Prevention aprovisionado y alojado. El Dell Server captura todos los eventos y datos de amenazas en Modo desconectado.

Para determinar si un Dell Server se está ejecutando en Modo desconectado, haga clic sobre el ícono con la imagen de un engranaje en la parte superior derecha de la Remote Management Console y seleccione "Acerca de". La pantalla "Acerca de" indica que un Dell Server se encuentra en Modo desconectado, debajo de la versión del Dell Server.

El Modo desconectado es distinto a la instalación conectada estándar de un Dell Server de las siguientes formas.

Activación del cliente

Un token de instalación se genera cuando el administrador carga una licencia de Advanced Threat Prevention, lo que permite que el cliente de Advanced Threat Prevention se active.

Consola de administración

Los siguientes elementos **no están disponibles** en la consola de administración cuando el Dell Server se ejecuta en Modo desconectado:

- Las siguientes áreas específicas de Advanced Threat Prevention: Amenazas avanzadas por prioridad, Eventos (amenazas avanzadas) por clasificación, diez principales Amenazas avanzadas y Eventos de Advanced Threat Prevention.
- En la pestaña **Empresa > Amenazas avanzadas** se muestra información detallada sobre eventos para toda la empresa, incluida una lista de los dispositivos en los que se han producido eventos, y las acciones emprendidas en estos dispositivos para dichos eventos.
- (Panel de navegación de la izquierda) Administración de servicios que permite la habilitación del servicio Advanced Threat Prevention y la inscripción en notificaciones del producto.

El siguiente elemento **está disponible** en la consola de administración para que sea compatible con el Modo desconectado:

- Pestaña **Empresa > Eventos de amenazas avanzados**, que muestra información sobre los eventos para toda la empresa basándose en la información disponible en el Dell Server, aun cuando funcione en Modo desconectado.

Funcionalidad

La siguiente funcionalidad no está disponible en la consola de administración cuando el Dell Server se ejecuta en Modo desconectado:

- Actualización y migración de Security Management Server
- Actualización automática de Security Management Server Virtual: la actualización se debe realizar de forma manual
- Actualizar perfiles en la nube
- Actualización automática de Advanced Threat Prevention
- Carga de archivos ejecutables No seguros o Anómalos para análisis de Advanced Threat Prevention
- Carga de archivo de Advanced Threat Prevention y de archivos de registro

La siguiente funcionalidad difiere:

- El Dell Server envía la lista de seguridad global, la lista de cuarentena y la lista de seguridad a los agentes.
- La lista de seguridad global se importa al Dell Server mediante la política Permisión global.
- La lista de cuarentena se importa al Dell Server mediante la política de la lista de cuarentena.
- La lista de seguridad se importa al Dell Server mediante la política Lista de seguridad.

Estas políticas están disponibles solo en modo desconectado. Para obtener más información sobre estas políticas, consulte *AdminHelp*, disponible en la Remote Management Console.

Para obtener más información sobre el Modo desconectado, consulte "Modo desconectado" en *AdminHelp*, disponible en la consola de administración.

Identificar y administrar las amenazas en modo desconectado

Para administrar las amenazas en modo desconectado, en primer lugar debe establecer las siguientes políticas de Advanced Threat Prevention que se aplican a su organización:

- Permisión global
- Lista de cuarentena
- Lista de seguridad

Estas políticas se envían al cliente de Advanced Threat Prevention, solamente si el Dell Server detecta un token de instalación en Modo desconectado, el cual tiene el prefijo "DELLAG".

Consulte *AdminHelp* para ver ejemplos de estas políticas.

Para ver los archivos que Advanced Threat Prevention identifica como las posibles amenazas, vaya a la pestaña **Empresa > Eventos de amenazas avanzadas**. Esta ficha contiene una lista de información de eventos para toda la empresa y la acción que se realiza, como Bloqueado o Finalizado.

6

Solución de problemas

Recuperar Advanced Threat Prevention

Servicio de recuperación

Necesitará su certificado, del que ha hecho una copia de seguridad, para recuperar el servicio de Advanced Threat Prevention.

1. En el panel izquierdo de la consola de administración, haga clic en **Administración > Administración de servicios**.
2. Haga clic en **Recuperar el servicio de Advanced Threat Prevention**.
3. Siga las indicaciones para la recuperación del servicio y cargue el certificado de Advanced Threat Prevention cuando se le indique.

Buscar el código del producto con Windows PowerShell

- Mediante este método, es muy sencillo identificar el código del producto si dicho código cambia más adelante.

  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT
  IdentifyingNumber, Name, LocalPackage
  ```

  La salida mostrará la ruta completa y el nombre del archivo .msi (el nombre convertido hexadecimal del archivo).

Advanced Threat Prevention

- Para que el complemento Advanced Threat Prevention supervise HKLM\SOFTWARE\Dell\Dell Data Protection para determinar si se han producido cambios en el valor de LogVerbosity, y actualizar el nivel de registro de cliente según corresponda, defina el siguiente valor.

  [HKLM\SOFTWARE\Dell\Dell Data Protection]

  "LogVerbosity"=DWORD:<see below>

  Dump: 0

  Fatal: 1

  Error 3

  Warning 5

  Info 10

  Verbose 12

  Trace 14

  Debug 15

  El valor de registro se comprueba cuando se inicia el servicio Advanced Threat Prevention o cuando el valor cambia. Si el valor de registro no existe, no se produce ningún cambio a nivel de registro.

  Utilice esta configuración de registro solo para realizar pruebas o depuraciones, ya que este ajuste controla el nivel de detalle de registro de otros componentes, incluidos Encryption y Encryption Management Agent.

- El Modo de compatibilidad permite que se ejecuten aplicaciones en el equipo cliente mientras que están habilitadas las políticas de Protección de memoria o de Protección de memoria y Control de secuencias de comandos. La activación del modo de compatibilidad requiere la adición de un valor de registro en el equipo cliente.

  Para activar el modo de compatibilidad, siga estos pasos:

1. En la consola de administración, deshabilite la política *Protección de memoria habilitada*. Si la política de *Control de secuencias de comandos* está habilitada, deshabilítela.
2. Agregue el valor de registro CompatibilityMode.
   a. Al utilizar el Editor de registro en el equipo cliente, vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`.
   b. Haga clic con el botón derecho del mouse en **Escritorio**, haga clic en **Permisos**, y asuma la propiedad y otórguese Control completo.
   c. Haga clic con el botón derecho del mouse en **Escritorio** y, a continuación, seleccione **Nuevo Valor binario**.
   d. Para el nombre, escriba `CompatibilityMode`.
   e. Abra la configuración de registro y cambie el valor a `01`.
   f. Haga clic en **Aceptar** y, a continuación, cierre el Editor de registro.

   Para agregar el valor de registro con un comando, puede utilizar una de las siguientes opciones de línea de comandos para que se ejecute en el equipo cliente:

   - (Para un equipo) Psexec:

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

   - (Para varios equipos) 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}
     ```

3. En la consola de administración, vuelva a habilitar la política *Protección de memoria habilitada*. Si la política de *Control de secuencias de comandos* se había habilitado anteriormente, vuelva a habilitarla.