Dell Threat Defense

Guia de Instalação e do Administrador

Com tecnologia Cylance

v17.11.06

2017-11-06

Índice

VISÃO GERAL

O Dell Threat Defense, com tecnologia Cylance, detecta e bloqueia malwares antes de eles poderem afetar um dispositivo. A Cylance usa uma abordagem matemática para a identificação de malwares, com técnicas de aprendizagem automática em vez de assinaturas reativas, sistemas baseados em confiança ou áreas de segurança. Essa abordagem torna novos malwares, vírus, robôs e variantes futuras inúteis. O Threat Defense analisa as execuções de arquivo potenciais em busca de malwares no sistema operacional.

Este guia explica o uso do Threat Defense Console, a instalação do agente do Threat Defense e como configurá-los.

Como funciona

O Threat Defense consiste em um pequeno agente instalado em cada host que se comunica com o Console baseado na nuvem. O agente detecta e bloqueia o malware no host com o uso de modelos matemáticos testados, não precisa de conectividade de nuvem contínua nem de atualizações constantes de assinatura, e funciona em redes abertas ou isoladas. À medida que o cenário de ameaças evolui, o mesmo acontece com o Threat Defense. Com um treinamento constante em enormes conjuntos de dados do mundo real, o Defense Threat permanece um passo à frente dos invasores.

- Ameaça: Quando uma ameaça é baixada para o dispositivo ou quando há uma tentativa de exploração.
- **Detecção de ameaças**: Como o agente do Threat Defense identifica as ameaças.
    - **Varredura** de processos: Verifica os processos em execução no dispositivo.
    - **Controle de execução:** Analisa apenas os processos em execução. Inclui todos os arquivos que são executados durante a inicialização, aqueles configurados para reprodução automática e aqueles executados manualmente pelo usuário.
- **Análise**: Como os arquivos são identificados como mal-intencionados ou seguros.
    - **Pesquisa na nuvem para pontuação** de ameaças: O modelo matemático na nuvem usado para pontuar os arquivos.
    - **Local:** O modelo matemático contido no agente. Permite a análise quando o dispositivo não está conectado à Internet.
- **Ação:** O que o agente faz quando um arquivo é identificado como uma ameaça.
    - **Global**: Verifica as configurações das políticas, incluindo a *Quarentena global* e as *Listas de arquivos seguros*.
    - **Local:** Verifica os arquivos colocados manualmente *em Quarentena* ou *Ignorados*.

Sobre este guia

A Dell recomenda que os usuários se familiarizem com o console baseado na nuvem antes de instalar os agentes nos endpoints. Entender como os endpoints são gerenciados torna mais fácil a proteção e a manutenção deles. Este fluxo de trabalho é uma recomendação. Os usuários podem abordar a implementação em seu ambiente de uma maneira que faça sentido para eles.

Exemplo: As zonas ajudam a agrupar dispositivos na organização. Por exemplo, configure uma Zona com uma Regra da zona que adicione automaticamente novos dispositivos a uma Zona de acordo com os critérios selecionados (como, por exemplo, Sistema operacional, Nome do dispositivo ou Nome do domínio).

Nota: As instruções para a instalação do agente vêm depois de saber mais sobre Políticas e Zonas. Se necessário, os usuários podem iniciar com a instalação do agente.

CONSOLE

O Threat Defense Console é um site no qual se faz login para ver as informações de ameaças da organização. O console facilita a organização dos dispositivos em grupos (Zonas), a configuração de que ações serão tomadas ao descobrir ameaças em um dispositivo (Política) e o download dos arquivos de instalação (Agente).

O Threat Defense Console suporta os seguintes idiomas.

Francês	Alemão	Italiano	Japonês
Português (Portugal)	Coreano	Espanhol	Português (Brasil)

Tabela 1: Idiomas suportados pelo Threat Defense Console

Login

Após a ativação da sua conta, você receberá um e-mail com informações de login no Threat Defense Console. Clique no link existente no e-mail para ir para a página de login ou acesse:

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

Política do dispositivo

Uma política define como o agente lida com um malware encontrado. Por exemplo, coloca um malware automaticamente *em quarentena* ou o ignora se estiver em uma pasta específica. Todo dispositivo precisa estar em uma política e apenas uma política pode ser aplicada a um dispositivo. Restringir um dispositivo a uma única política elimina o conflito entre recursos (como, por exemplo, bloquear um arquivo quando ele deveria ser Permitido para esse dispositivo). O dispositivo será colocado na política Padrão se nenhuma política for atribuída a ele.

Apenas o Controle de execução é ativado para a política Padrão, o qual analisa apenas os processos em execução. Ele fornece uma proteção básica para o dispositivo, não deve interromper operações no dispositivo e fornece um tempo para testar os recursos da política antes de implementar a política no ambiente de produção.

Para adicionar uma política

1. Faça login no Console (http://dellthreatdefense.com) como um administrador. Apenas administradores podem criar políticas.
2. Selecione **Configurações >** Política do dispositivo.
3. Clique em **Adicionar nova política**.
4. Digite um Nome da política e selecione as opções da política.
5. Clique em **Criar**.

Ações de arquivo

CONFIGURAÇÕES > Política do dispositivo > [selecione uma política] > Ações de arquivo

As ações de arquivo fornecem diferentes opções para lidar com os arquivos detectados pelo Threat Defense como Inseguro ou Anormal.

Dica: Para saber mais sobre a classificação de arquivos *Inseguros* ou *Anormais*, consulte a seção Proteção - ameaças.

Quarentena automática com controle de execução

Esse recurso coloca em *Quarentena* ou bloqueia o arquivo Inseguro ou Anormal para impedi-lo de ser executado. Colocar um arquivo em *Quarentena* vai transferi-lo de seu local original para o diretório Quarentena, **`C:\ProgramData\Cylance\Desktop\q`**.

Alguns malwares são projetados para colocar certos arquivos em determinados diretórios. Esses malwares permanecem tentando colocar o arquivo até conseguirem. O Threat Defense modifica o arquivo colocado de modo que ele não será executado, com o objetivo de impedir que esse tipo de malware continue colocando continuamente o arquivo removido.

Dica: A Dell recomenda que a *Quarentena Automática* seja testada em uma pequena quantidade de dispositivos antes de aplicá-la no ambiente de produção. Os resultados do teste devem ser observados para confirmar que nenhum aplicativo essencial da empresa será bloqueado durante sua execução.

Upload automático

A Dell recomenda que os usuários habilitem o Upload automático para arquivos Inseguros e Anormais. O Threat Defense carrega automaticamente qualquer arquivo Inseguro ou Anormal detectado no Cylance Infinity Cloud para realizar uma análise mais aprofundada do arquivo e fornece detalhes adicionais.

O Threat Defense apenas faz o upload e analisa arquivos PE (executável portátil) desconhecidos. Se o mesmo arquivo desconhecido for descoberto em múltiplos dispositivos na organização, o Threat Defense transferirá por upload apenas um arquivo para análise, e não um arquivo por dispositivo.

Lista de arquivos seguros da política

No nível da Política, adicione os arquivos considerados seguros. O agente não aplicará nenhuma ação da ameaça aos arquivos nesta lista.

Para obter mais informações sobre como lidar com exceções de arquivo (*Quarentena* ou *Seguro*) em diferentes níveis (*local*, *política* ou *global*), consulte Apêndice B:Lidar com exceções.

1. Faça login no Console (http://dellthreatdefense.com) como um administrador. Apenas administradores podem criar políticas.
2. Selecione **Configurações >** Política do dispositivo.
3. Adicione uma nova política ou edite uma existente.
4. Clique em **Adicionar arquivo** sob *Lista de arquivos seguros da política*.
5. Digite a informação **SHA256**. Ou então adicione o MD5 e o Nome do arquivo, se forem conhecidos.
6. Selecione uma **Categoria** para ajudar a identificar o que este arquivo faz.
7. Explique o motivo de adicionar esse arquivo à *Lista de arquivos seguros da política*.
8. Clique em **Enviar**.

Configurações de proteção

`CONFIGURAÇÕES > Política do dispositivo > [selecione uma política] > Configurações de proteção`

Controle de execução

O Threat Defense está sempre atento a execução de processos mal-intencionados e alerta quando algo Inseguro ou Anormal tenta ser executado.

Prevenção contra desligamento do serviço a partir do dispositivo

Se selecionado, o serviço Threat Defense é protegido contra desligamento manual ou por outro processo.

Cópia de amostras de malware

Permite a especificação de um compartilhamento de rede para o qual copiar as amostras de malware. Permite que os usuários façam suas próprias análises dos arquivos que o Threat Defense considera Inseguros ou Anormais.

- Oferece suporte para compartilhamentos de rede CIFS/SMB.
- Especifique um local de compartilhamento de rede. Exemplo: **`c:\test`**e.
- Todos os arquivos que atendem aos critérios são copiados para o compartilhamento de rede, incluindo arquivos duplicados. Nenhum teste de exclusividade é realizado.
- Os arquivos não são compactados.
- Os arquivos não são protegidos por senha.

AVISO: OS ARQUIVOS NÃO SÃO PROTEGIDOS POR SENHA. DEVE-SE TOMAR CUIDADO PARA QUE O ARQUIVO MAL-INTENCIONADO NÃO SEJA INADVERTIDAMENTE EXECUTADO.

Controle de scripts

O controle de scripts protege os dispositivos, impedindo que scripts Active Script e PowerShell mal-intencionados sejam executados.

1. Faça login no Console (http://dellthreatdefense.com).
2. Selecione **Configurações >** Política do dispositivo.
3. Selecione uma política e clique em **Configurações de proteção**.
4. Marque a caixa de seleção para habilitar o **Controle de scripts.**
    a. **Alerta:** Monitore os scripts em execução no ambiente. Recomendado para a implementação inicial.
    b. **Bloquear:** Permite a execução de scripts apenas a partir de determinadas pastas. Use depois de testar no Modo de alerta.
    c. **Aprovar scripts nessas pastas (e subpastas)**: As exclusões de pastas de scripts precisam especificar o caminho relativo da pasta.
    d. **Bloquear o uso do Console do PowerShell**: Impede a inicialização do console do PowerShell. Isso oferece segurança adicional protegendo contra o uso de one-liners de PowerShell.

    Nota: Se o script iniciar o console do PowerShell e o Controle de scripts estiver definido para bloquear o console do PowerShell, o script falhará. É recomendável que os usuários alterem seus scripts para chamar os scripts do PowerShell, não o console do PowerShell.
5. Clique em **Salvar**.

Logs do agente

`CONFIGURAÇÕES > Política do dispositivo > [selecione uma política] > Logs do agente`

Ativa os Logs do agente no Console para fazer upload de arquivos de log e permitir a exibição no console.

1. Faça login no Console (http://dellthreatdefense.com).
2. Selecione **Configurações >** Política do dispositivo.
3. Selecione uma política e clique em **Logs do agente**. Confirme que o dispositivo selecionado cujos arquivos de log serão obtidos está atribuído a esta política.

4. Selecione **Habilitar upload automático de arquivos de log** e clique em **Salvar**.
5. Clique na aba **Dispositivos** e selecione um dispositivo.
6. Clique em **Logs do agente**. Os arquivos de log são mostrados.
7. Clique em um arquivo de log. O nome do arquivo de log é a data do log.

Práticas recomendadas da política

Depois de criar as políticas, a Dell recomenda que seus recursos sejam implementados em uma abordagem em fases para assegurar-se de que o desempenho e as operações não sejam impactados. Crie novas políticas com mais recursos ativados à medida que o seu entendimento sobre como o Threat Defense funciona no ambiente aumentar.

1. Ao criar políticas iniciais, ative apenas o **Upload automático**.
    a. O agente usa o Controle de execução e o Monitor de processos para analisar apenas os processos em execução.

        Inclui todos os arquivos que são executados durante a inicialização, aqueles configurados para reprodução automática e aqueles executados manualmente pelo usuário.

        O agente apenas envia os alertas para o Console. Nenhum arquivo é bloqueado ou colocado em *Quarentena*.

    b. Consulte o Console para ver os alertas de ameaças.

        O objetivo é encontrar todos os aplicativos e processos cuja execução é necessária no endpoint e que estão sendo considerados uma ameaça (*Anormal* ou *Insegura*).

        Defina uma configuração de política ou Console para *Permitir* que eles sejam executados se isso acontecer (por exemplo, *Excluir* pastas em uma política, *Ignorar* os arquivos desse dispositivo ou adicionar os arquivos à *Lista de arquivos seguros*).

    c. Use essa política inicial por um dia para permitir que os aplicativos e os processos normalmente usados no dispositivo sejam executados e analisados.

IMPORTANTE: Podem existir aplicativos e processos que são executados periodicamente em um dispositivo (por exemplo, uma vez por mês) e que podem ser considerados uma ameaça. Cabe a você decidir se você quer executá-los durante esta política inicial ou lembrar de monitorar o dispositivo ao executá-los conforme agendado.

2. Em Configurações de proteção, ative **Eliminar processos inseguros em execução** depois que o Controle de execução e o Monitoramento de processos estiverem concluídos.

    Eliminar processos inseguros em execução e seus subprocessos elimina os processos (e os subprocessos), independentemente do estado, quando uma ameaça é detectada (EXE ou MSI).

3. Em Ações de arquivo, ative **Quarentena automática**.

    A *Quarentena automática* move quaisquer arquivos mal-intencionados para a pasta *Quarentena*.

4. Em Configurações de proteção, ative **Controle de scripts**.

    O Controle de scripts protege os usuários contra a execução de scripts mal-intencionados em seus dispositivos.

    Os usuários podem aprovar a execução de scripts em determinadas pastas.

    As exclusões de pastas do Controle de scripts precisam especificar um caminho relativo da pasta (por exemplo, **`\Casos\ScriptsAllowed`**).

Zonas

Uma Zona é uma maneira de organizar e gerenciar os dispositivos. Por exemplo, os dispositivos podem ser separados de acordo com a sua localidade ou função. Se houver um grupo de dispositivos de missão crítica, eles podem ser agrupados e atribuídos com alta prioridade à Zona. Além disso, as políticas são aplicadas no nível da Zona, de modo que os dispositivos podem ser agrupados em uma Zona de acordo com a política que é aplicada a esses dispositivos.

Uma organização tem uma Zona padrão (Não zoneada) que apenas os administradores podem acessar. Os novos dispositivos são atribuídos como "Não zoneados", a menos que haja regras de zonas que atribuem automaticamente dispositivos a Zonas.

Os Gerentes de zona e os Usuários podem ser atribuídos a Zonas, o que permite que eles vejam como essa Zona está configurada. Isso também permite que os Gerentes de zona e os Usuários acessem os dispositivos pelos quais são responsáveis. Pelo menos uma Zona precisa ser criada para permitir que alguém com uma função de Gerente de zona ou Usuário a veja.

Um dispositivo pode pertencer a múltiplas Zonas, mas apenas uma política pode ser aplicada a um dispositivo. A permissão de múltiplas Zonas proporciona alguma flexibilidade em como os dispositivos estão agrupados. Restringir um dispositivo a uma única política elimina o conflito entre recursos (por exemplo, bloquear um arquivo quando ele deveria ser *Permitido* para esse dispositivo).

A existência de dispositivos em múltiplas Zonas pode ocorrer pelos seguintes motivos:

- O dispositivo foi adicionado manualmente a múltiplas Zonas
- O dispositivo está em conformidade com as regras de mais de uma Zona
- O dispositivo já reside em uma Zona e então fica em conformidade com as regras de outra Zona

Para formas recomendadas de usar as Zonas, consulte Práticas mais recomendadas de gerenciamento de zonas.

Para adicionar uma zona

1. Faça login no Console (http://dellthreatdefense.com) como um administrador. Apenas administradores podem criar zonas.
2. Clique em **Zonas**.
3. Clique em **Adicionar nova zona**.
4. Digite o Nome da zona, selecione uma Política e um Valor. Uma zona precisa ter uma política associada. O Valor é a prioridade da zona.
5. Clique em **Salvar**.

Para adicionar dispositivos a uma zona

1. Faça login no Console (http://dellthreatdefense.com) com uma conta de Administrador ou Gerente de zona.
2. Clique em **Zonas**.
3. Clique em uma Zona a partir da *Lista de zonas*. Os dispositivos atuais para essa Zona são exibidos na *Lista de dispositivos das zonas*, na parte inferior da página.
4. Clique em **Adicionar dispositivos a uma zona.** Uma lista de dispositivos é mostrada.
5. Selecione cada dispositivo a ser adicionado à Zona e clique em **Salvar**. Selecione opcionalmente **Aplicar política de zona aos dispositivos selecionados**. Adicionar um dispositivo a uma Zona não aplica automaticamente a Política da zona, pois uma Zona pode estar sendo usada para organizar dispositivos, e não gerenciar a política desses dispositivos.

Para remover uma zona

1. Faça login no Console (http://dellthreatdefense.com) como um administrador. Apenas administradores podem remover zonas.
2. Clique em **Zonas**.
3. Marque as caixas de seleção das zonas a serem removidas.
4. Clique em **Remover**.
5. Clique em **Sim** quando a mensagem pedindo a confirmação de remoção da Zona selecionada.

Propriedades da zona

As propriedades da zona podem ser editadas conforme necessário.

Sobre a prioridade da zona

As zonas podem receber diferentes níveis de prioridade (Baixo, Normal ou Alto), os quais classificam a importância ou o estado de urgência dos dispositivos nessa zona. Em várias áreas do painel, os dispositivos são mostrados em ordem de prioridade para ajudar a identificar que dispositivos precisam ser tratados imediatamente.

A prioridade pode ser definida durante a criação de uma zona ou ao editar a zona para alterar o valor da prioridade.

Para editar as propriedades da zona

1. Faça login no Console (http://dellthreatdefense.com) como Administrador ou Gerente de zona.
2. Clique em **Zonas**.
3. Clique em uma Zona a partir da *Lista de zonas*.
4. Digite um novo nome no campo **Nome** para alterar o Nome da zona.
5. Selecione uma política diferente no menu suspenso **Política** para mudar a política.
6. Selecione uma intensidade **Baixa**, **Normal** ou **Alta**.
7. Clique em **Salvar**.

Regra da zona

Os dispositivos podem ser atribuídos automaticamente a uma Zona seguindo determinados critérios. Essa automação é vantajosa ao adicionar muitos dispositivos às Zonas. Quando novos dispositivos são adicionados e eles correspondem a uma Regra da zona, esses dispositivos são automaticamente atribuídos a essa Zona. Se **Aplicar agora para todos os dispositivos existentes** for selecionado, todos os dispositivos pré-existentes que correspondem à regra são adicionados a essa Zona.

Nota: As regras das zonas adicionam automaticamente dispositivos a uma zona, mas não podem remover dispositivos. Alterar o endereço IP ou o nome de host do dispositivo não o remove de uma zona. Os dispositivos precisam ser removidos manualmente de uma zona.

Há uma opção de aplicar a Política da zona aos dispositivos que forem adicionados à Zona como um resultado da correspondência à Regra da zona. Isso significa que a política existente do dispositivo será substituída pela Política da zona especificada. A aplicação automática de uma política com base na Regra da zona deve ser usada com cuidado. Se não gerenciado corretamente, um dispositivo pode ser atribuído à política errada porque o dispositivo correspondeu a uma Regra da zona.

Veja a página Detalhes do dispositivo no Console para ver que política está aplicada a um dispositivo.

Para adicionar uma Regra da zona

1. Faça login no Console (http://dellthreatdefense.com) como Administrador ou Gerente de zona.
2. Clique em **Zonas** e selecione uma Zona na *Lista de zonas*.
3. Clique em **Criar regra** em Regra da zona,
4. Especifique os critérios para a zona selecionada. Clique no sinal de adição para adicionar mais condições. Clique no sinal de subtração para remover uma condição.
5. Clique em **Salvar**.

Critérios da regra da zona

- **Quando um novo dispositivo é adicionado à organização**: Todo novo dispositivo adicionado à organização que corresponder à Regra da zona será adicionado à zona.
- **Quando qualquer atributo de um dispositivo for alterado**: Quando atributos em um dispositivo existente mudarem e então corresponderem à Regra da zona, esse dispositivo será adicionado à zona.
- **Endereço IPv4 na faixa**: Digite uma faixa de endereços IPv4.
- **Nome do dispositivo:**
  - Inicia com: Os nomes dos dispositivos precisam começar desta forma.
  - Contém: Os nomes dos dispositivos precisam conter essa string, mas ela pode estar em qualquer parte dentro do nome.
  - Termina com: Os nomes dos dispositivos precisam terminar desta forma.
- **Sistema operacional:**
  - É: O sistema operacional precisa ser o sistema selecionado.
  - Não é: O sistema operacional não pode ser o sistema selecionado. Por exemplo, se a Regra da zona apenas indica que o sistema operacional não pode ser Windows 8, todos os sistemas operacionais, inclusive dispositivos não Windows, serão adicionados a essa zona.
- **Nome de domínio:**
  - Inicia com: O nome do domínio precisa começar desta forma.
  - Contém: O nome do domínio precisa conter essa string, mas ela pode estar em qualquer parte dentro do nome.
  - Termina com: O nome do domínio precisa terminar desta forma.
- **Nome diferenciado:**
  - Inicia com: O nome distinto precisa começar desta forma.
  - Contém: O nome distinto precisa conter essa string, mas ela pode estar em qualquer parte dentro do nome.
  - Termina com: O nome distinto precisa terminar desta forma.
- **Membro do (LDAP)**:
  - É: O Membro de (Grupo) precisa corresponder a ele.
  - Contém: O Membro de (Grupo) precisa contê-lo.

- **Seguintes condições atendidas**:
    - Todas: Para adicionar o dispositivo todas as condições na Regra da zona precisam coincidir.
    - Qualquer: Para adicionar o dispositivo pelo menos uma condição na Regra da zona precisa coincidir.
- **Aplicação de política da zona:**
    - Não aplicar: Não aplica a Política da zona conforme os dispositivos são adicionados à zona.
    - Aplicar: Aplica a Política da zona conforme os dispositivos são adicionados à zona.

      Aviso: Aplicar automaticamente uma Política da zona pode influenciar negativamente alguns dispositivos na rede. Aplique automaticamente a Política de zona *somente* se estiver certo de que a Regra de zona *só* encontrará dispositivos que devem ter essa Política de zona específica.
- **Aplicar agora para todos os dispositivos existentes**: Aplica a Regra da zona a todos os dispositivos na organização. Não se aplica a Política da zona.

Sobre Nomes Distintos (DN)

Algumas coisas para se saber sobre Nomes Distintos (DN) ao usá-los nas regras das zonas.

- Não é permitido o uso de curingas, mas a condição "Contém" obtém resultados similares.
- Os erros e exceções de DN relacionados ao agente são capturados nos arquivos de log.
- Se o agente encontrar informações do DN no dispositivo, elas serão automaticamente enviadas ao Console.
- Quando for adicionar as informações do DN, elas precisam ser formatadas adequadamente da seguinte forma.
    - Exemplo: CN=JDoe,OU=Sales,DC=dell,DC=COM
    - Exemplo: OU=Demo,OU=SEngineering,OU=Sales

Lista de dispositivos das zonas

A *Lista de dispositivos das zonas* mostra todos os dispositivos atribuídos a essa Zona. Os dispositivos podem pertencer a múltiplas zonas. Use **Exportar** para fazer o download de um arquivo CSV com informações para todos os dispositivos da *Lista de dispositivos da Zona*.

Nota: Se não tiver permissão para ver uma zona e assim mesmo clicar no link da zona na coluna Zonas, uma página Recurso não encontrado será mostrada.

Práticas mais recomendadas de gerenciamento de zonas

A melhor maneira de imaginar as zonas são como etiquetas, onde qualquer dispositivo pode pertencer a múltiplas zonas (ou ter múltiplas etiquetas). Embora não haja restrições no número de zonas que podem ser criadas, as práticas mais recomendadas identificam três diferentes associações de zonas entre teste, política e granularidade da função do usuário dentro da organização.

Essas três zonas consistem em:

- Gerenciamento de atualizações
- Gerenciamento de políticas
- Gerenciamento de acesso baseado na função

Organização de zonas para o gerenciamento de atualizações

Um uso comum das zonas é ajudar no gerenciamento das atualizações dos agentes. O Threat Defense suporta a versão mais recente do agente e a versão anterior. Isso permite que a empresa altere as janelas de congelamento e realize testes completos nas novas versões de agente.

Há três tipos de zonas sugeridos usados para conduzir e especificar as fases de testes e de produção do agente:

- **Atualizar zona – Grupo de teste:** Estas zonas devem conter os dispositivos de teste que representam adequadamente os dispositivos (e os softwares usados nesses dispositivos) na organização. Isso permite o teste do agente mais recente e garante que a implementação desse agente nos dispositivos de produção não irá interferir nos processos da empresa.
- **Atualizar zona – Grupo piloto:** Esta zona pode ser usada como uma Zona de teste secundária ou como uma Zona de produção secundária. Como uma Zona de teste secundária, permite testar novos agentes em um grupo maior de dispositivos antes de distribuir para a produção. Como uma Zona de produção secundária, permite duas versões diferentes de agente; porém, dessa forma, você precisará gerenciar duas Zonas de produção diferentes.
- **Zona de atualização - Produção**: A maioria dos dispositivos deve estar nas zonas atribuídas à produção.

Nota: Para a atualização do Agente para a Zona de produção, consulte Atualização do agente.

Adicionar uma zona de teste ou piloto

1. Faça login no Console (http://dellthreatdefense.com) com uma conta de Administrador ou Gerente de zona.
2. Selecione **Configurações > Atualização do agente**.
3. Para zonas de teste ou piloto:
    a. Clique em **Selecionar zonas de teste** ou **Selecionar zonas piloto**.
    b. Clique em uma zona.

    Se a Zona de produção for definida como **Atualização automática**, as Zonas de teste e piloto não estarão disponíveis. Altere a Atualização automática na Zona de produção para algo diferente para habilitar as zonas de teste e piloto.
4. Clique em **Selecione a versão**.
5. Selecione uma versão de agente para aplicá-la à zona de teste ou piloto.
6. Clique em **Aplicar**.

Organização de zonas para o gerenciamento de políticas

Outro conjunto de Zonas a ser criado ajuda a aplicar diferentes políticas a diferentes tipos de endpoints. Considere os exemplos a seguir:

- Zona de política – Estações de trabalho
- Zona de política – Estações de trabalho – Exclusões
- Zona de política – Servidores
- Zona de política – Servidores – Exclusões
- Zona de política – Executivos – Alta proteção

A Dell sugere aplicar, por padrão, em cada uma dessas zonas, uma política a todos os dispositivos contidos nessa Zona de política. Tome cuidado para não colocar um dispositivo em mais de uma Zona de política, pois isso pode gerar um conflito sobre qual política é aplicada. Lembre-se também de que o mecanismo da Regra da zona pode ajudar a organizar automaticamente esses hosts de acordo com o IP, Nome de host, Sistema operacional e Domínio.

Organização de zonas para o gerenciamento de acesso baseado na função

O acesso baseado na função é usado para limitar o acesso de um usuário do Console a um subconjunto de dispositivos pelos quais ele é responsável por gerenciar. Isso pode incluir a separação por Faixa de IPs, Nomes de host, Sistema operacional ou Domínio. Considere agrupamentos por localização geográfica, tipo ou ambos.

Exemplo:

- Zona RBAC – Computadores de mesa – Europa
- Zona RBAC – Servidores – Ásia
- Zona RBAC – Diretoria

Usando os exemplos de Zona acima, um Gerente de zona poderia ser atribuído à *Zona RBAC - Desktops - Europa*, e só teria acesso a dispositivos nessa Zona. Se esse usuário Gerente de zona tentar ver outras zonas, uma mensagem de erro será recebida indicando que ele não tem permissão para vê-las. Embora um dispositivo possa estar em múltiplas zonas e o Gerente de zona consiga ver esse dispositivo, se ele tentar ver as outras zonas às quais o dispositivo está associado, ele não terá permissão e verá a mensagem de erro.

Em outras partes do Console, como o painel, o Gerente de zona para *Zona RBAC - Desktops - Europa* também ficaria limitado a ameaças e outras informações relacionadas à Zona ou aos dispositivos atribuídos a essa Zona.

As mesmas restrições se aplicam aos usuários atribuídos a uma zona.

Gerenciamento de usuários

Os administradores têm permissões globais e podem adicionar ou remover usuários, atribuir usuários a zonas (como um Usuário ou um Gerente de zona), adicionar ou remover dispositivos, criar políticas e criar zonas. Os administradores podem também apagar usuários, dispositivos, políticas e zonas permanentemente do Console.

Os Usuários e Gerentes de zona apenas têm acesso e privilégios pertencentes à zona a qual estão atribuídos. Isso se aplica a dispositivos atribuídos à zona, ameaças encontradas nesses dispositivos e informações no painel.

Para obter uma lista completa das permissões do usuário permitidas para cada usuário, consulte o Apêndice C: Permissões do usuário.

Para adicionar usuários

1. Faça login no Console (http://dellthreatdefense.com) como um administrador. Apenas administradores podem criar usuários.
2. Selecione **Configurações > Gerenciamento de usuários**.
3. Digite o endereço de e-mail do usuário.
4. Selecione uma função no menu suspenso Função.
5. Ao adicionar um Gerente de zona ou Usuário, selecione uma zona atribuir a eles.
6. Clique em **Adicionar**. Um e-mail será enviado ao usuário com um link para criar uma senha.

Para alterar as funções de um usuário

1. Faça login no Console (http://dellthreatdefense.com) como um administrador. Apenas administradores podem criar usuários.
2. Selecione **Configurações > Gerenciamento de usuários**.
3. Clique em um usuário. A página Detalhes do usuário é mostrada.
4. Selecione uma função e clique em **Salvar**.

Para remover usuários

1. Faça login no Console (http://dellthreatdefense.com) como um administrador. Apenas administradores podem criar usuários.
2. Selecione **Configurações > Gerenciamento de usuários**.
3. Marque a caixa de seleção do usuário ou dos usuários a serem removidos.
4. Clique em **Remover**.
5. Clique em **Sim** quando a mensagem pedindo a confirmação de remoção.

Configurações relacionadas à rede

Configure a rede para permitir que o agente do Threat Defense se comunique com o Console pela Internet. Esta seção aborda as configurações de firewall e as configurações de proxy.

Firewall

Nenhum software local é necessário para gerenciar os dispositivos. Os agentes do Threat Defense são gerenciados pelo Console e se comunicam com ele (interface do usuário baseada na nuvem). A porta 443 (HTTPS) é usada para a comunicação e precisa estar aberta no firewall para que os agentes consigam se comunicar com o console. O Console é hospedado pelo Amazon Web Services (AWS) e não possui endereço IP fixo. Verifique se os agentes conseguem se comunicar com os sites a seguir:

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

Ou então, permita o tráfego HTTPS para *.cylance.com.

Proxy

O suporte de proxy do Threat Defense é configurado por meio de uma entrada de registro. Quando um proxy é configurado, o agente usa o endereço IP e a porta existente na entrada de registro em todas as comunicações de saída com os servidores do Console.

1. Acesse o registro.

   Nota: Pode ser que sejam necessários privilégios elevados ou apropriar-se do registro dependendo de como o agente foi instalado (Modo protegido habilitado ou não).

2. No Editor de registro, navegue até **`HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`**.
3. Crie um novo Valor da cadeia de caracteres (REG_SZ):
   - Nome do valor = ProxyServer
   - Dados do valor = configurações de proxy (por exemplo, http://123.45.67.89:8080)

Em ambientes autenticados, o agente tenta usar as credenciais do usuário atualmente conectado para se comunicar pela Internet. Se houver um servidor proxy autenticado configurado, mas não houver um usuário conectado ao dispositivo, o agente não poderá se autenticar no proxy nem poderá se comunicar com o Console. Nesse caso:

- Configure o proxy e adicione uma regra para permitir todo o tráfego para *.cylance.com.
- Use outra política de proxy, permitindo acesso não autorizado ao proxy para hosts da Cylance (*.cylance.com).

Dessa forma, se não houver um usuário conectado ao dispositivo, o agente não precisará se autenticar e conseguirá se conectar à nuvem e se comunicar com o Console.

Dispositivos

Depois de instalar um agente em um endpoint, ele se torna disponível como um dispositivo no console. Comece a gerenciar dispositivos atribuindo uma política (para lidar com *Ameaças* identificadas), agrupe dispositivos (usando *Zonas*) e realize ações manualmente em cada dispositivo (*Quarentena e Ignorado*).

Gerenciamento de dispositivos

Os dispositivos são computadores com um agente do Threat Defense. Gerencie os dispositivos a partir do Console.

1. Faça login no Console (http://dellthreatdefense.com) como um administrador. Apenas administradores podem gerenciar dispositivos.
2. Clique em **Dispositivos**.
3. Marque a caixa de seleção de um dispositivo para permitir as ações a seguir:
    - **Exportar:** Cria e faz download de um arquivo CSV. O arquivo contém informações do dispositivo (Nome, Estado e Política) de todos os dispositivos na organização.
    - **Remover:** Remove os dispositivos selecionados da *Lista de dispositivos*. Isso não desinstala o agente do dispositivo.
    - **Atribuir política**: Permite atribuir os dispositivos selecionados a uma política.
    - **Adicionar a zonas**: Permite adicionar os dispositivos selecionados a uma ou mais zonas.
4. Clique em um dispositivo para mostrar a página Detalhes do dispositivo.
    - **Informações do dispositivo**: Mostra informações como Nome de host, Versão do agente e Versão do sistema operacional.
    - **Propriedades do dispositivo**: Permite alterar o Nome do dispositivo, a Política, as Zonas e o Nível de log.
    - **Ameaças e atividades:** Mostra as informações da ameaça e outras atividades relacionadas ao dispositivo.
5. Clique em **Adicionar novo dispositivo** para mostrar uma caixa de diálogo com um Token de instalação e links para baixar o instalador do Agente.
6. Na coluna Zonas, clique em um Nome da zona para mostrar a página Detalhes da zona.

Ameaças e atividades

Mostra as informações da ameaça e outras atividades relacionadas ao dispositivo selecionado.

Ameaças

Mostra todas as ameaças encontradas no dispositivo. Por padrão, as ameaças são agrupadas por status (*Inseguras*, *Anormais*, *Quarentena* e Ignoradas).

- **Exportar:** Cria e faz download de um arquivo CSV com informações de todas as ameaças encontradas no dispositivo selecionado. As informações das ameaças são informações como Nome, Caminho do arquivo, Pontuação segundo a Cylance e Status.
- **Quarentena:** *Coloca em Quarentena* as ameaças selecionadas. Esta é uma *Quarentena local*, o que significa que esta ameaça está em *quarentena* apenas neste dispositivo. Para colocar uma ameaça em *Quarentena* para todos os dispositivos na organização, certifique-se de que a caixa de seleção **Além disso, colocar esta ameaça em quarentena sempre que for encontrada em qualquer dispositivo** esteja selecionada (*Quarentena global*) quando um arquivo é colocado em *Quarentena*.
- **Ignorar:** Altera o status das ameaças selecionadas como *Ignoradas*. É permitido executar um arquivo *Ignorado*. Este é um *Ignorado local*, o que significa que este *arquivo é permitido* apenas neste dispositivo. Para permitir esse arquivo em todos os dispositivos da organização, marque a caixa de seleção **Além disso, marque como seguro em todos os dispositivos** (*Lista de arquivos seguros*) quando um arquivo for *Ignorado*.

Tentativas de explorar vulnerabilidade

Mostra todas as tentativas de exploração no dispositivo. Inclui informações sobre o Nome do processo, o ID, o Tipo e a Ação tomada.

Logs do agente

Mostra os arquivos de log transferidos por upload pelo agente no dispositivo. O nome do arquivo de log é a data do log.

Para ver os arquivos de log do agente:

1. Faça upload do arquivo de log atual de um único dispositivo.
    a. Clique em Dispositivos > Logs do agente.
    b. Clique em **Fazer upload arquivo de log atual**. Isso pode levar alguns minutos, dependendo do tamanho do arquivo de log.

OU

1. Configurações das políticas
    a. Clique em Configurações > Política do dispositivo > [selecione uma política] > Logs do agente.
    b. Clique em Ativar o upload automático de arquivos de log.
    c. Clique em **Salvar**.

Para ver logs detalhados, altere o Nível de log do agente antes de fazer o upload de qualquer arquivo de log.

1. No Console: **Dispositivos > [clique em um dispositivo]**, selecione **Detalhado** no menu suspenso Nível de log do agente, e clique em **Salvar**. Após o upload dos arquivos de log detalhado, a Dell recomenda alterar o Nível de log do agente de volta para *Informações*.
2. No dispositivo, feche a interface do usuário do Threat Defense (clique com o botão direito no ícone do Threat Defense na bandeja do sistema e, em seguida, clique em **Sair**).

OU

1. Abra a linha de comando como administrador. Digite a seguinte linha de comando e pressione a tecla **Enter.**

   ```
   cd C:\Arquivos de Programas\Cylance\Desktop
   ```

2. Digite a seguinte linha de comando e pressione a tecla **Enter.**

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

3. O ícone do Threat Defense é mostrado na bandeja do sistema. Clique com o botão direito, selecione **Registrar em log**, em seguida, clique em **Tudo** (igual a Detalhado no Console).

OU (para macOS)

1. Saia da interface do usuário atualmente em execução.
2. Execute o seguinte comando no terminal.

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

3. Clique com o botão direito na nova interface do usuário depois que ela abrir. Selecione **Registrar em log > Tudo.**

Controle de scripts

Mostra todas as atividades pertinentes para o Controle de scripts, como os scripts negados.

Dispositivos duplicados

Quando o agente do Threat Defense é instalado pela primeira vez em um dispositivo, um identificador único é criado, o qual será usado pelo Console para identificar e referenciar esse dispositivo. Entretanto, certos eventos, como o uso de uma imagem de máquina virtual para criar múltiplos sistemas, podem fazer com que um segundo identificador seja gerado para o mesmo dispositivo. Selecione o dispositivo e clique em **Remover** se uma entrada duplicada for exibida na página Dispositivos no Console.

Para auxiliar na identificação de tais dispositivos, use o recurso de classificação de coluna na página Dispositivos para classificar e comparar os dispositivos, geralmente pelo nome do dispositivo. Como alternativa, a *Lista de dispositivos* pode ser exportada em um arquivo .CSV e, em seguida, visualizada no Microsoft Excel ou algo semelhante que tenha recursos avançados de classificação/organização.

Exemplo usando o Microsoft Excel

1. Abra o arquivo CSV do dispositivo no Microsoft Excel.
2. Selecione a coluna de nome do dispositivo.
3. Na guia Página inicial, selecione Formatação condicional > Realçar regras das células > Valores duplicados.
4. Certifique-se de que **Duplicado** seja selecionado, em seguida, selecione uma opção de realce.
5. Clique em **OK**. Os itens duplicados são realçados.

Nota: O comando Remover apenas remove o dispositivo da página Dispositivo. Ele não emite um comando de desinstalação para o agente do Threat Defense. O agente precisa ser desinstalado no endpoint.

Atualização do agente

A manutenção e o gerenciamento dos agentes do Threat Defense são simples e fáceis. Os agentes baixam automaticamente as atualizações do Console e o Console é mantido pela Cylance.

O agente contata o Console a cada 1-2 minutos. O Console reporta o estado atual do Agente (*On-line* ou *Off-line*, *Inseguro* ou *Protegido*), as Informações de versão, o Sistema operacional e Status da ameaça.

O Threat Defense libera atualizações ao agente mensalmente. Essas atualizações podem conter revisões de configuração, novos módulos e alterações do programa. Quando há uma atualização de agente disponível (conforme indicado pelo Console em Configurações > Atualizações do agente), o agente baixa e aplica automaticamente a atualização. Para controlar o tráfego de rede durante as atualizações de agente, todas as organizações são ajustadas para acomodar no máximo 1.000 atualizações de dispositivo simultaneamente. Os usuários podem também o recurso para desabilitar a Atualização automática se preferirem.

Nota: O número máximo de dispositivos que podem ser atualizados simultaneamente pode ser modificado pelo suporte da Dell.

Atualização baseada na zona

A atualização baseada na zona permite que uma organização avalie um novo agente em um subconjunto de dispositivos antes de implementá-lo no ambiente inteiro (Produção). Uma ou mais zonas atuais podem ser temporariamente adicionadas a uma das duas Zonas de testes (Teste e Piloto), as quais podem usar um agente diferente da Produção.

Para configurar atualizações baseadas na zona:

1. Faça login no Console (http://dellthreatdefense.com) com uma Conta de administrador.
2. Selecione **Configurações > Atualização do agente**. As três versões de agente mais recentes são mostradas.

   Se a Zona de produção for definida como **Atualização automática**, as Zonas de teste e piloto não estarão disponíveis. Altere a Atualização automática na Zona de produção para algo diferente para habilitar as zonas de teste e piloto.
3. Selecione uma versão de agente específica na lista suspensa Produção.
4. Para a Zona de produção, selecione também Atualização automática ou Não atualizar.
   a. A **Atualização automática** permite que todos os Dispositivos de produção sejam atualizados automaticamente para a versão mais recente na *Lista de versões suportadas do agente*.
   b. **Não atualizar** proíbe todos os Dispositivos de produção de atualizar o Agente.
5. Para a Zona de teste, escolha uma ou mais zonas na lista suspensa Zona e, em seguida, selecione uma versão de agente específica na lista suspensa de versão.
6. Se quiser, repita a etapa 5 para a Zona piloto.

Nota: Quando um dispositivo é adicionado a uma zona que faz parte da zona de teste ou piloto, esse dispositivo começa a usar a versão do agente da zona de teste ou piloto. Se um dispositivo pertence a mais de uma zona e uma dessas zonas pertence à zona de teste ou piloto, a versão do agente da zona de teste ou piloto terá precedência.

Para acionar uma atualização do agente

Para acionar uma atualização do agente antes do próximo intervalo a cada hora:

1. Clique com o botão direito no ícone do agente do Threat Defense na bandeja do sistema e selecione **Verificar se há atualizações**.
2. Reinicie o serviço Threat Defense. Essa ação forcará ele a contatar o Console imediatamente.

OU

- As atualizações podem ser iniciadas a partir da linha de comando. Execute o seguinte comando a partir do diretório da Cylance:

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

Painel

A página Painel é mostrada ao se conectar ao Threat Defense Console. O Painel fornece uma visão geral das ameaças no ambiente e acesso a diferentes informações do Console em uma página.

Estatísticas de ameaças

As Estatísticas de ameaças fornecem o número de ameaças encontradas nas *Últimas 24 horas* e o *Total* para a organização. Clique em *Estatísticas de ameaças* para ir para a página Proteção e visualize a lista de ameaças relacionadas a esta estatística.

- **Ameaças em execução:** Arquivos identificados como ameaças que estão em execução em dispositivos na organização.
- **Ameaças com execução automática:** Ameaças definidas para executar automaticamente.
- **Ameaças em quarentena:** As ameaças em *Quarentena* nas últimas 24 horas e o total.
- **Exclusivas da Cylance**: Ameaças identificadas pela Cylance, mas não por outras fontes de antivírus.

Porcentagens de proteção

Exibe as porcentagens para Proteção contra ameaças e Proteção de dispositivos.

- **Proteção contra ameaças:** A porcentagem de ameaças para as quais ações foram executadas (Quarentena, Quarentena global, Ignorar e Listas de arquivos seguros).
- **Proteção do dispositivo**: A porcentagem de dispositivos associados a uma política com Quarentena automática ativada.

Ameaças por prioridade

Exibe o número total de ameaças que exigem uma ação (*Quarentena, Quarentena global, Ignorar e Listas de arquivos seguros)*. As ameaças são agrupadas por prioridade (Alta, Média e Baixa). Esta visão geral mostra o número total de ameaças que exigem uma ação, divide esse total por prioridade, fornece uma porcentagem total e quantos dispositivos estão afetados.

As ameaças são apresentadas na lista por prioridade no canto inferior esquerdo da página Painel. É especificado o número total de ameaças em uma organização agrupadas conforme suas classificações de prioridade.

Uma ameaça é classificada como Baixa, Média ou Alta com base no número dos seguintes atributos que ela possui:

- O arquivo tem uma pontuação segundo a Cylance superior a 80.
- O arquivo está em execução atualmente.
- O arquivo foi executado anteriormente.
- O arquivo está definido para reprodução automática.
- A prioridade da zona na qual a ameaça foi encontrada.

Essa classificação ajuda administradores a determinar que ameaças e dispositivos tratar primeiro. Clique na ameaça ou no Número do dispositivo para ver os detalhes de dispositivo e de ameaça.

Eventos de ameaças

Mostra um gráfico de linhas com o número de ameaças descobertas nos últimos 30 dias. Linhas são codificadas por cores para arquivos *Inseguros, Anormais, em Quarentena, Ignorado e na Lista de arquivos seguros*.

- Coloque o cursor sobre um ponto no gráfico para ver os detalhes.
- Clique em uma das cores na legenda para mostrar ou ocultar essa linha.

Classificações de ameaças

Mostra um mapa de calor dos tipos de ameaças encontradas na organização, como vírus ou malware. Clique em um item no mapa de calor para ir para a página Proteção e mostrar uma lista de ameaças desse tipo.

Listas das cinco principais

Mostra as listas das Cinco principais ameaças encontradas na maioria dos dispositivos, dos Cinco principais dispositivos com a maioria das ameaças e das Cinco principais zonas com a maioria das ameaças na organização. Clique em um item de uma lista para obter mais detalhes.

As Listas das cinco principais no painel destacam as ameaças *Inseguras* na organização que não foram resolvidas, como a *Quarentena ou Ignorada*. Na maioria das vezes estas listas devem estar vazias. Embora as ameaças *Anormais* também devam ser resolvidas, o foco das Listas das cinco principais é chamar sua atenção para as ameaças críticas.

Proteção – Ameaças

O Threat Defense pode fazer muito mais do que simplesmente classificar arquivos como Inseguros ou Anormais. Ele pode fornecer detalhes sobre as características estáticas e dinâmicas de arquivos. Isso permite que administradores não apenas bloqueiem ameaças, como também compreendam o comportamento das ameaças para mitigar ainda mais ou responder a elas.

Tipo de arquivo

Inseguro: Um arquivo com uma pontuação de 60 a 100. Um arquivo *Inseguro* é aquele no qual o mecanismo do Threat Defense localiza atributos que se parecem muito com malware.

Anormal: Um arquivo com uma pontuação de 1 a 59. Um arquivo Anormal possui alguns atributos de malware, mas inferior do que um arquivo *Inseguro* e, dessa forma, apresenta menos probabilidade de ser malware.

Nota: Ocasionalmente, um arquivo pode ser classificado como *Inseguro* ou *Anormal* ainda que a pontuação mostrada não corresponda ao intervalo de tais classificações. Isso pode ser resultante de constatações atualizadas ou análises adicionais de arquivo após a detecção inicial. Para obter a análise mais atualizada, ative a opção Carregamento automático na Política do dispositivo.

Pontuação segundo a Cylance

Uma pontuação da Cylance é atribuída a cada arquivo considerado *Anormal* ou *Inseguro*. A pontuação representa o nível de confiança de que o arquivo é um conteúdo de malware. Quanto maior for o número, maior a confiança.

Ver informações de ameaças

A guia Proteção no Console mostra informações detalhadas das ameaças, os dispositivos em que as ameaças foram encontradas e as ações executadas nesses dispositivos quanto a essas ameaças.

Nota: A *Lista de ameaças* na guia Proteção tem colunas configuráveis. Clique na seta para baixo em qualquer coluna para acessar o menu e, em seguida, mostre/oculte vários detalhes das ameaças. O menu contém um submenu de filtragem.

Para ver os detalhes de uma ameaça

1. Faça login no Console (http://dellthreatdefense.com).
2. Clique na guia **Proteção** para mostrar uma lista de ameaças encontradas nesta organização.

3. Use o filtro na barra de menus esquerda para filtrar por Prioridade (Alta, Média ou Baixa) e por Status (*Quarentena, Ignorado, Inseguro ou Anormal*).

   Nota: Os números mostrados em vermelho no painel esquerdo indicam as ameaças pendentes que ainda não foram colocadas em *Quarentena ou Ignoradas*. Filtre esses itens para ver uma lista de arquivos que precisam ser analisados.

4. Para adicionar colunas de modo que informações adicionais de ameaças possam ser vistas, clique na seta para baixo ao lado de um dos nomes de coluna e, em seguida, selecione um nome de coluna.

5. Para ver informações adicionais sobre uma ameaça específica, clique no link do nome da ameaça (os detalhes são mostrados em uma nova página) ou clique em qualquer parte na linha da ameaça (os detalhes são mostrados na parte inferior da página). Ambas as visões mostram o mesmo conteúdo, mas terão diferentes estilos de apresentação. Entre os detalhes, estão uma visão geral dos metadados do arquivo, uma lista de dispositivos com a ameaça e relatórios de evidência.

   a. Metadados do arquivo

      - Classificação [atribuído pela equipe Advanced Threat and Alert Management (ATAM) da Cylance]
      - Pontuação segundo a Cylance (nível de confiança)
      - Convicção da AV Industry (links para VirusTotal.com para comparação com outros fornecedores)
      - Data em que foi encontrado pela primeira vez, Data em que foi encontrado pela última vez
      - SHA256
      - MD5
      - Informações do arquivo (autor, descrição, versão e assim por diante)
      - Detalhes da assinatura

   b. Dispositivos

      A Lista de dispositivos/zonas para uma ameaça pode ser filtrada pelo estado da ameaça (*Insegura, em Quarentena, Ignorada e Anormal*). Clique nos links de filtro de estado para mostrar os dispositivos com a ameaça nesse estado.

      - *Inseguro:* O arquivo é classificado como *Inseguro*, mas nenhuma ação foi feita.
      - *Em Quarentena*: O arquivo já foi *colocado em Quarentena* devido a uma configuração de política.
      - Ignorado: O arquivo foi *Ignorado* ou *Listado como seguro* pelo Administrador.
      - *Anormal:* O arquivo é classificado como *Anormal*, mas nenhuma ação foi feita.

   c. Relatórios de evidências

      - **Indicadores de ameaças:** Observações sobre um arquivo que o mecanismo do Cylance Infinity analisou. Esses indicadores ajudam a compreender a razão por trás da classificação de um arquivo e fornecem informações sobre os atributos e comportamento de um arquivo. Indicadores de ameaça são agrupados em categorias para auxiliar no contexto.
      - **Dados detalhados de ameaça:** A seção Dados detalhados de ameaça fornece amplo resumo das características estáticas e dinâmicas de um arquivo, incluindo metadados de arquivo adicionais, detalhes de estrutura de arquivo e comportamentos dinâmicos, como arquivos incluídos, chaves de registro criadas ou modificadas e URLs com os quais ele tentou se comunicar.

Para ver os indicadores de uma ameaça:

1. Faça login no Console (http://dellthreatdefense.com).
2. Clique em **Proteção** no menu superior para visualizar uma lista de ameaças (ou clique em **Dispositivos** e, em seguida, selecione um dispositivo).
3. Clique no nome de uma ameaça. A página Detalhes da ameaça é mostrada.
4. Clique em **Relatórios** de evidências.

Categorias dos indicadores da ameaça:

Cada categoria representa uma área que foi observada muitas vezes em softwares mal-intencionados e é baseada em uma análise profunda de mais de 100 milhões de arquivos binários. O relatório Indicadores de ameaças indica quantas dessas categorias estavam presentes no arquivo.

Anormalidades
O arquivo possui elementos inconsistentes ou anômalos de alguma maneira. Muitas vezes, são inconsistentes na estrutura do arquivo.

Coleta
O arquivo possui uma evidência de coleta de dados. Ele pode conter uma enumeração de configuração de dispositivo ou uma coleta de informações confidenciais.

Perda de dados
O arquivo possui uma evidência de vazamento de dados. Ele pode conter conexões de rede de saída, evidências de atuar como um navegador ou outras comunicações de rede.

Fraude
O arquivo possui uma evidência de tentativas de fraude. A fraude pode estar na forma de seções ocultas, de inclusão de código com o objetivo de evitar sua detecção ou de indicadores de marcação inadequada em metadados ou em outras seções.

Destruição
O arquivo possui uma evidência de habilidades destrutivas. A destruição abrange a capacidade de apagar recursos do dispositivo, como arquivos e diretórios.

Diversos
Todos os outros indicadores que não se encaixam nas demais categorias.

Nota: Ocasionalmente, as seções Indicadores de ameaças e Dados detalhados de ameaça não possuem resultados ou não estão disponíveis. Isso ocorre quando o arquivo não foi carregado. O log de depuração pode oferecer informações sobre o motivo de o arquivo não ter sido carregado.

Lidar com ameaças

O tipo de ação a ser executada em algumas ameaças pode depender do usuário atribuído a um dispositivo.
As ações aplicadas às ameaças podem ser aplicadas no nível do Dispositivo ou em um nível Global.
Você encontrará a seguir as diferentes ações que podem ser executadas contra ameaças detectadas ou arquivos:

- ***Quarentena:*** Colocar um arquivo específico em *Quarentena* impedirá que ele seja executado nesse dispositivo.

  Nota: Você pode colocar uma ameaça em quarentena usando a linha de comando em um dispositivo. Disponível somente com o Agente para Windows. Para obter mais informações, consulte Quarentena pela linha de comando.

- ***Quarentena global:*** Colocar um arquivo em *Quarentena global* impedirá que ele seja executado em qualquer dispositivo em toda a organização.

  Nota: Colocar um arquivo em *Quarentena* vai transferi-lo de seu local original para o diretório *Quarentena* (`C:\ProgramData\Cylance\Desktop\q`).

- ***Ignorar:*** *Ignorar* um arquivo específico permitirá que ele seja executado no dispositivo especificado.

- ***Segurança global***: Adicionar um arquivo à *Lista de arquivos seguros global* permite que ele seja executado em qualquer dispositivo em toda a organização.

  Nota: Ocasionalmente, o Threat Defense pode colocar em *Quarentena* ou denunciar um arquivo "bom" (isso poderá ocorrer se os recursos do arquivo se parecerem muito com os de arquivos maliciosos). *Ignorar* ou *Listar o arquivo como globalmente seguro* pode ser útil nessas instâncias.

- ***Fazer upload do arquivo:*** Faça o upload manualmente de um arquivo para o Cylance Infinity para análise. Se a opção Upload automático estiver ativada, os arquivos novos (aqueles que ainda não foram analisados pela Cylance) serão transferidos automaticamente por upload para o Cylance Infinity. Se o arquivo já existe no Cylance Infinity, o botão Fazer upload do arquivo estará indisponível (esmaecido).

- ***Fazer download do arquivo***: Faz o download de um arquivo para os seus próprios fins de teste. Esse recurso precisa ser ativado pela organização. O usuário precisa ser administrador. A ameaça precisa ter sido detectada com um agente versão 1320 ou superior.

  Nota: O arquivo precisa estar disponível no Cylance Infinity e todos os três hashes (SHA256, SHA1 e MD5) precisam corresponder entre o Cylance Infinity e o agente. Caso contrário, o botão Fazer download do arquivo não estará disponível.

Lidar com ameaças em um dispositivo específico

1. Faça login no Console (http://dellthreatdefense.com) como Administrador ou Gerente de zona.
2. Clique na guia **Dispositivos**.
3. Procure e selecione o dispositivo.
4. Como alternativa, pode existir um link disponível para o dispositivo na guia Proteção se ele estiver na lista com uma ameaça associada.
5. Todas as ameaças nesse dispositivo são apresentadas na lista na parte inferior da página. Selecione a ameaça para colocar em *Quarentena* ou *Ignorar* o arquivo nesse dispositivo.

Lida com as ameaças globalmente

Arquivos adicionados à *Lista de quarentena global ou Lista de arquivos seguros global* são colocados em Quarentena ou *Permitidos* em todos os dispositivos em todas as zonas.

1. Faça login no Console (http://dellthreatdefense.com) como um administrador.
2. Clique em **Configurações >** Lista global.
3. Clique em Quarentena global ou Arquivo seguro global.
4. Clique em **Adicionar arquivo**.
5. Adicione o SHA256 (obrigatório), o MD5 e o nome do arquivo, e o motivo de colocá-lo na *Lista global*.
6. Clique em **Enviar**.

Proteção – Controle de scripts

O Threat Defense fornece detalhes sobre os scripts Active e PowerShell que foram bloqueados ou que geraram alertas. Com o Controle de scripts ativado, os resultados são mostrados na guia Controle de scripts da página Proteção. Ela fornece detalhes sobre o script e os dispositivos afetados.

Para ver os resultados do Controle de scripts

1. Faça login no Console (http://dellthreatdefense.com) como um administrador.
2. Clique em Proteção.
3. Clique em Controle de scripts.
4. Selecione um script na tabela. Isso atualizará a tabela Detalhes com uma lista de dispositivos afetados.

Descrição das colunas do Controle de scripts

- **Nome do arquivo:** O nome do script.
- **Intérprete**: O recurso de controle de scripts que identificou o script.
- **Encontrado pela última vez:** A data e hora em que o script foi executado pela última vez.
- **Tipo de unidade**: O tipo de unidade em que o script foi encontrado (exemplo: disco rígido interno).
- **SHA256**: O hash SHA 256 do script.
- # de dispositivos: O número de dispositivos afetados por esse script.
- **Alerta:** O número de vezes em que houve um alerta para esse script. Pode ser múltiplas vezes para o mesmo dispositivo.
- **Bloquear:** O número de vezes que o script foi bloqueado. Pode ser múltiplas vezes para o mesmo dispositivo.

Descrição das colunas de detalhes

- **Nome do dispositivo:** O nome do dispositivo afetado pelo script. Clique no nome do dispositivo para ir para a página Detalhes do dispositivo.
- **Estado:** O estado do dispositivo (on-line ou off-line).
- **Versão do agente:** O número da versão do agente atualmente instalado no dispositivo.
- **Caminho de arquivo:** O caminho do arquivo a partir do qual o script foi executado.
- **Quando**: A data e hora em que o script foi executado.
- **Nome de usuário:** O nome do usuário logado no momento que o script foi executado.
- **Ação:** A ação tomada em relação ao script (Alertar ou Bloquear).

Lista global

A *Lista global* permite que um arquivo para ser marcado como *Quarentena* ou *Permite* esses arquivos em todos os dispositivos na organização.

- **Quarentena global:** Todos os Agentes na organização podem colocar em *Quarentena* qualquer arquivo que seja detectado no dispositivo na *Lista de quarentena global*.
- **Seguro:** Todos os Agentes na organização podem *Permitir* qualquer arquivo que seja detectado no dispositivo na *Lista* de arquivos seguros.
- **Não atribuído:** Toda ameaça identificada na organização não atribuída à *Quarentena global ou Lista de arquivos seguros.*

Alterar o status da ameaça

Para alterar um status de ameaça (*Quarentena global, Seguro ou Não atribuído*):

1. Faça login no Console (http://dellthreatdefense.com) como um administrador.
2. Selecione **Configurações > Lista global**.
3. Selecione a lista atual à qual a ameaça está atribuída. Por exemplo, clique em Não atribuído para alterar uma ameaça não atribuída para *Seguro ou Quarentena global.*
4. Selecione as caixas de seleção das ameaças a serem alteradas e clique em um botão de status.
    a. Seguro: Move os arquivos para a *Lista* de arquivos seguros.
    b. Quarentena global: Adiciona o arquivo à *Lista de quarentena global.*
    c. Remover da lista: Move os arquivos para a *Lista não atribuída*.

Adicionar um arquivo

Adicionar manualmente um arquivo à *Quarentena global ou Lista de arquivos seguros*. É necessário ter a informação hash SHA256 do arquivo sendo adicionado.

1. Faça login no Console (http://dellthreatdefense.com) como um administrador.
2. Selecione **Configurações > Lista global**.
3. Selecione a lista à qual adicionar o arquivo (*Quarentena global ou Lista de arquivos seguros*).
4. Clique em **Adicionar arquivo**.
5. Digite a informação hash SHA256. Ou então digite as informações MD5 e Nome do arquivo.
6. Explique o motivo de adicionar esse arquivo.
7. Clique em **Enviar**.

Lista de arquivos seguros por certificado

Os clientes podem adicionar os arquivos à *Lista de arquivos seguros* por certificado assinado, que permite que qualquer software personalizado que esteja devidamente assinado execute sem interrupção.

Nota: Esse recurso funciona atualmente apenas com sistemas operacionais Windows.

- Esta funcionalidade permite que os clientes estabeleçam uma *Lista de permissão/Lista segura* por um certificado assinado que seja representado pela impressão digital SHA1 do certificado.
- As informações do certificado são extraídas pelo Console (Marca de hora, Assunto, Emissor e Impressão digital). O certificado não é carregado nem salvo no Console.
- A marca de hora do certificado representa quando o certificado foi criado.
- O Console não verifica se o certificado é atual ou se está vencido.
- Se o certificado mudar (por exemplo, renovado ou novo), ele deve ser adicionado à *Lista segura* no Console.

1. Adicione os detalhes do certificado ao Repositório de certificados.
    a. Identifique a impressão digital do certificado para o PE (executável portátil) assinado.
    b. Selecione **Configurações > Certificados**.
    c. Clique em **Adicionar certificado**.

d. Clique em **Procurar por certificados para adicionar** ou arraste e solte o certificado na caixa de mensagem.

e. Se for procurar os certificados, a janela Abrir é mostrada para permitir a seleção dos certificados.

f. Ou então adicione as notas sobre esse certificado.

g. Clique em **Enviar**. O Emissor, o Assunto, a Impressão digital e as Notas (se inseridas) são adicionadas ao repositório.

2. Adicionar um Certificado à *Lista segura*.

a. Selecione **Configurações > Lista global**.

b. Clique na guia **Seguro.**

c. Clique em **Certificados**.

d. Clique em **Adicionar certificado**.

e. Selecione um certificado da *Lista segura*. Ou então selecione uma Categoria e adicione o motivo de adicionar esse certificado.

f. Clique em **Enviar**.

Ver as impressões digitais de uma ameaça

Na guia Proteção, a seção Detalhes da ameaça mostra agora a impressão digital do certificado. Na tela, selecione **Adicionar ao certificado** para adicionar o certificado ao Repositório.

Privilégios

Adicionar ao certificado é uma função disponível para somente para administradores. Se o certificado já tiver sido adicionado ao Repositório de certificados, o Console mostrará **Ir para certificado**. Os certificados são somente para exibição pelos Gerentes de zona, que veem a opção **Ir para certificado**.

Perfil

O menu de perfil (canto superior direito) permite o gerenciamento da sua conta, a exibição dos logs de auditoria do Console e o acesso à ajuda do produto.

Minha conta

Altere sua senha e a configuração de notificação por e-mail na página Minha conta.

1. Faça login no Console (http://dellthreatdefense.com).
2. Clique no menu de perfil no canto superior direito e selecione **Minha conta**.
3. Para alterar sua senha:

a. Clique em Alterar a senha.

b. Digite sua senha antiga.

c. Digite sua nova senha e digite-a novamente para confirmá-la.

d. Clique em Atualizar.

4. Marque ou desmarque a caixa de seleção para ativar ou desativar as notificações por e-mail. A ativação e a desativação da caixa de seleção são salvas automaticamente. As notificações por e-mail estão disponíveis apenas para administradores.

Log de auditoria

Lista suspensa do ícone de usuário (canto superior direito do Console)

O Log de auditoria contém informações sobre as seguintes ações executadas a partir do Console:

- Login (Bem-sucedido, Falha)
- Política (Adicionar, Editar, Remover)
- Dispositivo (Editar, Remover)
- Ameaça (Quarentena, Ignorar, Quarentena global, Lista de arquivos seguros)
- Usuário (Adicionar, Editar, Remover)
- Atualização do agente (Editar)

O Log de auditoria pode ser visto do Console navegando pela lista suspensa de perfil no canto superior direito do Console e selecionado **Log de auditoria**. Os logs de auditoria estão disponíveis apenas para administradores.

Configurações

A página Configurações mostra as abas Aplicativo, Gerenciamento de usuários, Política do dispositivo, Lista global e Atualização do agente. O item de menu Configurações está disponível apenas para administradores.

APLICATIVO

Agente do Threat Defense

Os dispositivos são adicionados à organização com a instalação do agente do Threat Defense em cada endpoint. Uma vez conectado ao Console, aplique a política (para gerenciar as ameaças identificadas) e organize os dispositivos de acordo com as necessidades organizacionais.

O agente do Threat Defense foi desenvolvido para usar uma quantidade mínima de recursos do sistema. O agente trata os arquivos ou os processos que executa como prioridade, pois esses eventos podem ser mal-intencionados. Os arquivos que simplesmente estão em disco (em armazenamento, mas não em execução) recebem uma prioridade mais baixa, pois, embora possam ser mal-intencionados, não apresentam uma ameaça imediata.

Agente para Windows

Requisitos do sistema

A Dell recomenda que o hardware (CPU, GPU e assim por diante) do endpoint atenda ou exceda os requisitos recomendados do sistema operacional de destino. As exceções são mencionadas abaixo (RAM, espaço disponível no disco rígido e requisitos adicionais de software).

Sistemas operacionais	• Windows 7 *(32 bits e 64 bits)* • Windows Embedded Standard 7 *(32 bits)* e Windows Embedded Standard 7 Pro *(64 bits)* • Windows 8 e 8.1 *(32 bits e 64 bits)** • Windows 10 (32 bits e 64 bits)** • Windows Server 2008 e 2008 R2 *(32 bits e 64 bits)**** • Windows Server 2012 e 2012 R2 *(64 bits)**** • Windows Server 2016 – Standard, Data Center e Essentials*****

RAM	• 2 GB
Espaço disponível no disco rígido	• 300 MB
Requisitos/softwares adicionais	• .NET Framework 3.5 (SP1) ou superior (*Windows apenas*) • Navegador de Internet • Acesso à Internet para login, acesso ao instalador e registro do produto • Direitos de administrador local para instalar o software
Outros requisitos	• Há suporte a TLX 1.2 com Agent 1422 ou superior, e requer .NET Framework 4.5 ou superior

Tabela 2: Requisitos do sistema para Windows

*Não suportado: Windows 8.1 RT
**Windows 10 Anniversary Update exige Agent 1402 ou superior.
***Não suportado: Server Core (2008 e 2012) e Minimal Server (2012).
****Exige Agente 1412 ou superior.

Para fazer download do arquivo de instalação

1. Faça login no Console (http://dellthreatdefense.com).
2. Selecione **Configurações > Aplicativo**.
3. Copiar o **Token de instalação**.

   O Token de instalação é uma sequência de caracteres gerados aleatoriamente que permite ao agente informar sua conta atribuída no Console. O Token de instalação é exigido durante a instalação, no assistente de instalação ou como uma definição de parâmetro de instalação.
4. Faça download do instalador.
   a. Selecione o sistema operacional.
   b. Selecione o tipo de arquivo a ser baixado.

      No Windows, a Dell recomenda o uso do arquivo MSI para a instalação do agente.

Dica: Se a Regra da zona estiver configurada, os dispositivos podem ser atribuídos automaticamente a uma zona caso o dispositivo atenda aos critérios da Regra da zona.

Instalar o agente – Windows

Confirme que todos os pré-requisitos são atendidos antes de instalar o Threat Defense. Consulte Requisitos do sistema.

1. Clique duas vezes em DellThreatDefenseSetup.exe (ou MSI) para iniciar a instalação.
2. Clique em **Instalar** na janela de configuração do Threat Defense.
3. Digite o Token de instalação fornecido pelo locatário do Threat Defense. Clique em **Avançar**.

   Nota: Entre em contato com o administrador do Threat Defense ou consulte o artigo da base de conhecimento Como: Gerenciar o Threat Defense no caso de o acesso ao Token de instalação não estar disponível.
4. Ou então altere a pasta de destino do Threat Defense.

   Clique em **OK** para iniciar a instalação.
5. Clique em **Concluir** para concluir a instalação. Selecione a caixa de seleção para abrir o Threat Defense.

Parâmetros de instalação para Windows

O agente pode ser instalado de forma interativa ou não interativa através do GPO, do Microsoft System Center Configuration Manager (normalmente conhecido como SCCM) e do MSIEXEC. Os MSIs podem ser personalizados com parâmetros embutidos (mostrados a seguir) ou os parâmetros podem ser fornecidos a partir da linha de comando.

Propriedade	Valor	Descrição
PIDKEY	<Token de instalação>	Entrada automática do Token de instalação
LAUNCHAPP	0 ou 1	0: O ícone da bandeja do sistema e a pasta do menu Iniciar permanecem ocultos durante o tempo de execução 1: O ícone da bandeja do sistema e a pasta do menu Iniciar não permanecem ocultos durante o tempo de execução (padrão)
SELFPROTECTIONLEVEL	1 ou 2	1: Apenas administradores locais podem fazer alterações no registro e em serviços 2: Apenas o administrador de sistema pode fazer alterações no registro e em serviços (padrão)
APPFOLDER	<Pasta de destino da instalação>	Especifica o diretório de instalação do agente O local padrão é C:\Arquivos de Programas\Cylance\Desktop
VenueZone	"Zone_Name"	Exige a versão de Agente 1382 ou superior •Adiciona dispositivos a uma zona. •Se a zona não existir, a zona será criada usando o nome fornecido. •Substitua o zone_name com nome de uma zona existente ou de uma zona que você deseja criar. **Aviso:** Adicionar espaços antes ou depois do nome da zona criará uma nova zona.

Tabela 3: Parâmetros de instalação para Windows

O exemplo de linha de comando a seguir mostra como executar o Microsoft Windows Installer Tool (MSIEXEC) passando os parâmetros de instalação PIDKEY, APPFOLDER e LAUNCHAPP:

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

A instalação é silenciosa e o log de instalação é salvo em **`C:\temp`**. Quando o agente está em execução, o ícone da bandeja do sistema e a pasta do Threat Defense do menu Iniciar permanecem ocultos. Informações adicionais sobre diferentes opções de linha de comando aceitas pelo MSIEXEC podem ser encontradas no artigo da base de conhecimento KB 227091.

Instalar o agente para Windows usando o Wyse Device Manager (WDM)

Esta seção explica como criar um script de instalação, como criar um pacote RSP para o WDM e como adicionar o pacote ao WDM para instalar em múltiplos clientes finos simultaneamente sem a interação do usuário.

Crie um script de arquivo em lote que realizará a instalação do Threat Defense por linha de comando. O WDM executa esse script durante a implementação.

1. Abra o Notepad. Usando os parâmetros de linha de comando acima, digite o comando a seguir para executar a instalação, substituindo **<INSTALLATION TOKEN>** pelo token fornecido a você: ***msiexec /i C:\TDx86\DellThreatDefense_x86.msi PIDKEY=<INSTALLATION TOKEN> /q***

   C:\TDx86 é usado para o nosso diretório, pois essa pasta será copiada para esse local no thin client durante a instalação.

2. Salve o arquivo com a extensão **.bat** para a pasta TDx86. Por exemplo, **TDx86_Install.bat**.

   Crie um Pacote RSP com o qual o aplicativo Threat Defense Agent pode ser instalado em vários thin clients simultaneamente sem a interação do usuário.

3. Abra o Scriptbuilder em um computador que tenha o WDM instalado.
4. Digite um nome e uma descrição para o pacote.
   - Selecione Other Packages (Outros pacotes) em Package Category (Categoria do pacote).
   - Selecione Windows Embedded Standard 7 em Operating System (Sistema operacional).
5. Adicione comandos de script para verificar se os sistemas de destino são WES7 ou WES7p.
   - Selecione Confirm Operating System (CO) em Script Command (Comando de script).
   - Para o valor do parâmetro Device OS (SO do dispositivo), digite o sistema operacional adequado.
6. Use as setas duplas para adicionar o item.
7. Pressione **OK** no prompt.
8. Adicione um comando para bloquear o cliente fino e impedir a interação do usuário.
   - Selecione **Comando de script > Bloquear usuário**. Não é necessário adicionar nenhum valor. No entanto, neste exemplo, um **Valor** de **Sim** é digitado, de modo que a tela inicial será removida se o instalador falhar ou houver um erro.
9. Adicione um comando para copiar arquivos para o cliente fino.
   - Selecione o comando de script **X Copy (XC**).
   - Para o valor do **Diretório de repositórios**, adicione ***** ao fim do existente **<regroot>**.
   - Para o valor do **Diretório de dispositivos**, digite o caminho para os arquivos a serem copiados nos thin clients de destino. Neste exemplo, o nome do pacote é usado.
10. Adicione um comando para executar o script de instalação .bat.
    - Selecione **Comando de script > Executar no dispositivo (EX)**.
    - Para o valor do Nome do arquivo do dispositivo, digite o caminho **C:\TDx86\TDx86_install.bat**. A pasta TDx86 foi copiada a partir do comando anterior XC.
    - Adicione **+** como o valor de Execução síncrona. Isso diz para o WDM aguardar até o arquivo sendo executado terminar para continuar.
11. Adicione um comando para apagar os arquivos copiados do cliente fino.
    - Adicione o comando de script **Excluir árvore (DT)**.
12. Adicione comandos para desativar o bloqueio.
    - Adicione o comando de script **Bloquear fim (EL**).

13. Para revisar, o pacote de script deve se mostrar similar ao seguinte.
    - Se estiver implementando o Threat Defense em sistemas WES7P, atualize a seção do sistema operacional para WES7P; caso contrário, a instalação do pacote falhará.
14. Salve o pacote.
    - Clique em **Salvar** e navegue para o local da pasta **TDx86**, se estas instruções foram seguidas, a pasta estará na Área de trabalho.
15. Feche o Scriptbuilder.
16. Inicie **WyseDeviceManager** para adicionar o pacote para WDM.
17. Navegue até **WyseDeviceManager > Gerenciador de Pacotes > Outros pacotes**.
18. Selecione **Ação > Novo > Pacote** na barra de menu.
19. Selecione **Registrar um pacote de um arquivo de Script (.RSP)** e clique em **Avançar**.
20. Vá até o local em que o arquivo RSP criado na etapa anterior está e clique em **Avançar**.
21. Certifique-se de que **Ativo** esteja selecionado e clique em **Avançar.**
22. Clique em **Avançar** uma vez que WDM esteja pronto para registrar o pacote.
23. Clique em **Finalizar** quando o pacote estiver registrado com sucesso.
24. O pacote estará visível em **Outros pacotes.**
25. Verifique o conteúdo do pacote:
    - Abra o Explorador de Arquivos e navegue até **C:\inetpub\ftproot\Rapport** e localize a pasta **TDx86**.
    - Abra a pasta TDx86 e verifique se a pasta contém o instalador e o arquivo .bat.

Há agora um pacote disponível no WDM que pode implementar o Threat Defense em múltiplos clientes finos WES7 sem a interação do usuário.

Colocar em quarentena usando a linha de comando

Você pode colocar um arquivo em quarentena usando a linha de comando em um dispositivo. Está opção conhecimento de hash SHA256 para a ameaça.

Nota: Esse recurso é para apenas para Windows e exige Agent 1432 ou superior.

1. Abra a linha de comando no dispositivo Windows. Exemplo: No menu Iniciar, pesquise por cmd.exe.
2. Acesse o Dell.ThreatDefense.exe e inclua o argumento **-q: <hash>**, onde <hash> é o hash SHA256 para o arquivo. Isso solicitará que o Agent envie o arquivo para a pasta de quarentena.

   Exemplo de linha de comando (Dell Threat Defense instalado no local padrão):

   ```
   "C:\Arquivos de Programas\Cylance\Desktop\Dell.ThreatDefense.exe" -q:
   14233d4875e148c370a6bbe40fccabccdbfa194dac9e8bd41b0eadcf2351f941
   ```

Desinstalar o agente

Para desinstalar o Agente em um sistema Windows, use o recurso Adicionar/Remover Programas ou usar a Linha de comando.

Desinstalar o Agente não remove o dispositivo do Console. É preciso remover manualmente o dispositivo do Console.

Antes de tentar desinstalar o Agente:

- Se a opção **Solicitar senha para desinstalar agente** estiver ativada, certifique-se de que você possui a senha para prosseguir com a desinstalação.
- Se a opção **Evitar o desligamento de serviços no dispositivo** estiver ativada, desative-a na política ou aplique uma política diferente aos dispositivos dos quais deseja desinstalar o Agente.

Desinstalar usando a opção Adicionar/Remover Programas

1. Selecione **Iniciar > Painel de Controle**.
2. Clique em **Desinstalar um programa**. Se a opção Ícones estiver selecionada ao invés de Categorias, clique em Programas e Recursos.
3. Selecione **Dell Threat Defense** e, em seguida, clique em **Desinstalar**.

Usar a Linha de comando

1. Abra o Prompt de Comando como Administrador.
2. Use os seguintes comandos com base no pacote de instalação que você usou para instalar o Agente.
    a. DellThreatDefense_x64.msi
        i. Desinstalação padrão: msiexec /uninstall DellThreatDefense_x64.msi
        ii. Instalador do Windows: msiexec /x DellThreatDefense_x64.msi
    b. DellThreatDefense_x86.msi
        i. Desinstalação padrão: msiexec /uninstall DellThreatDefense_x86.msi
        ii. Instalador do Windows: msiexec /x DellThreatDefense_x86.msi
3. Os comandos a seguir são opcionais:
    a. Para desinstalação silenciosa: /quiet
    b. Para silenciosa e oculta: /qn
    c. Para desinstalação de proteção de senha UNINSTALLKEY=<password>
    d. Para desinstalar um arquivo de log: /Lxv* <path>
        i. Isso cria um arquivo de log no caminho designado (<path>), incluindo o nome do arquivo.
        ii. Exemplo: C:\Temp\Uninstall.log

Agente macOS

Requisitos do sistema

A Dell recomenda que o hardware (CPU, GPU e assim por diante) do endpoint atenda ou exceda os requisitos recomendados do sistema operacional de destino. As exceções são mencionadas abaixo (RAM, espaço disponível no disco rígido e requisitos adicionais de software).

Sistemas operacionais	• Mac OS X 10.9 • Mac OS X 10.10 • Mac OS X 10.11 • macOS 10.12* • macOS 10.13**
RAM	• 2 GB
Espaço disponível no disco rígido	• 300 MB

Tabela 4: Requisitos do sistema para macOS

**Exige Agente 1412 ou superior.
** Exige Agente 1452 ou superior.

Para fazer download do arquivo de instalação

1. Faça login no Console (http://dellthreatdefense.com).
2. Selecione **Configurações > Aplicativo**.
3. Copiar o **Token de instalação**.

   O Token de instalação é uma sequência de caracteres gerados aleatoriamente que permite ao agente informar sua conta atribuída no Console. O Token de instalação é exigido durante a instalação, no assistente de instalação ou como uma definição de parâmetro de instalação.
4. Faça download do instalador.
   a. Selecione o sistema operacional.
   b. Selecione o tipo de arquivo a ser baixado.

Dica: Se a Regra da zona estiver configurada, os dispositivos podem ser atribuídos automaticamente a uma zona caso o dispositivo atenda aos critérios da Regra da zona.

Instalar o agente – macOS

Confirme que todos os pré-requisitos são atendidos antes de instalar o Threat Defense. Consulte Requisitos do sistema.

Nota: O Agente macOS apresentará a marca Dell em versões futuras.

1. Clique duas vezes em **`DellThreatDefense.dmg`** para montar o instalador.
2. Clique duas vezes no ícone *Proteger* da interface de usuário PROTEGER para começar a instalação.
3. Clique em **Continuar** para verificar se o sistema operacional e o hardware atendem aos requisitos.
4. Clique em **Continuar** na tela de boas-vindas.
5. Digite o Token de instalação fornecido pelo locatário do Threat Defense. Clique em **Continuar**.

Nota: Entre em contato com o administrador do Threat Defense ou consulte o artigo da base de conhecimento Como: Gerenciar o Threat Defense no caso de o acesso ao Token de instalação não estar disponível.

6. Ou então altere o local de instalação do Threat Defense.

   Clique em **Instalar** para iniciar a instalação.

7. Digite o nome de usuário e a senha do administrador. Clique em **Instalar software**.

8. Clique em **Fechar** na tela de resumo.

Parâmetros de instalação para macOS

O agente do Threat Defense pode ser instalado usando opções de linha de comando em um Terminal.
Os exemplos a seguir usam o instalador PKG. No DMG, simplesmente altere a extensão do arquivo no comando.

Nota: Confirme que os endpoints de destino atendem aos requisitos do sistema e que a pessoa que estará instalando o software tem as credenciais adequadas para a instalação do software.

Propriedade	Valor	Descrição
InstallToken		Token de instalação disponível no Console
NoCylanceUI		O ícone do agente não deve ser mostrado na inicialização. O padrão é Visível
SelfProtectionLevel	0 ou 1	1: Apenas administradores locais podem fazer alterações no registro e em serviços. 2: Apenas o administrador de sistema pode fazer alterações no registro e em serviços (padrão).
LogLevel	0, 1, 2 ou 3	0: Erro – Apenas mensagens de erro são registradas. 1: Advertência – As mensagens de erro e de advertência são registradas. 2: Informação (padrão) – As mensagens de erro, de advertência e de informação são registradas. Pode ser que forneçam alguns detalhes durante a solução de problemas. 3: Detalhado – Todas as mensagens são registradas. Durante uma solução de problemas, este é o nível de log recomendado. Entretanto, os tamanhos dos arquivos de log detalhados podem aumentar muito. A Dell recomenda ativar o nível Detalhado durante a solução de problemas e então retornar para Informação ao concluir a solução de problemas.
VenueZone	“zone_name”	Exige a versão de Agente 1382 ou superior •Adiciona dispositivos a uma zona. •Se a zona não existir, a zona será criada usando o nome fornecido. •Substitua o zone_name com nome de uma zona existente ou de uma zona que você deseja criar. **Aviso:** Adicionar espaços antes ou depois do nome da zona criará uma nova zona.

Tabela 5: Parâmetros de instalação para macOS

Instalar o agente

Instalar sem o Token de instalação

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

Instalar com o Token de instalação

```
echo [token_de_instalação] > cyagent_install_token

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

Nota: Substitua **[install_token]** pelo Token de instalação. O comando de eco emite um arquivo **cyagent_install_token**, que é um arquivo de texto com uma opção de instalação por linha. Esse arquivo precisa estar na mesma pasta que o pacote de instalação. Tenha cautela com extensões de arquivo, o exemplo acima mostra que o arquivo cyagent_install_token não tem extensão de arquivo. As configurações padrão no macOS apresentam extensões ocultas. Criar manualmente este ficheiro com edição de texto ou outro editor de texto pode adicionar automaticamente uma extensão de arquivo que terá de ser removida.

Parâmetros opcionais de instalação

Digite o seguinte no Terminal para criar um arquivo (**cyagent_install_token**) que o instalador usa para aplicar as opções inseridas. Cada parâmetro precisa estar em sua própria linha. Esse arquivo precisa estar na mesma pasta que o pacote de instalação.

Veja o exemplo a seguir. Nem todos os parâmetros são necessários no arquivo. O Terminal inclui tudo contido dentro das aspas simples no arquivo. Certifique-se de pressionar Enter/Return depois de cada parâmetro para deixar cada um em sua própria linha no arquivo.

Um editor de texto pode também ser usado para criar o arquivo que contém cada parâmetro (em sua própria linha). Esse arquivo precisa estar na mesma pasta que o pacote de instalação.

Exemplo:

```
echo 'InstallToken

NoCylanceUI

SelfProtectionLevel=2

LogLevel=2'> cyagent_install_token

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

Desinstalar o agente

Sem senha

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

Com senha

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

Nota: Substitua **thisismypassword** com a senha de desinstalação criada no Console.

Serviço do agente

Iniciar serviço

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

Encerrar serviço

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

Verificação da instalação

Verifique os seguintes arquivos para verificar se a instalação do agente foi bem-sucedida.

1. A pasta do programa foi criada.
    - Padrão do Windows: **`C:\Arquivos de Programas\Cylance\Desktop`**
    - Padrão do macOS: **`/Applications/DellThreatDefense/`**
2. O ícone do Threat Defense fica visível na bandeja do sistema do dispositivo de destino.

    Isso não se aplica se o parâmetro LAUNCHAPP=0 (Windows) ou NoCylanceUI (macOS) for usado.
3. Há uma pasta do Threat Defense em Menu Iniciar\Todos os programas no dispositivo de destino.

    Isso não se aplica se o parâmetro LAUNCHAPP=0 (Windows) ou NoCylanceUI (macOS) for usado.
4. O serviço Threat Defense foi adicionado e está em execução. Um serviço do Threat Defense deve ser mostrado na lista como em execução no painel Serviços do Windows do dispositivo de destino.
5. O processo Dell.ThreatDefense.exe está em execução. Um processo Dell.ThreatDefense.exe deve ser mostrado na guia Processos, no Gerenciador de tarefas do Windows do dispositivo de destino.
6. O dispositivo está se comunicando com o Console. Faça login no Console e clique na guia Dispositivos, o dispositivo de destino deve aparecer e ser mostrado com o estado on-line.

Interface do usuário do agente

A interface do usuário do agente é ativada por padrão. Clique no ícone do agente na bandeja do sistema para exibi-la. Alternativamente, o agente pode ser instalado para ocultar o ícone do agente da bandeja do sistema.

Guia Ameaças

Mostra todas as ameaças descobertas no dispositivo e a ação tomada. *Inseguro* significa que nenhuma ação é tomada com relação à ameaça. *Em Quarentena* significa que a ameaça foi modificada (para impedir a execução do arquivo) e foi movido para a pasta *Quarentena*. Ignorado significa que o arquivo é considerado segura pelo administrador e é *Permitido* executar no dispositivo.

Guia Eventos

Mostra todos os eventos de ameaça ocorridos no dispositivo.

Guia Scripts

Mostra todos os scripts mal-intencionados que foram executados no dispositivo e as ações tomadas em relação ao script.

Menu do agente

O menu do agente oferece acesso à ajuda e às atualizações do Threat Defense. É também oferecido acesso à interface avançada do usuário que oferece mais opções de menu.

Menu do agente

O menu do agente permite que os usuários realizem algumas ações no dispositivo. Clique com o botão direito no ícone do agente para ver o menu.

- **Verificar se há atualizações:** O agente verifica se há alguma atualização disponível e a instala. As atualizações são restritas à versão do agente permitida para a zona à qual o dispositivo pertence.
- **Verificar atualizações de política:** O Agent verifica se uma atualização de política está disponível. Isso pode ser alterado para a política existente ou para uma outra política que está sendo aplicadas ao Agent.

  Nota: Verifique se existe suporte para atualização de política versão 1422 (ou superior) para Windows e verão 1432 (ou superior) para MacOS.
- **Sobre**: Mostra uma caixa de diálogo com a versão do agente, o nome da política atribuída ao dispositivo, a última vez em que o agente verificou se há uma atualização e o token de instalação usado durante a instalação.
- **Sair:** Fecha o ícone do agente na bandeja do sistema. Isso não desativa nenhum dos serviços do Threat Defense.
- **Opções > Mostrar notificações**: Selecione esta opção para mostrar quaisquer novos eventos como notificações.

Ativar opções avançadas da interface do usuário do agente

O agente do Threat Defense oferece algumas opções avançadas por meio da interface do usuário para fornecer recursos nos dispositivos sem conectividade com o Console. O CylanceSVC.exe precisa estar em execução quando as Opções avançadas são ativadas.

Windows

1. Se o ícone Agente estiver visível na bandeja do sistema, clique com o botão direito no ícone e selecione **Sair.**
2. Abra o prompt de comando e digite o comando a seguir. Pressione Enter ao concluir.

   ```
   cd C:\Arquivos de Programas\Cylance\desktop
   ```

   Se o aplicativo foi instalado em outro local, navegue até esse local no prompt de comando.
3. Digite o comando a seguir e pressione Enter ao concluir.

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

   O ícone do agente é mostrado na bandeja do sistema.
4. Clique com o botão direito no ícone. São exibidas as opções *Registrar em log, Executar uma detecção e Gerenciamento de ameaças.*

macOS

1. Se o ícone Agente estiver visível no menu superior, clique com o botão direito no ícone e selecione **Sair.**
2. Abra o terminal e execute

   a. Sudo /Applications/DellThreatDefense/DellThreatDefense.app/Contents/MacOS/DellThreatDefenseUI –a

   Nota: Este é o caminho de instalação padrão para o Dell Threat Defense. Pode ser necessário editar o caminho para corresponder ao seu ambiente adequadamente.
3. A interface de usuário do Agente será exibida agora com opções adicionais.

Registrar em log

Selecione o nível das informações de log a serem coletadas do agente. O padrão é Informação. A Dell recomenda definir o nível de log para Tudo (Detalhado) durante solução de problemas. Ao concluir a solução de problemas, altere de volta para Informação (registrar todas as informações pode gerar arquivos de log muito grandes).

Executar uma detecção

Permite aos usuários especificar uma pasta para examinar se há ameaças.

1. Selecione **Executar uma detecção > Especificar pasta**.
2. Selecione a pasta a ser examinada e clique em **OK**. Todas as ameaças encontradas são mostradas na interface do usuário do agente.

Gerenciamento de ameaças

Permite que os usuários apaguem arquivos em *Quarentena* no dispositivo.

1. Selecione **Gerenciamento de ameaças > Excluir quarentena**.
2. Clique em **OK** para confirmar.

Máquinas virtuais

Há algumas recomendações para quando o agente do Threat Defense for ser usado em uma imagem de máquina virtual.

Quando estiver criando uma imagem de máquina virtual que será usada como modelo, desabilite as configurações de rede da máquina virtual antes de instalar o agente. Isso impede o agente de se comunicar com o Console e configurar os Detalhes do dispositivo. Isso evita a criação de dispositivos duplicados no Console.

Desinstalação protegida por senha

CONFIGURAÇÕES > Aplicativo

Os administradores podem exigir uma senha para desinstalar o agente. Quando for desinstalar o agente com uma senha:

- Se o instalador MSI foi usado para instalar, desinstale usando o MSI ou use o Painel de controle.
- Se o instalador EXE foi usado para instalar, use o EXE para desinstalar. Não é possível usar o Painel de controle caso o instalador EXE tenha sido usado e uma senha seja necessária para desinstalar.
- Se for desinstalar usando a linha de comando, adicione a string de desinstalação: **`UNINSTALLKEY = [MyUninstallPassword]`**.

Para criar uma senha de desinstalação

1. Faça login no Console (http://dellthreatdefense.com) com uma Conta de administrador.
2. Selecione **Configurações > Aplicativo**.
3. Marque a caixa de seleção para **Exigir senha para desinstalar agente.**
4. Digite uma senha.
5. Clique em **Salvar**.

Integrações

O Threat Defense Console oferece integração com alguns programas de terceiros.

Syslog/SIEM

O Threat Defense pode integrar-se ao software Security Information Event Management (SIEM) usando o recurso Syslog. Os eventos do Syslog são persistentes, ao mesmo tempo, os eventos do agente são persistentes no Console.

Para obter os endereços IP mais recentes para as mensagens do Syslog, entrar em contato com o suporte da Dell.

Tipos de eventos

Log de auditoria

Selecione esta opção para enviar o log de auditoria das ações do usuário realizadas no Console (site) ao servidor do Syslog. Os eventos do log de auditoria são sempre mostrados na tela Log de auditoria, mesmo quando essa opção está desmarcada.

Exemplo de mensagem de um log de auditoria sendo encaminhado para o Syslog

Dispositivos

Selecione esta opção para enviar os eventos do dispositivo ao servidor do Syslog.

- Quando um novo dispositivo é registrado, são recebidas duas mensagens para este evento: Registration e SystemSecurity.

  Exemplo de mensagem de evento de dispositivo registrado

- Quando um dispositivo é removido.

  Exemplo de mensagem de evento de dispositivo removido

- Quando uma política, uma zona, um nome ou um nível de log do dispositivo foi alterado.

  Exemplo de mensagem de evento de dispositivo atualizado

Ameaças

Selecione esta opção para registrar todas as ameaças recém-encontradas ou as alterações observadas para quaisquer ameaças existentes no servidor do Syslog. As alterações incluem a ameaça ser *Removida, posta em Quarentena, Ignorada ou Executada*.

Há cinco tipos de eventos de ameaça:

- **threat_found**: uma nova ameaça foi encontrada em um status *Inseguro*.
- **threat_removed**: uma ameaça existente foi *Removida*.
- **threat_quarantined**: uma nova ameaça foi encontrada no status de *Quarentena.*
- **threat_waived**: uma nova ameaça foi encontrada no status *Ignorada*.
- **threat_changed**: O comportamento de uma ameaça existente foi alterado (exemplos: Pontuação, Status de quarentena, Status de execução).
- **threat_cleared**: Uma ameaça que tenha sido Ignorada, adicionada à Lista de arquivos seguros ou excluída da quarentena em um dispositivo.

Exemplo de mensagem de evento de ameaça

Classificações de ameaças
Centenas de ameaças são classificadas diariamente como malware ou programas potencialmente indesejados (PUPs). Se esta opção for selecionada, você se inscreve para ser notificado da ocorrência desses eventos.

Exemplo de mensagem de classificação de ameaça

SIEM (Security Information and Event Management)
Especifica o tipo de servidor do Syslog ou o SIEM para os quais os eventos devem ser enviados.

Protocolo
Esta opção deve corresponder com o que está configurado no servidor do Syslog. As opções são UDP ou TCP. UDP normalmente não é recomendado, pois não garante a entrega da mensagem. A Dell recomenda usar TCP (padrão).

TLS/SSL
Disponível apenas se o protocolo especificado for TCP. TLS/SSL garante que a mensagem do Syslog seja criptografada em trânsito do Threat Defense ao servidor do Syslog. A Dell incentiva que os clientes selecionem esta opção. Verifique se o servidor do Syslog está configurado para escutar mensagens TLS/SSL.

IP/Domínio
Especifica o endereço IP ou o nome de domínio totalmente qualificado do servidor do Syslog que o cliente tem a configuração. Confirme com o especialista da rede interna para ter certeza de que as configurações de firewall e de domínio estão corretas.

Porta
Especifica o número da porta nos dispositivos que o servidor do Syslog escuta mensagens. Precisa ser um número entre 1 e 65535. Os valores típicos são: 512 para UDP, 1235 ou 1468 para TCP e 6514 para TCP Seguro (exemplo: TCP com TLS/SSL ativado).

Severidade
Especifica a severidade das mensagens que devem ser mostradas no servidor do Syslog. É um campo subjetivo e pode ser definido para qualquer nível preferido. O valor de severidade não altera as mensagens que são encaminhadas para o Syslog.

Recurso
Especifica que tipo de aplicativo está registrando a mensagem. O padrão é Interno (ou Syslog). É usado para categorizar as mensagens ao serem recebidas pelo servidor do Syslog.

Testar a conexão
Clique em **Testar conectividade** para testar as configurações de IP/domínio, porta e protocolo. Se os parâmetros inseridos forem válidos, depois de alguns momentos é exibida uma confirmação.

Autenticação personalizada

Use provedores de identidade (IdP) externa para fazer login no Console. Esta opção exige definir as configurações com o IdP para obter um certificado X.509 e um URL para a verificação do seu login no IdP. A Autenticação personalizada funciona com o Microsoft SAML 2.0. Foi confirmado que este recurso funciona com OneLogin, OKTA, Microsoft Azure e PingOne. Este recurso também fornece uma configuração personalizada e deve funcionar com outros provedores de identidade que seguem o Microsoft SAML 2.0.

Nota: A Autenticação personalizada não suporta Serviços de Federação do Active Directory (ADFS).

- **Autenticação forte**: Fornece acesso de autenticação multifator.
- **Login único**: Fornece acesso de login único (SSO, Single Sign-On).

Nota: Uma seleção de Autenticação forte ou Login único não afeta as configurações de Autenticação personalizada, pois todas as definições de configuração são tratadas pelo provedor de identidade (IdP).

- **Permitir login com senha**: Selecione esta opção para permitir o login no Console diretamente usando SSO. Esta opção permite testar a configuração SSO sem ter o acesso ao Console bloqueado. Uma vez conectado satisfatoriamente no Console usando o SSO, a Dell recomenda desativar este recurso.
- **Provedor:** Selecione o provedor de serviços da autenticação personalizada.
- **Certificado X.509:** Digite as informações da certificação X.509.
- **URL** de login: Digite o URL para a autenticação personalizada.

Relatório de dados de ameaças

Uma planilha que contém as informações a seguir sobre a organização:

- **Ameaças:** Mostra uma lista de todas as ameaças descobertas na organização. Essas informações incluem o nome do arquivo e o status do arquivo (*Inseguro, Anormal, Ignorado e em Quarentena*).
- **Dispositivos:** Mostra uma lista de todos os dispositivos na organização com um agente do Threat Defense instalado. Apresenta o nome do dispositivo, a versão do sistema operacional, a versão do agente e a política aplicada.
- **Indicadores de ameaças:** Apresenta cada ameaça e as características associadas à ameaça.
- **Limpo**: Mostra uma lista com todos os arquivos que foram *Limpos* em sua organização. Essas informações incluem arquivos que foram *Ignorados*, adicionados à *Lista de arquivos seguros* ou *Excluídos* da pasta de *Quarentena* de um dispositivo.
- **Eventos**: Mostra uma lista de todos os eventos relacionados ao Gráfico de eventos de ameaça no Painel, para os últimos 30 dias. Apresenta o hash do arquivo, o nome do dispositivo, o caminho do arquivo e a data em que o evento ocorreu.

Quando este recurso está ativado, o relatório é atualizado automaticamente à 1:00h no horário padrão do Pacífico (PST). Clique em **Regenerar relatório** para gerar manualmente uma atualização.

O Relatório de dados de ameaças fornece um URL e um token que podem ser usados para baixar o relatório sem ser preciso fazer login no Console. Um token pode também ser apagado ou regenerado, conforme necessário, o que permite controlar quem tem acesso ao relatório.

SOLUÇÃO DE PROBLEMAS

Esta seção fornece uma lista de perguntas para responder e arquivos para coletar ao solucionar problemas com o Threat Defense. Estas informações permitem que o suporte da Dell ajude na resolução dos problemas.

Esta seção também contém alguns problemas comuns e soluções sugeridas.

Suporte

Parâmetros de instalação

- Qual é o método de instalação? Forneça todos os parâmetros usados.
    - Exemplo – Windows: Use LAUCHAPP=0 ao instalar a partir da linha de comando para ocultar o ícone do agente e a pasta do menu Iniciar durante o tempo de execução.

    - Exemplo – macOS: Use SelfProtectionLevel=1 ao instalar a partir da linha de comando para desativar a Autoproteção no agente.
- Que etapas da instalação podem ser verificadas?
    - Exemplo – Windows: O instalador MSI ou EXE foi usado?
    - Exemplo – Qualquer SO: Foi usada alguma opção de linha de comando? Tais como interface de usuário sem agente ou modo silencioso.
- Ativar o log detalhado para a instalação.

Questões de desempenho

- Faça uma captura de tela do Gerenciador de tarefas (Windows) ou do Monitor de atividade (macOS) que mostre os processos do Threat Defense e o consumo de memória.
- Capture um despejo do processo do Threat Defense.
- Colete os logs de depuração.
- Colete a saída das Informações do sistema durante o problema.
    - Para Windows: msinfo32 ou winmsd
    - Para macOS: Informações do sistema
- Colete todos os Logs de eventos (Windows) ou Informações do console (macOS) relevantes.

Problemas de atualização, status e conectividade

- Confirme que a porta 443 está aberta no firewall e que o dispositivo pode criar uma conexão e conectar-se aos sites da Cylance.com.
- O dispositivo é mostrado na lista da página Dispositivos do Console? Ele está on-line ou off-line? Qual é o horário da Última conexão?
- O dispositivo está usando um proxy para se conectar à Internet? As credenciais estão configuradas corretamente no proxy?
- Reinicie o serviço do Threat Defense de modo que ele tente se conectar ao Console.
- Colete os logs de depuração.
- Colete a saída das Informações do sistema durante o problema.
    - Para Windows: msinfo32 ou winmsd
    - Para macOS: Informações do sistema

Ativar o log de depuração

Por padrão, o Threat Defense mantém os arquivos de log armazenados em **`C:\Program Files\Cylance\Desktop\log`**. Para fins de solução de problemas, o Threat Defense pode ser configurado para produzir mais logs detalhados.

Incompatibilidades do Controle de scripts

Problema:

Quando o Controle de scripts está ativado em alguns dispositivos, ele pode causar conflitos com outros softwares em execução nesses dispositivos. Esses conflitos geralmente são devido à injeção do agente em determinados processos que estão sendo chamados por outros softwares.

Solução:

Dependendo do software, esse problema pode ser resolvido adicionando exclusões de processos específicos à Política do dispositivo no Console. Outra opção é ativar o Modo de compatibilidade (chave de registro) em cada dispositivo afetado. Entretanto, se as exclusões não forem efetivas, a Dell recomenda desativar o Controle de scripts na Política do dispositivo que está afetando os dispositivos com o objetivo de restaurar a funcionalidade normal do dispositivo.

Nota: Esta solução está em Modo de compatibilidade para a versão do Agente 1370. A partir do agente 1382 e superior, o processo de injeção foi atualizado para compatibilidade com outros produtos.

Modo de compatibilidade

Adicione a seguinte chave de registro para ativar o Modo de compatibilidade:

1. Usando o Editor de registro, vá para **`HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`**.
2. Clique com o botão direito em **Área de trabalho**, clique em **Permissões**, assuma a propriedade e conceda **Controle total.** Clique em **OK**.
3. Clique com o botão direito em **Área de trabalho** e selecione **Novo > Valor binário**.
4. Nomeie o arquivo como **CompatibilityMode**.
5. Abra a configuração do registro e altere o valor para **01**.
6. Clique em **OK** e feche o Editor do Registro.
7. Pode ser necessário reiniciar o dispositivo.

Opções de linha de comando

Usando o Psexec:

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

Para executar um comando em vários dispositivos, use **`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}
```

APÊNDICE A: GLOSSÁRIO

Anormal	Um arquivo suspeito com uma pontuação inferior (1 – 59), com menos probabilidade de ser malware
Administrador	Gerenciador de locatários do Threat Defense
Agente	O Threat Defense Endpoint Host que se comunica com o Console
Log de auditoria	Log que registra as ações realizadas a partir do Threat Defense Console
Quarentena automática	Impede automaticamente a execução de todos os arquivos *Inseguros* e/ou *Anormais*

Upload automático	Faça o upload automaticamente de qualquer arquivo Executável portátil (PE) desconhecido, detectado como *Inseguro* ou *Anormal*, para análise da Cylance Infinity Cloud.
Console	Interface do usuário de gerenciamento do Threat Defense
Política do dispositivo	Política do Threat Defense que pode ser configurada pelo administrador da organização e que define como as ameaças são tratadas em todos os dispositivos
Quarentena global	Impede a execução de um arquivo globalmente (em todos os dispositivos em uma organização)
Lista de arquivos seguros global	Permite a execução de um arquivo globalmente (em todos os dispositivos em uma organização)
Infinity	O modelo matemático usado para pontuar os arquivos
Organização	Uma conta de locatário que usa o serviço Threat Defense
Colocar em quarentena	Impede a execução de um arquivo localmente (em um dispositivo específico)
Ameaças	Arquivos potencialmente mal-intencionados detectados pelo Threat Defense, classificados como *Inseguro ou Anormal*
Inseguro	Um arquivo suspeito com uma alta pontuação (60 – 100), com alta probabilidade de ser malware.
Ignorar	Permite a execução de um arquivo localmente (em um dispositivo específico)
Zona	Uma forma de organizar e agrupar dispositivos dentro de uma organização de acordo com a prioridade, funcionalidade e assim por diante.
Regra da zona	Recurso que ativa a automação de atribuição de dispositivos a Zonas específicas com base no endereço IP, no sistema operacional e no nome do dispositivo.

APÊNDICE B: TRATAR AS EXCEÇÕES

Há momentos em que os usuários precisam colocar manualmente em *Quarentena ou Permitir (Ignorar) um arquivo*. O Threat Defense fornece maneiras de lidar com exceções para cada dispositivo (*Local*), para um grupo de dispositivos (*Política*) ou para toda a organização (*Global*).

Arquivos

Local: *Colocar em Quarentena* ou *Ignorar* (Lista de arquivos seguros) um arquivo no dispositivo. Útil para *Bloquear* temporariamente ou *Permitir* um arquivo até que haja tempo para analisá-lo. Ignorar a um arquivo em um dispositivo também é útil se esse dispositivo for o único no qual o arquivo deverá ser autorizado a *Executar*. A Dell recomenda o uso de *Política* ou *Global* se esta ação precisar ser executada em vários dispositivos.

Política: Adiciona um arquivo à Lista de arquivos seguros em todos os dispositivos atribuídos a uma política. Útil para permitir um arquivo para um grupo de dispositivos (por exemplo, permitir que os dispositivos de TI executem ferramentas que poderiam ser usadas para fins mal-intencionados, como o PsExec). *Colocar em Quarentena* um arquivo a nível de Política não está disponível.

Global: *Colocar em Quarentena* ou na Lista de arquivos seguros um arquivo para a organização. *Colocar em Quarentena* um arquivo conhecido na organização. Adicionar à Lista de arquivos seguros um arquivo que é conhecido como sendo bom e é usado na organização, mas o Agente está sinalizando como mal-intencionado.

Scripts

Política: O Controle de scripts permite aprovar scripts a serem executados a partir de uma determinada pasta. Ao permitir a execução de scripts em uma pasta, quaisquer scripts em suas subpastas poderão também ser executados.

Certificados

Global: Adiciona certificados ao Console e, em seguida, adiciona-os à *Lista de arquivos seguros global*. Permite a execução de aplicativos assinados por esse certificado na organização.

Para adicionar um certificado, selecione **Configurações > Certificados**, em seguida, clique em **Adicionar certificado**.

Para adicionar o certificado *à **Lista de arquivos seguros global***, selecione **Configurações > Lista global**, marque a guia **Seguro**, selecione a guia **Certificados** e, em seguida, clique em **Adicionar certificado**.

APÊNDICE C: PERMISSÕES DO USUÁRIO

As ações que os usuários podem realizar dependem das permissões do usuário (função) atribuídas a eles. Em geral, os administradores podem realizar ações em qualquer lugar na organização. Os gerentes de zona e os usuários são restritos às zonas às quais estão atribuídos. Essa restrição inclui apenas a capacidade de acessar os dispositivos dentro de uma zona e de ver os dados de ameaças relacionados a esses dispositivos. Se um gerente de zona ou usuário não pode ver um dispositivo ou ameaça, é provável que o dispositivo não pertença a nenhuma zona atribuída a ele.

	USUÁRIO	GERENTE DE ZONA	ADMINISTRADOR
Atualização do agente			
Ver/Editar			X
Log de auditoria			
Ver			X
Dispositivos			
Adicionar dispositivos – Global			X
Adicionar dispositivos a uma zona			X
Remover dispositivos – Global			X
Remover dispositivos de uma zona		X	X
Editar o nome do dispositivo		X	X
Zonas			
Criar zonas			X
Apagar zonas			X
Editar o nome da zona – Todas			X
Editar o nome da zona atribuída		X	X
Política			
Criar política – Global			X
Criar a política de uma zona			X
Adicionar política – Global			X
Adicionar uma política a uma zona		X	X
Remover política – Global			X
Remover a política de uma zona		X	X
Ameaças			
Colocar arquivos em quarentena – Global			X
Colocar arquivos em quarentena em uma zona	X	X	X
Ignorar arquivos – Global			X
Ignorar arquivos em uma zona	X	X	X
Quarentena global/Seguro			X

	USUÁRIO	GERENTE DE ZONA	ADMINISTRADOR
Configurações			
Gerar ou apagar um token de instalação			X
Gerar ou apagar um URL de convite			X
Copiar um token de instalação	X	X	X
Copiar um URL de convite			X
Gerenciamento de usuários			
Atribuir usuários a qualquer zona			X
Atribuir usuários à zona gerenciada		X	X
Atribuir gerente de zona – Global			X
Atribuir gerente de zona às zonas gerenciadas		X	X
Apagar usuários do Console			X
Remover usuários de uma zona – Global			X
Remover usuários da zona gerenciada		X	X

APÊNDICE D: FILTRO DE GRAVAÇÃO COM BASE EM ARQUIVOS

O Dell Threat Defense Agent pode ser instalado em um sistema executando o Windows Embedded Standard 7 (Thin Client). Em dispositivos incorporados, pode não ser permitida a gravação no armazenamento do sistema. Nesse caso, o sistema pode usar um Filtro de gravação com base em arquivos (FBWF) para redirecionar quaisquer gravações do armazenamento do sistema para o cache na memória do sistema. Isso pode causar problemas fazendo com que o agente perca alterações sempre que o sistema for reiniciado.

Ao usar o Agente em um sistema incorporado, use o seguinte procedimento:

1. Antes de instalar o agente, desative o FBWF usando o comando: `fbwfmgr /disable`.
2. Reinicie o sistema. Isso permite que a desativação do FBWF entre em vigor.
3. Instale o Dell Threat Defense Agent.
4. Depois de instalar o agente, reative o FBWF usando o comando: `fbwfmgr /enable`.
5. Reinicie o sistema. Isso permite que a ativação do FBWF entre em vigor.
6. No FBWF, exclua as seguintes pastas:
    a. C:\Program Files\Cylance\Desktop – Excluir esta pasta permite que as atualizações do Agente permaneçam após o reinício do sistema.
7. Use o seguinte comando para excluir a pasta da área de trabalho: `fbwfmgr /addexclusion C: "\Program Files\Cylance\Desktop\"`
    a. Isso pressupõe que você esteja instalando no diretório padrão. Altere a exclusão para a pasta para a qual o Agente foi instalado.
8. Se você planeja armazenar ameaças na máquina para testar contra o Agente, exclua também o local de armazenamento do FBWF (`C:\Samples`, por exemplo).