Dell Threat Defense

Guia de instalação e administrador

Com tecnologia Cylance

v17.11.06

2017-11-06

Índice

DESCRIÇÃO GERAL

O Dell Threat Defense, com tecnologia Cylance, deteta e bloqueia malware antes que este afete o dispositivo. O Cylance faz uma abordagem matemática à identificação do malware, utilizando técnicas de aprendizagem automática em vez de assinaturas reativas, sistemas baseados em confiança ou sandboxes. Esta abordagem torna o novo malware, vírus, bots e futuras variantes inúteis. O Threat Defense analisa possíveis execuções de ficheiros quanto à presença de malware no sistema operativo.

Este guia explica como utilizar a Consola Threat Defense, instalar o Agente Threat Defense e como configurá-los.

Como funciona

O Threat Defense consiste num pequeno Agente, instalado em cada anfitrião, que comunica com a Consola baseada em nuvem. O Agente deteta e impede a presença de malware no anfitrião utilizando modelos matemáticos testados, não requer conectividade de nuvem contínua, nem atualizações de assinaturas contínuas, e funciona em redes abertas e isoladas. À medida que o panorama das ameaças evolui, o mesmo acontece com o Threat Defense. Ao treinar constantemente com conjuntos de dados reais de grande dimensão, o Threat Defense mantém-se um passo à frente dos atacantes.

- **Ameaça**: Quando uma ameaça é transferida para o dispositivo ou quando ocorre uma tentativa exploração.
- **Deteção de ameaças**: A forma como o Agente Threat Defense identifica as ameaças.
    - **Análise de processos**: Verifica os processos em execução no dispositivo.
    - **Controlo de execução**: Analisa os processos apenas aquando da execução. Isto inclui todos os ficheiros em execução aquando do arranque, que estão definidos para execução automática e que são executados manualmente pelo utilizador.
- **Análise**: A forma como os ficheiros são identificados como maliciosos ou seguros.
    - **Pesquisa na nuvem para pontuações de ameaças**: O modelo matemático na nuvem e é utilizado para pontuação de ficheiros.
    - **Local**: O modelo matemático incluído com o Agente. Permite a análise quando o dispositivo não está ligado à Internet.
- **Ação**: O que o Agente faz quando um ficheiro é identificado como uma ameaça.
    - **Global**: Verifica as definições de política, incluindo a *Quarentena Global* e *Listas seguras*.
    - **Local**: Verifica manualmente se há ficheiros *Em quarentena* ou *Renunciados*.

Sobre este guia

A Dell recomenda que os utilizadores se familiarizem com a Consola baseada em nuvem antes de instalar o Agente nos endpoints. Compreender a forma como os endpoints são geridos facilita a proteção e a manutenção dos mesmos. Este fluxo de trabalho é uma recomendação. Os utilizadores podem abordar a implementação no respetivo ambiente de uma forma que faça sentido para os mesmos.

Exemplo: As zonas ajudam a agrupar os dispositivos na organização. Por exemplo, a configuração de uma Zona com uma Regra de zona que adiciona automaticamente novos dispositivos a uma Zona com base em critérios selecionados (como o Sistema operativo, o Nome do dispositivo ou o Nome de domínio).

Nota: As instruções de instalação do Agente surgem após a obtenção de informações sobre Políticas e Zonas. Os utilizadores podem iniciar a instalação do Agente, se necessário.

CONSOLA

A Consola Threat Defense é um Web site no qual é necessário iniciar sessão, para visualizar as informações sobre ameaças da organização. A Consola faz com que seja mais fácil organizar os dispositivos em grupos (Zonas), configurar as ações a adotar quando são detetadas ameaças num dispositivo (Política) e transferir os ficheiros de instalação (Agente).

A Consola Threat Defense suporta os seguintes idiomas.

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

Tabela 1: Idiomas suportados pela Consola Threat Defense

Iniciar sessão

Aquando da ativação da sua conta, irá receber um e-mail com as suas informações de início de sessão na Consola Threat Defense. Clique na ligação apresentada no e-mail para aceder à página de início de sessão ou aceda a:

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

Política de dispositivos

Uma política define a forma como o Agente processa o malware que encontra. Por exemplo, coloca automaticamente em *Quarentena* o software maligno, ou ignora-o se estiver numa pasta específica. Todos os dispositivos devem estar numa política, e apenas pode ser aplicada uma política a um dispositivo. Restringir um dispositivo a uma única política elimina conflitos entre funcionalidades (como bloquear um ficheiro quando este devia ser Permitido para esse dispositivo). Se nenhuma política for atribuída, o dispositivo é colocado na política Predefinida.

Apenas o Controlo de execução está ativado para a política Predefinida, que analisa os processos apenas aquando da execução. Isto fornece proteção básica ao dispositivo, não deve interromper as operações no dispositivo e proporciona tempo para testar as funcionalidades de política antes de implementar a política no ambiente de produção.

Para adicionar uma política

1. Inicie sessão na Consola (http://dellthreatdefense.com) como Administrador. Apenas os Administradores podem criar Políticas.
2. Selecione **Definições > Política de dispositivos**.
3. Clique em **Adicionar política nova**.
4. Introduza um Nome da política e selecione as opções da política.
5. Clique em **Criar**.

Ações do ficheiro

DEFINIÇÕES > Política de dispositivos > [selecionar uma política] > Ações de ficheiro

As Ações do ficheiro disponibilizam diferentes opções para processamento dos ficheiros detetados pelo Threat Defense como *Não seguro* ou *Anormal*.

Sugestão: Para saber mais sobre a classificação de ficheiros *Não seguros* ou *Anormais*, consulte a secção Proteção – Ameaças.

Quarentena automática com Controlo de execução

Esta funcionalidade coloca em *Quarentena* ou bloqueia o ficheiro *Não seguro* ou *Anormal* para evitar que seja executado. Colocar um ficheiro em *Quarentena* irá mover o ficheiro da sua localização original para o diretório *Quarentena*, **`C:\ProgramData\Cylance\Desktop\q`**.

Algum malware é concebido para remover outros ficheiros em determinados diretórios. Este malware continua a fazê-lo até que o ficheiro seja removido com êxito. O Threat Defense modifica o ficheiro removido de modo a não ser executado, para impedir a remoção contínua do ficheiro removido por este tipo de malware.

Sugestão: A Dell recomenda vivamente que a *Quarentena automática* seja testada num pequeno número de dispositivos antes de ser aplicada no ambiente de produção. Os resultados do teste devem ser observados para assegurar que nenhuma aplicação essencial da empresa é bloqueada aquando da execução.

Carregamento automático

A Dell recomenda que os utilizadores ativem o Carregamento automático para os ficheiros *Não seguros* e *Anormais*. A Threat Defense carrega automaticamente todos os ficheiros *Não seguros* ou *Anormais* detetados pelo Cylance Infinity Cloud para realizar uma análise mais detalhada do ficheiro e fornecer detalhes adicionais.

O Threat Defense apenas carrega e analisa ficheiros PE (Portable Executable) desconhecidos. Se o mesmo ficheiro desconhecido for detetado em vários dispositivos da organização, o Threat Defense carrega apenas um ficheiro para análise, e não um ficheiro por dispositivo.

Lista segura de políticas

Adicione ficheiros considerados seguros, a nível da Política. O Agente não irá aplicar quaisquer ações contra ameaças a ficheiros incluídos nesta lista.

Para obter mais informações sobre como manusear exceções de ficheiros (*Quarentena* ou *Seguro*) nos diferentes níveis (*Local*, *Política* ou *Global*), consulte o Apêndice B: Processamento de exceções.

1. Inicie sessão na Consola (http://dellthreatdefense.com) como Administrador. Apenas os Administradores podem criar Políticas.
2. Selecione **Definições > Política de dispositivos**.
3. Adicione uma nova política ou edite uma política existente.
4. Clique em **Adicionar ficheiro** em *Lista segura de políticas*.
5. Introduza as informações do **SHA256**. Opcionalmente, inclua o MD5 e o Nome do ficheiro, se conhecidos.
6. Selecione uma **Categoria** para o ajudar a identificar o que este ficheiro faz.
7. Indique um motivo para adicionar este ficheiro à *Lista segura de políticas*.
8. Clique em **Enviar**.

Definições de proteção

`DEFINIÇÕES > Política de dispositivos > [selecionar uma política] > Definições de proteção`

Controlo de execução

O Threat Defense monitoriza sempre a execução de processos maliciosos e emite alertas aquando da tentativa de execução de elementos *Não seguros* ou *Anormais*.

Impedir o encerramento do serviço a partir do dispositivo

Se selecionar, o serviço Threat Defense é protegido contra encerramento manual ou através de qualquer outro processo.

Copiar amostras de malware

Permite a especificação de uma partilha de rede para copiar amostras de malware. Isto permite que os utilizadores façam a sua própria análise dos ficheiros que o Threat Defense considera *Não seguros* ou *Anormais*.

- Suporta as partilhas de rede CIFS/SMB.
- Especifique uma localização da partilha de rede. Exemplo: **`c:\test`**.
- Todos os ficheiros que cumpram os critérios são copiados para a partilha de rede, incluindo os duplicados. Não é efetuado qualquer teste de exclusividade.
- Os ficheiros não são comprimidos.
- Os ficheiros não são protegidos por palavra-passe.

AVISO: OS FICHEIROS NÃO SÃO PROTEGIDOS POR PALAVRA-PASSE. DEVE PROCEDER COM CUIDADO PARA QUE O FICHEIRO MALICIOSO NÃO SEJA ACIDENTALMENTE EXECUTADO.

Controlo de script

O Controlo de scripts protege os dispositivos bloqueando a execução de scripts Ativos e scripts PowerShell maliciosos.

1. Inicie sessão na Consola (http://dellthreatdefense.com).
2. Selecione **Definições > Política de dispositivos**.
3. Selecione uma política e clique em **Definições de proteção**.
4. Selecione a caixa de verificação para ativar o **Controlo de scripts**.
    a. **Alerta**: Monitoriza os scripts em execução no ambiente. Recomendado para implementação inicial.
    b. **Bloquear**: Apenas permite a execução de scripts a partir de pastas específicas. Utilize depois de testar em Modo de alerta.
    c. **Aprovar scripts nestas pastas (e subpastas)**: As exclusões de pastas de scripts devem especificar o caminho relativo da pasta.
    d. **Bloquear a utilização da Consola da Powershell**: Bloqueia o arranque da Consola da Powershell. Oferece segurança adicional através da proteção contra a utilização única de PowerShell.

    Nota: Se o script iniciar a Consola da Powershell, e o Controlo de scripts estiver configurado para bloquear a Consola da Powershell, o script irá falhar. Recomenda-se que os utilizadores alterem os seus scripts para invocarem scripts PowerShell e não a consola PowerShell.
5. Clique em **Guardar**.

Registos de agente

`DEFINIÇÕES > Política de dispositivos > [selecionar uma política] > Registos do Agente`

Ative os Registos do Agente na Consola para carregar ficheiros de registo e permitir a visualização na Consola.

1. Inicie sessão na Consola (http://dellthreatdefense.com).
2. Selecione **Definições > Política de dispositivos**.

3. Selecione uma política e clique em **Registos do agente**. Certifique-se de que o dispositivo selecionado para ficheiros de registo está atribuído a esta política.
4. Selecione **Ativar o carregamento automático dos ficheiros de registo** e clique em **Guardar**.
5. Clique no separador **Dispositivos** e selecione um dispositivo.
6. Clique em **Registos do agente**. São apresentados os ficheiros de registo.
7. Clique num ficheiro de registo. O nome do ficheiro de registo é a data do registo.

Melhores práticas para políticas

Aquando da criação inicial das políticas, a Dell recomenda a implementação de funcionalidades de política numa abordagem progressiva para assegurar que o desempenho e as operações não são afetados. Crie novas políticas com mais funcionalidades ativas, como a explicação da forma como o Threat Defense funciona no ambiente.

1. Quando criar as políticas iniciais, ative apenas o **Carregamento automático**.
    a. O Agente utiliza o Controlo de execução e Monitor de processos para analisar apenas os processos em execução.

       Isto inclui todos os ficheiros em execução aquando do arranque, que estão definidos para execução automática e que são executados manualmente pelo utilizador.

       O Agente apenas envia alertas para a Consola. Nenhum ficheiro está bloqueado ou em *Quarentena*.
    b. Verifique se existem quaisquer alertas de ameaça na Consola.

       O objetivo é detetar quaisquer aplicações ou processos que seja necessário executar no ponto final e que sejam considerados uma ameaça (*Anormais* ou *Não seguros*).

       Configure uma definição de política ou Consola para *Permitir* que estes ficheiros sejam executados se isto acontecer (por exemplo, *Exclua* pastas numa política, *Renuncie* aos ficheiros para esse dispositivo ou adicione os ficheiros à *Lista segura*).
    c. Utilize esta política inicial durante um dia para permitir a execução e análise de aplicações e processos normalmente utilizados no dispositivo.

IMPORTANTE: Poderá haver aplicações e processos periodicamente executados num dispositivo (por exemplo, uma vez por mês) que sejam considerados uma ameaça. É o utilizador que deve decidir se pretende executá-los durante esta política inicial, ou lembrar-se de que deve monitorizar o dispositivo aquando das execuções programadas.

2. Em Definições de proteção, ative **Eliminar processos não seguros em execução** após o Controlo de execução e o Monitor de processos estarem concluídos.

   Eliminar processos não seguros em execução e os respetivos Processos secundários elimina processos (e processos secundários), independentemente do estado, quando é detetada uma ameaça (EXE ou MSI).
3. Em Ações do ficheiro, ligue a **Quarentena automática**.

   A *Quarentena automática* desloca todos os ficheiros malignos para a pasta *Quarentena*.
4. Em Definições de proteção, ligue o **Controlo de scripts**.

   O Controlo de scripts protege os utilizadores contra scripts maliciosos em execução nos respetivos dispositivos.

   Os utilizadores podem aprovar a execução de scripts para pastas específicas.

   As exclusões da pasta Controlo de scripts devem especificar um caminho relativo da pasta (por exemplo, **`\Cases\ScriptsAllowed`**).

Zonas

Uma Zona é uma forma de organizar e gerir dispositivos. Por exemplo, os dispositivos podem ser divididos com base na geografia ou função. Se existir um grupo de dispositivos essenciais para a missão, esses dispositivos podem ser agrupados e atribuídos com prioridade elevada à Zona. Adicionalmente, são aplicadas políticas ao nível da Zona para que os dispositivos possam ser agrupados numa Zona com base na política que é aplicada a esses dispositivos.

Uma organização inclui uma Zona predefinida (Zona extra) à qual apenas os Administradores podem aceder. Os dispositivos novos são atribuídos à Zona extra, exceto se existirem Regras de zona que atribuam automaticamente os dispositivos às Zonas.

É possível atribuir Utilizadores e Gestores de zona às Zonas, permitindo-lhes visualizar a forma como a Zona está configurada. Isto permite também que os Utilizadores e os Gestores de zona acedam aos dispositivos pelos quais são responsáveis. Deve ser criada, pelo menos, uma Zona para permitir que qualquer pessoa com função de Utilizador ou Gestor de zona a visualize.

Um dispositivo pode pertencer a várias zonas, mas apenas pode ser aplicada uma política a um dispositivo. Permitir várias zonas proporciona alguma flexibilidade na forma como os dispositivos são agrupados. Restringir um dispositivo a uma única política elimina conflitos entre funcionalidades (por exemplo, bloquear um ficheiro quando este devia ser *Permitido* para esse dispositivo).

Poderá haver dispositivos existentes em várias Zonas pelos seguintes motivos:

- O dispositivo é manualmente adicionado a várias Zonas
- O dispositivo está em conformidade com as regras de mais do que uma Zona
- O dispositivo já está incluído numa Zona e está em conformidade com regras de outra Zona

Para ver formas recomendadas de utilizar as Zonas, consulte Melhores práticas para gestão de zonas.

Para adicionar uma zona

1. Inicie sessão na Consola (http://dellthreatdefense.com) como Administrador. Apenas os Administradores podem criar Zonas.
2. Clique em **Zonas**.
3. Clique em **Adicionar zona nova**.
4. Introduza um Nome da zona, selecione uma Política e selecione um Valor. A Zona deve ter uma Política associada. O Valor é a Prioridade da Zona.
5. Clique em **Guardar**.

Para adicionar dispositivos a uma zona

1. Inicie sessão na Consola (http://dellthreatdefense.com) com conta de Administrador ou Gestor de zona.
2. Clique em **Zonas**.
3. Clique numa Zona da *Lista de zonas*. Os dispositivos atuais nessa Zona são apresentados na *Lista de dispositivos da zona*, na parte inferior da página.
4. Clique em **Adicionar dispositivos a uma zona**. É apresentada uma lista de dispositivos.
5. Selecione cada dispositivo a adicionar à Zona e clique em **Guardar**. Opcionalmente, selecione **Aplicar a política de zona a dispositivos selecionados**. Adicionar um dispositivo a uma Zona não aplica automaticamente a Política de zona, uma vez que uma Zona poderá estar a ser utilizada para organizar dispositivos, e não para gerir a política relativa a esses dispositivos.

Para remover uma zona

1. Inicie sessão na Consola (http://dellthreatdefense.com) como Administrador. Apenas os Administradores podem remover Zonas.
2. Clique em **Zonas**.
3. Selecione as caixas de verificação das Zonas a remover.
4. Clique em **Remover**.
5. Clique em **Sim** na mensagem a solicitar confirmação para remoção da Zona selecionada.

Propriedades da zona

As propriedades da zona podem ser editadas conforme necessário.

Sobre a prioridade da zona

É possível atribuir às Zonas diferentes níveis de prioridade (Baixa, Normal ou Elevada) que classificam a significância e os pontos críticos dos dispositivos nessa Zona. Em várias áreas do dashboard, os dispositivos são apresentados por prioridade para ajudar a identificar os dispositivos que necessitam de intervenção imediata.

A prioridade pode ser definida quando uma Zona é criada, ou edite a Zona para alterar o valor da prioridade.

Para editar propriedades da zona

1. Inicie sessão na Consola (http://dellthreatdefense.com) como Administrador ou Gestor de zona.
2. Clique em **Zonas**.
3. Clique numa Zona da *Lista de zonas*.
4. Introduza um nome novo no campo **Nome** para alterar o Nome da zona.
5. Selecione uma política diferente no menu pendente **Política** para alterar a política.
6. Selecione um valor **Baixo**, **Normal** ou **Elevado**.
7. Clique em **Guardar**.

Regra de zona

Os dispositivos podem ser automaticamente atribuídos a uma Zona com base em determinados critérios. Esta automatização é útil quando adicionar vários dispositivos a Zonas. Quando forem adicionados novos dispositivos que correspondam a uma Regra de zona, esses dispositivos são automaticamente atribuídos a essa Zona. Se a opção **Aplicar agora a todos os dispositivos existentes** estiver selecionada, todos os dispositivos preexistentes que cumpram a regra são adicionados a essa Zona.

Nota: As Regras de zona adicionam automaticamente dispositivos a uma Zona, mas não podem remover dispositivos. Alterar o endereço IP ou o nome de anfitrião não remove esse dispositivo de uma Zona. Os dispositivos devem ser manualmente removidos da Zona em questão.

Existe uma opção para aplicar a Política de zona a dispositivos que são adicionados à Zona como resultado da correspondência com a Regra de zona. Isto significa que a política existente do dispositivo é substituída pela Política de zona especificada. A aplicação automática de uma política com base na Regra de zona deve ser utilizada com cuidado. Se o dispositivo corresponder a uma Regra de zona, pode ser atribuída a política errada ao mesmo dispositivo, se não for gerido corretamente.

Consulte a página Detalhes do dispositivo na Consola para visualizar a política aplicada a um dispositivo.

Para adicionar uma regra de zona

1. Inicie sessão na Consola (http://dellthreatdefense.com) como Administrador ou Gestor de zona.
2. Clique em **Zonas** e selecione uma Zona na *Lista de zonas*.
3. Clique em **Criar regra** em Regra de zona,
4. Especifique os critérios da Zona selecionada. Clique no sinal de adição para adicionar mais condições. Clique no sinal de subtração para adicionar mais condições.
5. Clique em **Guardar**.

Critérios da regra de zona

- **Quando é adicionado um dispositivo novo à organização**: Qualquer dispositivo novo adicionado à organização, que corresponda à Regra de zona, é adicionado à Zona.
- **Quando qualquer atributo de um dispositivo foi alterado**: Quando os atributos de um dispositivo existente mudam e passam a corresponder à Regra de zona, esse dispositivo existente é adicionado à Zona.
- **Endereço IPv4 no intervalo**: Introduza um intervalo de endereços IPv4.
- **Nome do dispositivo**:
    - Começa com: Os nomes dos dispositivos devem começar assim.
    - Contém: Os nomes dos dispositivos devem conter esta cadeia de caracteres, mas esta pode ser incluída em qualquer secção do nome.
    - Termina com: Os nomes dos dispositivos devem terminar assim.
- **Sistema operativo**:
    - É: O sistema operativo deve ser o sistema selecionado.
    - Não é: O sistema operativo não deve ser o sistema selecionado. Por exemplo, se a única Regra de zona indicar que o Sistema operativo não deve ser o Windows 8, todos os Sistemas operativos, incluindo dispositivos não Windows, são adicionados a esta Zona.
- **Nome de domínio**:
    - Começa com: O nome de domínio deve começar assim.
    - Contém: O nome de domínio deve conter esta cadeia de caracteres, mas esta pode ser incluída em qualquer secção do nome.
    - Termina com: O nome de domínio deve terminar assim.
- **Nome único**:
    - Começa com: O nome único deve começar assim.
    - Contém: O nome único deve conter esta cadeia de caracteres, mas esta pode ser incluída em qualquer secção do nome.
    - Termina com: O nome único deve terminar assim.
- **Membro de (LDAP)**:
    - É: O Membro de (Grupo) deve corresponder a estes elementos.
    - Contém: O Membro de (Grupo) deve conter estes elementos.

- **As seguintes condições são cumpridas**:
    - Todas: Todas as condições da Regra de zona devem coincidir para adicionar o dispositivo.
    - Qualquer: Para ser possível adicionar o dispositivo, pelo menos, uma condição da Regra de zona deve coincidir.
- **É aplicável a Política de zona**:
    - Não aplicar: Não aplicar a Política de zona à medida que os dispositivos são adicionados à Zona.
    - Aplicar: Aplicar a Política de zona à medida que os dispositivos são adicionados à Zona.

      Aviso: Aplicar automaticamente uma Política de zona poderá afetar negativamente alguns dos dispositivos da rede. Aplique a Política de zona automaticamente *apenas* se tiver a certeza de que a Regra de zona *apenas* vai encontrar dispositivos que *têm* de ter esta Política de zona específica.
- **Aplicar agora a todos os dispositivos existentes**: Aplica a Regra de zona a todos os dispositivos da organização. Não aplica a Política de zona.

Sobre os nomes únicos (DN)

Alguns factos que deve saber sobre os Nomes únicos (DN) quando os utilizar nas Regras de zona.

- Não são permitidos caracteres universais, mas a condição "Contém" tem resultados similares.
- As exceções e os erros de DN relacionados com o Agente são capturados nos ficheiros de registo.
- Se o Agente encontrar informações de DN no dispositivo, essas informações são automaticamente enviadas para a Consola.
- Quando adicionar informações de DN, as mesmas devem estar corretamente formatadas, do seguinte modo.
    - 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 da zona* apresenta todos os dispositivos atribuídos a esta zona. Os dispositivos podem pertencer a várias Zonas. Utilize **Exportar** para transferir um ficheiro CSV com informações para todos os dispositivos na *Lista de dispositivos da zona*.

Nota: Se não existir permissão para visualizar uma Zona, mas mesmo assim clicar na ligação para a Zona na coluna Zonas, é apresentada uma página Recurso não encontrado.

Melhores práticas para gestão de zonas

As Zonas podem ser entendidas como etiquetas, sendo que qualquer dispositivo pode pertencer a várias Zonas (ou ter várias etiquetas). Uma vez que não existem quaisquer restrições ao número de Zonas que podem ser criadas, as melhores práticas identificam três membros da Zona diferentes entre teste, política e granularidade da função do utilizador na organização.

Estas três Zonas consistem em

- Gestão de atualizações
- Gestão de políticas
- Gestão de acessos com base na função

Organização de zonas para gestão de atualizações

Uma das utilizações comuns das Zonas é ajudar a gerir as Atualizações do Agente. O Threat Defense suporta a versão mais recente e a versão anterior do Agente. Isto permite que a empresa suporte a alteração de janelas fixas e efetue testes rigorosos às novas versões do Agente.

São utilizados três tipos de Zonas sugeridos para orientar e especificar as fases de teste e produção do Agente:

- **Atualizar zona – Grupo de teste**: Estas Zonas devem ter dispositivos de teste que representem corretamente os dispositivos (e o software utilizado nesses dispositivos) na organização. Isto permite testar o Agente mais recente e assegura que a implementação deste Agente em dispositivos de Produção não interfere com os processos da empresa.
- **Atualizar zona – Grupo piloto**: Esta Zona pode ser utilizada como Zona de teste secundária ou como Zona de produção secundária. Como Zona de teste secundária, permite testar novos Agentes num grupo maior de dispositivos antes da implementação na Produção. Como Zona de produção secundária, isto iria permitir duas versões diferentes do Agente – mas, neste caso, é necessário gerir duas Zonas de produção diferentes.
- **Atualizar zona – Produção**: A maioria dos dispositivos devem estar na Zona atribuída à Produção.

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

Adicionar uma zona piloto ou de teste

1. Inicie sessão na Consola (http://dellthreatdefense.com) com conta de Administrador ou Gestor de zona.
2. Selecione **Definições > Atualização do Agente**.
3. Para Zonas piloto ou de teste:
    a. Clique em **Selecionar zonas de teste** ou **Selecionar zonas piloto**.
    b. Clique numa Zona.

    Se a Zona de produção estiver configurada com **Atualização automática**, as Zonas piloto e de teste não estão disponíveis. Altere a Atualização automática na Zona de produção para um valor diferente para ativar as Zonas piloto e de teste.
4. Clique em **Selecionar versão**.
5. Selecione uma versão do Agente para aplicar à Zona piloto ou de teste.
6. Clique em **Aplicar**.

Organização de zonas para gestão de políticas

Outro conjunto de Zonas a criar ajuda a aplicar políticas diferentes a tipos de endpoints diferentes. Considere os exemplos seguintes:

- 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 – Proteção elevada

A Dell sugere a aplicação de uma política por predefinição a todos os dispositivos nesta Zona de política em cada uma destas Zonas. Proceda com cuidado para não colocar um dispositivo em várias Zonas de política, uma vez que isto pode criar um conflito em relação a qual das políticas é aplicada. Tenha também em atenção que o motor da Regra de zona pode ajudar a organizar automaticamente estes anfitriões com base no IP, Nome de anfitrião, Sistema operativo e Domínio.

Organização de zonas para gestão de acessos com base na função

O acesso com base na função é utilizado para limitar o acesso de um utilizador da Consola a um conjunto secundário de dispositivos cuja gestão é da responsabilidade do mesmo. Isto poderá incluir a separação por Intervalo de IP, Nomes de anfitrião, Sistema operativo ou Domínio. Considere o agrupamento por localização geográfica, tipo ou ambos.

Exemplo:

- Zona RBAC – Computadores de secretária – Europa
- Zona RBAC – Computadores de secretária – Ásia
- Zona RBAC – Red Carpet (Executivos)

Utilizando os exemplos de Zona acima, pode ser atribuído um Gestor de zona à *Zona RBAC – Computadores de secretária – Europa*, e este apenas teria acesso a dispositivos dentro dessa Zona. Se o utilizador Gestor de zona tentar visualizar as outras Zonas, irá receber uma mensagem de erro com indicação de que não tem permissão para visualização. Apesar de um dispositivo poder estar atribuído a várias Zonas e o Gestor de zona conseguir visualizar esse dispositivo, se tentar visualizar as outras Zonas às quais o dispositivo está associado, não será possível fazê-lo e será visualizada uma mensagem de erro.

Noutras partes da Consola, como o painel de navegação, o Gestor de zona para a *Zona RBAC – Computadores de secretária – Europa* também estaria limitado a ameaças e outras informações relacionadas com a Zona ou dispositivos atribuídos a essa zona.

Aplicam-se as mesmas restrições aos Utilizadores atribuídos a uma Zona.

Gestão de utilizadores

Os administradores têm permissões globais e podem adicionar ou remover utilizadores, atribuir utilizadores a Zonas (como Utilizador ou Gestor de zona), adicionar ou remover dispositivos, criar políticas e crias Zonas. Os administradores podem também eliminar permanentemente utilizadores, dispositivos, políticas e Zonas da Consola.

Os Utilizadores e Gestores de zona apenas têm acesso e privilégios pertencentes à Zona a que estão atribuídos. Isto é aplicável a dispositivos atribuídos à Zona, ameaças detetadas nesses dispositivos e informações no dashboard.

Para uma lista abrangente de permissões de utilizador aprovadas para cada utilizador, consulte o Apêndice C: Permissões do utilizador.

Para adicionar utilizadores

1. Inicie sessão na Consola (http://dellthreatdefense.com) como Administrador. Apenas os Administradores podem criar Utilizadores.
2. Selecione **Definições > Gestão de utilizadores**.
3. Introduza o endereço de correio eletrónico do utilizador.
4. Selecione uma Função no menu pendente Função.
5. Quando adicionar um Gestor de zona ou um Utilizador, selecione a Zona para onde os pretende atribuir.
6. Clique em **Add** (Adicionar). É enviado um e-mail para o utilizador com uma ligação para criar uma palavra-passe.

Para alterar funções do utilizador

1. Inicie sessão na Consola (http://dellthreatdefense.com) como Administrador. Apenas os Administradores podem criar Utilizadores.
2. Selecione **Definições > Gestão de utilizadores**.
3. Clique num utilizador. É apresentada a página Detalhes do utilizador.
4. Selecione uma função e clique em **Guardar**.

Para remover utilizadores

1. Inicie sessão na Consola (http://dellthreatdefense.com) como Administrador. Apenas os Administradores podem criar Utilizadores.
2. Selecione **Definições > Gestão de utilizadores**.
3. Selecione a caixa de verificação do utilizador ou utilizadores a remover.
4. Clique em **Remover**.
5. Clique em **Sim** na mensagem a solicitar confirmação para remoção.

Relacionado com a rede

Configure a rede para permitir que o Agente Threat Defense comunique com a Consola através da Internet. Esta secção abrange as definições de firewall e as configurações de proxy.

Firewall

Não é necessário qualquer software no local para gerir os dispositivos. Os Agentes Threat Defense são geridos e reportam à Consola (interface do utilizador com base em nuvem). A porta 443 (HTTPS) é utilizada para comunicação e deve estar aberta na firewall para que os Agentes comuniquem com a Consola. A Consola é alojada por Amazon Web Services (AWS) e não tem quaisquer endereços IP fixos. Certifique-se de que os Agentes podem comunicar com os seguintes sites:

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

Como alternativa, permita todo o tráfego HTTPS para *.cylance.com.

Proxy

O suporte de proxy do Threat Defense é configurado através de uma entrada de registo. Quando um proxy é configurado, o Agente utiliza o endereço IP e a porta da entrada de registo para todas as comunicações externas para os servidores da Consola.

1. Aceda ao registo.

   Nota: Dependendo da forma como o Agente foi instalado (Modo protegido ativado ou não), poderá ser necessário ter privilégios elevados ou obter propriedade do registo.

2. No Editor de registo, aceda a **`HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`**.
3. Criar um novo Valor da cadeia (REG_SZ):
    - Nome do valor = ProxyServer
    - Dados do valor = definições de proxy (por exemplo, http://123.45.67.89:8080)

O Agente tenta utilizar as credenciais do utilizador atualmente com sessão iniciada para comunicar com a Internet em ambientes autenticados. Se for configurado um servidor proxy autenticado e não existir um utilizador com sessão iniciada no dispositivo, o Agente não consegue efetuar a autenticação no proxy nem comunicar com a Consola. Neste caso:

- Configure o proxy e adicione uma regra para permitir todo o tráfego para *.cylance.com.
- Utilize uma política de proxy diferente, permitindo o acesso de proxy não autorizados aos anfitriões Cylance (*.cylance.com).

Desta forma, se nenhum utilizador tiver sessão iniciada no dispositivo, não é necessário que o Agente efetue a autenticação e deve ser possível efetuar ligação à nuvem e comunicar com a Consola.

Dispositivos

Depois de instalar um Agente num endpoint, este fica disponível como dispositivo na Consola. Comece a gerir dispositivos através da atribuição de políticas (para lidar com *Ameaças* identificadas), de dispositivos de grupo (utilizando *Zonas*) e tomando medidas manuais em cada dispositivo (*Quarentena* e *Renúncia*).

Gestão de dispositivos

Os dispositivos são computadores com um Agente Threat Defense. Efetue a gestão dos dispositivos a partir da Consola.

1. Inicie sessão na Consola (http://dellthreatdefense.com) como Administrador. Apenas os Administradores podem gerir Dispositivos.
2. Clique em **Dispositivos**.
3. Selecione a caixa de verificação de um dispositivo para permitir as seguintes ações:
    - **Exportar**: Cria e transfere um ficheiro CSV. O ficheiro contém informações do dispositivo (Nome, Estado e Política) para todos os dispositivos da organização.
    - **Remover**: Remove os dispositivos selecionados da *Lista de dispositivos*. Isto 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 Zona ou Zonas.
4. Clique num dispositivo para visualizar a página Detalhes do dispositivo.
    - **Informações do dispositivo**: Apresenta informações como o Nome de anfitrião, a Versão do Agente e a Versão do Sistema operativo.
    - **Propriedades do dispositivo**: Permite alterar o Nome do dispositivo, a Política, as Zonas e o Nível de registo.
    - **Ameaças e atividades**: Apresenta informações da ameaça e outras atividades relacionadas com o dispositivo.

5. Clique em **Adicionar dispositivo novo** para apresentar uma caixa de diálogo com um token de instalação e links para transferir o programa de instalação do Agente.
6. Na coluna Zonas, clique no Nome da zona para visualizar a página Detalhes da zona.

Ameaças e Atividades

Apresenta informações da ameaça e outras atividades relacionadas com o dispositivo selecionado.

Ameaças

Apresenta todas as ameaças detetadas no dispositivo. Por predefinição, as ameaças são agrupadas por estado (*Não seguro*, *Anormal*, *Em quarentena* e *Renunciado*).

- **Exportar**: Cria e transfere um ficheiro CSV que contém informações sobre todas as ameaças detetadas no dispositivo selecionado. As informações da ameaça incluem informações como Nome, Caminho do ficheiro, Pontuação Cylance e Estado.
- **Quarentena**: Coloca as ameaças selecionadas em *Quarentena*. Trata-se de uma *Quarentena local*, o que significa que esta ameaça apenas é colocada em *Quarentena* neste dispositivo. Para colocar uma ameaça em *Quarentena* para todos os dispositivos na organização, certifique-se de que a caixa de verificação **Colocar esta ameaça em quarentena sempre que for encontrada em qualquer dispositivo** está selecionada (*Quarentena global*) quando um ficheiro é colocado em *Quarentena*.
- **Renunciar**: Altera o estado das ameaças selecionadas para *Renunciadas*. Um ficheiro *Renunciado* pode ser executado. Trata-se de uma *Renúncia local*, o que significa que este ficheiro apenas é permitido neste dispositivo. Para permitir este ficheiro em todos os dispositivos na organização, selecione a caixa de verificação **Marcar como seguro em todos os dispositivos** (*Lista segura*) quando um ficheiro é *Renunciado*.

Tentativas de exploração

Apresenta todas as tentativas de exploração detetadas no dispositivo. Isto inclui informações sobre o Nome do processo, ID, Tipo e Ação adotada.

Registos de agente

Apresenta ficheiros de registo carregados pelo Agente no dispositivo. O nome do ficheiro de registo é a data do registo.

Para visualizar ficheiros de registo do Agente:

1. Carregue o Ficheiro de registo atual para um único dispositivo.
   a. Clique em Dispositivos > Registos do Agente.
   b. Clique em **Carregar ficheiro de registo atual**. Isto poderá demorar alguns minutos, dependendo do tamanho do ficheiro de registo.

OU

1. Definições da política:
   a. Clique em Definições > Política de dispositivos > [selecionar uma política] > Registos do Agente.
   b. Clique em Ativar o carregamento automático dos ficheiros de registo.
   c. Clique em **Guardar**.

Para visualizar registos verbosos, altere o Nível de registo do Agente antes de carregar quaisquer ficheiros de registo.

1. Na Consola: **Dispositivos > [clique num dispositivo]**, selecione **Verboso** no menu pendente do Nível de registo do Agente e clique em **Guardar**. Após o carregamento dos ficheiros de registo verbosos, a Dell recomenda que volte a alterar o Nível de registo do Agente para *Informação*.
2. No dispositivo, feche a interface do utilizador Threat Defense (clique com o botão direito do rato no ícone do Threat Defense no tabuleiro do sistema e, em seguida, clique em **Sair**).

OU

1. Abra a Linha de comandos como Administrador. Introduza a seguinte linha de comandos e, em seguida, prima **Enter**.

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

2. Introduza a seguinte linha de comandos e, em seguida, prima **Enter**.

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

3. O ícone do Threat Defense é apresentado no tabuleiro do sistema. Clique com o botão direito do rato, selecione **Registo**, em seguida, clique em **Tudo** (o mesmo que Verboso na Consola).

OU (para macOS)

1. Saia da interface do utilizador atualmente em execução.
2. Execute o comando seguinte a partir do terminal.

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

3. Clique com o botão direito do rato na nova interface do utilizador quando esta abrir. Selecione **Registo > Tudo**.

Controlo de script

Apresenta todas as atividades relevantes para o Controlo de scripts, como scripts negados.

Dispositivos duplicados

Quando o Agente Threat Defense é instalado pela primeira vez num dispositivo, é criado um identificador único que é utilizado pela Consola para identificar e mencionar esse dispositivo. No entanto, alguns eventos, como a utilização de uma imagem de máquina virtual para criar vários sistemas, poderão dar origem a um segundo identificador para o mesmo dispositivo. Selecione o dispositivo e clique em **Remover** se for apresentada uma entrada duplicada na página Dispositivos na Consola.

Para ajudar a identificar estes dispositivos, utilize a funcionalidade de ordenação por coluna na página Dispositivos para ordenar e comparar os dispositivos, normalmente por nome do dispositivo. Em alternativa, a *Lista de dispositivos* pode ser exportada como ficheiro .CSV e visualizada no Microsoft Excel ou algo semelhante com funcionalidades potentes de ordenação/organização.

Exemplo utilizando o Microsoft Excel

1. Abra o ficheiro CSV do dispositivo no Microsoft Excel.
2. Selecione a coluna com o nome do dispositivo
3. No separador Base, selecione Formatação condicional > Realçar regras das células > Valores duplicados.
4. Certifique-se de que **Duplicado** está selecionado e, em seguida, selecione uma opção de destaque.
5. Clique em **OK**. Os itens duplicados são realçados.

Nota: O comando Remover apenas remove o dispositivo da página Dispositivo. Isto não emite qualquer comando de desinstalação para o Agente Threat Defense. O Agente deve ser desinstalado no endpoint.

Atualização do Agente

A manutenção e gestão de Agentes Threat Defense são simples. Os Agentes transferem automaticamente as atualizações a partir da Consola, e a Consola é mantida pelo Cylance.

O Agente verifica a Consola a cada 1-2 minutos. A Consola comunica o estado atual do Agente (*Online* ou *Offline*, *Não seguro* ou *Protegido*), informações sobre a versão, sistema operativo e estado de ameaça.

O Threat Defense disponibiliza atualizações para o Agente mensalmente. Estas atualizações podem incluir revisões das configurações, novos módulos e alterações aos programas. Quando estiver disponível uma atualização para o Agente (conforme comunicado pela Consola em Definições > Atualizações do Agente), o Agente transfere e aplica automaticamente a atualização. Para controlar o tráfego de rede durante as atualizações do Agente, todas as organizações estão configuradas para acomodar, no máximo, 1000 atualizações de dispositivo em simultâneo. Além disso, os utilizadores podem desativar a funcionalidade de atualização automática, se preferirem.

Nota: O número máximo de dispositivos para atualização em simultâneo podem ser modificados pelo Apoio Técnico da Dell.

Atualização com base na zona

A Atualização com base na zona permite que a organização avalie um novo Agente num conjunto secundário de dispositivos antes de o implementar em todo o ambiente (Produção). É possível adicionar uma ou mais Zonas atuais a uma das duas Zonas de teste (Teste e Piloto), que podem utilizar um Agente diferente do da Produção.

Para configurar atualizações com base em zonas:

1. Inicie sessão na Consola (http://dellthreatdefense.com) com uma conta de Administrador.
2. Selecione **Definições > Atualização do Agente**. São apresentadas as três versões mais recentes do Agente.

   Se a Zona de produção estiver configurada com **Atualização automática**, as Zonas piloto e de teste não estão disponíveis. Altere a Atualização automática na Zona de produção para um valor diferente para ativar as Zonas piloto e de teste.
3. Selecione uma versão específica do Agente na lista pendente Produção.
4. Para 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** impede todos os dispositivos de Produção de atualizar o Agente.
5. Para a Zona de teste, selecione uma ou mais Zonas na lista pendente Zona e, em seguida, selecione uma versão específica do Agente na lista pendente de versões.
6. Se pretendido, repita o passo 5 para a Zona piloto.

Nota: Quando um dispositivo é adicionado a uma Zona que faz parte da Zona piloto ou de teste, o mesmo começa a utilizar a versão do Agente da Zona piloto ou de teste. Se o dispositivo pertencer a mais do que uma Zona, e uma dessas Zonas pertencer à Zona piloto ou de teste, a versão do Agente da Zona piloto ou de teste tem prioridade.

Para acionar uma atualização do Agente

Para acionar uma atualização do Agente antes do intervalo programado seguinte:

1. Clique com o botão direito do rato no ícone do Agente do Threat Defense no tabuleiro do sistema e selecione **Procurar atualizações**.
2. Reinicie o serviço Threat Defense. Isto força-o a verificar imediatamente a Consola.

OU

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

  `Dell.ThreatDefense.exe – atualização`

Painel

A página Dashboard é apresentada depois de iniciar sessão na Consola Threat Defense. O Dashboard fornece uma descrição geral das ameaças no ambiente e proporciona acesso a diferentes informações da Consola a partir de uma página.

Estatísticas da ameaça

As estatísticas da ameaça apresentam o número de ameaças encontradas nas *Últimas 24 horas* e o *Total* da organização. Clique numa *Estatística da ameaça* para aceder à página Proteção e visualize a lista de ameaças relativas a essa estatística.

- **Ameaças em execução**: Ficheiros identificados como ameaças atualmente em execução em dispositivos da organização.
- **Ameaças em execução automática**: Ameaças definidas para serem executadas automaticamente.
- **Ameaças em quarentena**: Ameaças em *Quarentena* nas últimas 24 horas e o total.
- **Exclusivo do Cylance**: As ameaças identificadas pelo Cylance, mas não por antivírus de outras fontes.

Percentagens de proteção

Apresenta percentagens para Threat Protection e Proteção do dispositivo.

- **Threat Protection**: A percentagem de ameaças para as quais foi adotada uma ação (Em quarentena, Quarentena global, Dispensada e Listas seguras).
- **Proteção do dispositivo**: A percentagem de dispositivos associados a uma política com Quarentena automática ativada.

Ameaças por prioridade

Apresenta o número total de ameaças que requerem uma ação (*Quarentena*, *Quarentena global*, *Renúncia* e *Listas seguras*). As ameaças são agrupadas por prioridade (Elevada, Média e Baixa). Esta descrição geral apresenta o número total de ameaças que necessitam de ação, separa o total por prioridade, indica uma percentagem total e o número de dispositivos afetados.

As ameaças são apresentadas por prioridade no canto inferior esquerdo da página Dashboard. É especificado o número total de ameaças numa organização agrupadas pelas respetivas classificações de prioridade.

Uma ameaça é priorizada como Baixa, Média ou Alta com base no número de atributos seguintes que possui:

- O ficheiro tem uma pontuação Cylance superior a 80.
- O ficheiro encontra-se neste momento em execução.
- O ficheiro foi executado anteriormente.
- O ficheiro encontra-se definido para execução automática.
- A prioridade da Zona em que a ameaça foi detetada.

Esta classificação ajuda os administradores a determinarem as ameaças e dispositivos a abordar em primeiro lugar. Clique na ameaça ou no Número do dispositivo para visualizar os detalhes do Dispositivo e da ameaça.

Eventos de Ameaça

Apresenta um gráfico de linhas com o número de ameaças detetadas nos últimos 30 dias. As linhas estão identificadas por cores para ficheiros *Não seguros*, *Anormais*, em *Quarentena*, *Renunciados* e *Desmarcados*.

- Coloque o cursor sobre um ponto do gráfico para visualizar os detalhes.
- Clique numa das cores na legenda para mostrar ou ocultar essa linha.

Classificações de ameaças

Apresenta um mapa térmico dos tipos de ameaças detetadas na organização, como vírus ou malware. Clique num item no mapa térmico para aceder à página Proteção e visualizar uma lista de ameaças desse tipo.

Listas dos cinco principais

Apresenta listas com as Cinco principais ameaças detetadas na maioria dos dispositivos, os Cinco principais dispositivos com mais ameaças e as Cinco principais zonas com mais ameaças na organização. Clique num item da lista para obter mais detalhes.

As listas dos Cinco principais no painel de navegação destacam as ameaças *Não seguras* na organização que não foram alvo de uma ação, como, por exemplo, colocadas em *Quarentena* ou *Renunciadas*. A maioria das vezes, estas listas deverão estar vazias. Apesar de as ameaças *Anormais* também precisarem de uma ação, o objetivo das Listas dos Cinco principais é chamar a sua atenção para ameaças críticas.

Proteção – Ameaças

O Threat Defense faz mais do que classificar meramente os ficheiros como *Não seguros* ou *Anormais*. Pode fornecer detalhes sobre as características estáticas e dinâmicas de ficheiros. Isto permite aos administradores não só bloquear ameaças, mas também compreender o comportamento das mesmas de modo a mitigar ou responder às ameaças.

Tipo de Ficheiro

Não seguro: Um ficheiro com uma pontuação entre 60 e 100. Um ficheiro *Não seguro* é um ficheiro em que o motor Advanced Threat Protection encontra atributos que se assemelham bastante a software maligno.

Anormal: um ficheiro com uma pontuação entre 1 e 59. Um ficheiro Anormal possui alguns atributos de software maligno, mas menos do que um ficheiro *Não seguro*, sendo menor a probabilidade de se tratar de software maligno.

Nota: Ocasionalmente, um ficheiro pode ser classificado como *Não seguro* ou *Anormal*, apesar de a pontuação apresentada não corresponder ao intervalo da classificação. Isto poderá ser o resultado de descobertas atualizadas ou análises adicionais aos ficheiros após a deteção inicial. Para a análise mais atualizada, ative o Carregamento automático na Política de dispositivos.

Pontuação Cylance

É atribuída uma pontuação Cylance a cada ficheiro que é considerado *Anormal* ou *Não seguro*. A pontuação representa o nível de confiança de que o ficheiro é software maligno. Quanto maior o número, mais elevada a confiança.

Visualizar informações da ameaça

O separador Proteção na Consola apresenta informações detalhadas da ameaça, os Dispositivos onde foram detetadas ameaças e as ações adotadas nesses Dispositivos para as mesmas.

Nota: A *Lista de ameaças* no separador Proteção tem colunas configuráveis. Clique na seta para baixo em qualquer coluna para aceder ao menu e, em seguida, Mostrar/Ocultar vários detalhes da ameaça. O menu inclui um menu secundário de filtragem.

Para visualizar detalhes da ameaça

1. Inicie sessão na Consola (http://dellthreatdefense.com).
2. Clique no separador **Proteção** para visualizar uma lista de ameaças encontradas nessa organização.
3. Utilize o filtro da barra de menus do lado esquerdo para filtrar por Prioridade (Elevada, Média ou Baixa) e Estado (*Em quarentena*, *Renunciado*, *Não seguro* ou *Anormal*).

   Nota: Os números apresentados a vermelho no painel do lado esquerdo indicam ameaças pendentes que não foram colocadas em *Quarentena* ou *Renunciadas*. Filtre estes itens para visualizar uma lista de ficheiros que é necessário analisar.
4. Para adicionar colunas de modo a ser possível visualizar informações adicionais da ameaça, clique na seta para baixo junto ao nome de uma das colunas e, em seguida, selecione o nome de uma coluna.
5. Para visualizar informações adicionais de uma ameaça específica, clique na ligação do nome da ameaça (os detalhes são apresentados numa página nova) ou clique em qualquer ponto da linha da ameaça (os detalhes são apresentados na parte inferior da página). Ambas as visualizações apresentam o mesmo conteúdo, mas possuem estilos diferentes de apresentação. Os detalhes incluem uma descrição geral dos metadados do ficheiro, uma lista dos dispositivos com ameaças e relatórios de evidências.
   a. Metadados do ficheiro
      - Classificação [atribuída pela Equipa Cylance Advanced Threat and Alert Management (ATAM)]
      - Pontuação Cylance (nível de confiança)
      - Convicção da indústria audiovisual (ligações a VirusTotal.com para comparação com outros fornecedores)
      - Data da primeira deteção, Data da última deteção
      - SHA256
      - MD5
      - Informações do ficheiro (autor, descrição, versão, etc.)
      - Detalhes da assinatura

   b. Dispositivos

      A *Lista de dispositivos*/*zonas* para uma ameaça pode ser filtrada de acordo com o estado da ameaça (*Não seguro*, em *Quarentena*, *Dispensado* e *Anormal*). Clique nas ligações do filtro de estado para mostrar os dispositivos com a ameaça nesse estado.
      - *Não seguro*: O ficheiro está classificado como *Não seguro*, mas nenhuma ação foi efetuada.
      - Em *Quarentena*: O ficheiro já estava em *Quarentena* devido a uma definição de política.
      - *Renunciado*: O ficheiro foi *Renunciado* ou colocado na *Lista branca* pelo Administrador.
      - *Anormal*: O ficheiro está classificado como *Anormal*, mas nenhuma ação foi efetuada.

   c. Relatórios de provas
      - **Indicadores de ameaças**: Observações sobre um ficheiro analisado pelo motor Cylance Infinity. Estes indicadores ajudam a compreender o motivo da classificação de um ficheiro e fornecem informações sobre os atributos e comportamento de um ficheiro. Os indicadores de ameaças estão agrupados em categorias para auxiliar no contexto.

- **Dados detalhados da ameaça**: Os Dados detalhados da ameaça fornecem um resumo completo das características estáticas e dinâmicas de um ficheiro, incluindo metadados do ficheiro adicionais, detalhes da estrutura do ficheiro e comportamentos dinâmicos, como ficheiros removidos, chaves de registo criadas ou modificadas e URL com os quais tenta comunicar.

Para visualizar indicadores de ameaças:

1. Inicie sessão na Consola (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 qualquer ameaça. É apresentada a página Detalhes da ameaça.
4. Clique em **Relatórios de provas**.

Categorias do indicador de ameaças:

Cada categoria representa uma área detetada com frequência no software malicioso e tem como base uma análise aprofundada de mais de 100 milhões de binários. O relatório de Indicadores de ameaças indica quantas dessas categorias estavam presentes no ficheiro.

Anomalias
O ficheiro inclui elementos, de alguma forma, considerados inconsistentes ou anómalos. Frequentemente, são inconsistências na estrutura do ficheiro

Recolha
O ficheiro tem provas de recolha de dados. Isto pode incluir a enumeração de configurações do dispositivo ou a recolha de informações confidenciais.

Perda de dados
O ficheiro tem provas de fuga de dados. Isto pode incluir ligações de rede enviadas, provas de atuação como browser ou outras comunicações de rede.

Fraude
O ficheiro tem provas de tentativas de fraude. A fraude pode assumir a forma de secções ocultas, inclusão de códigos para evitar a deteção ou indicações de etiquetagem incorreta nos metadados ou outras secções.

Destruição
O ficheiro tem provas de capacidades destrutivas. A destruição inclui a capacidade de eliminar recursos do dispositivo, como ficheiros e diretórios.

Diversos
Todos os outros indicadores que não se enquadram noutras categorias.

Nota: Ocasionalmente, as secções Indicadores de ameaças e Dados detalhados da ameaça não apresentam quaisquer resultados ou não estão disponíveis. Isto acontece quando o ficheiro não tiver sido carregado. O registo de depuração poderá explicar por que motivo não foi possível carregar o ficheiro.

Abordar ameaças

O tipo de ação a adotar para algumas ameaças poderá depender do utilizador atribuído ao Dispositivo. As ações aplicadas às ameaças podem ser aplicadas a nível do Dispositivo ou a um nível Global. A seguir são apresentadas as diferentes ações que podem ser adotadas contra ameaças ou ficheiros:

- ***Quarentena***: Coloca um ficheiro específico em *Quarentena* para impedir que o ficheiro seja executado neste dispositivo.

  Nota: Pode utilizar a linha de comandos de um dispositivo para colocar uma ameaça em quarentena: Esta funcionalidade está apenas disponível no Agente Windows. Consulte "Quarentena através da linha de comandos" para obter mais informações.

- ***Quarentena global***: Coloca um ficheiro em *Quarentena global* para impedir que esse ficheiro seja executado em qualquer dispositivo em toda a organização.

  Nota: Colocar um ficheiro em *Quarentena* irá mover o ficheiro da sua localização original para o diretório *Quarentena* (`C:\ProgramData\Cylance\Desktop\q`).

- ***Renunciar***: *Renunciar* um ficheiro irá permitir que esse ficheiro seja executado no dispositivo especificado.

- ***Seguro global***: Colocar um ficheiro na *Lista segura global* irá permitir que esse ficheiro seja executado em qualquer dispositivo em toda a organização.

  Nota: Ocasionalmente, o Threat Defense poderá colocar um ficheiro em *Quarentena* ou informar que é um ficheiro "bom" (isto pode acontecer se as funcionalidades do ficheiro se assemelharem às dos ficheiros maliciosos). *Renunciar* ou marcar o ficheiro na *Lista segura global* pode ser útil nestes casos.

- ***Carregar ficheiro***: Carregue manualmente um ficheiro para o Cylance Infinity para análise. Se o Carregamento automático estiver ativado, os ficheiros novos (que não tenham sido analisados pelo Cylance) são automaticamente carregados para o Cylance Infinity. Se o ficheiro existir no Cylance Infinity, o botão Carregar ficheiro fica indisponível (esbatido).

- ***Transferir ficheiro***: Transfira um ficheiro para teste. Esta funcionalidade deve ser ativada para a organização. O utilizador deve ser um Administrador. A ameaça deve ser detetada utilizando o Agente versão 1320 ou superior.

  Nota: O ficheiro deve estar disponível no Cylance Infinity e os três hashes (SHA256, SHA1 e MD5) devem coincidir entre o Cylance Infinity e o Agente. Caso contrário, o botão Transferir ficheiro não está disponível.

Abordar ameaças num dispositivo específico

1. Inicie sessão na Consola (http://dellthreatdefense.com) como Administrador ou Gestor de zona.
2. Clique no separador **Dispositivos**.
3. Procure e selecione o Dispositivo.
4. Em alternativa, poderá estar disponível uma ligação para o dispositivo a partir do separador Proteção, caso seja apresentado com uma ameaça associada.
5. Todas as ameaças nesse dispositivo são apresentadas na parte inferior da página. Selecione a ameaça para colocar em *Quarentena* ou *Renunciar* o ficheiro nesse dispositivo.

Abordar ameaças a nível global

Os ficheiros adicionados à *Lista de quarentena global* ou *Lista segura global* estão em *Quarentena* ou são *Permitidos* em todos os dispositivos em todas as zonas.

1. Inicie sessão na Consola (http://dellthreatdefense.com) como Administrador.
2. Clique em **Definições > Lista global**.
3. Clique em Quarentena global ou Seguro.

4. Clique em **Adicionar ficheiro**.
5. Adicione o SHA256 (necessário), MD5, nome do ficheiro e o motivo para colocação do mesmo na *Lista global*.
6. Clique em **Enviar**.

Proteção – Controlo de scripts

O Threat Defense fornece detalhes sobre os scripts Ativos e PowerShell que foram bloqueados ou para os quais existe um alerta. Com o Controlo de scripts ativado, os resultados são apresentados no separador Controlo de scripts na página Proteção. Isto fornece detalhes sobre o script e os Dispositivos afetados.

Para visualizar resultados do controlo de scripts

1. Inicie sessão na Consola (http://dellthreatdefense.com) como Administrador.
2. Clique em Proteção.
3. Clique em Controlo de scripts.
4. Selecione um script na tabela. Isto atualiza a tabela Detalhes com uma lista de dispositivos afetados:

Descrições da coluna Controlo de scripts

- **Nome do ficheiro**: O nome do script.
- **Intérprete**: A funcionalidade de controlo de scripts que identificou o script.
- **Última deteção**: A data e a hora em que o script foi analisado pela última vez.
- **Tipo de unidade**: O tipo de unidade onde o script foi detetado (exemplo: disco rígido interno).
- **SHA256**: O hash SHA 256 do script.
- **N. º de dispositivos**: O número de dispositivos afetados por este script.
- **Alerta**: O número de vezes que foram apresentados alertas para o script. Podem ser várias vezes para o mesmo dispositivo.
- **Bloquear**: O número de vezes que o script foi bloqueado. Podem ser várias vezes para o mesmo dispositivo.

Descrições da coluna Detalhes

- **Nome do dispositivo**: O nome do dispositivo afetado pelo script. Clique no nome do dispositivo para aceder à página Detalhes do dispositivo.
- **Estado**: O estado do dispositivo (online ou offline).
- **Versão do Agente**: O número da versão do Agente atualmente instalado no dispositivo.
- **Caminho do ficheiro**: O caminho do ficheiro a partir do qual o script foi executado.
- **Quando**: A data e a hora em que o script foi executado.
- **Nome de utilizador**: O nome do utilizador com sessão iniciada quando o script foi executado.
- **Ação**: A ação adotada relativamente ao script (Alerta ou Bloquear).

Lista global

A *Lista global* permite que um ficheiro seja assinalado para *Quarentena* ou para *Permitir* esses ficheiros em todos os dispositivos na organização.

- **Quarentena global:** Todos os Agentes na organização colocam em *Quarentena* qualquer ficheiro na *Lista de quarentena global* que seja descoberto no dispositivo.
- **Seguro:** Todos os Agentes na organização *Permitem* qualquer ficheiro na *Lista segura* que seja descoberto no dispositivo.
- **Não atribuído:** Qualquer ameaça identificada na organização que não seja atribuída à *Quarentena global* ou *Lista segura*.

Alterar estado da ameaça

Para alterar o estado de uma ameaça (*Quarentena global*, *Segura*, ou *Não atribuída*):

1. Inicie sessão na Consola (http://dellthreatdefense.com) como Administrador.
2. Selecione **Definições > Lista global**.
3. Selecione a lista atual à qual a ameaça está atribuída. Por exemplo, clique em Não atribuída para mudar uma ameaça não atribuída para *Segura* ou *Quarentena global*.
4. Selecione as caixas de verificação das ameaças a alterar e clique num botão de estado.
    a. Seguro: Move os ficheiros para a *Lista segura*.
    b. Quarentena global: Move os ficheiros para a *Lista de quarentena global*.
    c. Remover da lista: Move os ficheiros para a *Lista não atribuída*.

Adicionar um ficheiro

Adicionar um ficheiro manualmente à *Quarentena global* ou à *Lista segura*. São necessárias as informações do hash SHA256 do ficheiro a adicionar.

1. Inicie sessão na Consola (http://dellthreatdefense.com) como Administrador.
2. Selecione **Definições > Lista global**.
3. Selecione a lista onde pretende adicionar o ficheiro (*Quarentena global* ou *Seguro*).
4. Clique em **Adicionar ficheiro**.
5. Introduza as informações do hash SHA256. Opcionalmente, introduza as informações do MD5 e de Nome do ficheiro.
6. Indique um motivo para adicionar este ficheiro.
7. Clique em **Enviar**.

Lista segura por certificado

Os clientes têm a capacidade de colocar ficheiros na *Lista segura* através de um certificado assinado, que permite que qualquer software personalizado, devidamente assinado, funcione sem interrupção.

Nota: Atualmente, esta funcionalidade apenas funciona com sistemas operativos Windows.

- Esta funcionalidade permite aos clientes estabelecer uma *Lista branca*/*Lista segura* através de certificado assinado representado pelo thumbprint SHA1 do certificado.
- As informações do certificado são extraídas pela Consola (Carimbo de data/hora, Requerente, Emissor e Thumbprint). O certificado não é carregado nem guardado na Consola.

- O carimbo de data/hora do certificado indica quando o certificado foi criado.
- A Consola não verifica se o certificado é atual ou está expirado.
- Se o certificado mudar (por exemplo, for renovado ou novo), deve ser adicionado à *Lista segura* na Consola.

1. Adicione os detalhes do certificado ao Repositório de certificados.
    a. Identifique o thumbprint do certificado do PE (Portable Executable) assinado.
    b. Selecione **Definições > Certificados**.
    c. Clique em **Adicionar certificado**.
    d. Clique em **Procurar certificados para adicionar** ou arraste e largue o certificado na caixa de mensagem.
    e. Se estiver a procurar certificados, a janela Abrir é apresentada para permitir a seleção dos certificados.
    f. Opcionalmente, adicione notas sobre este certificado.
    g. Clique em **Enviar**. O Emissor, Requerente, Thumbprint e Notas (se introduzido) são adicionados ao repositório.
2. Adicione um certificado à *Lista segura*.
    a. Selecione **Definições > Lista global**.
    b. Selecione o separador **Seguro**.
    c. Clique em **Certificados**.
    d. Clique em **Adicionar certificado**.
    e. Selecione um certificado da *Lista segura*. Opcionalmente, selecione uma Categoria e adicione um motivo para adicionar este certificado.
    f. Clique em **Enviar**.

Visualizar thumbprints de uma ameaça

No separador Proteção, Detalhes da ameaça apresenta o thumbprint do certificado. No ecrã, selecione **Adicionar ao certificado** para adicionar o certificado ao Repositório.

Privilégios

Adicionar ao certificado é uma função disponível apenas para Administradores. Se o certificado já tiver sido adicionado ao Repositório de certificados, a Consola apresenta **Ir para certificado**. Os certificados apenas são visualizados pelos Gestores de zona, com acesso à opção **Ir para certificado**.

Perfil

O menu de perfis (canto superior direito) permite a gestão da sua conta, a visualização de registos de auditoria da Consola e o acesso à ajuda dos produtos.

A minha conta

Altere a sua palavra-passe e as definições de notificações por correio eletrónico na página A minha conta.

1. Inicie sessão na Consola (http://dellthreatdefense.com).
2. Clique no menu de perfis no canto superior direito e selecione **A minha conta**.

3. Para alterar a sua palavra-passe:
    a. Clique em Alterar palavra-passe.
    b. Introduza a palavra-passe antiga.
    c. Introduza a nova palavra-passe e introduza-a novamente para confirmar.
    d. Clique em Update (Atualizar).
4. Selecione ou anule a seleção da caixa de verificação para ativar ou desativar as Notificações por correio eletrónico. A ação de ativar e desativar a caixa de verificação é guardada automaticamente. As Notificações por correio eletrónico apenas estão disponíveis para Administradores.

Registo de auditoria

Lista pendente de ícones do utilizador (canto superior direito da Consola)

O Registo de auditoria contém informações sobre as seguintes ações realizadas a partir da Consola:

- Iniciar sessão (Êxito, Falha)
- Política (Adicionar, Editar, Remover)
- Dispositivo (Editar, Remover)
- Ameaça (Quarentena, Renunciar, Quarentena global, Lista segura)
- Utilizador (Adicionar, Editar, Remover)
- Atualização do Agente (Editar)

O Registo de auditoria pode ser visualizado na Consola navegando até à lista pendente de perfis do lado superior direito da Consola e selecionando **Registo de auditoria**. Os registos de auditoria apenas estão disponíveis para Administradores.

Definições

A página Definições apresenta os separadores Aplicação, Gestão de utilizadores, Política de dispositivos, Lista global e Atualização do Agente. O item do menu Definições apenas está disponível para Administradores.

APLICAÇÃO

Agente Threat Defense

Os dispositivos são adicionados à organização através da instalação do Agente Threat Defense em cada endpoint. Uma vez ligado à Consola, aplique a política (para gestão de ameaças identificadas) e organize os dispositivos com base nas necessidades organizacionais.

O Agente Threat Defense foi concebido para utilizar uma quantidade mínima de recursos do sistema. O Agente trata ficheiros ou processos executados como prioridade, uma vez que estes eventos podem ser maliciosos. Os ficheiros que se encontrem apenas no disco (armazenados, mas não em execução) têm uma prioridade inferior, uma vez que, apesar de existir a possibilidade de serem maliciosos, não são uma ameaça imediata.

Agente Windows

Requisitos do sistema

A Dell recomenda que o hardware do endpoint (CPU, GPU, etc.) cumpra ou supere os requisitos recomendados do Sistema operativo de destino. As exceções são indicadas abaixo (RAM, espaço disponível no disco rígido e requisitos de software adicionais).

Sistemas operativos	• 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
Software/requisitos adicionais	• .NET Framework 3.5 (SP1) ou superior (*apenas Windows*) • Browser • Acesso à Internet para iniciar sessão, aceder ao instalador e registar o produto • Direitos de administrador local para instalar o software
Outros Requisitos	• O TLS 1.2 é suportado com o Agente 1422 ou posterior e requer o .NET Framework 4.5 ou posterior

Tabela 2: Requisitos do sistema para Windows

*Não suportado: Windows 8.1 RT
**A atualização de Aniversário do Windows 10 requer o Agente 1402 ou posterior.
***Não suportado: Server Core (2008 e 2012) e servidor mínimo (2012).
****Requer o Agente 1412 ou posterior.

Para transferir o ficheiro de instalação

1. Inicie sessão na Consola (http://dellthreatdefense.com).
2. Selecione **Definições > Aplicação**.
3. Copie o **Token de instalação**.

   O Token de instalação é uma cadeia de caracteres gerada aleatoriamente que permite que o Agente reporte à respetiva conta atribuída na Consola. O Token de instalação é necessário durante a instalação, no assistente de instalação ou como uma definição dos parâmetros de instalação.
4. Transfira o Instalador.
   a. Selecione o Sistema operativo.
   b. Selecione o tipo de ficheiro a transferir.

      Para Windows, a Dell recomenda a utilização do ficheiro MSI para instalação do Agente.

Sugestão: Se a Regra de zona estiver configurada, os Dispositivos podem ser automaticamente atribuídos a uma Zona caso o dispositivo corresponda aos critérios da Regra de zona.

Instalar o Agente – Windows

Antes de instalar o Threat Defense, certifique-se de que todos os pré-requisitos são cumpridos. 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. Introduza o Token de instalação fornecido pelo Inquilino Threat Defense. Clique em **Seguinte**.

   Nota: Contacte o seu administrador do Threat Defense ou consulte o artigo KB Procedimentos: Gerir o Threat Defense se o acesso ao token de instalação não estiver disponível.
4. Opcionalmente, altere a pasta de destino do Threat Defense.

   Clique em **OK** para dar início à instalação.
5. Clique em **Concluir** para finalizar a instalação. Selecione a caixa de verificação para iniciar o Threat Defense.

Parâmetros de instalação do Windows

O Agente pode ser instalado de forma interativa ou não interativa através de GPO, Microsoft System Center Configuration Manager (normalmente conhecido como SCCM) e MSIEXEC. Os MSI podem ser personalizados com parâmetros integrados (abaixo apresentados) ou os parâmetros podem ser fornecidos a partir da linha de comandos.

Propriedade	Valor	Descrição
PIDKEY	<Token de instalação>	Introdução automática do Token de instalação
LAUNCHAPP	0 ou 1	0: O ícone do tabuleiro do sistema e a pasta do menu Iniciar estão ocultos no momento da execução 1: O ícone do tabuleiro do sistema e a pasta do menu Iniciar não estão ocultos no momento da execução (predefinição)
SELFPROTECTIONLEVEL	1 ou 2	1: Apenas os Administradores locais podem fazer alterações ao registo e aos serviços 2: Apenas o Administrador do sistema pode fazer alterações ao registo e aos serviços (predefinição)
APPFOLDER	<Pasta de instalação de destino>	Especifica o diretório de instalação do Agente A localização predefinida é C:\Program Files\Cylance\Desktop
VenueZone	"Nome_da_Zona"	Requer a versão do Agente 1382 ou posterior •Adiciona dispositivos a uma zona. •Se a zona não existir, a zona é criada utilizando o nome fornecido. •Substitua nome_da_zona pelo nome de uma zona existente ou de uma zona que pretende criar. **Aviso**: Adicionar espaços antes ou depois do nome da zona irá criar uma nova zona.

Tabela 3: Parâmetros de instalação para Windows

O seguinte exemplo de linha de comandos mostra como gerir a Ferramenta de instalador do Microsoft Windows (MSIEXEC) transmitindo-lhe 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 registo de instalação é guardado em **C:\temp**. Quando o Agente está em execução, o ícone do tabuleiro do sistema e a pasta Threat Defense do menu Iniciar são ocultos. Pode consultar informações adicionais relativas aos diferentes comutadores da linha de comandos aceites por MSIEXEC em KB 227091.

Instalar o Agente Windows utilizando o Wyse Device Manager (WDM)

Esta secção explica como criar um script de instalação, como criar pacote RSP para WDM e como adicionar o pacote ao WDM para instalação em vários clientes magros em simultâneo sem interação do utilizador.

Crie um script de ficheiro batch para efetuar a instalação da linha de comandos do Threat Defense. O WDM executa este script durante a implementação.

1. Abra o Bloco de notas. Utilizando os parâmetros da linha de comandos acima indicados, introduza o comando seguinte para executar a instalação, substituindo **<INSTALLATION TOKEN>** pelo token fornecido:
   msiexec /i C:\TDx86\DellThreatDefense_x86.msi PIDKEY=<INSTALLATION TOKEN> /

   C:\TDx86 é utilizado para o nosso diretório, visto que esta pasta é copiada para este local no cliente magro durante a instalação.
2. Guarde o ficheiro com uma extensão **.bat** na pasta TDx86. Por exemplo, **TDx86_Install.bat**.

   Crie um pacote RSP com o qual a aplicação do Agente do Threat Defense possa ser instalada em vários thin clients em simultâneo sem interação com o utilizador.
3. Abra o Construtor de scripts num computador com o WDM instalado.
4. Introduza um Nome do pacote e uma Descrição do pacote.
   - Selecione Outros pacotes em Categoria do pacote.
   - Selecione Windows Embedded Standard 7 em Sistema operativo.
5. Adicione Comandos de scripts para verificar se os sistemas de destino são WES7 ou WES7p.
   - Selecione Confirmar sistema operativo (CO) em Comando de scripts
   - Para o valor do SO do dispositivo, introduza o sistema operativo adequado.
6. Utilize as setas duplas para Adicionar item.
7. Prima **OK** quando solicitado.
8. Adicione um comando para bloquear o cliente magro e impedir a interação do utilizador.
   - Selecione **Comando de scripts > Bloqueio do utilizador (LU)**. Não é necessário qualquer valor. No entanto, neste exemplo é introduzido um **Valor** de **Sim**, para que o ecrã inicial seja removido se o programa de instalação falhar ou se ocorrer um erro.
9. Adicione um comando para copiar ficheiros para o cliente magro.
   - Selecione o Comando de scripts **Copiar X (XC)**.
   - Para o valor do **Diretório do repositório**, adicione ***** até ao final do **regroot>** existente.
   - Para o valor do **Diretório de dispositivos**, introduza o caminho para o qual os ficheiros serão copiados nos clientes magros de destino. Neste exemplo, é utilizado o Nome do pacote.

10. Adicione um comando para executar o script de instalação .bat.
    - Selecione **Comando de scripts > Executar no dispositivo (EX)**.
    - Para o valor do Nome do ficheiro do dispositivo, introduza o caminho **`C:\TDx86\TDx86_install.bat`**. A pasta TDx86 é copiada a partir do comando XC anterior.
    - Adicione **+** como valor de execução síncrona. Isto indica ao WDM que deve aguardar que a execução do ficheiro esteja concluída para continuar.
11. Adicione um comando para eliminar ficheiros copiados a partir do cliente magro.
    - Adicione o Comando de scripts Elimine **Árvore (DT)**.
12. Adicione comandos para desativar o bloqueio.
    - Adicione o **Bloqueio do fim (EL)** do Comando de scripts.
13. Para rever, o pacote de scripts deve ser parecido com o seguinte.
    - Se implementar o Threat Defense em sistemas WES7P, atualize a secção do sistema operativo para WES7P. Caso contrário, a instalação do pacote irá falhar.
14. Guarde o pacote.
    - Clique em **Guardar** e procure a localização da pasta **TDx86**, se estas instruções tiverem sido cumpridas, a pasta está no Ambiente de trabalho.
15. Feche o Construtor de scripts.
16. Inicie o **WyseDeviceManager** para adicionar o pacote ao WDM.
17. Navegue para **WyseDeviceManager > Gestor de pacotes > Outros pacotes**.
18. Selecione **Ação > Novo > Pacote** na barra de menu.
19. Selecione **Registar um pacote a partir de um ficheiro de script (.RSP)** e clique em **Seguinte**.
20. Procure a localização do ficheiro RSP criado no passo anterior e clique em **Seguinte**.
21. Certifique-se de que **Ativo** está selecionado e clique em **Seguinte.**
22. Clique em **Seguinte** quando o WDM estiver pronto para registar o pacote.
23. Clique em **Concluir** quando o pacote estiver registado com sucesso.
24. O pacote será visível em **Outros pacotes**.
25. Verificar conteúdo do pacote:
    - Abra o Explorador de Ficheiros e navegue para **C:\inetpub\ftproot\Rapport** e localize a **pasta TDx86**.
    - Abra a pasta TDx86 e verifique se a pasta inclui o instalador e o ficheiro .bat.

Está agora disponível no WDM um pacote que permite a implementação do Threat Defense em vários clientes magros WES7 sem interação do utilizador.

Quarentena através da linha de comandos

Pode colocar um ficheiro em quarentena utilizando a linha de comandos de um dispositivo. Esta funcionalidade requer que o hash SHA256 da ameaça seja conhecido.

Nota: Esta funcionalidade está disponível apenas no Windows e requer o Agente 1432 ou superior.

1. Abra a linha de comandos no dispositivo Windows. Exemplo: No menu Iniciar, procure o ficheiro cmd.exe.
2. Invoque o Dell.ThreatDefense.exe e inclua o argumento **-q:<hash>**, no qual <hash> representa o hash SHA256 do ficheiro. Este processo fará com que o Agente envie o ficheiro para a pasta de quarentena.

   Exemplo de linha de comandos (com o Dell Threat Defense instalado na localização predefinida):

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

Desinstalar o Agente

Para desinstalar o Agente num sistema Windows, utilize a funcionalidade Adicionar/remover programas ou a Linha de comandos.

Ao desinstalar o Agente, o dispositivo não é removido da Consola. Tem de remover manualmente o dispositivo da Consola.

Antes de tentar desinstalar o Agente:

- Se a opção **Solicitar palavra-passe para desinstalar o Agente** estiver ativada, certifique-se de que tem a palavra-passe para efetuar a desinstalação.
- Se a opção **Impedir o encerramento do serviço a partir do dispositivo** estiver ativada, desative-a no grupo de políticas ou aplique uma política diferente para os dispositivos onde pretende desinstalar o Agente.

Desinstalar com a opção Adicionar/remover programas

1. Selecione **Iniciar > Painel de controlo**.
2. Clique em **Desinstalar um programa**. Se tiver selecionado Ícones em vez de Categorias, clique em Programas e funcionalidades.
3. Selecione **Dell Threat Defense** e, em seguida, clique em **Desinstalar**.

Utilizar a linha de comandos

1. Abra a Linha de comandos na qualidade de Administrador.
2. Utilize os seguintes comandos com base no pacote de instalação que utilizou para instalar o Agente.
   a. DellThreatDefense_x64.msi
      i. Desinstalação padrão: msiexec /uninstall DellThreatDefense_x64.msi
      ii. Windows Installer: msiexec /x DellThreatDefense_x64.msi
   b. DellThreatDefense_x86.msi
      i. Desinstalação padrão: msiexec /uninstall DellThreatDefense_x86.msi
      ii. Windows Installer: msiexec /x DellThreatDefense_x86.msi

3. Os seguintes comandos são opcionais:
    a. Para uma desinstalação silenciosa: /quiet
    b. Para uma desinstalação silenciosa e oculta: /qn
    c. Para uma desinstalação protegida por palavra-passe UNINSTALLKEY=<password>
    d. Para um ficheiro de registo da desinstalação: /Lxv* <path>
        i. Este comando cria um ficheiro de registo no caminho designado (<path>), incluindo o nome do ficheiro.
        ii. Exemplo: C:\Temp\Uninstall.log

Agente macOS

Requisitos do sistema

A Dell recomenda que o hardware do endpoint (CPU, GPU, etc.) cumpra ou supere os requisitos recomendados do Sistema operativo de destino. As exceções são indicadas abaixo (RAM, espaço disponível no disco rígido e requisitos de software adicionais).

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

Tabela 4: Requisitos do sistema para macOS

* Requer o Agente 1412 ou posterior.
** Requer o Agente 1452 ou posterior.

Para transferir o ficheiro de instalação

1. Inicie sessão na Consola (http://dellthreatdefense.com).
2. Selecione **Definições > Aplicação**.
3. Copie o **Token de instalação**.

    O Token de instalação é uma cadeia de caracteres gerada aleatoriamente que permite que o Agente reporte à respetiva conta atribuída na Consola. O Token de instalação é necessário durante a instalação, no assistente de instalação ou como uma definição dos parâmetros de instalação.
4. Transfira o Instalador.
    a. Selecione o Sistema operativo.
    b. Selecione o tipo de ficheiro a transferir.

Sugestão: Se a Regra de zona estiver configurada, os Dispositivos podem ser automaticamente atribuídos a uma Zona caso o dispositivo corresponda aos critérios da Regra de zona.

Instalar o Agente – macOS

Antes de instalar o Threat Defense, certifique-se de que todos os pré-requisitos são cumpridos. Consulte Requisitos do sistema.

Nota: O Agente macOS passará a ser da marca Dell numa versão futura.

1. Faça duplo clique em **`DellThreatDefense.dmg`** para iniciar o instalador.
2. Faça duplo clique no ícone *Proteger* na interface do utilizador PROTEGER para iniciar a instalação.
3. Clique em **Continuar** para confirmar que o sistema operativo e o hardware cumprem os requisitos.
4. Clique em **Continuar** no ecrã de boas-vindas.
5. Introduza o Token de instalação fornecido pelo Inquilino Threat Defense. Clique em **Continuar**.

Nota: Contacte o seu administrador do Threat Defense ou consulte o artigo KB Procedimentos: Gerir o Threat Defense se o acesso ao token de instalação não estiver disponível.

6. Opcionalmente, altere a localização de instalação do Threat Defense.

   Clique em **Instalar** para dar início à instalação.
7. Introduza um Nome de utilizador e Palavra-passe do administrador. Clique em **Instalar software**.
8. Clique em **Fechar** no ecrã de resumo.

Parâmetros de instalação do macOS

O Agente Threat Defense pode ser instalado utilizando as opções da linha de comandos em Terminal. Os exemplos abaixo apresentados utilizam o instalador PKG. Para DMG, basta alterar a extensão do ficheiro no comando.

Nota: Certifique-se de que os endpoints de destino cumprem os requisitos do sistema e que o responsável pela instalação do software tem as credenciais corretas para instalação do software.

Propriedade	Valor	Descrição
InstallToken		Token de instalação disponível na Consola
NoCylanceUI		O ícone do Agente não deve ser apresentado no arranque. A predefinição é Visível
SelfProtectionLevel	0 ou 1	1: Apenas os Administradores locais podem fazer alterações ao registo e aos serviços. 2: Apenas o Administrador do sistema pode fazer alterações ao registo e aos serviços (predefinição).
LogLevel	0, 1, 2 ou 3	0: Erro – Apenas são registadas mensagens de erro. 1: Aviso – São registadas mensagens de erro e de aviso. 2: Informações (predefinição) – São registadas mensagens de erro, aviso e informações. Isto poderá fornecer alguns detalhes durante a resolução de problemas. 3: Verboso – Todas as mensagens são registadas. Durante a resolução de problemas, este é o nível de registo recomendado. No entanto, os tamanhos de ficheiro de registo verboso podem ser bastante elevados. A Dell recomenda que ative a opção Verboso durante a resolução de problemas e, em seguida, mude novamente para Informações quando a resolução de problemas estiver concluída.

Propriedade	Valor	Descrição
VenueZone	“nome_da_zona”	Requer a versão do Agente 1382 ou posterior •Adiciona dispositivos a uma zona. •Se a zona não existir, a zona é criada utilizando o nome fornecido. •Substitua nome_da_zona pelo nome de uma zona existente ou de uma zona que pretende criar. **Aviso**: Adicionar espaços antes ou depois do nome da zona irá criar 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 [install_token] > cyagent_install_token

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

Nota: Substitua **`[install_token]`** pelo token de instalação. O comando echo produz um ficheiro **`cyagent_install_token`**, que é um ficheiro de texto com uma opção de instalação por linha. O ficheiro e o pacote de instalação devem estar na mesma pasta. Tenha especial cuidado com as extensões de ficheiro, o exemplo acima mostra que o ficheiro cyagent_install_token não tem extensão de ficheiro. As predefinições no macOS têm extensões ocultas. Construir este ficheiro manualmente com a edição de texto ou outro editor de texto pode adicionar automaticamente uma extensão de ficheiro que terá de ser removida.

Parâmetros de instalação opcionais

Introduza o seguinte no Terminal para criar um ficheiro (**`cyagent_install_token`**) que o programa de instalação utiliza para aplicar as opções introduzidas. Cada parâmetro deve estar na respetiva linha. O ficheiro e o pacote de instalação devem estar na mesma pasta.

Em seguida, é apresentado um exemplo. Não são necessários todos os parâmetros no ficheiro. O terminal inclui todos os elementos entre plicas existentes no ficheiro. Certifique-se de que pressiona Enter/Voltar depois de cada parâmetro para manter cada parâmetro na respetiva linha no ficheiro.

Poderá também ser utilizado um editor de texto para criar o ficheiro que inclui cada parâmetro (na respetiva linha). O ficheiro e o pacote de instalação devem estar na mesma pasta.

Exemplo:

```
echo 'InstallToken

NoCylanceUI

SelfProtectionLevel=2

LogLevel=2'> cyagent_install_token

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

Desinstalar o Agente

Sem palavra-passe

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

Com palavra-passe

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

Nota: Substitua **thisismypassword** pela palavra-passe de desinstalação criada na Consola.

Serviço de Agente

Iniciar serviço

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

Parar serviço

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

Verificação da instalação

Verifique os seguintes ficheiros para confirmar se o Agente foi instalado com êxito.

1. A pasta de programas foi criada.
    - Predefinição Windows: **C:\Program Files\Cylance\Desktop**
    - Predefinição macOS: **/Applications/DellThreatDefense/**
2. O ícone do Threat Defense é visível no tabuleiro do sistema do dispositivo de destino.

    Não aplicável se o parâmetro LAUNCHAPP=0 (Windows) ou NoCylanceUI (macOS) for utilizado.
3. Existe uma pasta Threat Defense no menu Iniciar\Todos os programas no dispositivo de destino.

    Não aplicável se o parâmetro LAUNCHAPP=0 (Windows) ou NoCylanceUI (macOS) for utilizado.
4. O serviço Threat Defense foi adicionado e está a ser executado. Um serviço Threat Defense deve ser apresentado na lista como estando em execução no painel Serviços do Windows do dispositivo de destino.
5. O processo Dell.ThreatDefense.exe está a ser executado. Um processo Dell.ThreatDefense.exe deve ser apresentado no separador Processos no Gestor de tarefas do Windows do dispositivo de destino.
6. O dispositivo reporta à Consola. Inicie sessão na Consola e clique no separador Dispositivos, o dispositivo de destino deverá aparecer e ser apresentado com estado online.

Interface do utilizador do Agente

A interface do utilizador do Agente está ativada por predefinição. Clique no ícone do Agente no tabuleiro do sistema para visualizar. Em alternativa, o Agente pode ser instalado de modo a ocultar o ícone do Agente no tabuleiro do sistema.

Separador Ameaças

Apresenta todas as ameaças detetadas no dispositivo e a ação adotada. *Não seguro* significa que não foram tomadas medidas em relação à ameaça. Em *Quarentena* significa que a ameaça foi modificada (para impedir o ficheiro de ser executado) e foi movida para a pasta *Quarentena* . *Renunciado* significa que o ficheiro é considerado seguro pelo administrador e é *Permitido* executá-lo no dispositivo.

Separador Eventos

Apresenta quaisquer eventos de ameaça que tenham ocorrido no dispositivo.

Separador Scripts

Apresenta quaisquer scripts maliciosos que tenham sido executados no dispositivo e quaisquer ações adotadas relativamente ao script.

Menu Agente

O menu Agente faculta acesso à ajuda e a atualizações do Threat Defense. É também facultado acesso à Interface do utilizador avançada, que disponibiliza mais opções de menu.

Menu Agente

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

- **Procurar atualizações**: O Agente procura e instala quaisquer atualizações disponíveis. As atualizações estão restringidas à versão do Agente permitida para a Zona à qual o dispositivo pertence.
- **Procurar atualizações de política**: O Agente verifica se existem atualizações de política disponíveis. Podem tratar-se de alterações a uma política existente ou de uma política diferente que esteja a ser aplicada ao Agente.

  Nota: Verifique se a atualização de política é suportada na versão 1422 (ou posterior) no Windows e na versão 1432 (ou posterior) no macOS.
- **Sobre**: Apresenta uma caixa de diálogo com a versão do Agente, o nome da política atribuída ao dispositivo, a hora da última verificação de atualizações para o Agente e o token de instalação utilizado durante a instalação.
- **Sair**: Fecha o ícone do Agente no tabuleiro do sistema. Isto não desativa quaisquer serviços Threat Defense.
- **Opções > Mostrar notificações**: Selecione esta opção para visualizar quaisquer novos eventos como notificações.

Ativar opções avançadas da interface do utilizador do Agente

O Agente Threat Defense disponibiliza algumas opções avançadas através da interface do utilizador para proporcionar funcionalidades em dispositivos sem conectividade à Consola. O CylanceSVC.exe deve estar em execução quando as Opções avançadas estiverem ativadas.

Windows

1. Se o ícone do Agente estiver visível no tabuleiro do sistema, clique com o botão direito do rato no ícone e selecione **Sair**.
2. Inicie a Linha de comandos e introduza o comando seguinte. Pressione Enter quando concluir.

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

   Se a aplicação estiver instalada numa localização diferente, navegue até essa localização na linha de comandos.

3. Introduza o seguinte comando e pressione enter quando concluir.

   `Dell.ThreatDefense.exe –a`

   O ícone do Agente é apresentado no tabuleiro do sistema.

4. Clique com o botão direito do rato no ícone. As opções *Registo*, *Executar uma deteção* e *Gestão de ameaças* são apresentadas.

macOS

1. Se o ícone do Agente estiver visível no menu superior, clique com o botão direito do rato no ícone e selecione **Sair**.

2. Abrir terminal e executar

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

   Nota: Este é o caminho de instalação predefinido para o Threat Defense da Dell. Pode ser necessário editar o caminho para corresponder ao seu ambiente em conformidade.

3. A interface do utilizador do Agente agora será apresentada com opções adicionais.

Registar

Selecione o nível das informações de registo a recolher a partir do Agente. A predefinição é Informações. A Dell recomenda que, quando executar a resolução de problemas, defina o nível de registo para Todos (Verboso). Quando a resolução de problemas estiver concluída, mude novamente para Informações (registar Todas as informações pode gerar ficheiros de registo muito grandes).

Executar uma deteção

Permite que os utilizadores especifiquem uma pasta para verificar se existem ameaças.

1. Selecione **Executar uma deteção > Especificar pasta**.

2. Selecione uma pasta para verificar e clique em **OK**. Quaisquer ameaças detetadas são apresentadas na interface do utilizador do Agente.

Gestão de ameaças

Permite aos utilizadores eliminar os ficheiros em *Quarentena* no dispositivo.

1. Selecione **Threat Management > Eliminar em Quarentena**.

2. Clique em **OK** para confirmar.

Máquinas virtuais

Existem algumas recomendações a ter em conta quando utilizar o Agente Threat Defense numa imagem de máquina virtual.

Quando criar uma imagem de máquina virtual para ser utilizada como modelo, desligue as definições de rede da máquina virtual antes de instalar o Agente. Isto impede a comunicação do Agente com a Consola e a configuração dos Detalhes do dispositivo. Isto impede a existência de dispositivos duplicados na Consola.

Desinstalação protegida por palavra-passe

DEFINIÇÕES > Aplicação

Os Administradores podem exigir uma palavra-passe para desinstalar o Agente. Quando desinstalar o Agente com uma palavra-passe:

- Se o instalador MSI for utilizado para instalar, desinstale utilizando o MSI ou utilize o Painel de controlo.
- Se tiver sido utilizado um instalador EXE na instalação, utilize o EXE para desinstalar. Se o instalador EXE for utilizado e for necessária uma palavra-passe para desinstalação, não é possível utilizar o Painel de controlo.
- Se desinstalar utilizando a linha de comandos, adicione a cadeia de carateres de desinstalação. **`UNINSTALLKEY = [MyUninstallPassword]`**.

Para criar uma palavra-passe de desinstalação

1. Inicie sessão na Consola (http://dellthreatdefense.com) com uma conta de Administrador.
2. Selecione **Definições > Aplicação**.
3. Selecione a caixa de verificação para **Solicitar palavra-passe para desinstalar o Agente**.
4. Introduza uma palavra-passe.
5. Clique em **Guardar**.

Integrações

A Consola Threat Defense oferece integração com alguns programas de terceiros.

Syslog/SIEM

O Threat Defense permite a integração com o software de Gestão de eventos de segurança de informação (SIEM) utilizando a funcionalidade Syslog. Os eventos Syslog são persistidos ao mesmo tempo que os eventos do Agente são persistidos para a Consola.

Para os mais recentes endereços IP para mensagens Syslog, contacte o Apoio Técnico da Dell.

Tipos de eventos

Registo de auditoria

Selecione esta opção para enviar o registo de auditoria de ações do utilizador realizadas na Consola (Web site) para o servidor Syslog. Os eventos de registo de auditoria são sempre apresentados no ecrã Registo de auditoria, mesmo quando a seleção desta opção é anulada.

Exemplo de mensagem de registo de auditoria reencaminhado para o Syslog

Dispositivos

Selecione esta opção para enviar eventos do dispositivo para o servidor Syslog.

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

  Exemplo de mensagem para evento de registo de dispositivo

- Quando um dispositivo é removido.

  Exemplo de mensagem para evento de remoção de dispositivo

- Quando a política, Zona, nome ou nível de registo de um dispositivo forem alterados.

  Exemplo de mensagem para evento de atualização de dispositivo

Ameaças

Selecione esta opção para registar quaisquer ameaças ou alterações recentemente detetadas observadas para qualquer ameaça existente, no servidor Syslog. As alterações incluem uma ameaça que está no estado *Removido*, em *Quarentena*, *Renunciado* ou *Executado*.

Existem cinco tipos de Eventos de ameaça:

- **ameaça_detetada**: Foi detetada uma nova ameaça num estado *Não seguro*.
- **ameaça_removida**: Uma ameaça existente foi *Removida*.
- **ameaça_em_quarentena**: Foi detetada uma nova ameaça no estado em *Quarentena*.
- **ameaça_dispensada**: Foi detetada uma nova ameaça no estado *Renunciado*.
- **ameaça_alterada**: O comportamento de uma ameaça existente foi alterado (exemplos: Pontuação, Estado Em quarentena, Estado Em execução).
- **ameaça_desmarcada**: Uma ameaça que foi Renunciada, adicionada à Lista segura ou eliminada da quarentena num dispositivo.

Exemplo de mensagem de evento de ameaça

Classificações de ameaças

Todos os dias, centenas de ameaças são classificadas como Malware ou Programas potencialmente indesejáveis (PUP). Se selecionar esta opção, subscreve as notificações de ocorrência destes eventos.

Exemplo de mensagem de classificação de ameaças

SIEM (Gestão de eventos de segurança de informação)

Especifica o tipo do servidor Syslog ou SIEM para onde os eventos devem ser enviados.

Protocolo

Deve corresponder à configuração do seu servidor Syslog. As opções são UDP ou TCP. Geralmente, UDP não é recomendado, uma vez que não garante a entrega da mensagem. A Dell recomenda TCP (predefinição).

TLS/SSL

Apenas disponível se o Protocolo especificado for TCP. TLS/SSL assegura que a mensagem Syslog é encriptada em trânsito do Threat Defense para o servidor Syslog. A Dell encoraja os clientes a selecionarem esta opção. Certifique-se de que o servidor Syslog está configurado para escutar mensagens TLS/SSL.

IP/Domínio

Especifica o endereço IP ou o nome de domínio totalmente qualificado do servidor configurado pelo cliente. Consulte os seus especialistas de rede internos para assegurar que as definições do domínio e firewall estão corretamente configuradas.

Porta
Especifica o número da porta nos dispositivos onde o servidor Syslog realiza a escuta de mensagens. Deve ser um número entre 1 e 65535. Os valores normais são: 512 para UDP, 1235 ou 1468 para TCP e 6514 para TCP seguro (exemplo: TCP com TLS/SSL ativo).

Gravidade
Especifica a gravidade das mensagens que devem ser apresentadas no servidor Syslog. Este é um campo subjetivo e poderá ser definido para o seu nível preferido. O valor da gravidade não altera as mensagens que são reencaminhadas para o Syslog.

Função
Especifica que tipo de aplicação regista a mensagem. A predefinição é Interna (ou Syslog). É utilizada para classificar as mensagens quando as mesmas são recebidas pelo servidor Syslog.

Testar a ligação
Clique em **Testar ligação** para testar as definições de IP/Domínio, Porta e Protocolo. Se forem introduzidos valores válidos, após alguns momentos, é apresentada uma confirmação de *êxito*.

Autenticação personalizada

Utilize Fornecedores de identidade (IdP) externos para iniciar sessão na Consola. Isto requer a configuração das definições com o seu IdP para obter um certificado X.509 e um URL para verificação do seu início de sessão IdP. A Autenticação personalizada é compatível com o Microsoft SAML 2.0. A compatibilidade desta funcionalidade com o OneLogin, OKTA, Microsoft Azure e PingOne foi confirmada. Esta funcionalidade oferece também uma definição Personalizada e deve ser compatível com outros Fornecedores de identidade que seguem o Microsoft SAML 2.0.

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

- **Autenticação forte**: Faculta acesso a autenticação multifator.
- **Início de sessão único**: Faculta acesso a início de sessão único (SSO).

  Nota: Selecionar Autenticação forte ou Início de sessão único não afeta as definições de Autenticação personalizada, uma vez que todas as definições de configuração são processadas pelo Fornecedor de identidade (IdP).
- **Permitir início de sessão com palavra-passe**: Selecione esta opção para permitir o início de sessão direto na Consola, utilizando SSO. Isto permite testar a definição SSO sem ficar bloqueado fora da Consola. Depois de efetuar com êxito o início de sessão na Consola utilizando SSO, a Dell recomenda que esta funcionalidade seja desativada.
- **Fornecedor:** Selecione o fornecedor de serviços para a autenticação personalizada.
- **Certificado X.509**: Introduza as informações de certificação X.509.
- **URL de início de sessão**: Introduza o URL para a autenticação personalizada.

Relatório de dados da ameaça

Uma folha de cálculo que contém as seguintes informações sobre a organização:

- **Ameaças**: Apresenta uma lista de todas as ameaças detetadas na organização. Estas informações incluem o nome do ficheiro e estado do ficheiro (*Não seguro*, *Anormal*, *Renunciado* e em *Quarentena*).
- **Dispositivos**: Apresenta uma lista de todos os dispositivos da organização com o Agente Threat Defense instalado. Estas informações incluem o Nome do dispositivo, a Versão do sistema operativo, a Versão do agente e a Política aplicada.

- **Indicadores de ameaças**: Apresenta cada ameaça e as características da ameaça associadas.
- **Desmarcado**: Apresenta uma lista de todos os ficheiros que tenham sido *Desmarcados* na organização. Estas informações incluem os ficheiros que foram *Renunciados*, adicionados à *Lista Segura* e *Eliminados* da pasta *Quarentena* num dispositivo.
- **Eventos**: Apresenta uma lista de todos os eventos relacionados com o Gráfico de eventos de ameaça no Dashboard relativos aos últimos 30 dias. Estas informações incluem Hash de ficheiro, Nome do dispositivo, Caminho do ficheiro e Data de ocorrência do evento.

Quando esta funcionalidade está ativada, o relatório é automaticamente atualizado à 01h00 Hora padrão do Pacífico (PST). Clique em **Gerar relatório** para gerar uma atualização manualmente.

O Relatório de dados da ameaça fornece um URL e um token que podem ser utilizados para transferir o relatório sem que seja necessário iniciar sessão na Consola. É também possível eliminar ou regenerar um token, conforme necessário, o que permite controlar quem tem acesso ao relatório.

RESOLUÇÃO DE PROBLEMAS

Esta secção fornece uma lista de perguntas para responder e ficheiros para recolher ao resolver problemas do Threat Defense. Estas informações permitem que o Apoio Técnico da Dell ajude na resolução de problemas.

Esta secção contém também alguns problemas comuns e soluções sugeridas.

Suporte

Parâmetros de instalação

- Qual é o método de instalação? Disponibilize quaisquer parâmetros utilizados.
  - Exemplo – Windows: Utilize LAUCHAPP=0 aquando da instalação a partir da linha de comandos para ocultar o ícone do Agente e a pasta do menu Iniciar no momento da execução.
  - Exemplo – macOS: Utilize SelfProtectionLevel=1 aquando da instalação a partir da linha de comandos para desativar a Proteção automática no Agente.
- Que passos da instalação foi possível verificar?
  - Exemplo – Windows: O instalador MSI ou EXE foi utilizado?
  - Exemplo – Qualquer SO: Foram utilizadas quaisquer opções da linha de comandos? Como interface do utilizador Sem Agente ou Modo silencioso.
- Ativar registo verboso para a instalação.

Problemas de desempenho

- Efetue uma captura de ecrã do Gestor de tarefas (Windows) ou do Monitor de atividade (macOS) que apresente os processos do Threat Defense e o consumo de memória.
- Capture uma cópia de segurança do processo do Threat Defense.
- Recolha os registos de depuração.
- Recolha o resultado das Informações do sistema durante o problema.
  - Para Windows: msinfo32 ou winmsd
  - Para macOS: Informações do sistema
- Recolha quaisquer Registos de eventos (Windows) ou Informações da consola (macOS) relevantes.

Problemas de atualização, estado e conectividade

- Certifique-se de que a porta 443 está aberta na firewall e o dispositivo consegue resolver e efetuar ligação aos sites Cylance.com.
- O dispositivo é indicado na página Dispositivos da Consola? Está Online ou Offline? Qual é a Hora da última ligação?
- O dispositivo está a utilizar um proxy para efetuar a ligação à Internet? As credenciais estão corretamente configuradas no proxy?
- Reinicie o serviço Threat Defense para que o mesmo tente efetuar ligação à Consola.
- Recolha os registos de depuração.
- Recolha o resultado das Informações do sistema durante o problema.
    - Para Windows: msinfo32 ou winmsd
    - Para macOS: Informações do sistema

Ativar o registo de depuração

Por predefinição, o Threat Defense mantém os ficheiros de registo guardados em **`C:\Program Files\Cylance\Desktop\log`**. Para fins de resolução de problemas, o Threat Defense pode ser configurado de modo a produzir mais registos verbosos.

Incompatibilidades de controlo de scripts

Problema:

Quando o Controlo de scripts é ativado em alguns dispositivos, pode provocar conflitos com outro software em execução nesses dispositivos. Normalmente, este conflito deve-se à inserção do Agente em determinados processos que estão a ser chamados por outro software.

Solução:

Dependendo do software, este problema pode ser resolvido adicionando exclusões de processo específicas à Política de dispositivos na Consola. Outra opção é ativar o Modo de compatibilidade (tipo de registo) em cada dispositivo afetado. No entanto, se não existirem exclusões em vigor, a Dell recomenda que desative o Controlo de scripts na Política de dispositivos que afeta os dispositivos, para restaurar o normal funcionamento do dispositivo.

Nota: Esta solução de modo de compatibilidade é para a versão do Agente 1370. Começando pelo Agente 1382 e superior, o processo de injeção foi atualizado para obter mais informações sobre a compatibilidade com outros produtos.

Modo de compatibilidade

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

1. Utilizando o Editor de registo, aceda a **`HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`**.
2. Clique com o botão direito em **Ambiente de trabalho**, clique em **Permissões** e, em seguida, obtenha propriedade e conceda **Controlo total**. Clique em **OK**.
3. Clique com o botão direito do rato em **Ambiente de trabalho**, selecione **Novo > Valor binário**.
4. Dê ao ficheiro o nome **Modo de compatibilidade**.
5. Abra a definição de registo e altere o valor para **01**.

6. Clique em **OK** e, em seguida, feche o Editor de Registo.
7. Poderá ser necessário reiniciar o dispositivo.

Opções da linha de comandos

Utilizar 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, utilize o **`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 ficheiro suspeito com uma pontuação reduzida (1 – 59) com menor probabilidade de ser software maligno
Administrador	Gestor de inquilinos para Threat Defense
Agent	Threat Defense Endpoint Host que comunica com a Consola
Registo de auditoria	Registo que grava ações realizadas a partir da Consola Threat Defense
Quarentena automática	Impede automaticamente a execução de todos os ficheiros *Não seguros* e/ou *Anormais*
Carregamento automático	Carrega automaticamente quaisquer ficheiros PE (Portable Executable), detetados como *Não seguros* ou *Anormais*, na Cylance Infinity Cloud para análise.
Consola	Interface do utilizador de gestão do Threat Defense
Política de dispositivos	Política do Threat Defense que pode ser configurada pelo administrador da organização que define a forma como as ameaças são processadas em todos os dispositivos
Quarentena global	Impedir a execução de um ficheiro a nível global (em todos os dispositivos numa organização)
Lista segura global	Permitir a execução de um ficheiro a nível global (em todos os dispositivos numa organização)
Infinity	O modelo matemático utilizado para pontuação de ficheiros
Organização	Uma conta de inquilino que utiliza o serviço Threat Defense
Quarentena	Impedir a execução de um ficheiro a nível local (num dispositivo específico)
Ameaças	Ficheiros potencialmente maliciosos detetados pelo Threat Defense, classificados como *Não seguros* ou *Anormais*
Não seguro	Um ficheiro suspeito com uma pontuação elevada (60 – 100) com probabilidade de ser malware
Dispensar	Permitir a execução de um ficheiro a nível local (num dispositivo específico)
Zona	Uma forma de organizar e agrupar dispositivos numa organização de acordo com a prioridade, a funcionalidade, etc.
Regra de zona	Funcionalidade que permite a automatização da atribuição de dispositivos a Zonas específicas com base em endereços IP, no Sistema operativo e nos nomes do dispositivo.

APÊNDICE B: PROCESSAMENTO DE EXCEÇÕES

Há alturas em que os utilizadores têm, de forma manual, que colocar um ficheiro em *Quarentena* ou *Permitir* (*Renunciar*). O Threat Defense disponibiliza formas para lidar com exceções para cada dispositivo (*Local*), para um grupo de dispositivos (*Política*), para toda a organização (*Global*).

Ficheiros

Local: Coloca um ficheiro em *Quarentena* ou *Renuncia* (coloca-o na *Lista segura*) no dispositivo. Útil para *Bloquear* ou *Permitir* temporariamente um ficheiro até haver tempo para o analisar. *Renunciar* um ficheiro num dispositivo também é útil caso esse dispositivo seja o único dispositivo no qual o ficheiro deva estar autorizado a ser *Executado*. A Dell recomenda o uso de *Política* ou *Global* se esta ação tiver de ser executada em vários dispositivos.

Política: Coloca um ficheiro na *Lista segura* em todos os dispositivos atribuídos a uma política. Útil para permitir um ficheiro para um grupo de dispositivos (por exemplo, permitir que os dispositivos de TI executem ferramentas que possam ser utilizadas para fins mal intencionados, como PsExec). Colocar um ficheiro em *Quarentena* ao nível da Política não está disponível.

Global: Coloca um ficheiro em *Quarentena* ou na *Lista segura* para a organização. Coloca em *Quarentena* um ficheiro maligno conhecido na organização. Coloca na *Lista segura* um ficheiro que se sabe que está em boas condições e é utilizado na organização, mas que o Agente está a assinalar como malicioso.

Scripts

Política: O Controlo de scripts permite aprovar a execução de scripts a partir de uma pasta designada. Permitir a execução de scripts para uma pasta permite também scripts em pastas secundárias.

Certificados

Global: Adicione certificados à Consola e, em seguida, adicione-os à *Lista segura global*. Isto permite que as aplicações assinadas por este certificado sejam executadas na organização.

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

Para adicionar o certificado à *Lista segura global*, selecione **Definições > Lista global**, selecione o separador **Seguro**, selecione o separador **Certificados** e, em seguida, clique em **Adicionar certificado**.

APÊNDICE C: PERMISSÕES DO UTILIZADOR

As ações que podem ser realizadas pelos utilizadores dependem da permissão (função) de utilizador atribuída aos mesmos. Em geral, os Administradores podem realizar ações em qualquer nível da organização. Os Utilizadores e os Gestores de zona estão restringidos às Zonas às quais são atribuídos. Esta restrição inclui apenas poder aceder a dispositivos numa Zona e visualizar apenas dados de ameaças relacionados com esses dispositivos. Se o Utilizador ou Gestor de zona não conseguirem ver um dispositivo ou ameaça, é possível que o dispositivo não pertença a quaisquer Zonas atribuídas aos mesmos.

	UTILIZADOR	GESTOR DE ZONA	ADMIN
Atualização do Agente			
Ver/Editar			X
Registo 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 nome do dispositivo		X	X
Zonas			
Criar zona			X
Eliminar zona			X
Editar nome da zona – Qualquer			X
Editar nome da zona atribuído		X	X
Política			
Criar política – Global			X
Criar política para uma zona			X
Adicionar política – Global			X
Adicionar política a uma zona		X	X
Remover política – Global			X
Remover política de uma zona		X	X
Ameaças			
Ficheiros em quarentena – Global			X
Ficheiros em quarentena numa zona	X	X	X
Ficheiros dispensados – Global			X
Ficheiros dispensados numa zona	X	X	X
Quarentena global/Seguro			X
Definições			
Gerar ou eliminar o token de instalação			X
Gerar ou eliminar o URL de convite			X
Copiar o token de instalação	X	X	X
Copiar URL de convite			X
Gestão de utilizadores			
Atribuir utilizadores a qualquer zona			X
Atribuir utilizadores à zona gerida		X	X
Atribuir gestor de zona – Global			X
Atribuir gestor de zona às zonas geridas		X	X
Eliminar utilizadores da Consola			X
Remover utilizadores da zona – Global			X
Remover utilizadores da zona gerida		X	X

APÊNDICE D: FILTRO DE ESCRITA BASEADO EM FICHEIROS

O Agente do Threat Defense da Dell pode ser instalado num sistema com o Windows Embedded Standard 7 (cliente magro). Em dispositivos incorporados, pode não ser permitido guardar no armazenamento do sistema. Neste caso, o sistema poderá utilizar um Filtro de escrita baseado em ficheiros (FBWF) para redirecionar as gravações no armazenamento do sistema para a cache na memória do sistema. Isto pode causar problemas com a perda de alterações do Agente sempre que o sistema reinicia.

Ao utilizar o agente num sistema incorporado, siga o seguinte procedimento:

1. Antes de instalar o Agente, desative o FBWF utilizando o comando: `fbwfmgr /disable`.
2. Reinicie o sistema. Isto permite que a desativação do FBWF entre em vigor.
3. Instale o Agente do Threat Defense da Dell.
4. Depois de instalar o Agente, volte a ativar o FBWF utilizando o comando: `fbwfmgr /enable`.
5. Reinicie o sistema. Isto 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 persistam após o reinício do sistema.
7. Utilize o seguinte comando para excluir a pasta Ambiente de trabalho: `fbwfmgr /addexclusion C: "\Program Files\Cylance\Desktop\"`
    a. Este assume que está a instalar no diretório predefinido. Mude a exclusão para a pasta em que instalou o Agente.
8. Se pretender guardar as ameaças no computador para testar em comparação com o Agente, não se esqueça de excluir também a localização de armazenamento do FBWF (`C:\Samples` por exemplo).