Dell Endpoint Security Suite Enterprise

Advanced Threat Prevention Quick Start Guide v3.9

January 2024
Rev. A01

DELL Technologies

Notas, avisos e advertências

NOTA: NOTA fornece informações importantes para ajudar você a usar melhor o computador.

CUIDADO: Um AVISO indica possíveis danos ao hardware ou perda de dados e ensina como evitar o problema.

ATENÇÃO: Uma ADVERTÊNCIA indica possíveis danos à propriedade, lesões corporais ou risco de morte.

Contents

1

Introduction

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

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

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

Entre em contato com o Dell ProSupport for Software

Ligue para 877-459-7304, extensão 4310039 para obter suporte por telefone 24x7, para o seu produto Dell.

Há também disponível o serviço de suporte on-line para os produtos Dell no site dell.com/support. O suporte on-line inclui drivers, manuais, orientações técnicas, perguntas frequentes e problemas emergentes.

Quando telefonar, tenha em mãos a Etiqueta de serviço ou Código de serviço expresso, para nos ajudar a garantir que possamos direcioná-lo rapidamente ao especialista técnico correto.

Para obter os números de telefone de fora dos Estados Unidos, veja Números de telefone internacionais do Dell ProSupport for Software.

2

Introdução

Este capítulo detalha as etapas recomendadas para começar a administrar o Advanced Threat Prevention.

As etapas recomendadas para começar a administrar o Advanced Threat Prevention incluem as seguintes fases:

- Provisionar um locatário para o Advanced Threat Prevention
  - Necessário para implementar o Advanced Threat Prevention
  - As licenças do Advanced Threat Prevention precisam estar presentes no Dell Server.
- Configurar Atualização automática do agente do Advanced Threat Prevention
  - Inscrever-se para obter atualizações automáticas do Advanced Threat Prevention (opcional)
  - As atualizações são liberadas mensalmente
- Atribuir ou modificar funções de administrador
  - Provisionar ou recuperar o serviço do Advanced Threat Prevention
  - Fazer backup e download de certificados existentes no Advanced Threat Prevention
  - Visualizar, modificar e confirmar políticas
- Configurar notificações
  - Configurar as notificações de e-mail e do painel para alertas do Advanced Threat Prevention (opcional)
  - Personalizar as notificações com base em suas necessidades corporativas

Provisionar um locatário

Um locatário precisa ser provisionado no Dell Server para que a imposição de políticas do Advanced Threat Prevention possa ser ativada.

Pré-requisitos

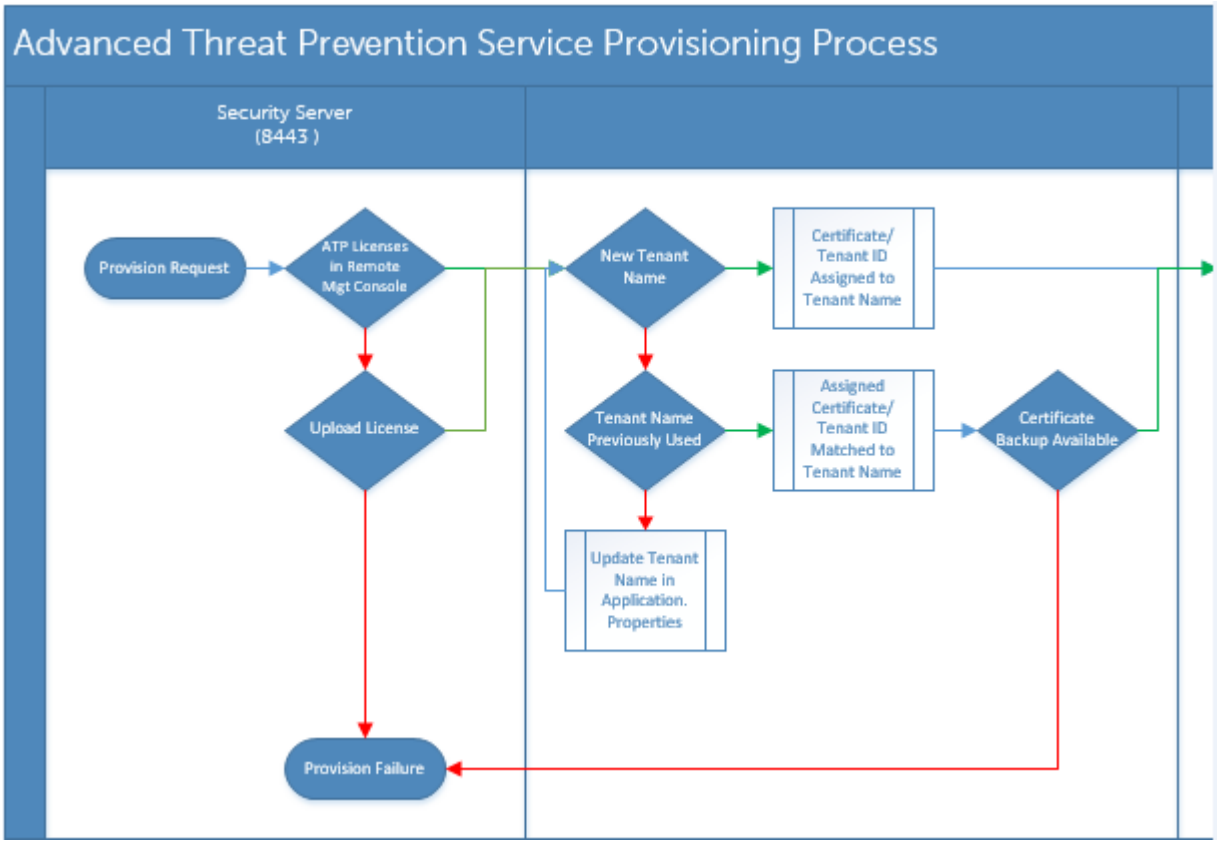
- Precisa ser realizado por um administrador com a função de administrador do sistema.
- É necessária conectividade com a Internet para provisionar no Dell Server.
- É necessária conectividade do cliente com a Internet para exibir a integração do serviço online do Advanced Threat Prevention no Management Console.
- O provisionamento é baseado em um token gerado a partir de um certificado durante o provisionamento.
- As licenças do Advanced Threat Prevention precisam estar presentes no Dell Server.

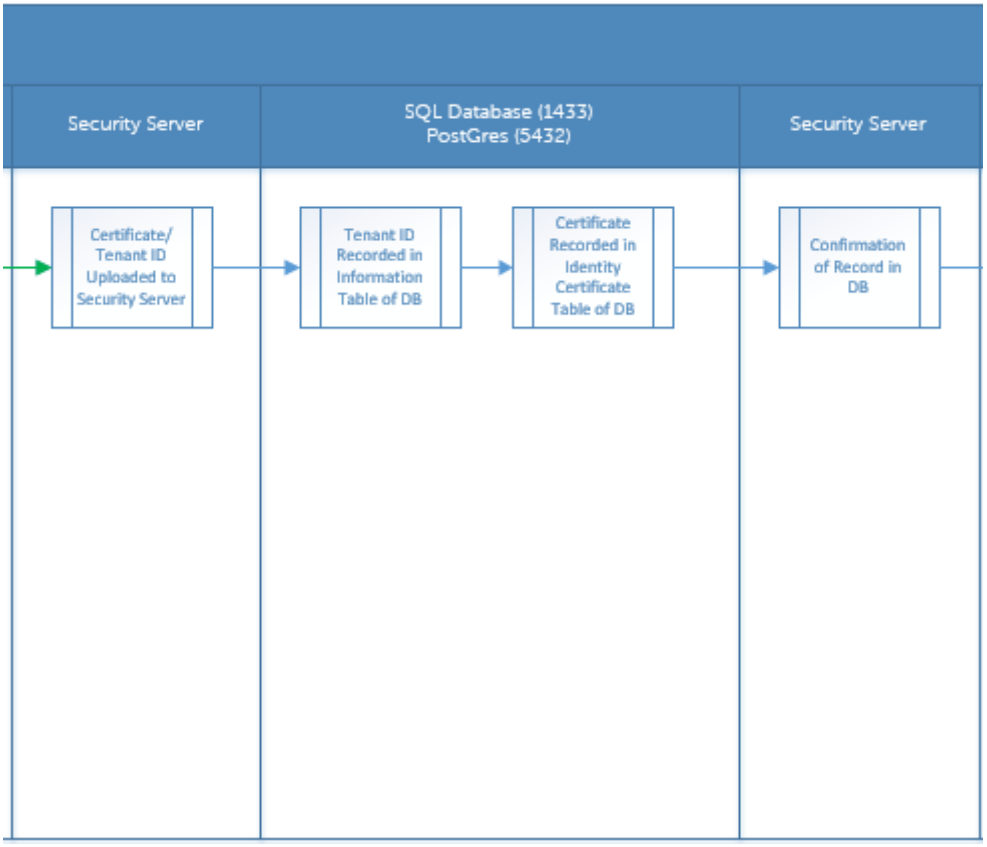
Provisionar um locatário

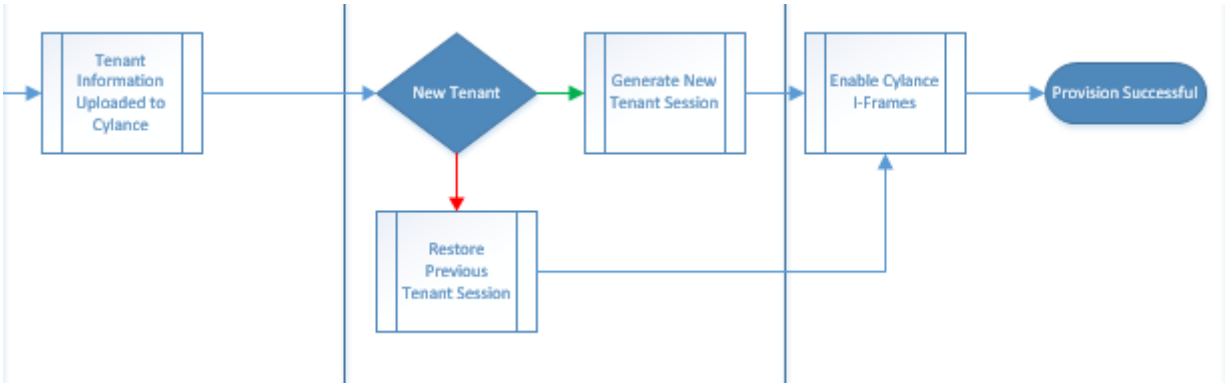
1. Como um administrador Dell, faça login no Management Console.
2. No painel esquerdo do Management Console, clique em **GerenciamentoGerenciamento de serviços**.
3. Clique em **Configurar o serviço Advanced Threat Protection**. Importe as licenças do Advanced Threat Prevention, caso ocorra uma falha nesse ponto.
4. A instalação guiada começa logo após a importação das licenças. Clique em **Avançar** para começar.
5. Leia e concorde com o EULA e clique em **Avançar**.
6. Forneça credenciais de identificação ao Dell Server para provisionamento do Usuário. Clique em **Avançar**. *Não há suporte para o provisionamento de um usuário existente da marca Cylance.*
7. Baixe o certificado. Isso é necessário para a recuperação se ocorrer um desastre com o Dell Server. O backup deste certificado não é feito automaticamente. Faça backup do certificado em um local seguro em outro computador. Marque a caixa de seleção para confirmar que você fez o backup do Certificado e clique em **Avançar**.
8. A configuração foi concluída. Clique em **OK**.

Provisionamento e comunicação do agente

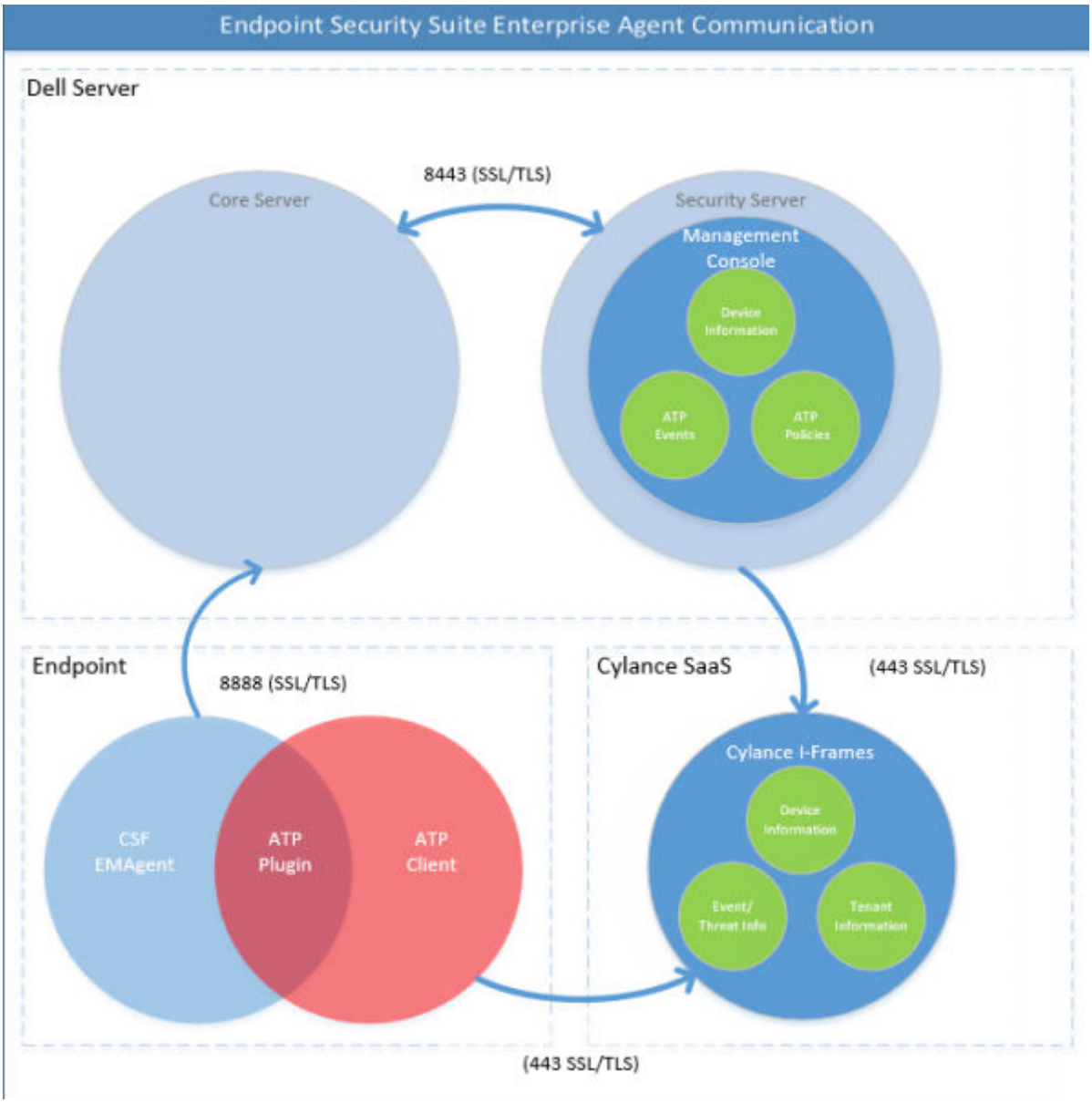
Os diagramas a seguir ilustram o processo de provisionamento do serviço Advanced Threat Prevention.



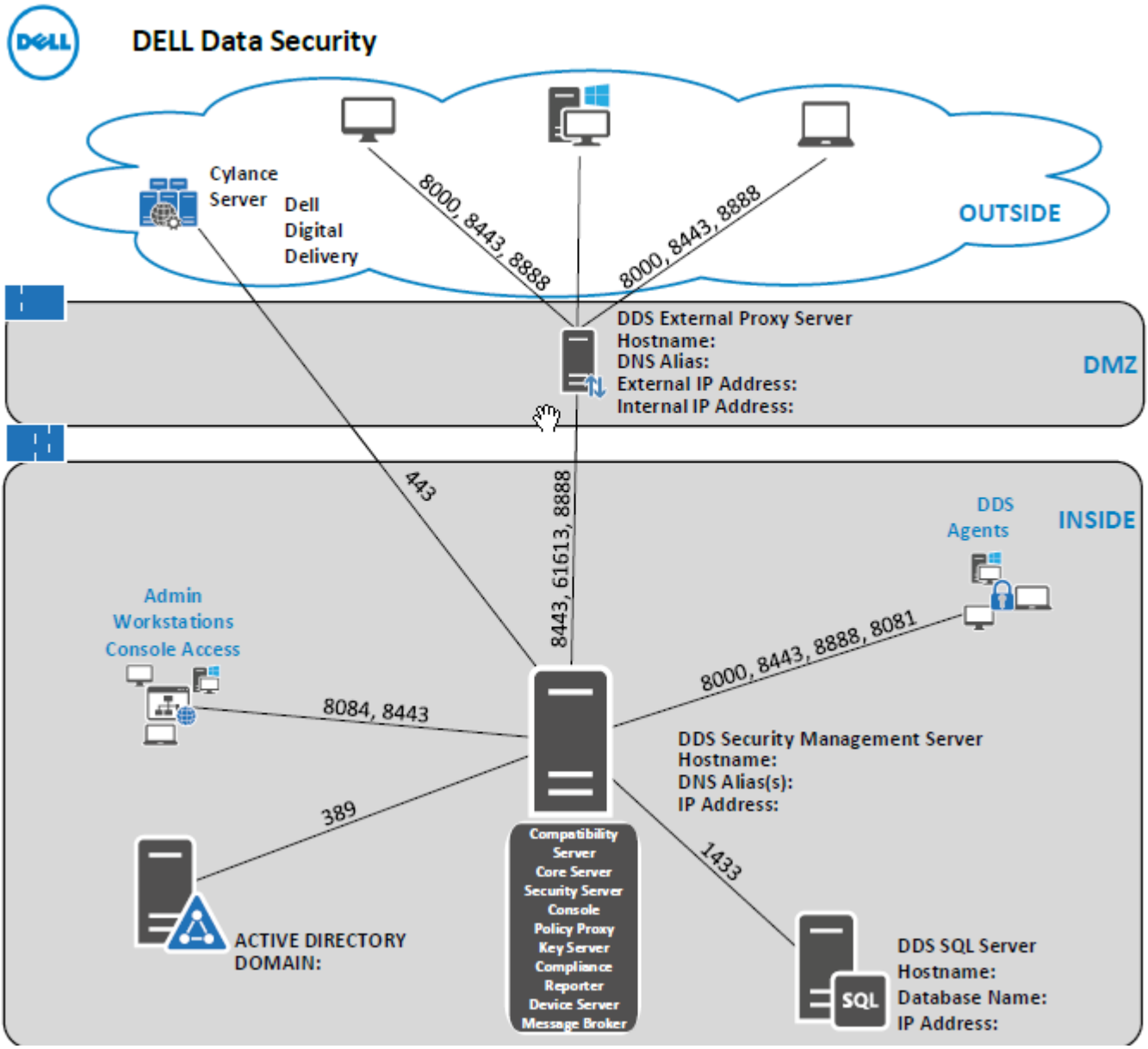




O diagrama a seguir ilustra o processo de comunicação do agente do Advanced Threat Prevention.



O diagrama a seguir ilustra a arquitetura e a comunicação do Dell Server.



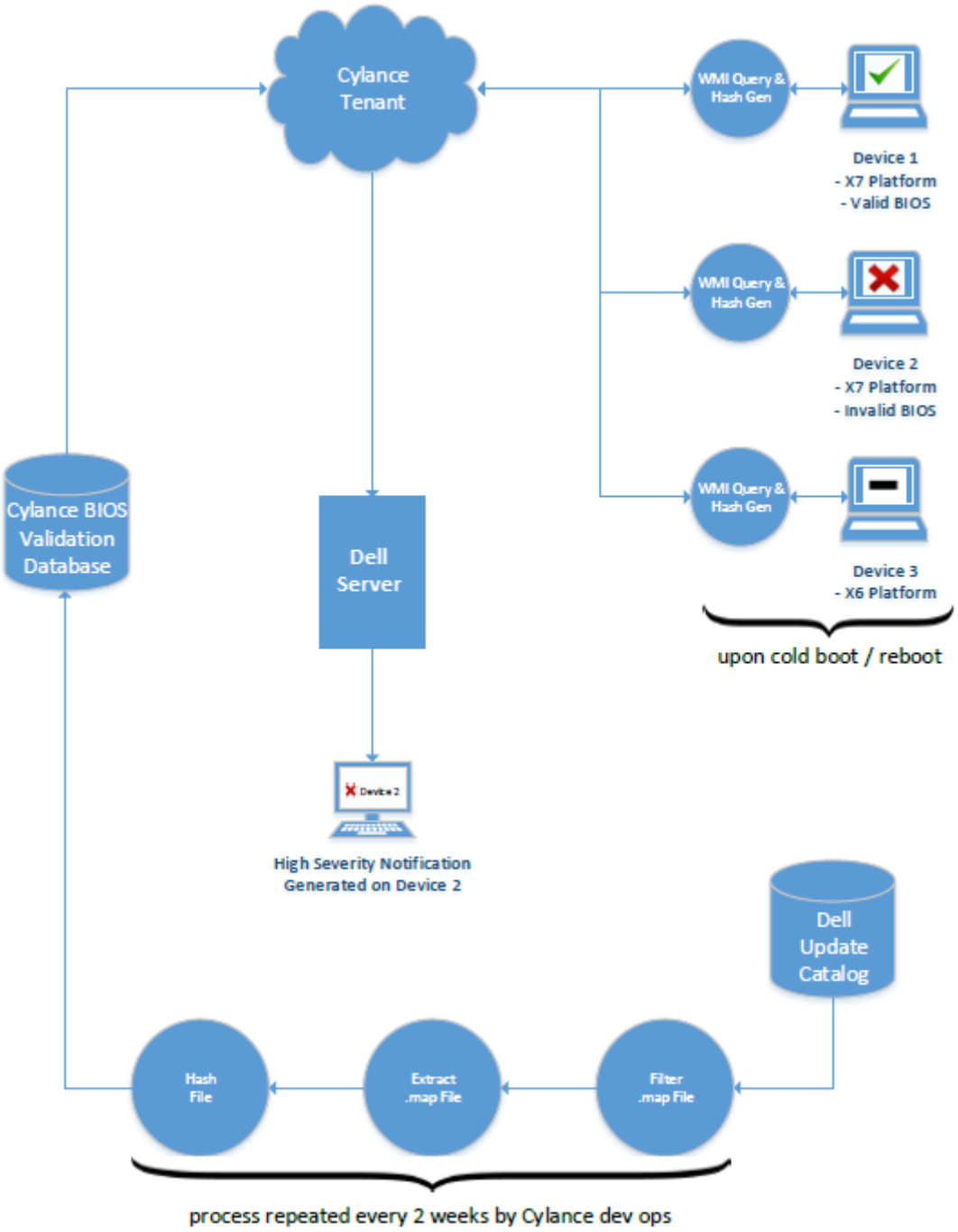
Habilitar a verificação da integridade da imagem da BIOS

A política de verificação da integridade da imagem da BIOS está habilitada por padrão quando o interruptor principal do Advanced Threat Prevention está habilitado.

Para obter uma visão geral do processo de verificação de integridade da imagem da BIOS, consulte Processo de verificação da integridade da imagem da BIOS.

Processo de verificação

O diagrama a seguir ilustra o processo de verificação de integridade da imagem do BIOS.



Se a política *Ativar certificação de BIOS* estiver selecionada no Management Console, o locatário do Cylance valida um hash do BIOS nos sistemas dos usuários finais para garantir que o BIOS não foi modificado na versão de fábrica da Dell, o que é um possível vetor de ataque. Se uma ameaça for detectada, uma notificação será passada para o Dell Server e o administrador de TI será alertado no Remote Management Console. Para obter uma visão geral do processo, consulte Processo de verificação de integridade da imagem do BIOS.

NOTA: Não é possível usar uma imagem de fábrica personalizada com esse recurso, pois o BIOS foi modificado.

Modelos de computador Dell compatíveis com a Verificação de integridade da imagem do BIOS	
• Latitude 3470 • Latitude 3570 • Latitude 7275 • Latitude 7370	• OptiPlex 5040 • OptiPlex 7040 • OptiPlex 7440 • Precision Mobile Workstation 3510

Modelos de computador Dell compatíveis com a Verificação de integridade da imagem do BIOS		
• Latitude E5270 • Latitude E5470 • Latitude E5570 • Latitude E7270 • Latitude E7470 • Latitude Rugged 5414 • Latitude Rugged 7214 Extreme • Latitude Rugged 7414 • OptiPlex 3040 • OptiPlex 3240	• Precision Mobile Workstation 5510 • Precision Workstation 3620 • Precision Workstation 7510 • Precision Workstation 7710 • Precision Workstation T3420 • Venue 10 Pro 5056 • Venue Pro 5855 • Venue XPS 12 9250 • XPS 13 9350 • XPS 9550	

Configurar a atualização automática do agente do Advanced Threat Prevention

No Management Console do Dell Server, você pode se inscrever para receber atualizações automáticas do agente do Advanced Threat Prevention. A inscrição para receber atualizações do agente automáticas permite aos clientes fazer download automaticamente das atualizações e aplicá-las a partir do serviço Advanced Threat Prevention. As atualizações são liberadas mensalmente.

NOTA:

Atualizações automáticas do agente são suportadas com o Dell Server v9.4.1 ou posterior.

Receber atualizações automáticas do agente

Para se inscrever para receber atualizações automáticas do agente:

1. No painel esquerdo do Management Console, clique em **Gerenciamento** > **Gerenciamento de serviços**.
2. Na guia *Ameaças avançadas*, em *Atualização automática do agente*, clique no botão **Ativar** e, em seguida, clique no botão **Salvar preferências**.

   Pode demorar alguns minutos para que as informações sejam preenchidas e as atualizações automáticas, exibidas.

Para de receber atualizações automáticas do agente

Para parar de receber atualizações automáticas do agente

1. No painel esquerdo do Management Console, clique em **Gerenciamento** > **Gerenciamento de serviços**.
2. Na guia *Ameaças avançadas*, em *Atualização automática do agente*, clique no botão **Desativar** e, em seguida, clique no botão **Salvar preferências**.

Atribuir ou modificar funções de administrador

Visualizar ou modificar os privilégios de administrador existentes na página Administradores do Management Console.

Funções do administrador

O login do administrador está integrado com o Active Directory para simplificar o processo de gerenciamento de administradores e permitir que você aproveite a sua infraestrutura de autenticação de usuário existente. Aos administradores são atribuídas funções que definem a qual nível de acesso cada administrador tem permissão. Por exemplo, alguns administradores só podem ser autorizados a implementar recuperação assistida de suporte técnico, enquanto outros têm acesso completo para editar políticas de segurança. Você pode atribuir funções de Administrador a grupos do Active Directory, assim você pode facilmente mudar o nível de acesso de Administrador dos usuários com uma simples alteração de membros do grupo AD. Usuários sem domínio podem ter acesso apenas a relatórios via Compliance Reporter.

A função Administrador do sistema é necessária para executar as seguintes tarefas:

- Provisionar ou recuperar o serviço do Advanced Threat Prevention
- Inscrever-se para obter atualizações automáticas do Advanced Threat Prevention
- Definir notificações por e-mail ou do painel para alertas do Advanced Threat Prevention

- Fazer backup e download de certificados existentes no Advanced Threat Prevention

NOTA: A função administrador de segurança é necessária para visualizar, modificar ou confirmar políticas.

Para ver ou modificar permissões de administrador existentes, siga essas etapas:
1. No painel esquerdo, clique em **Populações > Administradores**.
2. Pesquise ou selecione pela linha que mostra o nome de usuário do administrador adequado para ver os Detalhes de usuário.
3. Veja ou modifique as funções de administrador no painel à direita.
4. Clique em **Salvar**.

NOTA: A Dell recomenda atribuir funções de administrador a nível de grupo em vez de nível de usuário.

Para ver, atribuir ou modificar funções de administrador a nível de grupo, siga essas etapas:
1. No painel esquerdo, clique em **Populações > Grupos de usuários**.
2. Pesquise ou selecione um Nome de grupo e selecione a guia **Administrador**. A página Detalhes de grupo de usuários será mostrada.
3. Marque ou desmarque as funções de administrador atribuídas ao grupo.
4. Clique em **Salvar**.

Se você remover um grupo que possui permissões administrativas e re-adicionar o grupo posteriormente, ele permanece um grupo de administrador.

Para visualizar, atribuir ou modificar Funções de administrador no Nível de usuário, siga estas etapas:
1. No painel esquerdo, clique em **Populações > Usuários**.
2. Pesquise ou selecione um nome de usuário e selecione a guia Administrador.
3. Marque ou desmarque as funções de administrador atribuídas ao usuário.
4. Clique em **Salvar**.

Funções de administrador - Atribua ou modifique funções para o usuário e clique em **Salvar**.

Funções de grupo herdadas - Uma lista somente-leitura de funções que o usuário herdou de um grupo. Para modificar as funções, clique na guia **Grupos de usuários** desse usuário e selecione o Nome de grupo.

Funções designadas - Delegue direitos de administrador a um usuário.

Configurar notificações

No Remote Management Console, você pode se inscrever para receber notificações. A lista Notificações fornece um resumo configurável de notícias, alertas e eventos que podem ser mostrados no painel ou enviados como notificações por e-mail.

Tipo de notificação

Você pode selecionar os tipos de notificação incluídos na lista. As notificações dos outros tipos ficam ocultas. As notificações de **Threat Protection** e **Advanced Threat Event** pertencem ao Advanced Threat Prevention.

Os tipos são:
- **Atualização** - Notícias de atualizações de produto. É preciso se inscrever para ver e receber atualizações de produtos. Selecione **Gerenciamento de serviços > Notificações de produtos**, clique em **Ativado** e clique em **Salvar preferências**.
- **Config** - Notícias sobre mudanças de configuração.
- **Base de conhecimento** - Resume os artigos da base de conhecimento e se vincula a estes com informações técnicas avançadas, como soluções temporárias e métodos de configuração.
- **Comunicado** - Notícias de novas versões e novos produtos.
- **Licença** - Fornece um alerta quando a disponibilidade da licença de volume está baixa ou quando a contagem de licença de acesso para cliente é excedida.
- **Proteção contra ameaça** - Um alerta de ameaça do Advanced Threat Prevention.
- **Evento de ameaça avançada** - Um evento detectado pelo Advanced Threat Prevention. O resumo contém uma lista de eventos Críticos, Principais, Menores, de Aviso e de Informações com links para informações mais detalhadas.
- **Evento de ameaça** - Um evento detectado pela Proteção contra ameaça.
- **Certificado** - Notificação de vencimento do certificado.
- **Exceções do Dell Server** - Um problema de comunicação do Dell Server está afetando as entregas das seguintes notificações: Threat Protection, Atualização, Config, Base de conhecimento e Anúncio.

Depois de selecionar um ou mais tipos, clique no espaço neutro acima da lista para aplicar as seleções.

Selecione **Limpar itens selecionados** para redefinir as seleções nesta lista.

Níveis de prioridade

NOTA: Os níveis de prioridade de notificação não estão relacionados aos níveis de prioridade mostrados no painel, exceto na área Notificações.

As prioridades são Crítica, Alta, Média e Baixa. Esses níveis de prioridade só são relativos entre si dentro de um tipo de notificação.

Você pode selecionar os níveis de prioridade das notificações a serem incluídas na área de notificações do painel ou nas listas de notificações por e-mail. As notificações dos outros níveis de prioridade não são incluídas no painel nem nas listas de notificações por e-mail.

Selecione **Limpar itens selecionados** para redefinir as seleções nesta lista. Todas as notificações serão mostradas (a menos que filtradas em outro lugar).

3

Políticas

Este capítulo detalha o gerenciamento de políticas do Advanced Threat Prevention.

- Habilitar o Advanced Threat Prevention
- Configurações de política recomendadas
- Confirmar as modificações da política

Para obter a lista completa de políticas do Advanced Threat Prevention e suas descrições, consulte o *AdminHelp*, disponível no Management Console.

Habilitar o Advanced Threat Prevention

A política do Advanced Threat Prevention está **desativada** por padrão e deve ser **ativada** para habilitar as políticas do Advanced Threat Prevention. As políticas do Advanced Threat Prevention são aplicáveis nos níveis do Enterprise, do Endpoint Group e do Endpoint.

Para ativar a política do Advanced Threat Prevention no nível do Enterprise, siga estas etapas:

1. No painel esquerdo, clique em **Populações > Empresa**.
2. Clique em **Prevenção de ameaças**.
3. Alterne o interruptor mestre de Advanced Threat Prevention de **Off** para **On**.

Para habilitar a política do Advanced Threat Prevention no nível do Endpoint Group, siga estas etapas:

1. No painel esquerdo, clique em **Populações > Grupo de pontos de extremidade**.
2. Clique em **Prevenção de ameaças**.
3. Alterne o interruptor mestre de Advanced Threat Prevention de **Off** para **On**.

Para habilitar a política de Advanced Threat Prevention no nível de ponto de extremidade, siga estas etapas:

1. No painel esquerdo, clique em **Populações > Pontos de extremidade**.
2. Clique em **Prevenção de ameaças**.
3. Alterne o interruptor mestre de Advanced Threat Prevention de **Off** para **On**.

Configurações de política recomendadas

- Para obter a lista mais atualizada de configurações de políticas recomendadas, consulte o artigo da base de conhecimento SLN301562.

Confirmar as modificações da política

Para confirmar políticas que foram modificadas e salvas:

1. No painel esquerdo do Management Console, clique em **Gerenciamento > Confirmar**.
2. Em Comentário, digite uma descrição da alteração.
3. Clique em **Confirmar políticas**.

Uma confirmação/publicação de política ocorre quando um administrador clica em **Confirmar políticas**. As seguintes informações são mostradas:

- Mudanças de política pendentes - O número de mudanças de política prontas para confirmação.
- Data de confirmação - Data e hora nas quais as políticas foram confirmadas.
- Alterado por - Nome de usuário do administrador que realizou a confirmação de política.
- Comentário - Quaisquer comentários que foram adicionados quando as políticas foram confirmadas.
- Versão - O número de salvamentos de política desde a última confirmação de política acrescido da versão anterior.

4

Ameaças

Este capítulo apresenta detalhes sobre como identificar e gerenciar ameaças encontradas em um ambiente empresarial, depois da instalação do Advanced Threat Prevention.

- Identificar uma ameaça
  - Ver eventos de ameaças
  - Atualizações da pontuação da Cylance e do modelo de ameaça
  - Visualizar dados detalhados da ameaça
- Gerenciar uma ameaça
  - Exportar dados da ameaça para CSV
  - Gerenciar a lista de quarentena global

Identificar uma ameaça

Notificações por e-mail e notificações do painel

Se você configurou as notificações por e-mail para o Threat Protection e o Advanced Threat Events, um administrador será notificado por e-mail sobre eventos e ameaças do Advanced Threat Prevention.

O painel Resumo de notificações no Management Console exibe ameaças e eventos do Advanced Threat Prevention, como tipos de notificação do Threat Protection e do Advanced Threat Events.

- Tipo de proteção contra ameaças - Um alerta de ameaça do Advanced Threat Prevention.
- Tipo de evento de ameaça avançada - Um evento detectado pelo Advanced Threat Prevention. Um evento não é necessariamente uma ameaça.

A tabela abaixo detalha as informações sobre ameaças, rótulos de ameaças e severidade.

Rótulo	Severidade	Detalhe
ThreatFound	Crítico	Indica que um Executável Portátil (PE) foi identificado em um dispositivo, mas não foi bloqueado nem colocado em quarentena no endpoint, o que indica uma ameaça ativa no sistema.
ThreatBlocked	Aviso	Indica que um Executável Portátil foi identificado no dispositivo, embora sua execução tenha sido bloqueada. Essa ameaça não foi especificamente colocada em quarentena, o que provavelmente se deve ao fato de que a política de Quarentena Automática não foi ativada ou de que o arquivo está em uma localização na qual não podemos gravar com a conta SYSTEM local (compartilhamento de rede, dispositivo USB que tenha sido removido etc.).
ThreatTerminated	Aviso	Indica que um Executável Portátil (PE) foi identificado no dispositivo e que seu processo foi encerrado, pois estava sendo executado ativamente. Isso não indica que o arquivo também foi colocado em quarentena, pois o PE pode ter sido executado a partir de outra localização. A sugestão é para que o usuário procure outro evento correlacionado a esse endpoint e executável para confirmar se a ameaça foi devidamente contida.
MemoryViolationBlocked	Aviso	Indica que houve uma tentativa de execução de um executável ou script, mas que isso violou a política de Proteção de Memória ou Controle de Scripts. Posteriormente, a execução do executável ou do script foi bloqueada. Normalmente, isso indica que a política correlacionada descrita de Proteção de Memória ou Controle de Scripts foi definida como Bloquear.

Rótulo	Severidade	Detalhe
MemoryViolationTerminated	Aviso	Indica que um executável ou script foi encontrado em execução ativa, em violação à política de Proteção de Memória ou Controle de Scripts. Posteriormente, o executável ou script foi encerrado. Normalmente, isso indica que a política correlacionada descrita de Proteção de Memória ou Controle de Scripts foi definida como Encerrar.
MemoryViolation	Aviso	Indica que foi encontrado um executável ou script que violou a política de Proteção de Memória ou Controle de Scripts. Nenhuma ação foi realizada em relação ao executável nem ao script, provavelmente porque a política estava definida como Permitir.
ThreatRemoved	Informações	Indica que um Executável Portátil (PE) sinalizado anteriormente, considerado uma ameaça, foi removido do endpoint. Isso pode indicar que o PE foi removido da quarentena ou removido da localização inicial. Isso é comum com PEs que foram inicialmente detectados em mídia removível (USB, CD-ROM etc.)
ThreatQuarantined	Informações	Indica que foi determinado que um Executável Portátil (PE) era uma possível ameaça e, posteriormente, ele foi colocado em quarentena com sucesso. Isso indica que a política de Quarentena Automática de ameaças, com base em sua classificação Anormal (pontuação Cylance de 0 a 60) ou Inseguro (pontuação Cylance de 60 a 100), está ativada.
ThreatWaived	Informações	Indica que um Executável Portátil (PE) que foi determinado como uma possível ameaça foi Isento com base na Lista Segura Global ou por uma Isenção local. Isso também pode indicar que o hash SHA256 foi adicionado às políticas "Isentar" ou "Lista Segura Global" do Dell Security Management Server.
ThreatChanged	Informações	Indica que a pontuação Cylance de um Executável Portátil (PE) foi alterada. Geralmente, isso acontece devido à pontuação de duas etapas que é feita pela Cylance. A análise da ameaça pelo mecanismo local de pontuação pode não ter correspondido à análise do mecanismo de nuvem da Cylance. Nesses casos, devido aos dados adicionais do mecanismo de nuvem da Cylance, é usada a pontuação derivada pelo mecanismo de nuvem da Cylance. Isso também pode indicar que uma atualização da Cylance inicializou uma nova análise de arquivos que, anteriormente, foram considerados ameaças, e que uma nova pontuação foi calculada para que esse PE não seja mais considerado uma ameaça.
ProtectionStatusChanged	Informações	Indica quando o status de proteção de um endpoint foi alterado. Isso é acionado quando o Dell Encryption Management Agent se reconecta aos serviços da Cylance por meio dos plug-ins Cylance. Geralmente, isso é acionado quando um endpoint é reinicializado, já que há um pequeno período em que o CSF pode não ter se conectado aos plug-ins Cylance durante a inicialização.

Clique em uma notificação para obter mais detalhes. O resumo inclui links para detalhes adicionais sobre o evento ou a ameaça.

A guia Ameaças avançadas

A guia Ameaças avançadas fornece uma exibição dinâmica de informações de eventos detalhadas de toda a empresa, incluindo uma lista dos dispositivos nos quais os eventos ocorreram e quaisquer ações realizadas nesses dispositivos para esses eventos.

Para acessar a guia Enterprise Advanced Threats, siga estas etapas:

1. No painel esquerdo, clique em **Populações > Empresa**.
2. Selecione a guia **Ameaças avançadas**.

As informações sobre eventos, dispositivos e ações são organizadas nestas guias:

- **Proteção** - Lista scripts e arquivos potencialmente prejudiciais e detalhes sobre eles, incluindo os dispositivos nos quais os scripts e arquivos são encontrados.
- **Agentes** - Fornece informações sobre dispositivos que executam o cliente do Advanced Threat Prevention, além da opção de exportar as informações ou remover dispositivos da lista.
- **Lista global** - Indica arquivos nas listas Quarentena global e Segura e fornece a opção de mover os arquivos para essas listas.
- **Opções** - Permite uma forma de integração com o Security Information Event Management (SIEM).
- **Certificado** - Permite fazer upload de certificados. Após o upload, os certificados são mostrados na guia Lista global e podem ser indicados como seguros.

As tabelas nas guias podem ser organizadas destas formas:

- Adicionar ou remover colunas da tabela - Clique na seta ao lado do cabeçalho de qualquer coluna, selecione **Colunas** e, em seguida, selecione as colunas que deseja exibir. Desmarque a caixa de seleção das colunas para ocultar.
- Classificar os dados - Clique em um cabeçalho de coluna.
- Agrupar por uma coluna - Arraste o cabeçalho da coluna para cima, até ela ficar verde.

Guia Eventos de ameaça avançada

A guia Eventos de ameaça avançada exibe informações sobre eventos em toda a empresa, com base nas informações disponíveis no Dell Server.

A guia mostra se o serviço Advanced Threat Prevention está provisionado e se há licenças disponíveis.

Para exportar dados da guia Eventos de ameaça avançada, clique em **Exportar** e selecione o formato de arquivo **Excel** ou **CSV**.

NOTA: Arquivos Excel são limitados a 65.000 linhas. CSV não tem limite de tamanho.

Atualizações da pontuação da Cylance e do modelo de ameaça

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

O modelo de risco preditivo usado para proteger dispositivos recebe atualizações periódicas para melhorar as taxas de detecção.

Duas colunas na página Proteção do Management Console mostram como um novo modelo de risco afeta sua organização. Exiba e compare as colunas Status da produção e Novo status para ver quais arquivos dos dispositivos podem ser afetados por uma alteração no modelo.

Para ver as colunas Status da produção e Novo status:

1. No painel esquerdo, clique em **Populações > Empresa**.
2. Selecione a guia **Ameaças avançadas**.
3. Clique na guia **Proteção**.
4. Clique na seta para baixo no cabeçalho de uma coluna da tabela.
5. Focalize **Colunas**.
6. Selecione as colunas **Status da produção** e **Novo status**.

Status da produção - Status do modelo atual (Seguro, Anormal ou Inseguro) do arquivo.

Novo status - Status do modelo do arquivo no novo modelo.

Por exemplo, um arquivo considerado Seguro no modelo atual poderá mudar para Inseguro no novo modelo. Se sua organização precisar desse arquivo, você poderá adicioná-lo à lista Segura. Um arquivo que nunca foi visto ou classificado pelo modelo atual pode ser considerado Inseguro pelo novo modelo. Se sua organização precisar desse arquivo, você poderá adicioná-lo à lista Segura.

Somente arquivos encontrados no dispositivo da sua organização e que tiverem sofrido alguma alteração na Pontuação da Cylance serão exibidos. Alguns arquivos podem ter uma alteração na pontuação, mas ainda permanecendo no seu Status atual. Por exemplo, se a Pontuação da Cylance para um arquivo variar de 10 a 20, o status do arquivo poderá permanecer Anormal e o arquivo será exibido na lista de modelos atualizados (se esse arquivo existir em dispositivos da sua organização).

Comparar Modelo atual com Novo modelo

Agora, você pode analisar as diferenças entre o modelo atual e o novo modelo.

Os dois cenários que você deve conhecer são:

Status da produção = Seguro, Novo Status = Anormal ou Inseguro

- Sua Organização considera o arquivo Seguro
- Sua organização definiu Anormal e/ou Inseguro como Quarentena automática

Nos cenários descritos acima, a recomendação é colocar na Lista segura os arquivos que serão permitidos em sua organização.

Identificar classificações

Para identificar classificações que possam afetar sua organização, a Dell recomenda a seguinte abordagem:

1. Aplique um filtro para a coluna Novo status para mostrar todos os arquivos Inseguros, Anormais e em Quarentena.
2. Aplique um filtro para a coluna Status da produção para mostrar todos os arquivos Seguros.
3. Aplique um filtro para a coluna Classificação para mostrar apenas Confiável - Ameaças locais.

Confiável - Os arquivos locais foram examinados pela Cylance e foram considerados Seguros. Coloque esses itens na Lista segura após a análise. Se você tiver um grande número de arquivos na lista filtrada, poderá ser necessário priorizar usando mais atributos. Por exemplo, adicione um filtro à coluna Detectado por para examinar ameaças encontradas pelo Controle de execução. Elas foram condenadas quando um usuário tentou executar um aplicativo e precisou de uma atenção mais urgente do que à dada a arquivos inativos condenados pela Detecção de ameaças em segundo plano ou o Observador de arquivos.

As informações para a comparação dos modelos vem do banco de dados, não dos seus dispositivos. Portanto, não é feita uma nova análise para a comparação de modelos. Entretanto, quando um novo modelo está disponível e o Agente correto está instalado, é feita uma nova análise na sua organização e qualquer alteração aos modelos é aplicada.

Consulte o *AdminHelp* para obter mais informações.

Visualizar eventos de Web Protection e de Firewall

As ameaças são categorizadas como Malware/Vulnerabilidade, Filtro da Web, Firewall ou Eventos não categorizados. A lista de eventos de ameaças pode ser classificada por qualquer um dos cabeçalhos de coluna. Você pode ver os eventos de ameaça para toda a empresa ou para um endpoint específico. Para ver eventos de ameaças para um endpoint específico, na guia Eventos de ameaça empresarial, selecione o dispositivo na coluna ID de dispositivo.

Para ver eventos de ameaças na empresa, siga essas etapas:

1. No painel esquerdo, clique em **Populações > Empresa**.
2. Clique na guia **Eventos de ameaça**.
3. Selecione o nível de gravidade desejado e o período de tempo para mostrar os eventos.

Para visualizar ameaças em um ponto de extremidade específico, siga estas etapas:

1. No painel esquerdo, clique em **Populações > Pontos de extremidade**.
2. Pesquise ou selecione um nome de host e depois clique na guia **Eventos de ameaça**.

Gerenciar uma ameaça

Você pode Colocar em quarentena, em Lista segura, Isentar e Exportar ameaças.

Execute as seguintes ações no nível do Enterprise:

- Exportar uma ameaça ou um script que tenha disparado um alerta
- Colocar uma ameaça em Quarentena
- Colocar uma ameaça na Lista segura
- Editar manualmente a Lista global

Para gerenciar uma ameaça identificada no nível do Enterprise:

1. No painel esquerdo, clique em **Populações > Empresa**.
2. Selecione a guia **Ameaças avançadas**.
3. Selecione Proteção.

Na tabela Controle de script, você pode exportar um script que aparece na tabela como uma possível ameaça.

Gerenciar ameaças empresariais avançadas

A guia Proteção oferece informações sobre arquivos e scripts potencialmente perigosos.

Tabela Ameaças

Na tabela Ameaças, você pode Exportar uma ameaça, colocá-la em Quarentena ou colocá-la em uma Lista segura. Você pode também adicionar manualmente uma ameaça à Lista de quarentena global.

A tabela mostra uma lista de todos os eventos encontrados na organização. Um evento pode também ser uma ameaça, mas não necessariamente.

Para visualizar informações adicionais sobre uma ameaça específica, clique no link do nome da ameaça para ver os detalhes em uma nova página ou clique em qualquer lugar da linha da ameaça para ver os detalhes na parte inferior da página.

Para ver informações adicionais sobre a ameaça na tabela, clique na seta suspensa sobre o cabeçalho de uma coluna para selecionar e adicionar colunas. As colunas exibem metadados sobre o arquivo, como Classificações, Pontuação da Cylance (nível

de confiança), Condenação pelo setor de AV (links para VirusTotal.com para comparação com outros fornecedores), a Data em que foi primeiramente encontrado, SHA256, MD5, Informações do arquivo (autor, descrição, versão) e Detalhes da assinatura.

Comandos

- **Exportar** - Exporte os dados de ameaças para um arquivo CSV. Selecione as linhas que deseja exportar e depois clique em **Exportar**.
- **Quarentena global** - Adicione um arquivo à lista de quarentena global. A ameaça é colocada permanentemente em quarentena em todos os dispositivos.
- **Seguro** - Adicione um arquivo à lista segura. O arquivo é tratado permanentemente como seguro em todos os dispositivos.

  NOTA: Ocasionalmente, um arquivo "seguro" pode ser relatado como inseguro (isso pode ocorrer se as características do arquivo se parecerem muito com aquelas de arquivos maliciosos). Ignorar ou listar o arquivo como seguro pode ser útil nesses casos.

- **Editar lista global** - Adicione ou remova arquivos da lista de quarentena global.
- **Isentar** - Adicione um arquivo à lista de isenções em um computador. É permitido executar este arquivo no computador.

Gerenciar ameaças avançadas do endpoint

Para gerenciar uma ameaça identificada em um computador específico:

1. No painel esquerdo, clique em **Populações > Empresa**.
2. Selecione a guia **Ameaças avançadas**.
3. Selecione Agentes.
4. Selecione um determinado nome de agente e escolha o comando adequado: **Exportar**, **Colocar em quarentena** ou **Isentar** uma ameaça.

5

Modo desconectado

O modo Desconectado permite que um Dell Server gerencie os pontos de extremidade do Advanced Threat Prevention sem conexão do cliente com a Internet ou com a rede externa. O modo Desconectado também permite que o Dell Server gerencie clientes sem conexão com a Internet ou um serviço provisionado e hospedado do Advanced Threat Prevention. No modo Desconectado, o Dell Server captura todos os eventos e dados de ameaça.

Para determinar se um Dell Server está funcionando no modo Desconectado, clique no ícone de engrenagem no canto superior direito do Remote Management Console e selecione Sobre. A tela Sobre indica que um Dell Server está no modo Desconectado abaixo da versão do Dell Server.

O modo Desconectado é diferente de uma instalação padrão conectada do Dell Server, conforme descrito a seguir.

Ativação do cliente

Um token de instalação é gerado quando o administrador faz upload de uma licença do Advanced Threat Prevention, o que permite que o cliente do Advanced Threat Prevention seja ativado.

Management Console

Os seguintes itens **não estão disponíveis** no Management Console quando o Dell Server está sendo executado no modo Desconectado:

- As seguintes áreas são específicas ao Advanced Threat Prevention: Ameaças avançadas por prioridade, Eventos (ameaças avançadas) por classificação, As dez principais ameaças avançadas e Eventos do Advanced Threat Prevention.
- Guia **Empresa > Ameças avançadas**, que fornece uma exibição dinâmica de informações de eventos detalhadas de toda a empresa, incluindo uma lista dos dispositivos nos quais os eventos ocorreram e quaisquer ações tomadas sobre esses dispositivos para tais eventos.
- (Painel de navegação esquerdo) Gerenciamento de serviços, que permite a ativação do serviço Advanced Threat Prevention e a inscrição para notificações do produto.

O seguinte item **está disponível** para o Management Console para oferecer suporte ao modo Desconectado:

- Guia **Enterprise > Advanced Threat Events**, que lista informações sobre eventos de toda a empresa com base nas informações disponíveis no Dell Server, mesmo quando estiver sendo executado no modo Desconectado.

Funcionalidade

As seguintes funcionalidades não estão disponíveis no Management Console quando o Dell Server está sendo executado no modo Desconectado:

- Upgrade, atualização e migração do Security Management Server
- Atualização automática do Security Management Server Virtual - a atualização deve ser realizada manualmente
- Atualização de perfil na nuvem
- Atualização automática do Advanced Threat Prevention
- Faça upload de arquivos executáveis inseguros ou anormais para análise do Advanced Threat Prevention
- Upload do arquivo e do arquivo de log do Advanced Threat Prevention

A seguinte funcionalidade é diferente:

- O Dell Server envia a Lista segura global, a Lista de quarentena e a Lista segura para os agentes.
- A Lista segura global é importada para o Dell Server por meio da política de Permissão global.
- A Lista de quarentena é importada para o Dell Server por meio da política de Lista de quarentena.
- A Lista segura é importada para o Dell Server por meio da política de Lista segura.

Essas políticas estão disponíveis somente no modo Desconectado. Para obter mais informações sobre essas políticas, consulte o *AdminHelp*, disponível no Remote Management Console.

Para obter mais informações sobre o modo Desconectado, consulte "Modo Desconectado" no *AdminHelp*, disponível no Management Console.

Identificar e gerenciar ameaças no modo Desconectado

Para gerenciar ameaças no modo Desconectado, você precisa primeiro configurar as seguintes políticas do Advanced Threat Prevention, conforme aplicável à sua organização:

- Permitir global
- Lista de quarentena
- Lista segura

Essas políticas serão enviadas para o cliente do Advanced Threat Prevention apenas se o Dell Server detectar um token de instalação do modo Desconectado, que recebe o prefixo "DELLAG".

Consulte o *AdminHelp* para ver exemplos dessas políticas.

Para visualizar os arquivos que o Advanced Threat Prevention identifica como possíveis ameaças, navegue até a guia **Enterprise > Eventos de ameaças avançadas**. Essa guia contém uma lista de informações de eventos para toda a empresa e toda ação tomada, como, por exemplo, Bloqueado ou Terminado.

6

Troubleshooting

Recuperar o Advanced Threat Prevention

Recuperar serviço

Você precisará de seu certificado salvo em backup para recuperar o serviço Advanced Threat Prevention.

1. No painel esquerdo do Management Console, clique em **Gerenciamento > Gerenciamento de serviços.**
2. Clique em **Recuperar o serviço Advanced Threat Prevention**.
3. Siga a recuperação de serviço orientada e faça upload do certificado do Advanced Threat Prevention quando solicitado.

Encontrar o código do produto com o Windows PowerShell

- Você pode identificar facilmente o código do produto, se ele mudar no futuro, usando este método.

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

  O resultado será o caminho inteiro e o nome do arquivo .msi (o nome hexadecimal do arquivo convertido).

Advanced Threat Prevention

- Para fazer com que o plugin do Advanced Threat Prevention monitore mudanças no valor de LogVerbosity em HKLM\SOFTWARE\Dell\Dell Data Protection e para atualizar o nível de log do cliente de maneira correspondente, configure o valor a seguir.

  [HKLM\SOFTWARE\Dell\Dell Data Protection]

  "LogVerbosity"=DWORD:<see below>

  Dump: 0

  Fatal: 1

  Error 3

  Warning 5

  Info 10

  Verbose 12

  Trace 14

  Debug 15

  O valor do registro é verificado quando o serviço Advanced Threat Prevention é iniciado ou sempre que o valor muda. Se o valor do registro não existir, não haverá mudança no nível de log.

  Use essa configuração de registro apenas para teste/depuração, pois ela controla o detalhamento do log para outros componentes, incluindo Encryption e o Encryption Management Agent.

- O Modo de compatibilidade permite a execução de aplicativos no computador cliente mesmo com as políticas Proteção de memória e Controle de scripts ativadas. A ativação do modo de compatibilidade precisa adicionar um valor de registro no computador cliente.

  Para ativar o modo de compatibilidade, execute este procedimento:

1. No Management Console, desative a política *Proteção de memória ativada*. Se a política *Script Control* estiver ativada, desative-a.
2. Adicione o valor do registro CompatibilityMode.
   a. Usando o Editor do Registro no computador cliente, vá para `HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`.
   b. Clique com o botão direito em **Desktop**, clique em **Permissões**, assuma a propriedade e conceda a você mesmo Controle total.
   c. Clique com o botão direito em **Desktop**, selecione **Novo Valor binário**.
   d. Para o nome, digite `CompatibilityMode`.
   e. Abra a configuração do registro e altere o valor para `01`.
   f. Clique em **OK** e feche o Editor do Registro.

   Para adicionar o valor do registro com um comando, você pode usar uma das seguintes opções de linha de comando no computador cliente:

   - (Para um computador) Psexec:

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

   - (Para múltiplos computadores) Invoke-Command cmdlet:

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

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

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

3. No Management Console, ative novamente a política *Proteção de memória ativada*. Se a política *Script Control* estava ativada anteriormente, ative-a novamente.