Dell Endpoint Security Suite Enterprise

Advanced Threat Prevention Quick Start Guide v3.9

January 2024
Rev. A01

DELL Technologies

Notas, avisos e advertências

NOTA: Uma NOTA fornece informações importantes para ajudar a utilizar melhor o produto.

AVISO: Um AVISO indica possíveis danos no hardware ou uma perda de dados e explica como pode evitar esse problema.

ADVERTÊNCIA: Uma ADVERTÊNCIA indica possíveis danos no equipamento, lesões corporais ou morte.

© 2012-2024 Dell Inc. All rights reserved. Registered trademarks and trademarks used in the Dell Encryption and Endpoint Security Suite Enterprise suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Cylance®, CylancePROTECT, and the Cylance logo are registered trademarks of Cylance, Inc. in the U.S. and other countries. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen tec® and Eikon® are registered trademarks of Authen tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Windows Vista®, Windows 10®, Active Directory®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. Dropbox ℠ is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, App Store℠, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle®, and iPod nano®, Macintosh®, and Safari® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc. Bing® is a registered trademark of Microsoft Inc. Ask® is a registered trademark of IAC Publishing, LLC. Other names may be trademarks of their respective owners.

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.

Contacte o Dell ProSupport for Software

Contacte o número 877-459-7304, extensão 4310039 para obter suporte telefónico permanente (24 x 7) para o seu produto Dell.

Adicionalmente, o suporte online para os produtos Dell encontra-se disponível em dell.com/support. O suporte online inclui controladores, manuais, conselhos técnicos, perguntas frequentes e problemas emergentes.

Ajude-nos a garantir que o direcionamos rapidamente para o especialista técnico mais indicado para si tendo a Etiqueta de serviço ou o Código de serviço expresso disponível quando nos contactar.

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

2

Introdução

Este capítulo descreve os passos recomendados para começar a administrar o Advanced Threat Prevention.

Os passos recomendados para começar a administrar o Advanced Threat Prevention incluem as seguintes fases:

- Configurar um inquilino para o Advanced Threat Prevention
  - Necessário para implementar o Advanced Threat Prevention
  - As licenças do Advanced Threat Prevention devem estar presentes no Dell Server
- Configurar a atualização automática do Advanced Threat Prevention Agent
  - Inscrição nas atualizações automáticas do Advanced Threat Prevention (opcional)
  - As atualizações são mensais
- Atribuir ou modificar papéis de administrador
  - Aprovisionar ou recuperar o serviço Advanced Threat Prevention
  - Fazer cópias de segurança e transferir certificados do Advanced Threat Prevention existentes
  - Ver, modificar e consolidar políticas
- Configurar notificações
  - Definir notificações de e-mail e painel para alertas do Advanced Threat Prevention (opcional)
  - Personalizar notificações com base nas suas necessidades empresariais

Configurar um inquilino

Deve ser aprovisionado um inquilino no Dell Server antes da ativação da aplicação de políticas do Advanced Threat Prevention.

Pré-requisitos

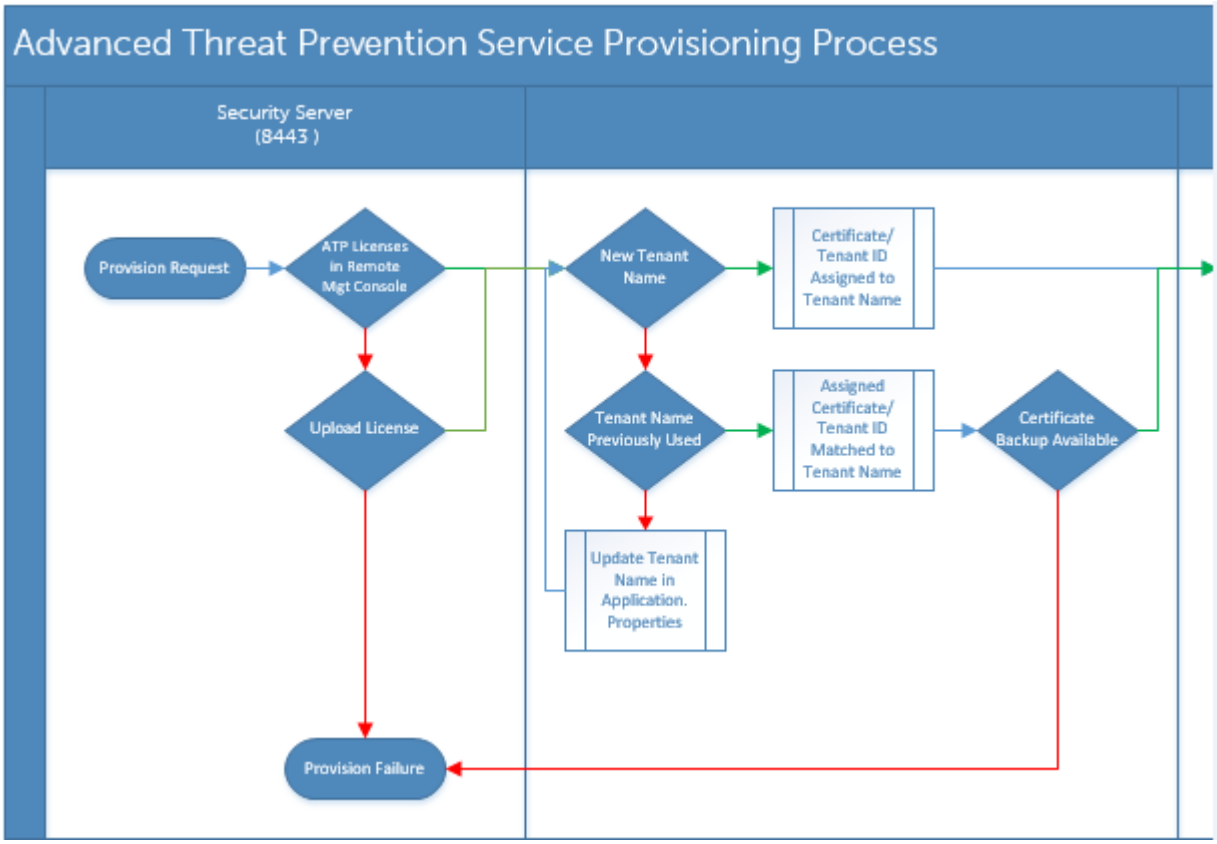
- Tem de ser efetuado por um administrador com função de administrador de sistema.
- Deve ter ligação à Internet para configuração no Dell Server.
- Tem de ter ligação à Internet no cliente para visualizar a integração do serviço online do Advanced Threat Prevention na Management Console.
- A configuração tem como base um token que é gerado a partir de um certificado durante a configuração.
- As licenças do Advanced Threat Prevention devem estar presentes no Dell Server.

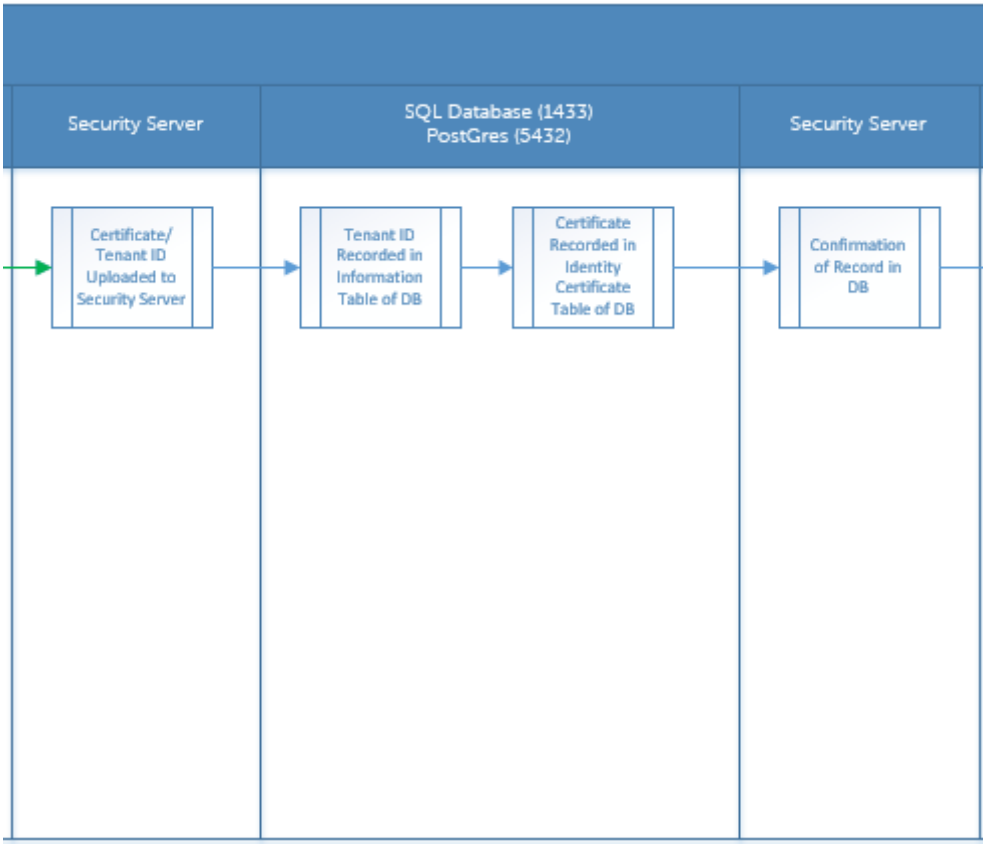
Configurar um inquilino

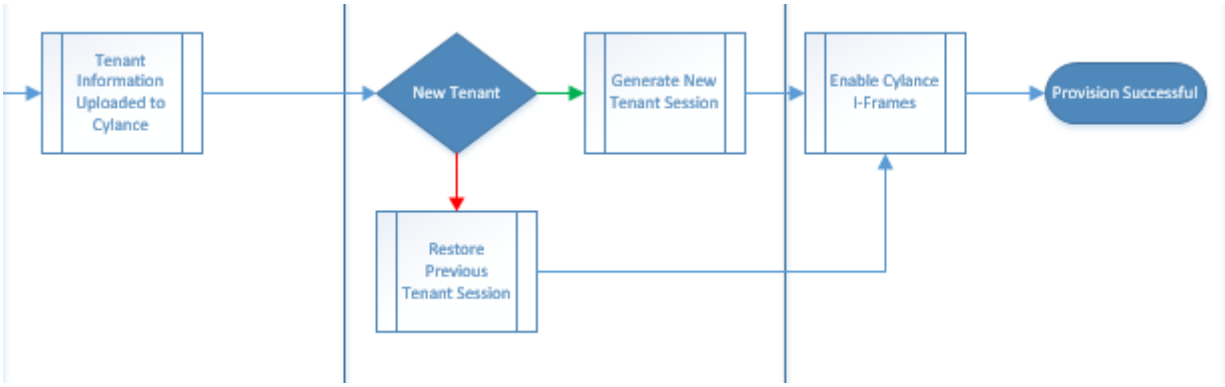
1. Como administrador Dell, inicie sessão na Management Console.
2. No painel esquerdo da Management Console, clique em **Gestão > Gestão de serviços**.
3. Clique em **Configurar serviço Advanced Threat Protection**. Se ocorrer qualquer falha neste momento, importe as suas licenças Advanced Threat Prevention.
4. A configuração com assistente é iniciada imediatamente após as licenças serem importadas. Clique em **Seguinte** para começar.
5. Leia e aceite o EULA e clique em **Seguinte**.
6. Disponibilize credenciais de identificação no Dell Server para configuração do Inquilino. Clique em **Seguinte**. *A configuração de um Inquilino existente da marca Cylance não é suportada.*
7. Transfira o Certificado. Este é necessário para recuperação em caso de desastres no Dell Server. Não é efetuada uma cópia de segurança deste Certificado. Efetue uma cópia de segurança do Certificado numa localização segura num computador diferente. Selecione a caixa de verificação para confirmar que efetuou uma cópia de segurança do Certificado e clique em **Seguinte**.
8. A configuração está concluída. Clique em **OK**.

Aprovisionamento e comunicação do agente

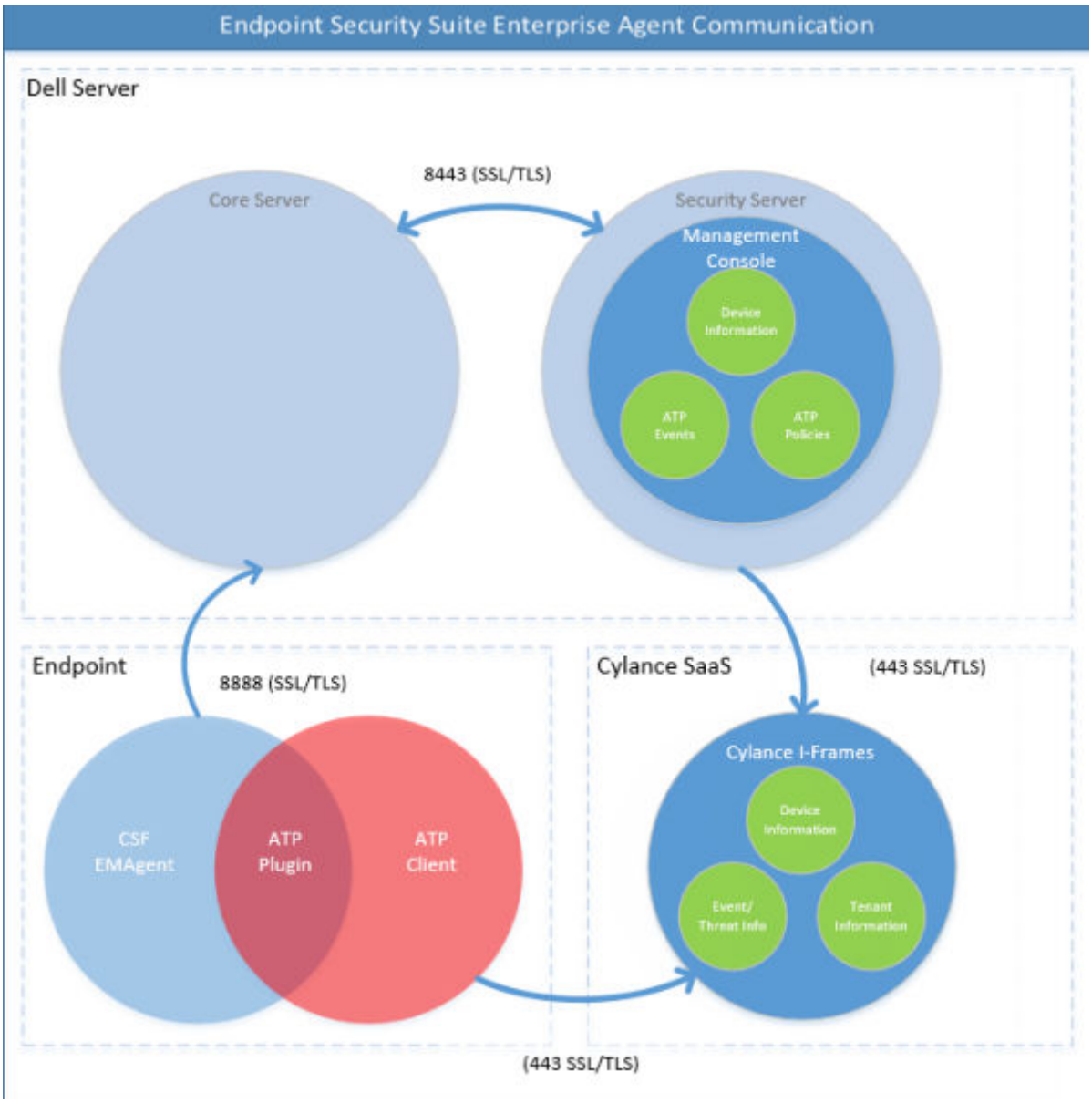
Os seguintes diagramas ilustram o processo de aprovisionamento do serviço do Advanced Threat Prevention.



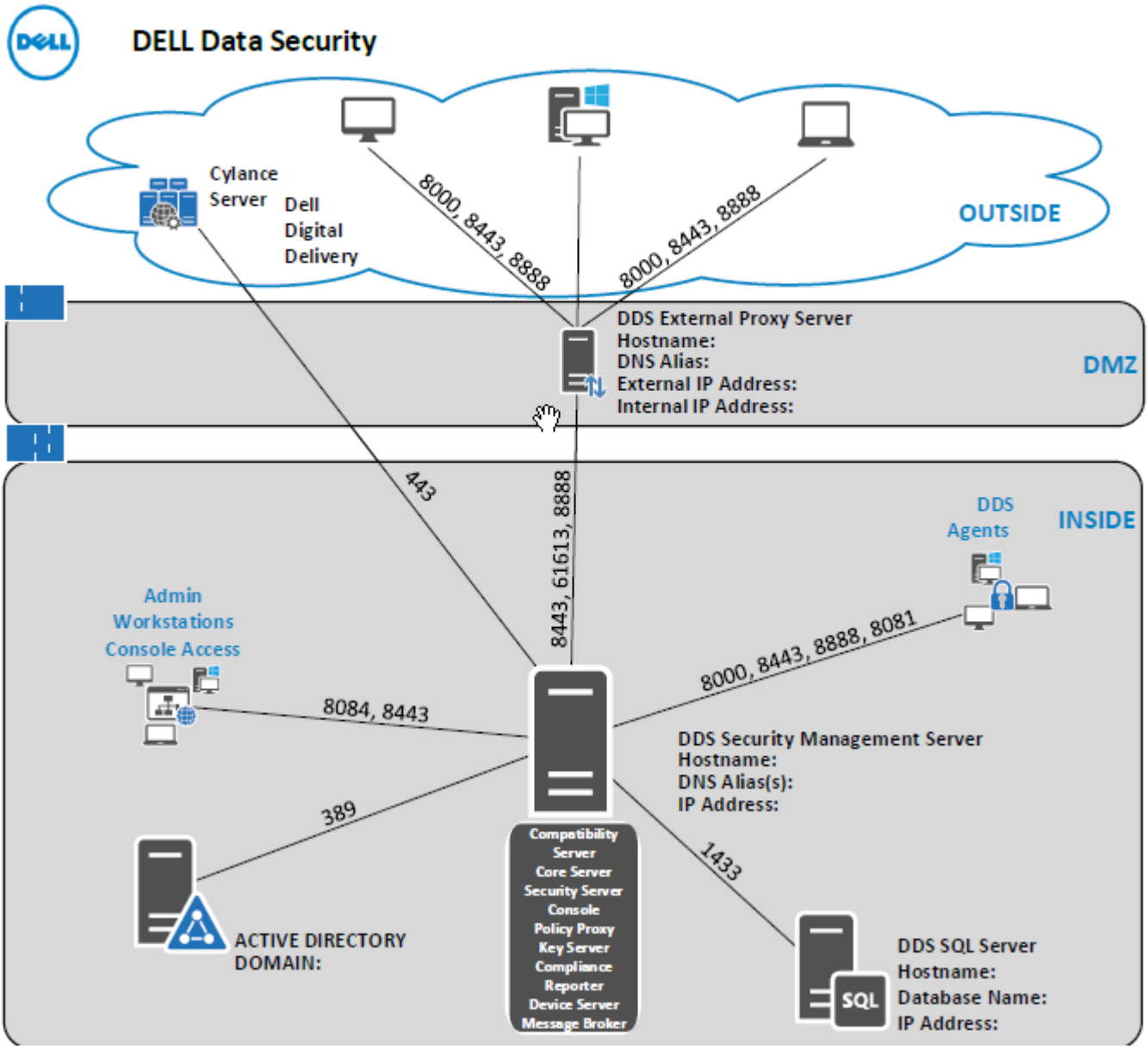




O diagrama seguinte ilustra o processo de comunicação do agente do Advanced Threat Prevention.



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



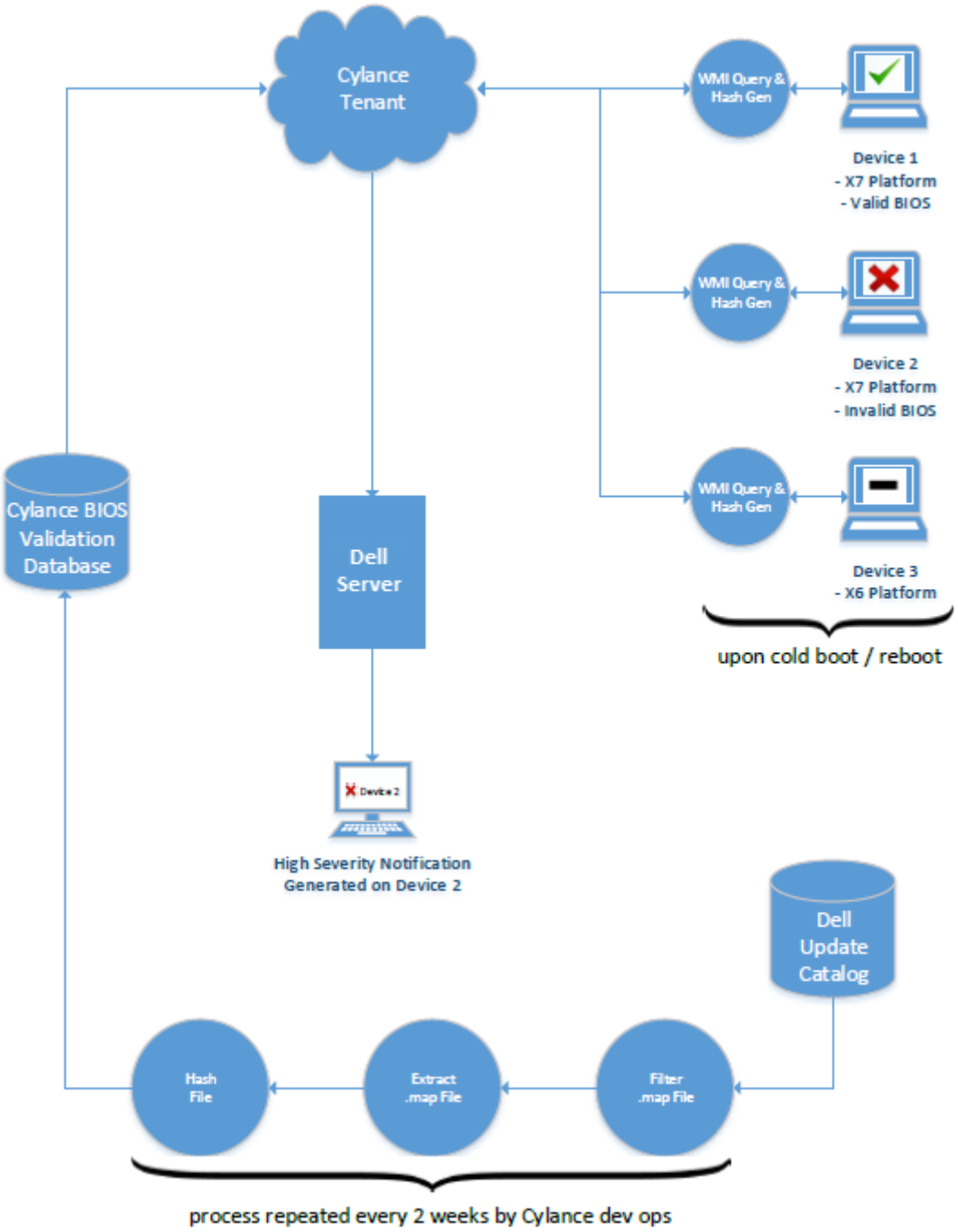
Ativar a verificação da integridade de imagem do BIOS

A política de verificação da integridade de imagem do BIOS está ativada por predefinição quando a opção principal do Advanced Threat Prevention está ativada.

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

Processo de verificação

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



Se a política *Ativar a garantia do BIOS* for selecionada na Management Console, o inquilino Cylance valida o hash do BIOS nos computadores de endpoint para assegurar que o BIOS não foi modificado face à versão de fábrica da Dell, o qual é um possível vetor de ataques. Se for detetada uma ameaça, é transmitida uma notificação para o Dell Server e o administrador de TI é alertado na Remote Management Console. Para uma descrição geral do processo, consulte Processo de verificação da integridade de imagem do BIOS.

NOTA: Não é possível utilizar uma imagem de fábrica personalizada com esta funcionalidade, uma vez que o BIOS foi modificado.

Modelos de computador Dell suportados pela Verificação da integridade de imagem do BIOS	
• Latitude 3470 • Latitude 3570 • Latitude 7275	• OptiPlex 5040 • OptiPlex 7040 • OptiPlex 7440

Modelos de computador Dell suportados pela Verificação da integridade de imagem do BIOS		
• Latitude 7370 • Latitude E5270 • Latitude E5470 • Latitude E5570 • Latitude E7270 • Latitude E7470 • Latitude Rugged 5414 • Latitude Rugged 7214 Extreme • Latitude Rugged 7414 • OptiPlex 3040 • OptiPlex 3240	• Estação de trabalho móvel Precision 3510 • Estação de trabalho móvel Precision 5510 • Estação de trabalho Precision 3620 • Estação de trabalho Precision 7510 • Estação de trabalho Precision 7710 • Estação de trabalho Precision T3420 • Venue 10 Pro 5056 • Venue Pro 5855 • XPS 12 9250 • XPS 13 9350 • XPS 9550	

Configurar a atualização automática do Advanced Threat Prevention

Na Management Console, pode inscrever-se para receber atualizações automáticas do agente Advanced Threat Prevention. A subscrição da receção de atualizações automáticas do agente permite aos clientes transferir e aplicar autoatualizações a partir do serviço de Advanced Threat Prevention. As atualizações são mensais.

NOTA:

As autoatualizações do agente são suportadas com o Dell Server v9.4.1 ou posterior.

Receber autoatualizações do agente

Para se inscrever e receber autoatualizações do agente:

1. No painel esquerdo da Management Console, clique em **Gestão** > **Gestão de Serviços**.
2. No separador *Advanced Threats*, sob *Atualização automática do agente*, clique em **Ligar** e, em seguida, clique em **Guardar preferências**.

   Poderá demorar alguns momentos até as informações serem propagadas e as autoatualizações serem apresentadas.

Deixar de receber autoatualizações do agente

Para deixar de receber autoatualizações do agente:

1. No painel esquerdo da Management Console, clique em **Gestão** > **Gestão de Serviços**.
2. No separador *Advanced Threats*, sob *Atualização automática do agente*, clique em **Desligar** e, em seguida, clique em **Guardar preferências**.

Atribuir ou modificar papéis de administrador

Ver ou modificar privilégios de Administrador existentes na página Administradores da Management Console.

Funções de administração

O início de sessão do administrador é integrado com o Active Directory para simplificar o processo de gestão de administradores e para lhe permitir aproveitar a infraestrutura existente de autenticação do utilizador. São atribuídos funções aos administradores que definem o nível de acesso autorizado para cada administrador. Por exemplo, é possível que alguns administradores só sejam autorizados a implementar a recuperação assistida pelo apoio técnico, ao passo que outros têm acesso total para editar as políticas de segurança. Pode atribuir funções de administrador a grupos do Active Directory, para que possa mudar facilmente o nível dos utilizadores com acesso de administrador com uma simples alteração para membro do grupo do AD. Os utilizadores sem domínio podem ter acesso apenas a relatórios através do Compliance Reporter.

A função de administrador de sistema é necessária para efetuar as seguintes tarefas:

- Aprovisionar ou recuperar o serviço Advanced Threat Prevention
- Inscrição nas atualizações automáticas do Advanced Threat Prevention
- Definir notificações de e-mail ou painel para alertas do Advanced Threat Prevention

- Fazer cópias de segurança e transferir certificados do Advanced Threat Prevention existentes

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

Para visualizar ou modificar os privilégios de administrador existentes, siga os passos abaixo:
1. No painel esquerdo, clique em **Populações > Administradores**.
2. Procure ou selecione a linha que apresenta o nome de utilizador do administrador adequado para apresentar os Detalhes do utilizador.
3. Visualize ou modifique os papéis de administrador no painel à direita.
4. Clique em **Guardar**.

NOTA: A Dell recomenda atribuir funções de administrador ao nível de grupo em vez de ao nível do utilizador.

Para visualizar, atribuir ou modificar funções de administrador ao nível do grupo, siga os seguintes passos:
1. No painel esquerdo, clique em **Populações > Grupos de utilizadores**.
2. Procure ou selecione um Nome de grupo e, em seguida, selecione o separador **Admin**. É apresentada a página de detalhes do grupo de utilizadores.
3. Selecione ou desmarque as seguintes funções de administrador atribuídos ao grupo.
4. Clique em **Guardar**.

Se remover um grupo que possua privilégios administrativos e, mais tarde, voltar a adicionar o grupo, este permanece um Grupo de administradores.

Para visualizar, atribuir ou modificar Papéis de administrador ao nível do Utilizador, siga estes passos:
1. No painel esquerdo, clique em **Populações > Utilizadores**.
2. Procure ou selecione um nome de utilizador e, em seguida, selecione o separador Admin.
3. Selecione ou desmarque as funções de administrador atribuídos ao utilizador.
4. Clique em **Guardar**.

Papéis de administrador - atribua ou modifique papéis para o utilizador e clique em **Guardar**.

Funções de grupo herdadas - uma lista apenas de leitura de funções que o utilizador herdou de um grupo. Para modificar as funções, clique no separador **Grupos de utilizadores** para esse utilizador e selecione o nome do grupo.

Funções designadas - Delegue direitos de administrador a um utilizador.

Configurar notificações

Na Remote Management Console, poderá inscrever-se para receber notificações. A lista de notificações fornece um resumo configurável de notícias, alertas e eventos para apresentar no Painel ou para enviar como notificações de e-mail.

Tipos de notificação:

Pode selecionar os tipos de notificação a incluir na lista. As notificações dos restantes tipos são ocultadas. As notificações de **Eventos do Advanced Threat** e **Threat Protection** dizem respeito ao Advanced Threat Prevention.

Os tipos incluem:
- **Atualizar** - Notícias de futuras atualizações de produtos. Para visualizar e receber atualizações de produtos, deve inscrever-se para as receber. Selecione **Gestão de serviços > Notificações de produto**, clique em **Ativar** e, em seguida, clique em **Guardar preferências**.
- **Config** - Notícias sobre alterações de configuração.
- **Base de dados de conhecimento** - Resumos e ligações para artigos da base de dados de conhecimento com informações técnicas aprofundadas, como por exemplo prazos e métodos de configuração.
- **Anúncio** - Notícias dos próximos lançamentos e novos produtos.
- **Licença** - Alerta-o quando a disponibilidade do seu licenciamento em volume é baixa ou quando o seu número de licenças de acesso de cliente foi ultrapassado.
- **Proteção contra ameaças** - Um alerta contra ameaças do Advanced Threat Prevention.
- **Evento Advanced Threat** - Um evento detetado pelo Advanced Threat Prevention. O resumo contém uma lista de eventos críticos, principais, secundários, avisos e de informações, com ligações para informações mais detalhadas.
- **Evento de ameaça** - Um evento detetado pelo Threat Protection.
- **Certificado** - Notificação de expiração de certificado.
- **Exceções do Dell Server** - Um problema de comunicação do Dell Server está a afetar as entregas das seguintes notificações: Proteção contra ameaças, Atualização, Configuração, Base de dados 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 reiniciar as seleções nesta lista.

Níveis de Prioridade:

NOTA: Os níveis de prioridade de notificação não estão relacionados com os níveis de prioridade apresentados no painel, a não ser na área de notificações.

As prioridades são Crítica, Alta, Média e Baixa. Estes níveis de prioridade estão apenas ligados entre si dentro de um tipo de notificação.

Pode selecionar os níveis de prioridade das notificações para incluir na área de notificações do painel ou listas de notificações de e-mail. As notificações dos níveis de prioridade restantes não estão incluídas nas listas de notificações de e-mail ou painel.

Selecione **Limpar itens selecionados** para reiniciar as seleções nesta lista. Serão apresentadas todas as notificações (exceto se filtradas noutro local).

3

Políticas

Este capítulo apresenta detalhes sobre a gestão de políticas do Advanced Threat Prevention.

- Ativar o Advanced Threat Prevention
- Definições de políticas recomendadas
- Consolidar modificações de políticas

Para obter a lista completa de políticas do Advanced Threat Prevention e as respetivas descrições, consulte *AdminHelp*, disponível na Management Console.

Ativar o Advanced Threat Prevention

A política do Advanced Threat Prevention está **Desligada** por predefinição e tem de ser **Ligada** para ativar as políticas do Advanced Threat Prevention. As políticas do Advanced Threat Prevention são aplicáveis nos níveis de Empresa, Grupo de endpoints e Endpoints.

Para ativar a política do Advanced Threat Prevention no nível de Empresa, siga estes passos:

1. No painel esquerdo, clique em **Populações > Empresa**.
2. Clique em **Threat Prevention**.
3. Mude o interruptor principal do Advanced Threat Prevention de **Desligado** para **Ligado**.

Para ativar a política do Advanced Threat Prevention no nível de Grupo de endpoints, siga estes passos:

1. No painel esquerdo, clique em **Populações > Grupo de endpoints**.
2. Clique em **Threat Prevention**.
3. Mude o interruptor principal do Advanced Threat Prevention de **Desligado** para **Ligado**.

Para ativar a política do Advanced Threat Prevention no nível de Endpoints, siga estes passos:

1. No painel esquerdo, clique em **Populações > Endpoints**.
2. Clique em **Threat Prevention**.
3. Mude o interruptor principal do Advanced Threat Prevention de **Desligado** para **Ligado**.

Definições de políticas recomendadas

- Para obter a lista mais atualizada de definições de políticas recomendadas, consulte o artigo BDC SLN301562.

Consolidar modificações de políticas

Para consolidar políticas que tenham sido modificadas e guardadas:

1. No painel esquerdo da Management Console, clique em **Gestão > Consolidar**.
2. Em Comentário, introduza uma descrição da alteração.
3. Clique em **Consolidar políticas**.

Uma publicação/consolidação de política ocorre quando um administrador clique em **Consolidar políticas**. São apresentadas as seguintes informações:

- Alterações de políticas pendentes - O número de alterações de políticas prontas a consolidar.
- Data de consolidação - Data e hora em que as políticas foram consolidadas.
- Alterado por - Nome de utilizador do administrador que efetuou a consolidação da política.
- Comentários - Quaisquer comentários que foram adicionados quando as políticas foram consolidadas.
- Versão - O número de gravações de políticas desde a última consolidação de política mais a versão anterior.

4

Ameaças colocadas

Este capítulo apresenta detalhes sobre como identificar e gerir ameaças encontradas num ambiente empresarial após a instalação do Advanced Threat Prevention.

Identificar uma ameaça

Notificações de e-mail e dashboard

Se configurou as notificações de e-mail para Eventos do Advanced Threat e Threat Protection, um administrador é notificado por e-mail relativamente a ameaças e eventos do Advanced Threat Prevention.

O Resumo de notificações do painel na Management Console apresenta ameaças e eventos do Advanced Threat Prevention como tipos de notificação de Eventos do Advanced Threat e Threat Protection.

- Tipo de Threat Protection - Um alerta de ameaça do Advanced Threat Prevention.
- Tipo de Evento do Advanced Threat - Um evento detetado pelo Advanced Threat Prevention. Um evento não é necessariamente uma ameaça.

Os detalhes da seguinte tabela apresentam a etiqueta, a gravidade e a informação sobre a ameaça.

Etiqueta	Gravidade	Detalhes
ThreatFound	Crítico	Indica que um Executável Portátil (PE) foi identificado num dispositivo, mas não foi bloqueado ou colocado em quarentena no ponto terminal, indicando que existe uma ameaça ativa no sistema.
ThreatBlocked	Aviso	Indica que um Executável Portátil foi identificado no dispositivo, embora a sua execução tenha sido bloqueada. Esta ameaça não foi colocada em quarentena especificamente, o que provavelmente se deve à política de Quarentena Automática não ter sido ativada, ou ao ficheiro estar num local no qual não é possível gravar com a conta do SISTEMA local (uma partilha de rede, um dispositivo USB que foi removido, etc.).
ThreatTerminated	Aviso	Indica que um Executável Portátil (PE) foi identificado no dispositivo e o seu processo foi terminado, pois estava a ser executado de forma ativa. Isto não indica que o ficheiro também foi colocado em quarentena, pois o PE poderia ter sido executado a partir de outro local. Recomenda-se que procure outro evento correlacionado com este ponto terminal e com o executável para confirmar que a ameaça foi contida corretamente.
MemoryViolationBlocked	Aviso	Indica que houve uma tentativa de execução de um executável ou script, mas estava em violação da política de Proteção de Memória ou de Controlo de Script. A execução do executável ou script foi subsequentemente bloqueada. Normalmente, é indicativo de que a política de Proteção de Memória ou de Controlo de Script correlacionada descrita foi definida para Bloquear.

Etiqueta	Gravidade	Detalhes
MemoryViolationTerminated	Aviso	Indica que houve uma tentativa de execução de um executável ou script, que estava a ser executado de forma ativa e em violação da política de Proteção de Memória ou de Controlo de Script. O executável ou script foi subsequentemente terminado. Normalmente, é indicativo de que a política de Proteção de Memória ou de Controlo de Script correlacionada descrita foi definida para Terminar.
MemoryViolation	Aviso	Indica que um executável ou script estava em violação da política de Proteção de Memória ou de Controlo de Script. O executável ou script não tinha nenhuma ação impeditiva, provavelmente por a política estar definida para Permitir.
ThreatRemoved	Informação	Indica que um Executável Portátil (PE) sinalizado anteriormente, que foi considerado uma ameaça, foi removido do ponto terminal. Isto pode indicar que o PE foi removido da quarentena ou removido da localização inicial. É comum acontecer com PEs que foram inicialmente detetados em suportes de dados amovíveis (USB, CD-ROM, etc.)
ThreatQuarantined	Informação	Indica que um Executável Portátil (PE) foi determinado como uma ameaça potencial e, subsequentemente, foi colocado em quarentena com êxito. Isto indica que a política de Quarentena Automática com base na classificação de ameaça Anormal (Pontuação Cyclance de 0 – 60) ou Não Seguro (Pontuação Cyclance de 60 – 100) está ativada.
ThreatWaived	Informação	Indica que um Executável Portátil (PE) que foi determinado como sendo uma potencial ameaça, foi Dispensado com base na Lista Global de Ficheiros Seguros ou por um Dispensar local. Isto também pode indicar que o hash SHA256 foi adicionado às políticas "Dispensar" ou "Lista Global de Ficheiros Seguros" no contidas no Dell Security Management Server.
ThreatChanged	Informação	Indica quando a pontuação Cylance de um Executável Portátil (PE) foi alterada. Normalmente, isto acontece devido à pontuação de dois passos que é realizada pela Cylance. A análise da ameaça por parte do mecanismo de pontuação local pode não ter correspondido à análise do mecanismo da nuvem da Cylance. Nestas instâncias, devido aos dados adicionais que o mecanismo da nuvem da Cylance possui, a pontuação derivada do mecanismo da nuvem da Cylance é usada. Isto também pode indicar que uma atualização da Cylance iniciou uma reanálise de ficheiros que foram considerados ameaças anteriormente, e uma nova pontuação foi calculada que decidiu que este PE já não era considerado uma ameaça.
ProtectionStatusChanged	Informação	Indica quando um ponto terminal sofreu uma alteração no estado de proteção. Isto é acionado quando o Dell Encryption Management Agent volta a estabelecer ligação aos serviços da Cylance por meio dos Plugins da Cylance. Habitualmente, isto é acionado quando um ponto terminal é reiniciado, visto que existe um pequeno período em que o CSF pode não ter estabelecido ligação aos Plugins da Cylance durante o arranque.

Clique numa notificação para obter mais detalhes. O resumo inclui ligações para detalhes adicionais do evento ou ameaça.

Separador Ameaças avançadas

O separador Ameaças avançadas apresenta informações detalhadas dos eventos para toda a empresa, incluindo uma lista dos dispositivos nos quais ocorreram eventos e quaisquer ações adotadas nesses mesmos dispositivos para os referidos eventos.

Para aceder ao separador Ameaças avançadas na empresa, siga estes passos:

1. No painel esquerdo, clique em **Populações > Empresa**.

2. Selecione o separador **Ameaças avançadas**.

As informações sobre eventos, dispositivos e ações estão organizadas nos seguintes separadores:

- **Proteção** - Indica os ficheiros e scripts potencialmente prejudiciais e os respetivos detalhes, incluindo os dispositivos nos quais se encontram os ficheiros e scripts.
- **Agentes** - Fornece informações sobre os dispositivos que executam o cliente Advanced Threat Prevention, bem como a opção de exportar as informações ou remover dispositivos da lista.
- **Lista global** - Indica os ficheiros em Quarentena global e na Lista segura e oferece a opção de mover os ficheiros para estas listas.
- **Opções** - Oferece uma forma de integrar com o software de Gestão de eventos de segurança de informação (SIEM).
- **Certificado** - Permite o carregamento do certificado. Após o carregamento, o certificado é apresentado no separador de Lista Global e pode ser listado como Seguro.

As tabelas existentes nos separadores podem ser organizadas da seguinte forma:

- Adicionar ou remover colunas da tabela - Clique na seta ao lado do cabeçalho de qualquer coluna, selecione **Colunas** e, em seguida, selecione as colunas a apresentar. Limpe a caixa de verificação das colunas a ocultar.
- Ordenar os dados - Clique num cabeçalho da coluna.
- Agrupar por coluna - Arraste o cabeçalho da coluna para cima até ficar verde.

Separador de Eventos do Advanced Threat

O separador de Eventos do Advanced Threat apresenta informações sobre eventos para toda a empresa com base nas informações disponíveis no Dell Server.

O separador indica se o serviço Advanced Threat Prevention é aprovisionado e se as licenças estão disponíveis.

Para exportar dados do separador de Eventos do Advanced Threat, clique em **Exportar** e selecione o formato de ficheiro, **Excel** ou **CSV**.

NOTA: Os ficheiros Excel estão limitados a 65 000 linhas. Os ficheiros CSV não têm limite de tamanho.

Atualizações da pontuação Cylance e do modelo de ameaça

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.

O modelo de ameaça preditiva utilizado para proteger os dispositivos recebe atualizações periódicas para melhorar as taxas de deteção.

Duas colunas na página Proteção na Management Console mostram como um novo modelo de ameaça afeta a sua organização. Apresente e compare as colunas Estado da produção e Novo estado para verificar quais são os ficheiros nos dispositivos que podem ser afetados pela alteração do modelo.

Para visualizar as colunas Estado da produção e Novo estado:

1. No painel esquerdo, clique em **Populações > Empresa**.
2. Selecione o separador **Ameaças avançadas**.
3. Clique no separador **Proteção**.
4. Clique na seta para baixo no cabeçalho de uma coluna na tabela.
5. Passe com o cursor do rato sobre **Colunas**.
6. Selecione as colunas **Estado da produção** e **Novo estado**.

Estado da produção - Estado atual do modelo (Seguro, Anormal ou Não seguro) do ficheiro.

Novo estado - Estado do modelo do ficheiro no novo modelo.

Por exemplo, um ficheiro considerado Seguro no modelo atual pode mudar para Não seguro no novo modelo. Se a sua organização necessitar desse ficheiro, pode adicioná-lo à lista segura. Um ficheiro que nunca tenha sido visto ou pontuado pelo modelo atual pode ser considerado Não seguro pelo novo modelo. Se a sua organização necessitar desse ficheiro, pode adicioná-lo à lista segura.

Apenas os ficheiros detetados no dispositivo da sua organização que têm uma alteração na sua Pontuação Cylance são apresentados. Alguns ficheiros podem ter uma alteração na Pontuação mas permanecem no seu estado atual. Por exemplo, se a Pontuação Cylance de um ficheiro passar de 10 para 20, o estado do ficheiro pode permanecer Anormal e o ficheiro surge na lista de modelos atualizada (se este ficheiro existir nos dispositivos da sua organização).

Comparar o modelo atual com o novo modelo

Agora é possível rever as diferenças entre o modelo atual e o novo modelo.

Os dois cenários que tem de ter em conta são:

Estado da produção = Seguro, Novo estado = Anormal ou Não seguro

- A sua organização considera o ficheiro Seguro
- A sua organização tem a opção Anormal e/ou Não seguro definida para Quarentena automática

Nos cenários indicados acima, recomenda-se que os ficheiros que pretende permitir na sua organização sejam colocados na Lista segura.

Identificar classificações

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

1. Aplique um filtro na coluna Novo estado para apresentar todos os ficheiros com o estado Não seguro, Anormal e Em quarentena.
2. Aplique um filtro na coluna Estado da produção para apresentar todos os ficheiros com o estado Seguro.
3. Aplique um filtro na coluna Classificação para apresentar apenas as ameaças com o estado Fidedigno - Local.

Fidedigno - Os ficheiros locais foram analisados pela Cylance e são considerados seguros. Coloque estes ficheiros na Lista segura após a revisão. Se tiver muitos ficheiros na lista filtrada, pode ter que priorizar mais atributos. Adicione por exemplo um filtro à coluna Detetado por para rever as ameaças detetadas pelo Controlo da execução. Estas foram avaliadas quando um utilizador tentou executar uma aplicação e necessitou de uma atenção mais urgente do que os ficheiros inativos avaliados pela Deteção de ameaças em segundo plano ou pelo Vigilante de ficheiros.

As informações para a comparação de modelos são fornecidas pela base de dados e não pelos seus dispositivos. Logo não é efetuada nenhuma reanálise para a comparação de modelos. Contudo, quando está disponível um novo modelo e o Agente adequado está instalado, é efetuada uma reanálise na sua organização e são aplicadas as alterações no modelo.

Consulte *AdminHelp* para obter mais informações.

Visualizar eventos de Web Protection e Firewall

As ameaças são categorizadas como software maligno/exploit, filtro de Web, firewall ou eventos não categorizados. A lista de eventos de ameaça pode ser ordenada por qualquer um dos cabeçalhos da coluna. Pode ver eventos de ameaça para toda a empresa ou para um endpoint específico. Para ver eventos de ameaça de um endpoint específico, no separador Eventos de ameaça da empresa, selecione o dispositivo na coluna ID do dispositivo.

Para visualizar eventos de ameaça na empresa, siga os seguintes passos:

1. No painel esquerdo, clique em **Populações > Empresa**.
2. Clique no separador **Eventos de ameaças**.
3. Selecione o nível de gravidade pretendido e o período de tempo referente aos eventos a exibir.

Para visualizar ameaças num endpoint específico, siga estes passos:

1. No painel esquerdo, clique em **Populações > Endpoints**.
2. Procure ou selecione um nome de anfitrião e, em seguida, selecione o separador **Eventos de ameaças**.

Gerir uma ameaça

Pode colocar as ameaças em Quarentena ou na Lista segura e Dispensar e Exportar as mesmas.

Execute as seguintes ações no nível de Empresa:

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

Para gerir uma ameaça identificada no nível de Empresa:

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

Na tabela de Controlo de script, pode Exportar um script apresentado na tabela como uma ameaça potencial.

Gerir ameaças avançadas na empresa

O separador Proteção disponibiliza informações sobre ficheiros e scripts potencialmente prejudiciais.

Tabela de ameaças

Na tabela de Ameaças, pode colocar uma ameaça em Quarentena ou na Lista segura e Exportar a mesma. Também pode adicionar manualmente uma ameaça à lista de Quarentena global.

A tabela enumera todos os eventos encontrados em toda a organização. Um evento também pode ser uma ameaça, mas isso nem sempre acontece.

Visualize as informações adicionais de uma ameaça específica clicando na ligação do nome da ameaça para visualizar os detalhes apresentados numa página nova, ou clicando em qualquer ponto da linha da ameaça para visualizar os detalhes na parte inferior da página.

Para visualizar as informações adicionais de uma ameaça na tabela, clique na seta para baixo no cabeçalho de uma coluna para selecionar e adicionar colunas. As colunas apresentam metadados sobre o ficheiro, como Classificações, Pontuação Cylance (nível de confiança), convicção da Indústria AV (ligações para VirusTotal.com para comparação com outros fornecedores), a data em que foi encontrado pela primeira vez, SHA256, MD5, informações do ficheiro (autor, descrição, versão) e detalhes da assinatura.

Comandos

- **Exportar** - Exporte os dados da ameaça para um ficheiro CSV. Selecione as linhas a exportar e, em seguida, clique em **Exportar**.
- **Quarentena global** - Adicione um ficheiro à lista de quarentena global. A ameaça é colocada em quarentena permanente em relação a todos os dispositivos.
- **Seguro** - Adicione um ficheiro à lista segura. O ficheiro é tratado permanentemente como seguro em todos os dispositivos.

  NOTA: Ocasionalmente, um ficheiro "bom" pode ser comunicado como não seguro (isto pode acontecer se as funcionalidades do ficheiro se assemelharem às dos ficheiros maliciosos). Dispensar ou colocar o ficheiro em lista segura pode ser útil nestas instâncias.

- **Editar a Lista global** - Adicione ou remova ficheiros da lista de quarentena global.
- **Dispensar** - Adicione um ficheiro à lista de Dispensados num computador. Este ficheiro pode ser executado no computador.

Gerir ameaças avançadas de endpoint

Para gerir uma ameaça identificada num computador específico:

1. No painel esquerdo, clique em **Populações > Empresa**.
2. Selecione o separador **Ameaças avançadas**.
3. Selecione Agentes.
4. Selecione um nome de agente específico e o comando adequado: colocar uma ameaça em **Quarentena** ou **Exportar** ou **Dispensar** a mesma.

5

Modo Desligado

O modo Desligado permite que um Dell Server faça a gestão de endpoints Advanced Threat Prevention sem ligação do cliente à Internet ou a uma rede externa. O modo Desligado também permite que o Dell Server faça a gestão de clientes sem ligação à Internet ou a um serviço Advanced Threat Prevention aprovisionado e alojado. O Dell Server capta todos os eventos e dados de ameaça no modo Desligado.

Para determinar se um Dell Server está em funcionamento no modo Desligado, clique no ícone de engrenagem no canto superior direito da Remote Management Console e selecione Acerca de. O ecrã Acerca de indica que um Dell Server está no modo Desligado, abaixo da versão do Dell Server.

O modo Desligado é diferente de uma instalação padrão do Dell Server da seguinte forma.

Ativação do cliente

É gerado um token de instalação quando o administrador carrega uma licença do Advanced Threat Prevention, o que permite a ativação do cliente Advanced Threat Prevention.

Management Console

Os seguintes itens **não estão disponíveis** na Management Console quando o Dell Server está em execução no modo Desligado:

- As seguintes áreas são específicas do Advanced Threat Prevention: ameaças avançadas por prioridade, eventos (Advanced Threat) por classificação, top dez de ameaças avançadas e eventos do Advanced Threat Prevention.
- O separador **Empresa > Ameaças avançadas**, que apresenta informações detalhadas dos eventos para toda a empresa, incluindo uma lista dos dispositivos nos quais ocorreram eventos e quaisquer ações adotadas nesses mesmos dispositivos para os referidos eventos.
- (Painel de navegação esquerdo) Gestão de serviços, que permite a ativação do serviço do Advanced Threat Prevention e a inscrição para receber notificações de produto.

O seguinte item **está disponível** para a Management Console para suporte no modo Desligado:

- O separador **Empresa > Eventos do Advanced Threat**, que enumera informações para toda a empresa com base em informações disponíveis no Dell Server, mesmo em execução no modo Desligado.

Funcionalidade

A seguinte funcionalidade não está disponível na Management Console quando o Dell Server está em execução no modo Desligado:

- Atualização e migração do Security Management Server
- Atualização automática do Security Management Server Virtual - a atualização tem de ser efetuada manualmente
- Atualização de perfil na nuvem
- Atualização automática do Advanced Threat Prevention
- Carregamento de ficheiros executáveis anormais ou não seguros para análise do Advanced Threat Prevention
- Carregamento do ficheiro do Advanced Threat Prevention e carregamento do ficheiro de registo

As seguintes funcionalidades diferem:

- O Dell Server envia a Lista segura global, a Lista de quarentena e a Lista segura para agentes.
- A Lista segura global é importada para o Dell Server através da política Permitir global.
- A Lista de quarentena é importada para o Dell Server através da política Lista de quarentena.
- A Lista segura é importada para o Dell Server através da política Lista segura.

Estas políticas estão disponíveis apenas no modo Desligado. Para mais informações sobre estas políticas, consulte *AdminHelp*, disponível na Remote Management Console.

Para obter mais informações sobre o modo Desligado, consulte "Modo Desligado" em *AdminHelp*, disponível na Management Console.

Identificar e gerir ameaças no modo Desligado

Para gerir ameaças no modo Desligado, primeiro tem de definir as seguintes políticas do Advanced Threat Prevention, conforme aplicável para a sua organização:

- Permitir global
- Lista de quarentena
- Lista segura

Estas políticas são enviadas para o cliente Advanced Threat Prevention apenas se o Dell Server detetar um token de instalação do modo Desligado, que contém o prefixo "DELLAG".

Consulte *AdminHelp* para obter exemplos destas políticas.

Para visualizar os ficheiros que o Advanced Threat Prevention identifica como potenciais ameaças, navegue até **Empresa >** separador **Eventos do Advanced Threat**. Este separador contém uma lista de informações de eventos para toda a empresa e a medida adotada, como Bloqueado ou Terminado.

6

Resolução de problemas

Recuperar o Advanced Threat Prevention

Recuperar o serviço

Será necessário efetuar uma cópia de segurança do certificado para recuperar o serviço do Advanced Threat Prevention.

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

Encontrar o código do produto com o Windows PowerShell

- Pode identificar facilmente o código do produto, se o código do produto mudar no futuro, utilizando este método.

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

  O resultado será o caminho completo e o nome do ficheiro .msi (o nome hexadecimal convertido do ficheiro).

Advanced Threat Prevention

- Para que o plug-in do Advanced Threat Prevention monitorize HKLM\SOFTWARE\Dell\Dell Data Protection quanto a alterações do valor de LogVerbosity, e atualize o nível de registo do cliente em conformidade, defina o seguinte valor.

  [HKLM\SOFTWARE\Dell\Dell Data Protection]

  "LogVerbosity"=DWORD:<see below>

  Dump: 0

  Fatal: 1

  Error 3

  Warning 5

  Info 10

  Verbose 12

  Trace 14

  Debug 15

  O valor de registo é verificado quando o serviço Advanced Threat Prevention é iniciado ou sempre que o valor muda. Se o valor de registo não existir, não há qualquer alteração no nível de registo.

  Utilize esta definição de registo apenas para testar/depurar, uma vez que esta definição de registo controla a verbosidade do registo de outros componentes, incluindo o Encryption e o Encryption Management Agent.

- O Modo de Compatibilidade permite que as aplicações sejam executadas no computador cliente enquanto as políticas de Controlo de Script e Proteção de Memória ou Proteção de Memória estão ativadas. A ativação do modo de compatibilidade requer a adição de um valor de registo no computador cliente.

  Para ativar o modo de compatibilidade, siga estes passos:

  1. Na Management Console, desative a política de *Proteção de memória ativada*. Se a política de *Controlo de script* estiver ativada, desative-a.

2. Adicione o valor de registo Modo de Compatibilidade.
   a. Utilizando o Editor de Registo no computador cliente, aceda a `HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`.
   b. Clique com o botão direito em **Desktop**, clique em **Permissões** e, em seguida, obtenha propriedade e conceda a si próprio Controlo Total.
   c. Clique com o botão direito do rato em **Ambiente de trabalho** e, em seguida, selecione **Novo Valor binário**.
   d. No nome, escreva `CompatibilityMode`.
   e. Abra a definição de registo e altere o valor para `01`.
   f. Clique em **OK** e, em seguida, feche o Editor de Registo.

   Para adicionar o valor de registo com um comando, pode utilizar uma das seguintes opções de linha de comandos para execução 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) cmdlet invocar comando:

     ```
     $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. Na Management Console, ative novamente a política *Proteção de memória ativada*. Se a política de *Controlo de script* tiver sido anteriormente ativada, ative-a novamente.