Dell Endpoint Security Suite Enterprise

Advanced Threat Prevention Quick Start Guide v3.9

January 2024
Rev. A01

DELL Technologies

メモ、注意、警告

メモ: 「メモ」は、製品をより上手に使用するための重要な情報であることを示します。

注意: **「注意」は、ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。**

警告: **「警告」は、物的損害、けが、または死亡の原因となる可能性があることを示しています。**

© 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.

Dell ProSupport for Software へのお問い合わせ

Dell 製品向けの 24 時間 365 日対応電話サポート（877-459-7304、内線 4310039）にご連絡ください。

さらに、Dell 製品のオンライン サポートも dell.com/support からご利用いただけます。オンラインサポートでは、ドライバ、マニュアル、テクニカル アドバイザリー、よくあるご質問（FAQ）、および緊急の問題を取り扱っています。

適切なサポート担当者に迅速におつなぎするためにも、お電話の際はお客様のサービスタグまたはエクスプレスサービスコードをご用意ください。

米国外の電話番号については、Dell ProSupport for Software の各国の電話番号を記載したページを参照してください。

2

はじめに

この章では、Advanced Threat Prevention の管理を開始するための推奨手順について説明します。

Advanced Threat Prevention の管理を開始するための推奨手順は、次のとおりです。

- Advanced Threat Prevention のためのテナントのプロビジョニング
  - Advanced Threat Prevention 導入の必要条件
  - Advanced Threat Prevention のライセンスが Dell Server 内に存在している必要があります。
- Advanced Threat Prevention エージェント自動アップデートの設定
  - Advanced Threat Prevention の自動アップデートの登録（オプション）
  - アップデートは毎月リリース
- 管理者役割の割り当てと変更
  - Advanced Threat Prevention サービスのプロビジョニングまたはリカバリ
  - 既存の Advanced Threat Prevention 証明書のバックアップとダウンロード
  - ポリシーの表示、修正、およびコミット
- 通知のセットアップ
  - Advanced Threat Prevention アラートに対する電子メールとダッシュボード通知の設定（オプション）
  - 企業のニーズに基づいて通知をカスタマイズします。

テナントのプロビジョニング

Advanced Threat Prevention のポリシーの施行がアクティブになる前に、テナントが Dell Server にプロビジョニングされる必要があります。

前提条件

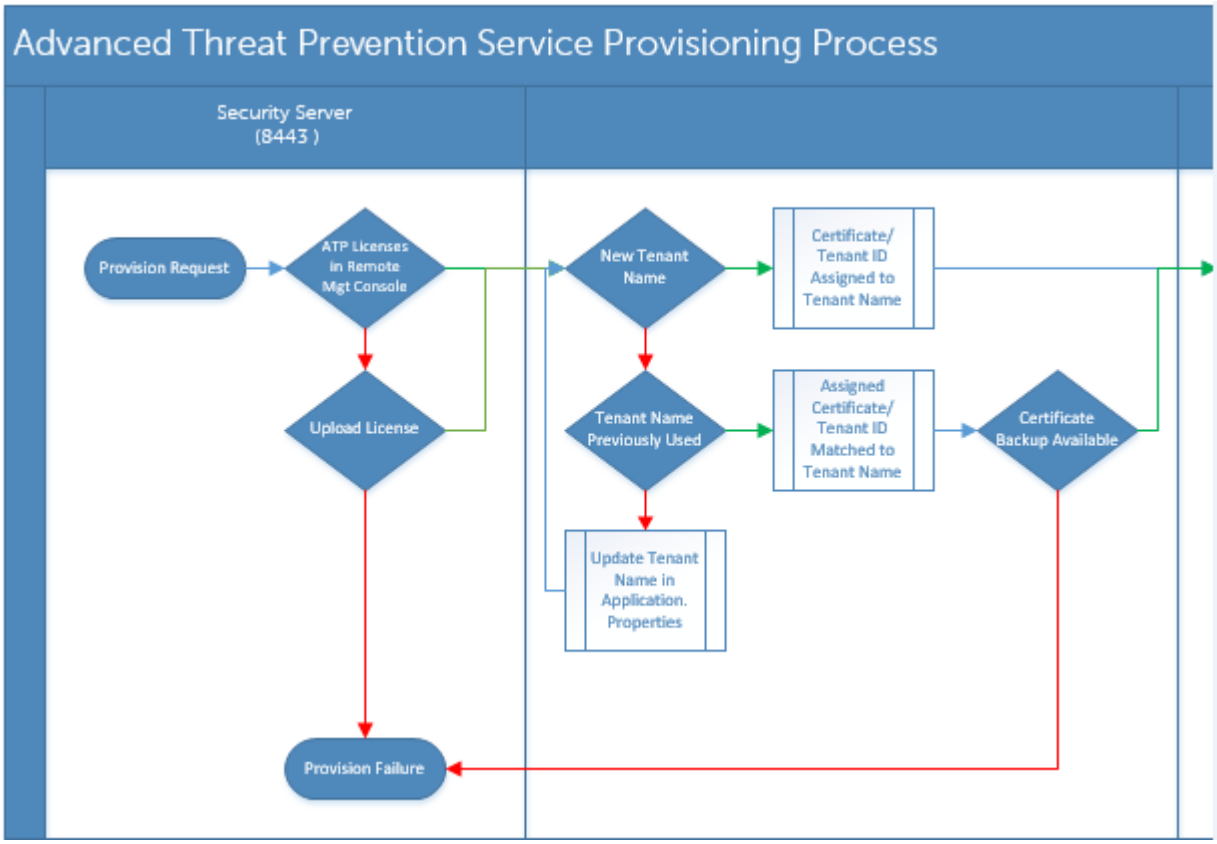
- システム管理者の役割を持つ管理者が実行する必要があります。
- Dell Server でプロビジョニングをするにはインターネット接続が必要です。
- 管理コンソールで Advanced Threat Prevention オンラインサービスの統合を表示するために、クライアント上でインターネット接続が必要です。
- プロビジョニングは、プロビジョニング中に証明書から生成されるトークンに基づいています。
- Advanced Threat Prevention のライセンスが Dell Server 内に存在している必要があります。

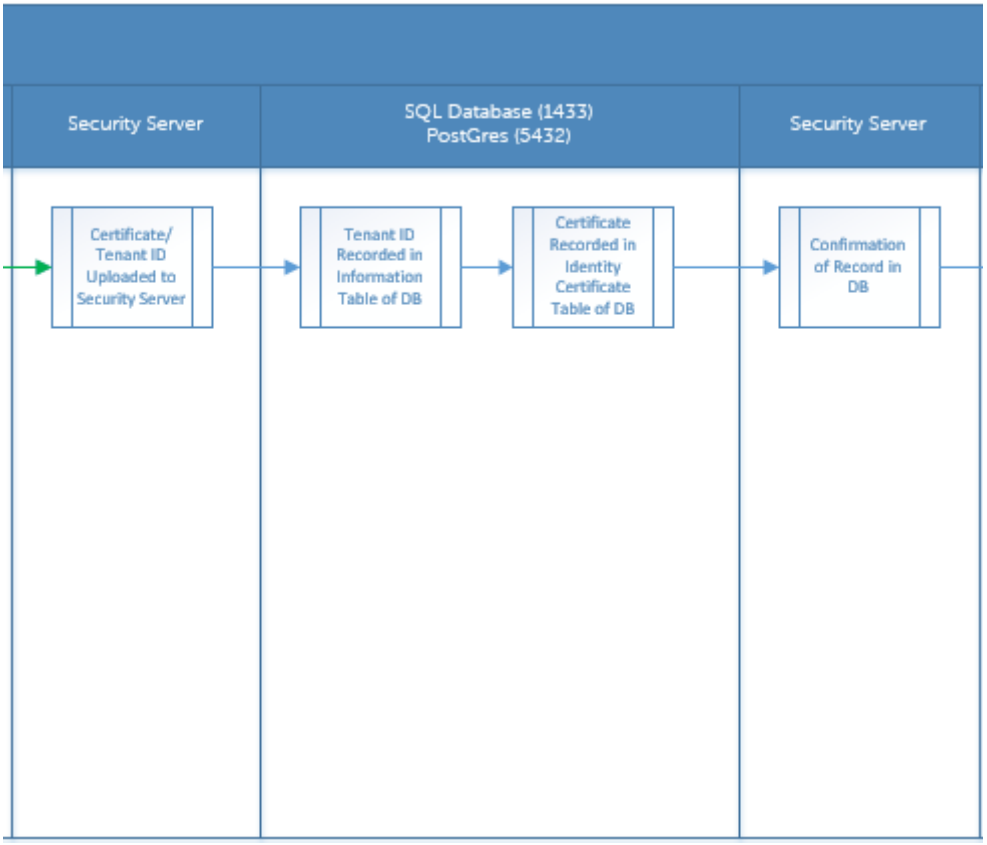
テナントのプロビジョニング

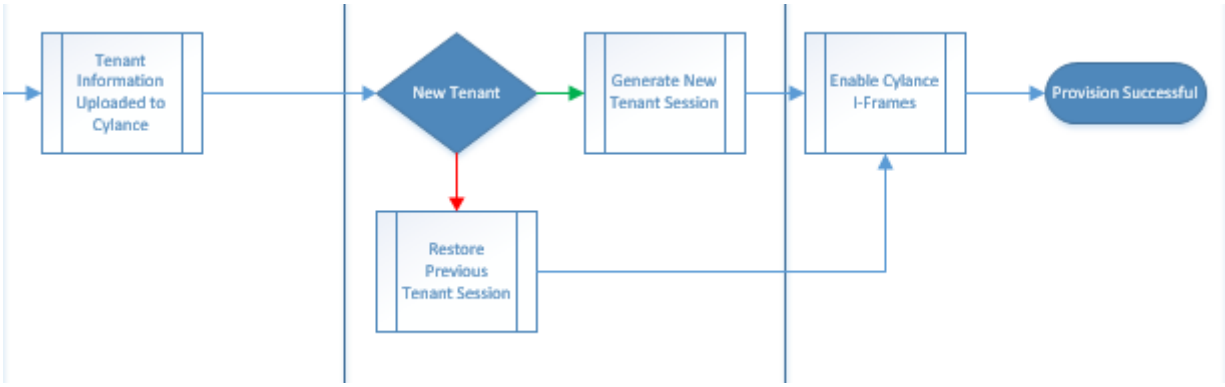
1. 管理コンソールに Dell 管理者としてログインします。
2. 管理コンソールの左ペインで、**管理** > **サービス管理** の順にクリックします。
3. **Advanced Threat Protection サービスのセットアップ** をクリックします。この時点で不具合が発生する場合は、Advanced Threat Prevention ライセンスをインポートします。
4. ラインセンスがインポートされると、ガイド付きのセットアップが始まります。**次へ** をクリックして開始します。
5. EULA を読み、合意した後、**次へ** をクリックします。
6. テナントのプロビジョニングのために Dell Server に ID 資格情報を入力します。**次へ** をクリックします。*Cylance* ブランドの既存テナントのプロビジョニングはサポートされていません。
7. 証明書をダウンロードします。これは Dell Server での災害シナリオが発生した場合のリカバリに必要です。この証明書は自動的にバックアップされません。別のコンピュータの安全な場所に証明書をバックアップします。証明書をバックアップしたことを確認するチェックボックスを選択してから **次へ** をクリックします。
8. セットアップが完了しました。**OK** をクリックします。

プロビジョニングとエージェント通信

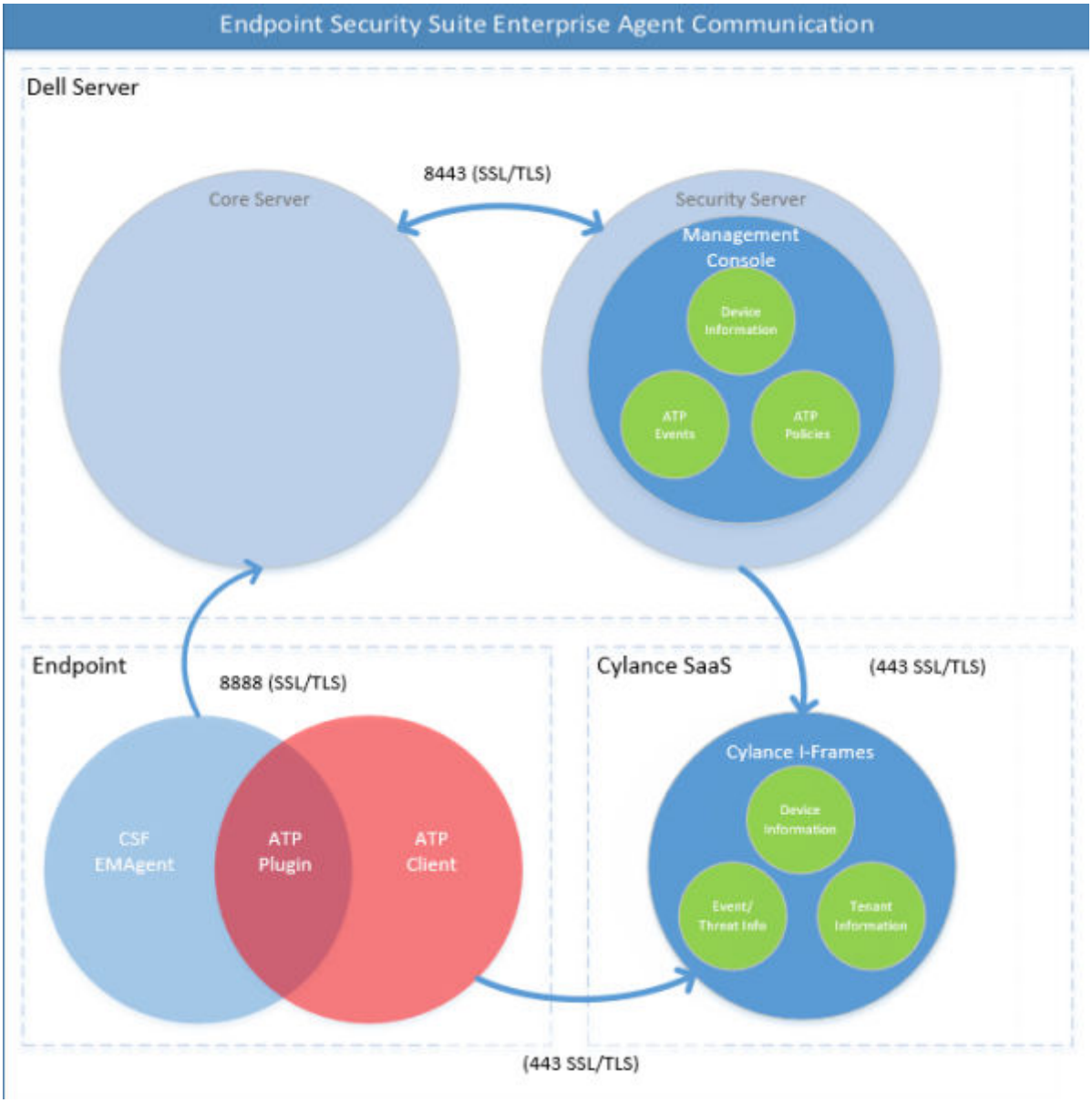
次の図は Advanced Threat Prevention サービスのプロビジョニングプロセスを表しています。



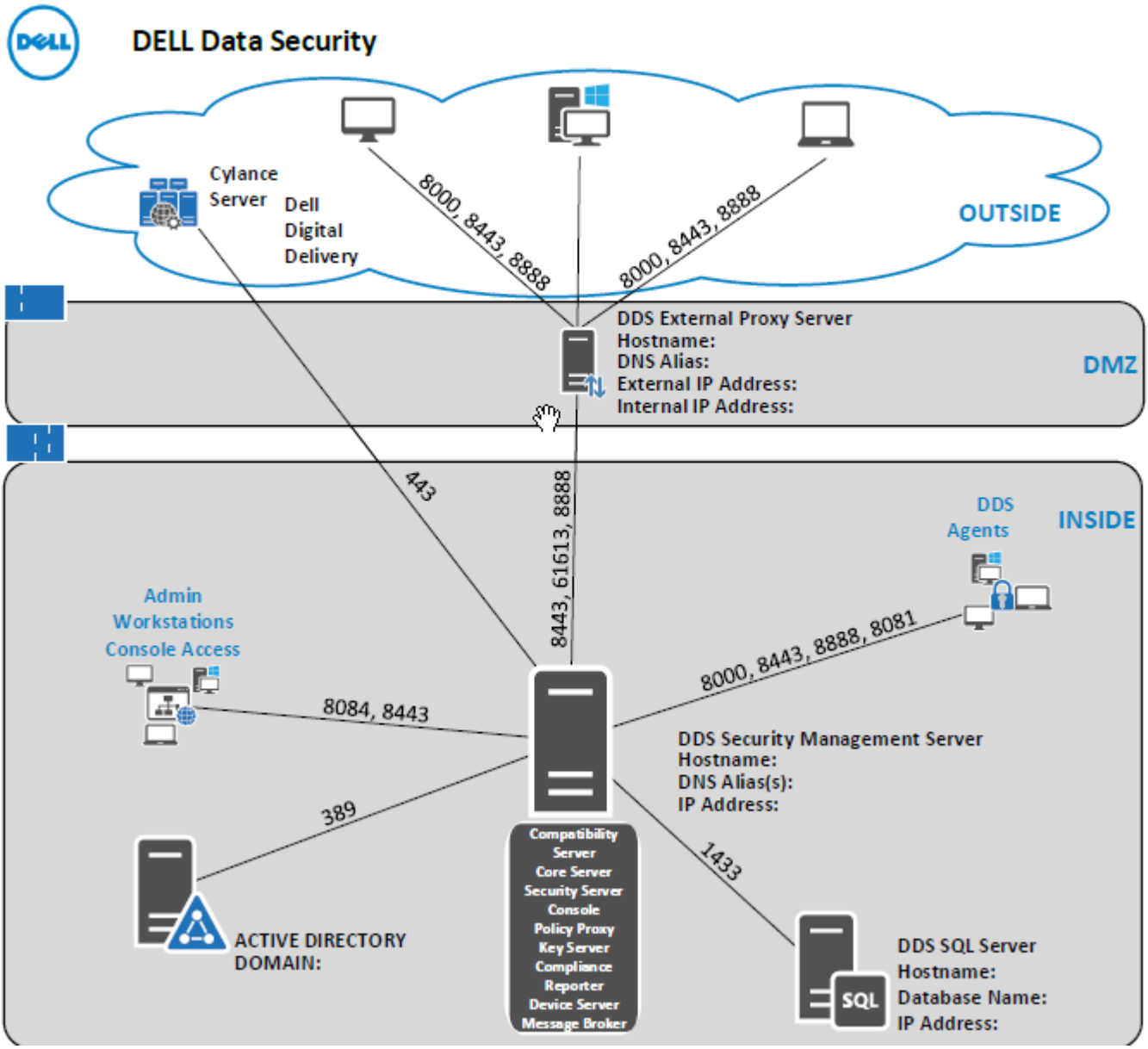




次の図は Advanced Threat Prevention のエージェント通信プロセスを表しています。



次の図は Dell サーバのアーキテクチャと通信を図示しています。



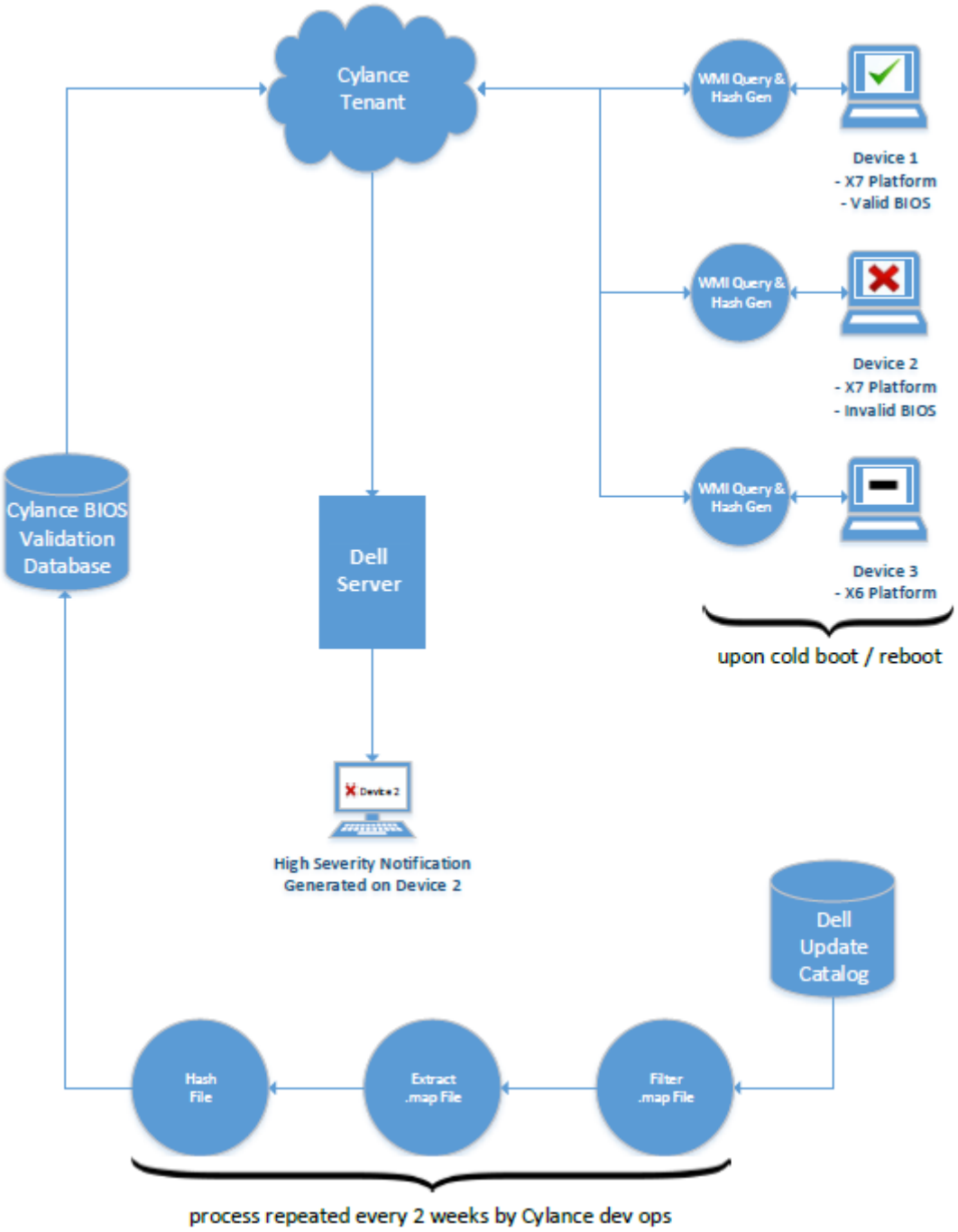
BIOS イメージの整合性検証の有効化

Advanced Threat Prevention のマスタースイッチが有効であれば、BIOS イメージの整合性検証ポリシーはデフォルトで有効です。

BIOS イメージの整合性検証プロセスの概要については、「BIOS イメージの整合性検証プロセス」を参照してください。

検証プロセス

次の図は、BIOS イメージの整合性の検証プロセスを表しています。



BIOS 保証の有効化 ポリシーが管理コンソールで選択されている場合は、Cylance のテナントが BIOS がデル工場出荷時のバージョンから変更されていないか（攻撃ベクターの 1 つ）を確認するために、エンドポイントコンピュータ上で BIOS ハッシュを検証します。脅威が検出された場合は、通知が Dell Server に渡され、IT 管理者はリモート管理コンソールでアラートを受けます。プロセスの概要については、「BIOS イメージの整合性検証プロセス」を参照してください。

メモ: カスタマイズされた工場出荷時イメージは、BIOS が変更されているため、この機能では使用できません。

BIOS イメージの整合性検証でサポートされる Dell コンピュータモデル	
• Latitude 3470 • Latitude 3570 • Latitude 7275 • Latitude 7370 • Latitude E5270	• OptiPlex 5040 • OptiPlex 7040 • OptiPlex 7440 • Precision Mobile Workstation 3510 • Precision Mobile Workstation 5510

BIOS イメージの整合性検証でサポートされる Dell コンピュータモデル		
• Latitude E5470 • Latitude E5570 • Latitude E7270 • Latitude E7470 • Latitude Rugged 5414 • Latitude Rugged 7214 Extreme • Latitude Rugged 7414 • OptiPlex 3040 • OptiPlex 3240	• VMware Workstation 3620 • VMware Workstation 7510 • VMware Workstation 7710 • Precision Workstation T3420 • Venue 10 Pro 5056 • Venue Pro 5855 • Venue XPS 12 9250 • XPS 13 9350 • XPS 9550	

Advanced Threat Prevention エージェント自動アップデートの設定

管理コンソールで、Advanced Threat Prevention エージェントの自動アップデートを受信するように登録できます。エージェントの自動アップデートを受信するよう登録することにより、クライアントが Advanced Threat Prevention サービスからアップデートを自動ダウンロードして適用できるようになります。アップデートは毎月リリースされます。

メモ:

エージェントの自動アップデートは Dell Server v9.4.1 以降でサポートされます。

エージェントの自動アップデートの受信

エージェントの自動アップデートを受信するよう登録するには、次の操作を行います。

1. 管理コンソールの左ペインで、**管理** > **サービス管理** を順にクリックします。
2. エージェントの自動アップデート の下の 高度な脅威 タブで **オン** をクリックして、**プリファレンスの保存** をクリックします。

   情報が入力され、自動アップデートが表示されるまで数分間かかることがあります。

エージェントの自動アップデート受信の停止

エージェントの自動アップデート受信を停止するには、次の操作を行います。

1. 管理コンソールの左ペインで、**管理** > **サービス管理** を順にクリックします。
2. エージェントの自動アップデート の下の 高度な脅威 タブで **オフ** をクリックして、**プリファレンスの保存** をクリックします。

管理者役割の割り当てと変更

管理コンソールの管理者ページで、既存の管理者権限を表示または変更します。

管理者役割

管理者ログインがアクティブディレクトリに統合されて管理者の管理プロセスが簡素化され、既存のユーザー認証インフラストラクチャを使用できるようになりました。管理者には、各管理者に許可されるアクセスレベルを定義した役割が割り当てられます。たとえば、ヘルプデスクによる回復の実施のみができる管理者もいれば、セキュリティポリシー編集のための完全なアクセス権がある管理者もいます。AD グループに管理者役割を割り当てると、AD グループのメンバシップに簡単な変更を加えれば、ユーザーに付与した管理者アクセスレベルを簡単に変更できます。非ドメインユーザーには、Compliance Reporter 経由のレポート専用アクセスを付与することができます。

次のタスクの実行にはシステム管理者の役割が必要です。

- Advanced Threat Prevention サービスのプロビジョニングまたはリカバリ
- Advanced Threat Prevention の自動アップデートの登録
- Advanced Threat Prevention アラートに対する電子メールまたはダッシュボードの通知の設定
- 既存の Advanced Threat Prevention 証明書のバックアップとダウンロード

メモ: ポリシーの表示、変更、コミットには、セキュリティ管理者の役割が必要です。

既存の管理者権限を表示または変更するには、次の手順に従います。

1. 左ペインで **ポピュレーション > 管理者** の順にクリックします。

2. 適切な管理者のユーザー名が表示されている行を検索または選択して、ユーザーの詳細を表示します。
3. 右ペインで、管理者役割を表示または変更します。
4. **保存** をクリックします。

メモ: 管理者役割は、ユーザーレベルではなくグループレベルで割り当てることをお勧めします。

管理者役割をグループレベルで表示、割り当て、変更するには、次の手順に従います。
1. 左ペインで **ポピュレーション > ユーザーグループ** の順にクリックします。
2. グループ名を検索または選択してから、**管理者** タブをクリックします。ユーザーグループ詳細 ページが表示されます。
3. グループに割り当てられる管理者役割を選択または選択解除します。
4. **保存** をクリックします。

管理者権限を持つグループを削除した後、再び追加した場合、そのグループは管理者グループとしての立場を維持します。

管理者役割をユーザーレベルで表示、割り当て、または変更するには、次の手順に従います。
1. 左ペインで、**ポピュレーション > ユーザー** の順にクリックします。
2. ユーザー名を検索または選択してから、管理者 タブをクリックします。
3. ユーザーに割り当てられる管理者役割を選択または選択解除します。
4. **保存** をクリックします。

管理者役割 - ユーザーの役割の割り当てまたは変更を行い、**保存** をクリックします。

継承したグループ役割 - ユーザーがグループから継承した役割の読み取り専用のリストです。役割を変更するには、そのユーザーの **ユーザーグループ** タブをクリックし、グループ名を選択します。

指定した役割 - 管理者権限をユーザーに委譲します。

通知のセットアップ

リモート管理コンソールで、通知の受信に登録できます。通知リストでは、ダッシュボードに表示する、または電子メール通知として送信する、設定可能なニュース、アラート、イベントのサマリを提供します。

通知タイプ

リストに含める通知タイプを選択することができます。残りのタイプの通知は、表示されません。**脅威保護**と**高度な脅威イベント**の通知は、Advanced Threat Prevention に関連しています。

タイプには次が含まれます。
- **アップデート** - 今後の製品のアップデートに関するニュース。製品アップデートを表示し、受信するには、これらを受信するように登録する必要があります。**サービス管理 > 製品の通知** と選択して、**オン** をクリックし、**プリファレンスの保存** をクリックします。
- **設定** - 設定変更に関するニュース。
- **ナレッジベース** - 詳細な技術情報（回避策や設定方法など）に関するナレッジベース記事の要約とリンク。
- **アナウンス** - 今後のリリースおよび新製品に関するニュースです。
- **ライセンス** - お使いのボリュームライセンスの可用性が低下した場合、またはお使いのクライアントアクセスライセンス数を超過した場合にアラートを通知します。
- **脅威保護** - Advanced Threat Prevention からの脅威アラート。
- **高度な脅威イベント** - Advanced Threat Prevention で検出されたイベント。サマリには、重要、メジャー、マイナー、警告、および情報イベントのリスト表示があり、詳細情報へのリンクも含まれています。
- **脅威イベント** - 脅威保護によって検出されたイベント。
- **証明書** - 証明書の有効期間通知。
- **Dell サーバの例外** - Dell サーバの通信の問題は、脅威保護、アップデート、設定、ナレッジベース、およびアナウンスの送信に影響を与えます。

1 つ、または複数のタイプを選択した後、リストの上のニュートラルな領域内をクリックして、選択内容を適用します。

選択した項目のクリア を選択して、このリストの選択内容をリセットします。

優先度レベル

メモ: 通知の優先度レベルは、通知領域以外の、ダッシュボードに表示された優先度レベルには関連しません。

優先度には、重要、高、中、低があります。これらの優先順位レベルは、通知タイプの内部でのみお互いに関連しています。

ダッシュボードの通知領域または電子メール通知の一覧に含める通知の優先度レベルは、選択可能です。選択しなかった優先度レベルの通知は、ダッシュボードまたは電子メール通知のリストに含まれることはありません。

選択した項目のクリア を選択して、このリストの選択内容をリセットします。 すべての通知が表示されます（別の場所でフィルタリングされた場合を除く）。

3

ポリシー

この章では、Advanced Threat Prevention のポリシー管理について詳しく説明します。

- Advanced Threat Prevention の有効化
- 推奨するポリシー設定
- ポリシー変更のコミット

Advanced Threat Prevention のポリシーとその説明の完全なリストについては、リモート管理コンソールからアクセスできる *AdminHelp* を参照してください。

Advanced Threat Prevention の有効化

Advanced Threat Prevention ポリシーは、デフォルトでは **オフ** です。Advanced Threat Prevention ポリシーを有効にするには、**オン** に切り替える必要があります。Advanced Threat Prevention ポリシーは、エンタープライズ、エンドポイントグループ、およびエンドポイントの各レベルで強制することができます。

Advanced Threat Prevention をエンタープライズのレベルで有効にするには、次の手順を実行します。

1. 左ペインで **ポピュレーション**、**Enterprise** の順にクリックします。
2. **脅威の防止** をクリックします。
3. Advanced Threat Prevention マスタースイッチを **オフ** から **オン** に切り替えます。

Advanced Threat Prevention ポリシーを有効にするには、エンドポイントグループのレベルで、次の手順を実行します。

1. 左ペインで **ポピュレーション**、**エンドポイントグループ** の順にクリックします。
2. **脅威の防止** をクリックします。
3. Advanced Threat Prevention マスタースイッチを **オフ** から **オン** に切り替えます。

Advanced Threat Prevention ポリシーを有効にするには、エンドポイントのレベルで、次の手順を実行します。

1. 左ペインで **ポピュレーション** > **エンドポイント** の順にクリックします。
2. **脅威の防止** をクリックします。
3. Advanced Threat Prevention マスタースイッチを **オフ** から **オン** に切り替えます。

推奨するポリシー設定

- 最新の推奨ポリシー設定リストについては、KB 文書 SLN301562 を参照してください。

ポリシー変更のコミット

変更して保存したポリシーをコミットするには、次の手順に従います。

1. リモート管理コンソールの左ペインで **管理** > **コミット** を順にクリックします。
2. コメント に、変更内容の説明を入力します。
3. **ポリシーのコミット** をクリックします。

管理者が **ポリシーのコミット** をクリックすると、ポリシーの発行またはコミットが行われます。次の情報が表示されます。

- 保留中のポリシー変更 - ポリシーに加えられた、コミット可能な変更の数。
- コミットされた日付 - ポリシーがコミットされた日時。
- 変更者 - ポリシーのコミットを実行した管理者のユーザー名。
- コメント - ポリシーがコミットされたときに追加されたコメント。
- バージョン - 最後のポリシーコミット以降ポリシーが保存された回数に前バージョンを足した数値。

4

脅威

この章では、Advanced Threat Prevention をインストールした後に、企業環境で発生した脅威の特定と管理を行う方法についての詳細を記載します。

- 脅威の特定
  - 脅威イベントの表示
  - Cylance スコアと脅威モデルの更新
  - 詳細な脅威データの表示
- 脅威の管理
  - 脅威データを CSV にエクスポート
  - グローバル隔離リストの管理

脅威の特定

電子メールおよびダッシュボードの通知

脅威保護および高度な脅威イベントに対して電子メール通知をセットアップした場合、Advanced Threat Prevention の電子メールでイベントと脅威が管理者に通知されます。

管理コンソールのダッシュボード通知の概要には、Advanced Threat Prevention の脅威とイベントが脅威保護と高度な脅威イベントの通知タイプで表示されます。

- 脅威保護タイプ - Advanced Threat Prevention からの脅威アラート。
- 高度な脅威イベントタイプ - Advanced Threat Prevention で検出されたイベント。イベントは必ずしも脅威であるとは限りません。

次の表で、脅威の名前、重大度、脅威の情報について詳しく説明します。

名前	重大度	詳細
ThreatFound	重大	Portable Executable（PE）がデバイスで特定されましたが、エンドポイントではブロックも隔離もされていません。システムに対するアクティブな脅威です。
ThreatBlocked	警告	Portable Executable がデバイスで特定されましたが、実行はブロックされています。この脅威は特に隔離されていません。自動隔離のためのポリシーが有効になっていないか、ファイルがローカルの SYSTEM アカウントでは書き込めない場所（ネットワーク共有、取り外された USB デバイスなど）にあるためと思われます。
ThreatTerminated	警告	Portable Executable（PE）がデバイスで特定され、アクティブに実行されていることが検出されたため、プロセスが強制終了されました。PE は別の場所で実行されていたため、ファイルの隔離は行われていません。このエンドポイントと実行可能ファイルに関連する別のイベントを探し、脅威が適切に封じ込まれていることを確認することをお勧めします。
MemoryViolationBlocked	警告	実行可能ファイルまたはスクリプトが実行されようとしていましたが、メモリー保護またはスクリプト制御ポリシーに違反していました。その後、実行可能ファイルまたはスクリプトの実行はブロックされました。これは通常、対応するメモリー保護またはスクリプト制御ポリシーで、ブロックするように設定されているためです。
MemoryViolationTerminated	警告	実行可能ファイルまたはスクリプトがアクティブに実行されているのが検出されましたが、メモリー保護またはスクリプト制御ポリシーに違反していました。その後、実行可能ファイルまたはスクリプトの実行は強制終了されました。こ

名前	重大度	詳細
		れは通常、対応するメモリー保護またはスクリプト制御ポリシーで、終了するように設定されているためです。
MemoryViolation	警告	実行可能ファイルまたはスクリプトが、メモリー保護またはスクリプト制御ポリシーに違反していることが判明しました。実行可能ファイルまたはスクリプトは、ポリシーに違反する操作を行っていません。ポリシーが許可に設定されている可能性があります。
ThreatRemoved	情報	以前にフラグが設定された Portable Executable（PE）であり、脅威と見なされたため、エンドポイントから削除されました。この PE は、隔離先の場所または最初に存在した場所のどちらかから削除されました。リムーバブル メディア（USB、CD-ROM など）で最初に検出された場合によくあるケースです。
ThreatQuarantined	情報	Portable Executable（PE）は潜在的な脅威であると判断され、隔離が完了しました。異常（Cylance Score 0～60）または危険（Cylance Score 60～100）の分類に基づく、脅威の自動隔離が有効になっているためです。
ThreatWaived	情報	Portable Executable（PE）は潜在的な脅威であると判断されましたが、グローバル セーフリストに基づいて、またはローカルの免除ポリシーによって免除されました。また、Dell Security Management Server 内の「免除」または「グローバル セーフリスト」ポリシーに、SHA256 ハッシュが追加されました。
ThreatChanged	情報	Portable Executable（PE）の Cylance Score が変更されました。通常、Cylance によって実行される 2 ステップのスコアリングが原因です。ローカルのスコア エンジンの脅威分析が、Cylance クラウド エンジンの分析と一致していない可能性があります。Cylance クラウド エンジンには追加データがあるため、このような場合は Cylance クラウド エンジンによるスコアが使用されます。また、Cylance のアップデートによって、以前は脅威とみなされたファイルの再解析が初期化され、新たにスコアが計算されて、この PE が脅威と見なされなくなった可能性もあります。
ProtectionStatusChanged	情報	エンドポイントの保護ステータスに何らかの変更がありました。これは、Dell Encryption Management Agent が Cylance プラグインを介して Cylance サービスに再接続するときに発生します。一般的にはエンドポイントが再起動された際に発生します。起動中に、短期間ながら CSF が Cylance プラグインに接続されていない期間があるためです。

詳細を表示するには、通知 をクリックします。追加の脅威またはイベントの詳細へのリンクなどが表示されます。

脅威の詳細 タブ

脅威の詳細 タブには、企業全体の動的な詳細なイベント情報が表示されます。この情報には、イベントが発生したデバイスのリストと、それらのイベントに対処するためにこれらのデバイスに対するアクションが含まれます。

エンタープライズ高度な脅威 タブにアクセスするには、次の手順に従います。

1. 左のペインで、**［ポピュレーション］＞［Enterprise］**の順にクリックします。
2. **脅威の詳細** タブを選択します。

イベント、デバイス、およびアクションに関する情報が、次のタブに整理統合されて表示されます。

- **保護** - 潜在的に有害なファイルとスクリプト、およびその詳細（ファイルとスクリプトが見つかったデバイスなど）を一覧表示します。
- **エージェント** - Advanced Threat Prevention クライアントを実行しているデバイスに関する情報と、情報をエクスポートしたり、リストからデバイスを削除したりするオプションを提供します。
- **グローバルリスト** - グローバル隔離と安全リスト内のファイルを一覧表示し、これらのリストにファイルを移動するオプションを提供します。
- **オプション** - Security Information Event Management（SIEM）と統合する方法を提供します。
- **証明書** - 証明書をアップロードできます。証明書のアップロード後には、グローバルリストに表示され、安全リストに掲載されます。

タブに表示される表は、次の方法で整理統合できます。

- 表に対して列を追加または削除 - 列ヘッダー横の矢印をクリックし、**列** を選択して表示する列を選択します。非表示にする列のボックスのチェックを外します。

- データの並べ替え - 列ヘッダをクリックします。
- 列ごとのグループ化 - 列ヘッダーを、緑色になるまで上方向にドラッグします。

高度な脅威イベントタブ

高度な脅威イベント タブには、Dell Server 内にある情報に基づいた、企業全体についての情報が表示されます。

Advanced Threat Prevention サービスがプロビジョニングされて、ライセンスを利用可能かどうかがタブに表示されます。

高度な脅威イベント タブからデータをエクスポートするには、**エクスポート** をクリックして、**Excel** または **CSV** ファイル形式を選択します。

メモ: Excel ファイルは 65,000 行に制限されます。CSV にはサイズ制限はありません。

Cylance スコアと脅威モデルの更新

Cylance スコアは異常または危険とみなされる各ファイルに割り当てられます。このスコアは、ファイルがマルウェアである確実性のレベルを表します。この数値が大きいほど、確実性が高くなります。

デバイスを保護するために使用されている予測脅威モデルは、検出率を向上させるため、定期的なアップデートを受信します。

管理コンソールの 保護 ページの 2 列には、新しい脅威モデルが組織にどのような影響を与えるかが表示されます。デバイス上のどのファイルがモデル変更によって影響を受ける可能性があるかを確認するには、本番ステータス と 新規ステータス の列を表示して比較します。

本番ステータスと新規ステータスの列を表示するには：

1. 左のペインで、**［ポピュレーション］ > ［Enterprise］** の順にクリックします。
2. **脅威の詳細** タブを選択します。
3. **保護** タブをクリックします。
4. 表内の列ヘッダーの下矢印をクリックします。
5. マウスカーソルを **列** に合わせます。
6. **本番ステータス** と **新規ステータス** の列を選択します。

本番ステータス - ファイルの現在のモデルステータス（安全、異常、危険）です。

新しいステータス - 新しいモデルのファイルのモデルステータスです。

たとえば、現在のモデルで 安全 と見なされたファイルが、新しいモデルでは 危険 に変更される可能性があります。組織がそのファイルを必要とする場合、そのファイルを安全リストに追加することができます。現在のモデルが認識しないか、またはスコアを付けていないファイルが、新しいモデルでは危険と見なされる場合があります。組織がそのファイルを必要とする場合、そのファイルを安全リストに追加することができます。

組織内のデバイスで見つかったファイルで、*Cylance Score* が変更されたファイルだけが表示されます。 スコアが変更されても現在のステータス内に残っているファイルもあります。たとえば、ファイルの Cylance Score が 10 から 20 に変更されても、ファイルのステータスが 異常 のままの場合、このファイルは更新されたモデルリストに表示されます（組織のデバイスにこのファイルが存在する場合）。

新しいモデルと現在のモデルの比較

現在のモデルと新しいモデルの違いを確認できるようになりました。

注意を必要とする 2 つのシナリオを次に示します。

本番ステータス = 安全、新しいステータス = 異常 または 危険

- 組織はこのファイルを 安全 と判断している
- 組織が自動隔離に対して、異常 および / または 危険 を設定している

上記のシナリオの推奨事項は、組織内で許可するファイルを安全リストに掲載することです。

分類の識別

組織に影響を及ぼす可能性がある分類を識別するため、デルは、次のアプローチを推奨します。

1. 新しいステータス 列にフィルタを適用して、危険、異常、隔離済みのファイルをすべて表示します。
2. 本番ステータス 列にフィルタを適用して、安全なファイルをすべて表示します。
3. 分類 列にフィルタを適用して、信頼済み - ローカルの脅威 のみを表示します。

信頼済み - ローカルファイルが Cylance によって分析され、安全であることがわかりました。レビュー後、これらのアイテムは安全リストに掲載されます。フィルタされたリストに多数のファイルがある場合、より多くの属性を使用して優先順位を決定する必要があります。たとえば、検知元 列にフィルタを追加して、実行制御が検出した脅威を見直します。これらの脅威はユーザーがアプリケーションを実行しようとしたときに検出され、Background Threat Detection や File Watcher によって検出された休止ファイルよりも緊急の注意が必要です。

モデルの比較情報は、デバイスからではなく、データベースから取得されます。そのため、モデル比較に関して、再分析は実行されません。ただし、新しいモデルが使用可能で、適切なエージェントがインストールされている場合、組織内で再分析が実行され、モデル変更が適用されます。

詳細については、*AdminHelp* を参照してください。

Web Protection およびファイアウォールイベントの表示

脅威は、マルウェア / 悪用、ウェブフィルタ、ファイアウォール、または 未分類 イベントに分類されます。脅威イベントのリストは、どのカラムヘッダーでも並べ替えることができます。脅威イベントはエンタープライズ全体で表示するか、特定のエンドポイントについて表示することができます。エンタープライズ脅威イベント タブから特定のエンドポイントの脅威イベントを表示するには、デバイス ID カラムでデバイスを選択します。

エンタープライズの脅威イベントを表示するには、次の手順に従います。
1. 左のペインで、**［ポピュレーション］＞［Enterprise］**の順にクリックします。
2. **脅威イベント** タブをクリックします。
3. イベントを表示する対象の重大度レベルと期間を選択します。

特定エンドポイントでの脅威を表示するには、次の手順に従います。
1. 左ペインで **ポピュレーション > エンドポイント** の順にクリックします。
2. ホスト名を検索または選択してから、**脅威イベント** タブをクリックします。

脅威の管理

脅威に対しては、隔離、安全リスト化、放棄、エクスポートができます。

エンタープライズのレベルで、次の処置を実行します。
- アラートをトリガーした脅威またはスクリプトをエクスポート
- 脅威の隔離
- 脅威の安全リスト化
- グローバルリストの手動編集

エンタープライズレベルで識別された脅威を管理します。
1. 左ペインで **ポピュレーション、Enterprise** の順にクリックします。
2. **脅威の詳細** タブを選択します。
3. 保護 を選択します。

スクリプトコントロールの表からは、潜在的な脅威として表にリストされているスクリプトをエクスポートできます。

エンタープライズ高度な脅威の管理

保護 タブは、有害の可能性のあるファイルとスクリプトに関する情報を提供します。

脅威表

脅威表からは、脅威のエクスポート、隔離、または安全リスト化ができます。また、グローバル隔離リストに脅威を手動で追加することもできます。

この表には、組織全体で見つかったイベントすべてがリストされます。イベントは、脅威である場合もありますが、必ずしも脅威であるとは限りません。

特定の脅威に関する追加情報を表示するには、脅威名のリンクをクリックするか（新しいページに詳細が表示されます）、脅威の行の任意の場所をクリックします（ページの下部に詳細が表示されます）。

表に追加の脅威情報を表示するには、列ヘッダーのドロップダウン矢印をクリックし、列を選択して追加します。ファイルに関するメタデータ（分類、Cylance スコア（信頼レベル）、AV 業界の評価（他のベンダーとの比較を目的とした VirusTotal.com へのリンク）、最初に検出された日付、SHA256、MD5、ファイル情報（作成者、説明、バージョン）、署名の詳細など）を表示する列。

コマンド
- **エクスポート** - 脅威データを .CSV ファイルにエクスポートします。エクスポートする行を選択して、**エクスポート** をクリックします。
- **グローバル隔離** - グローバル隔離リストにファイルを追加します。その脅威は、すべてのデバイスから恒久的に隔離されます。
- **安全** -ファイルを安全リストに追加します。そのファイルは、デバイス全体で恒久的に安全なファイルとして扱われます。

  メモ: ただし、「良い」ファイルが安全でないと報告される場合があります（これは、そのファイルの特徴が悪意のあるファイルの特徴と非常によく似ている場合に発生します）。このような場合、そのファイルを免除するか、または安全リストに加えると便利です。

- **グローバルリストの編集** - グローバル隔離リストに対して、ファイルを追加または削除します。
- **放棄** - コンピュータ上の放棄されるリストにファイルを追加します。このファイルは、コンピュータ上で実行することを許可されます。

エンドポイントの高度な脅威の管理

個別のコンピュータ上で識別された脅威を管理します。
1. 左ペインで **ポピュレーション、Enterprise** の順にクリックします。
2. **脅威の詳細** タブを選択します。
3. エージェントを選択します。

4. 特定のエージェント名を選択し、適切なコマンドを選択して、脅威の**エクスポート**、**隔離**、または**放棄**を選択します。

5

接続切断モード

接続切断モードを使用すると、Dell Server は、インターネットまたは外部ネットワークへの接続がなくても Advanced Threat Prevention エンドポイントを管理できます。また、接続切断モードでは、インターネット接続や、プロビジョニングおよびホスティングされた Advanced Threat Prevention がなくても、Dell Server はクライアントを管理できます。Dell Server はすべてのイベントと脅威のデータを接続切断モードでキャプチャします。

Dell Server が接続切断モードで動作しているかを調べるには、リモート管理コンソールの右上にあるギアのアイコンをクリックして、情報 を選択します。バージョン情報 画面で、Dell Server のバージョン情報の下に Dell Server が接続切断モードであることが表示されます。

接続切断モードは次の点で Dell Server の標準的な接続インストールとは異なります。

クライアントのアクティブ化

インストールトークンは、管理者が Advanced Threat Prevention ライセンスをアップロードすると生成されます。このトークンによって、Advanced Threat Prevention クライアントをアクティブ化することができます。

管理コンソール

Dell Server が接続切断モードで実行されている場合、管理コンソールで次のアイテムは**使用できません**。

- 以下の領域（Advanced Threat Prevention - 優先度別の高度な脅威、分類による（脅威の詳細）イベント、高度な脅威トップテン、Advanced Threat Prevention イベント）
- **Enterprise > 脅威の詳細** タブには、企業全体の動的な詳細なイベント情報が表示されます。この情報には、イベントが発生したデバイスのリストと、それらのイベントに対処するためにこれらのデバイスに対するアクションが含まれます。
- （左側のナビゲーションペイン）サービス管理 - 管理者は、Advanced Threat Prevention サービスの有効化と、どの製品通知をするかを登録することができます。

管理コンソールに次のアイテムが**使用可能になり**、接続切断モードがサポートされるようになりました。

- **Enterprise > 高度な脅威イベント** タブでは、接続切断モードで実行されている場合も含めて Dell Server で使用できる情報に基づいて、企業全体のイベント情報がリストされます。

機能

Dell Server が接続切断モードで実行されている場合、管理コンソールでは次のアイテムは使用できません。

- Security Management Server のアップグレード、アップデート、移行
- Security Management Server Virtual の自動アップデート - アップデートは手動で行う必要があり
- クラウドプロファイルのアップデート
- Advanced Threat Prevention の自動アップデート
- Advanced Threat Prevention 分析用の安全ではないファイルまたは異常な実行ファイルのアップロード
- Advanced Threat Prevention ファイルのアップロードおよびログファイルのアップロード

次の機能は以下のように異なっています。

- Dell Server は、グローバル安全リスト、隔離リスト、および安全リストをエージェントに送信します。
- グローバル安全リストは、グローバル許可ポリシーを通じて Dell Server にインポートされます。
- 隔離リストは、隔離リストポリシーを通じて Dell Server にインポートされます。
- 安全リストは、安全リストポリシーを通じて Dell Server にインポートされます。

これらのポリシーは、切断モードでのみ使用できます。これらのポリシーの詳細については、リモート管理コンソールで *AdminHelp* を参照してください。

切断モードの詳細については、管理コンソールの *AdminHelp* の「切断モード」を参照してください。

切断モードの脅威の識別および管理

切断モードでの脅威を管理するには、最初に次のような Advanced Threat Prevention ポリシーを組織に応じて設定する必要があります。

- グローバル許可
- 隔離リスト
- 安全リスト

これらのポリシーは、Dell Server が切断モードのインストールトークン（接頭語「DELLAG」があります）を検出する場合に限り、Advanced Threat Prevention クライアントに送信されます。

これらのポリシーの例については、*AdminHelp* を参照してください。

Advanced Threat Prevention が潜在的な脅威として識別するファイルを表示するには、**Enterprise > 高度な脅威イベント** タブに移動します。このタブには、ブロックされた、または終了したなど、企業全体に行った操作のイベント情報のリストが含まれます。

6

トラブルシューティング

Advanced Threat Prevention のリカバリ

リカバリサービス

Advanced Threat Prevention サービスのリカバリには、バックアップの証明書が必要です。

1. 管理コンソールの左ペインで、**管理 > サービス管理**を順にクリックします。
2. **Advanced Threat Prevention サービスのリカバリ**をリカバリします。
3. サービスリカバリのガイドに従って、プロンプトが表示されたら、Advanced Threat Prevention 証明書をアップロードします。

Windows Powershell を使用した製品コードの検索

- この方法を使用すれば、将来製品コードに変更があった場合に、製品コードを容易に見つけることができます。

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

  出力結果は、フルパスと .msi ファイル名（変換された 16 進法のファイル名）となります。

Advanced Threat Prevention

- Advanced Threat Prevention プラグインが、LogVerbosity 値への変更がないか HKLM\SOFTWARE\Dell\Dell Data Protection を監視し、変更に応じてクライアントログのレベルを更新するようにするには、次の値を設定します。

  [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

  レジストリ値は、Advanced Threat Prevention サービスが開始するとき、または値が変化するたびにチェックされます。レジストリ値がない場合は、ログのレベルの変化はありません。

  このレジストリ設定は、Encryption および Encryption Management Agent を含むその他のコンポーネントのログ冗長性を制御するため、テストまたはデバッグ用途にのみ使用してください。

- 互換性モードは、メモリ保護ポリシーまたはメモリー保護ポリシーとスクリプト制御ポリシーの両方が有効になっている際に、クライアントコンピュータでアプリケーションを実行することを可能にします。互換性モードを有効にするには、クライアントコンピュータ上でレジストリ値を追加する必要があります。

  互換性モードを有効にするには、次の手順に従います。

  1. 管理コンソールで、メモリ保護の有効化ポリシーを無効にします。スクリプト制御ポリシーが有効になっている場合は、無効にします。
  2. CompatibilityMode レジストリ値を追加します。
     a. クライアントコンピュータのレジストリエディタを使用して、`HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop` に移動します。

b. **デスクトップ**を右クリックして、**許可** をクリックし、 所有権を得て自分自身にフルコントロールを付与します。
c. **デスクトップ** を右クリックし、**新規 バイナリ値** の順に選択します。
d. 名前には、`CompatibilityMode` と入力します。
e. レジストリの設定を開いて、値を `01` に変更します。
f. **OK** をクリックして、レジストリエディタを閉じます。

コマンドでレジストリ値を追加するには、次のコマンドラインオプションのいずれかを使用して、クライアントコンピュータ上で実行することができます。

- （1 台のコンピュータの場合）Psexec:

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

- （複数のコンピュータの場合）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. 管理コンソールで、メモリ保護の有効化ポリシーを再び有効にします。スクリプト制御ポリシーが前に有効になっていた場合は、再び有効にします。