ワークロードを保護する

NetApp Ransomware Resilience

NetApp
February 17, 2026

目次

ワークロードを保護する . . . 1
NetApp Ransomware Resilience保護戦略でワークロードを保護する . . . 1
ランサムウェア対策戦略を理解する . . . 1
ワークロードのランサムウェア保護を表示する . . . 2
SnapCenterでアプリケーションまたは VM の一貫性のある保護を有効にする . . . 6
ランサムウェア対策戦略を追加する . . . 7
保護グループを作成する . . . 12
ランサムウェア対策戦略の管理 . . . 16
ランサムウェア耐性におけるNetApp Data Classificationで個人を特定できる情報をスキャン . . . 17
データ分類でプライバシーの露出を特定する . . . 17
プライバシーの露出を確認する . . . 18
プライバシーの露出がワークロードの重要性に与える影響 . . . 19
詳細情報 . . . 20

ワークロードを保護する

NetApp Ransomware Resilience保護戦略でワークロードを保護する

NetApp Ransomware Resilienceでワークロード一貫性保護を有効にするか、ランサムウェア保護戦略を作成することにより、ランサムウェア攻撃からワークロードを保護できます。

必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

ランサムウェア対策戦略を理解する

ランサムウェア保護戦略には、検出、保護、および_複製_のポリシーが含まれます。

- 検出ポリシー ランサムウェアの脅威を特定
- 保護ポリシー には、スナップショット ポリシーとバックアップ ポリシーが含まれます。保護戦略には検出およびスナップショット ポリシーが必要です。バックアップ ポリシーはオプションです。

  ワークロードを保護するために他のNetApp製品を使用している場合、Ransomware Resilience はそれらを検出し、次のいずれかのオプションを提供します。

  - ランサムウェア検出ポリシーを使用し、他のNetAppツールによって作成されたスナップショットおよびバックアップポリシーを引き続き使用するか、
  - Ransomware Resilience を使用して、検出、スナップショット、およびバックアップを管理します。
- レプリケーション ポリシー を使用すると、Ransomware Resilience からセカンダリ サイトにスナップショットをレプリケートできます。レプリケーション スケジュールは、時間ごと、日ごと、週ごと、または月ごとの頻度に設定できます。

  現在、スナップショットをレプリケートできるのはオンプレミスのONTAPストレージのみです。

Amazon FSx for NetApp ONTAPおよびAzure NetApp Filesの保護戦略を設定する場合は、"各サービスの制限"を参照してください。

データ資産の管理と保護を強化するために、"グループファイル共有" 1 つの戦略の下でボリュームをまとめて保護します。

他の**NetApp**マネージド サービスとの保護ポリシー

ランサムウェア耐性以外にも、次のサービスを使用して保護を管理できます。

- ファイル共有、VM ファイル共有向けのNetApp Backup and Recovery
- VMデータストア用のSnapCenter for VMware

- Oracle向けSnapCenter

これらのサービスからの保護情報は、Ransomware Resilience に表示されます。 Ransomware Resilience を使用して、これらのサービスに検出ポリシーを追加できます。 Ransomware Resilience を使用して保護ポリシーを追加すると、既存の保護ポリシーが置き換えられます。

ランサムウェア検出ポリシーがONTAPの Autonomous Ransomware Protection（ ONTAP のバージョンに応じて ARP または ARP/AI）と FPolicy によって管理されている場合、それらのワークロードは保護され、引き続き ARP と FPolicy によって管理されます。

> バックアップ先は、Amazon FSx for NetApp ONTAP または Azure NetApp Files のワークロードでは使用できません。FSx for ONTAP バックアップサービスを使用してバックアップ操作を実行します。FSx for ONTAP のワークロードのバックアップポリシーは、Ransomware Resilience ではなく AWS で設定します。バックアップポリシーは Ransomware Resilience に表示され、AWS から変更されません。

NetAppアプリケーションによって保護されていないワークロードの保護ポリシー

ワークロードが Backup and Recovery、Ransomware Resilience、 SnapCenter、またはSnapCenter Plug-in for VMware vSphereによって管理されていない場合は、 ONTAPまたはその他の製品の一部としてスナップショットが取得されている可能性があります。 ONTAP FPolicy 保護が設定されている場合は、 ONTAPを使用して FPolicy 保護を変更できます。

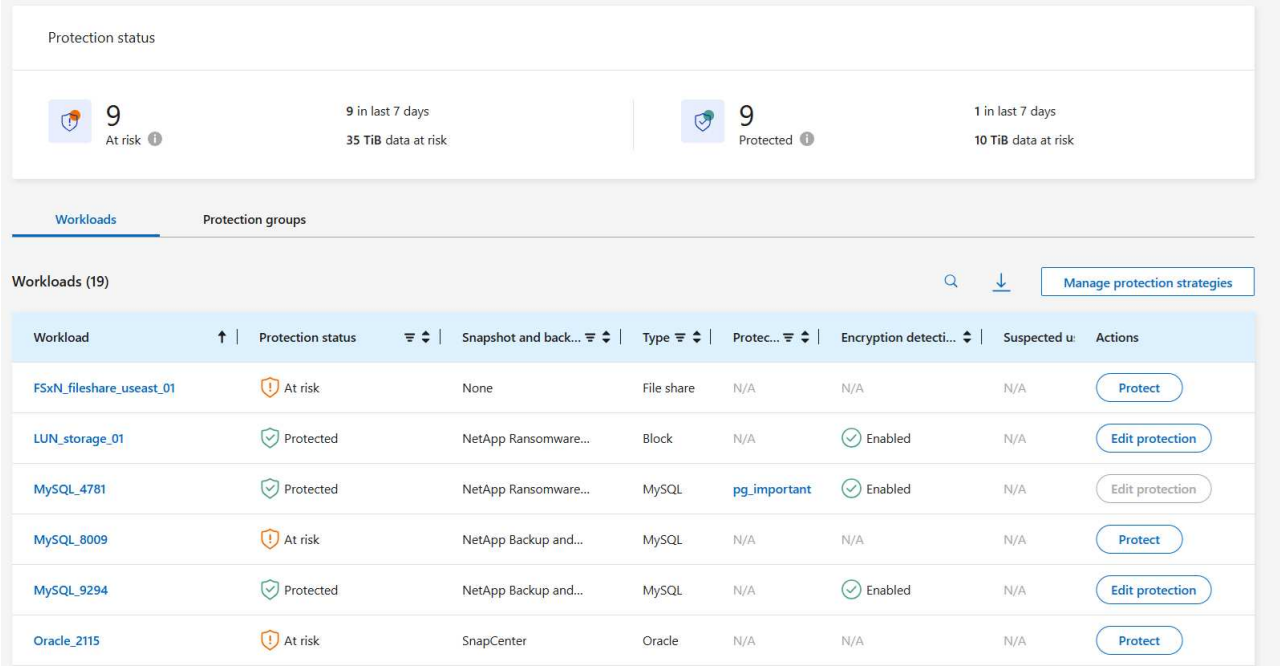
ワークロードのランサムウェア保護を表示する

ワークロードを保護するための最初のステップの 1 つは、現在のワークロードとその保護ステータスを確認することです。次の種類のワークロードを確認できます。

- アプリケーションワークロード
- ブロックワークロード
- ファイル共有ワークロード
- VMワークロード

手順

1. コンソールの左側のナビゲーションから、保護 > *ランサムウェア耐性*を選択します。
2. 次のいずれかを実行します。
    - ダッシュボードの「データ保護」ペインから、「すべて表示」を選択します。
    - メニューから*保護*を選択します。



3. このページから、ワークロードの保護の詳細を表示および変更できます。

> 見る"ランサムウェア対策戦略を追加する"SnapCenterまたは Backup and Recovery で既存の保護ポリシーがある場合に Ransomware Resilience を使用する方法について学習します。

保護ページを理解する

「保護」ページには、ワークロード保護に関する次の情報が表示されます。

保護ステータス: ワークロードは、ポリシーが適用されているかどうかを示す次のいずれかの保護ステータスを示します。

- 保護済み: ポリシーが適用されています。ワークロードに関連するすべてのボリュームで ARP (またはONTAPバージョンに応じて ARP/AI) が有効になっています。
- リスクあり: ポリシーは適用されません。ワークロードでプライマリ検出ポリシーが有効になっていない場合、スナップショットおよびバックアップ ポリシーが有効になっていても、ワークロードは「危険にさらされている」状態になります。
- 進行中: ポリシーは適用中ですが、まだ完了していません。
- 失敗: ポリシーは適用されましたが、機能していません。

検出ステータス: ワークロードは、次のいずれかのランサムウェア検出ステータスになります。

- 学習中: ランサムウェア検出ポリシーが最近ワークロードに割り当てられ、ランサムウェア耐性がワークロードをスキャンしています。
- アクティブ: ランサムウェア検出保護ポリシーが割り当てられています。
- 未設定: ランサムウェア検出保護ポリシーが割り当てられていません。
- エラー: ランサムウェア検出ポリシーが割り当てられましたが、Ransomware Resilience でエラーが発生しました。

ランサムウェア耐性で保護が有効になっている場合、ランサムウェア検出ポリシーのステータスが学習モードからアクティブ モードに変更された後に、アラートの検出とレポートが開始されます。

疑わしいユーザー行動アクティビティと FPolicy (疑わしいファイル拡張子) アクティビティは、検出ステータスとは別に表示されます。

検出ポリシー: ランサムウェア検出ポリシーが割り当てられている場合は、そのポリシーの名前が表示されます。検出ポリシーが割り当てられていない場合は、「N/A」と表示されます。

レプリケーション先: スナップショット レプリケーションを構成している場合は、宛先ストレージ VM とシステムの名前が一覧表示されます。レプリケーションがない場合、このフィールドには「なし」と表示されます。

スナップショットおよびバックアップ ポリシー: この列には、ワークロードに適用されているスナップショットおよびバックアップ ポリシーと、それらのポリシーを管理している製品またはサービスが表示されます。

- SnapCenterによる管理
- SnapCenter Plug-in for VMware vSphereによって管理されます
- バックアップとリカバリによって管理
- スナップショットとバックアップを管理するランサムウェア保護ポリシーの名前
- なし

ワークロードの重要度

ランサムウェア耐性は、各ワークロードの分析に基づいて、検出中に各ワークロードに重要度または優先度を割り当てます。ワークロードの重要度は、次のスナップショット頻度によって決まります。

- 重大: 1 時間あたり 1 回以上のスナップショット コピーが作成される (非常に積極的な保護スケジュール)
- 重要: スナップショットのコピーは、1時間ごとよりも頻度は低いですが、毎日よりも頻繁に作成されます。
- 標準: スナップショットコピーは1日に複数回作成されます

定義済みの検出ポリシー

ワークロードの重要度に合わせて、次のランサムウェア耐性定義済みポリシーのいずれかを選択できます。

暗号化ユーザー拡張 ポリシーは、疑わしいユーザーの動作の検出をサポートする唯一の定義済みポリシーです。

+ クリティカル レプリケーション ポリシー は、 ONTAPへのスナップショットのレプリケーションをサポートする唯一の定義済みポリシーです。

ポリシーレベル	**Snapshot**	頻度	保持期間（日数）	スナップショットコピーの数	スナップショットコピーの最大数
重要なワークロードポリシー	15分ごと	15分ごと	3	288	309
	日次	1日ごと	14	14	309
	週次	1週間ごと	35	5	309
	毎月	30日ごと	60	2	309
重要なワークロードポリシー	15分ごと	30分ごと	3	144	165
	日次	1日ごと	14	14	165
	週次	1週間ごと	35	5	165
	毎月	30日ごと	60	2	165
標準作業負荷ポリシー	15分ごと	30分ごと	3	72	93
	日次	1日ごと	14	14	93
	週次	1週間ごと	35	5	93
	毎月	30日ごと	60	2	93
暗号化ユーザー拡張機能	15分ごと	30分ごと	3	72	93
	日次	1日ごと	14	14	93
	週次	1週間ごと	35	5	93
	毎月	30日ごと	60	2	93
暗号化ユーザー拡張機能	15分ごと	30分ごと	3	72	93
	日次	1日ごと	14	14	93
	週次	1週間ごと	35	5	93
	毎月	30日ごと	60	2	93

ポリシーレベル	Snapshot	頻度	保持期間（日数）	スナップショットコピーの数	スナップショットコピーの最大数
重要なレプリケーションポリシー	15分ごと	15分ごと	3	288	309
	日次	1日ごと	14	14	309
	週次	1週間ごと	35	5	309
	毎月	30日ごと	60	2	309

SnapCenterでアプリケーションまたは VM の一貫性のある保護を有効にする

アプリケーションまたは VM の一貫性のある保護を有効にすると、アプリケーションまたは VM のワークロードを一貫した方法で保護し、静止状態と一貫性のある状態を実現して、後で回復が必要になった場合にデータ損失の可能性を回避することができます。

このプロセスは、バックアップとリカバリを使用して、アプリケーション用のSnapCenterソフトウェア サーバまたは VM 用の SnapCenter Plug-in for VMware vSphereの登録を開始します。

ワークロード一貫性保護を有効にした後、Ransomware Resilience で保護戦略を管理できます。保護戦略には、Ransomware Resilience で管理されるランサムウェア検出ポリシーに加えて、他の場所で管理されるスナップショットおよびバックアップ ポリシーが含まれます。

バックアップとリカバリを使用してSnapCenterまたはSnapCenter Plug-in for VMware vSphereを登録する方法については、次の情報を参照してください。

- "SnapCenter Serverソフトウェアの登録"
- "SnapCenter Plug-in for VMware vSphereを登録する"

手順

1. ランサムウェア耐性メニューから、*ダッシュボード*を選択します。
2. [推奨事項] ペインで、次のいずれかの推奨事項を見つけて、[確認して修正] を選択します。
    - 利用可能なSnapCenter ServerをNetApp Consoleに登録する
    - 利用可能なSnapCenter Plug-in for VMware vSphere (SCV) をNetApp Consoleに登録します。
3. 情報に従って、バックアップとリカバリを使用してSnapCenterまたはSnapCenter Plug-in for VMware vSphereに登録します。
4. ランサムウェア耐性に戻ります。
5. ランサムウェア耐性からダッシュボードに移動し、検出プロセスを再度開始します。
6. ランサムウェア耐性から、保護 を選択して、保護ページを表示します。
7. [保護] ページのスナップショットおよびバックアップ ポリシー列の詳細を確認し、ポリシーが他の場所で管理されていることを確認します。

ランサムウェア対策戦略を追加する

ランサムウェア保護戦略を追加するには、次の 3 つのアプローチがあります。

- スナップショットまたはバックアップ ポリシーがない場合は、ランサムウェア保護戦略を作成します。

  ランサムウェア保護戦略には以下が含まれます。

  - スナップショットポリシー
  - ランサムウェア検出ポリシー
  - バックアップ ポリシー
- **SnapCenter**またはバックアップとリカバリ保護の既存のスナップショットまたはバックアップ ポリシーを、**Ransomware Resilience** によって管理される保護戦略に置き換えます。

  ランサムウェア保護戦略には以下が含まれます。

  - スナップショットポリシー
  - ランサムウェア検出ポリシー
  - バックアップ ポリシー
- 他の**NetApp**製品またはサービスで管理されている既存のスナップショットおよびバックアップ ポリシーを使用して、ワークロードの検出ポリシーを作成します。

  検出ポリシーは、他の製品で管理されているポリシーを変更するものではありません。

  検出ポリシーは、他のサービスですでに有効になっている場合、自律ランサムウェア保護と FPolicy 保護を有効にします。詳細はこちら"自律型ランサムウェア対策"、"バックアップとリカバリ" 、 そして"ONTAP FPolicy"。

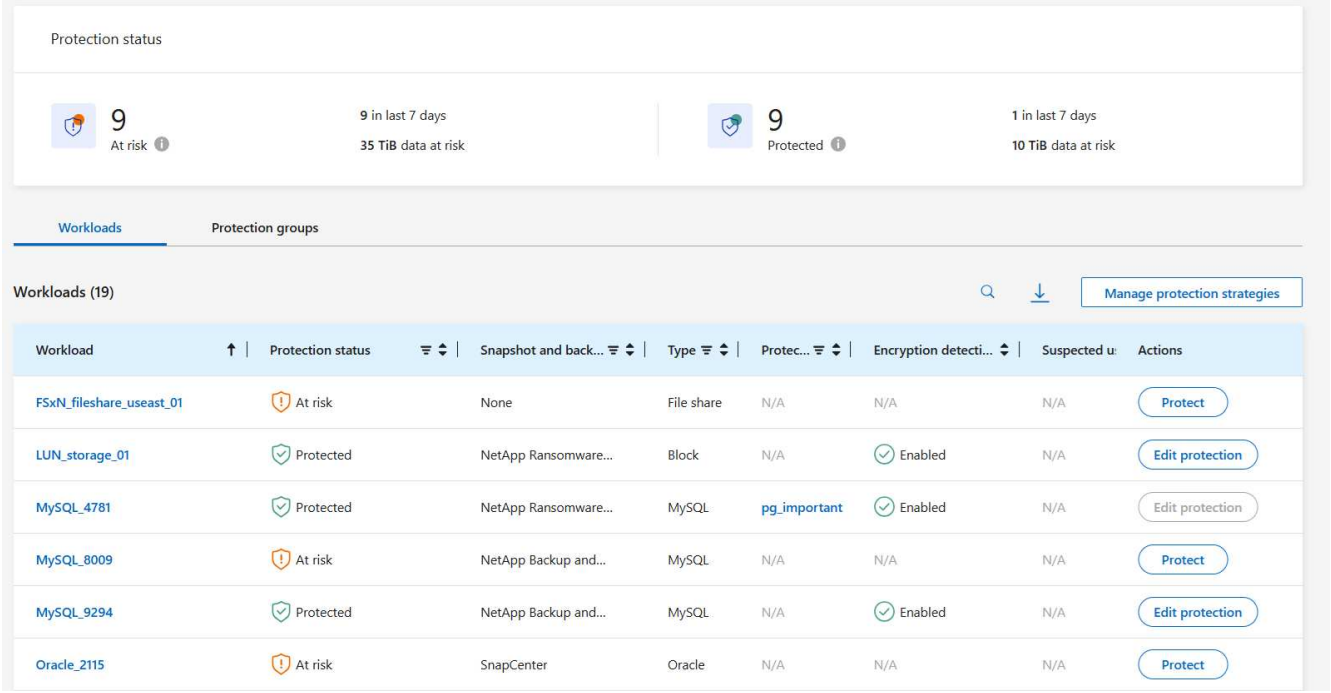
ランサムウェア対策戦略を作成する（スナップショットやバックアップポリシーがない場合）

ワークロードにスナップショットまたはバックアップ ポリシーが存在しない場合は、ランサムウェア保護戦略を作成できます。これには、Ransomware Resilience で作成する次のポリシーを含めることができます。

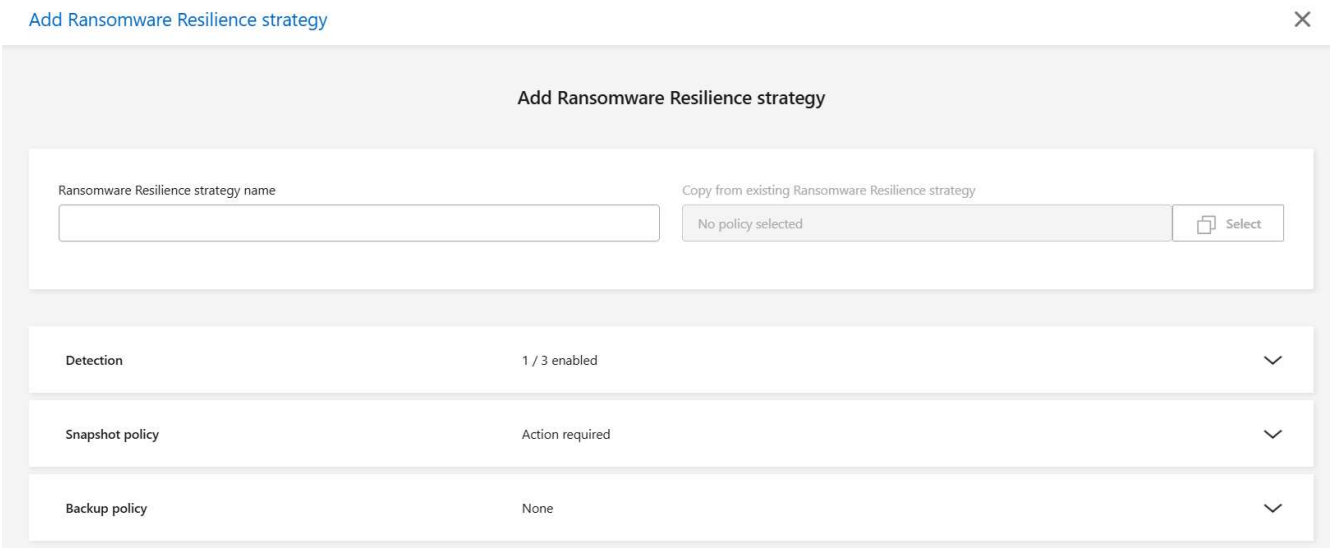
- スナップショットポリシー
- バックアップ ポリシー
- ランサムウェア検出ポリシー
- ONTAPへのセカンダリレプリケーション

ランサムウェア対策戦略を作成する手順

1. ランサムウェア耐性メニューから、*保護*を選択します。



2. [保護] ページでワークロードを選択し、[保護] を選択します。
3. ランサムウェア保護戦略ページで、[追加] を選択します。



4. 新しい戦略名を入力するか、既存の名前を入力してコピーします。既存の名前を入力する場合は、コピーする名前を選択し、「コピー」を選択します。

> 既存の戦略をコピーして変更することを選択した場合、Ransomware Resilience は元の名前に「_copy」を追加します。名前と少なくとも 1 つの設定を変更して、一意の名前にする必要があります。

5. 各項目について、*下矢印*を選択します。
   - 検出ポリシー:
     - ポリシー: 事前に設計された検出ポリシーの 1 つを選択します。

- 一次検出: ランサムウェア耐性を有効にして、潜在的なランサムウェア攻撃を検出します。
- 疑わしいユーザー行動の検出: ユーザー行動の検出を有効にすると、ユーザーアクティビティイベントが Ransomware Resilience に送信され、データ侵害などの疑わしいイベントが検出されます。
- ファイル拡張子をブロック: ランサムウェア耐性を有効にして、既知の疑わしいファイル拡張子をブロックします。ランサムウェア耐性は、プライマリ検出が有効になっている場合に自動スナップショット コピーを作成します。

  ブロックされたファイル拡張子を変更する場合は、System Manager で編集します。

◦ スナップショットポリシー:

- スナップショット ポリシー ベース名: ポリシーを選択するか、作成 を選択してスナップショットポリシーの名前を入力します。
- スナップショットのロック: これを有効にすると、プライマリ ストレージ上のスナップショットコピーがロックされ、ランサムウェア攻撃がバックアップ ストレージの保存先に侵入した場合でも、一定期間スナップショット コピーを変更または削除できなくなります。これは、_不変ストレージ_とも呼ばれます。これにより、復元時間が短縮されます。

  スナップショットがロックされている場合、ボリュームの有効期限はスナップショット コピーの有効期限に設定されます。

スナップショット コピー ロックは、 ONTAP 9.12.1 以降で使用できます。 SnapLockの詳細については、以下を参照してください。 "ONTAPのSnapLock" 。

◦ スナップショット スケジュール: スケジュール オプション、保持するスナップショット コピーの数を選択し、スケジュールを有効にするかどうかを選択します。

- レプリケーションポリシー:

◦ レプリケーション ポリシーのベース名: 新しい名前を入力するか、既存の名前を選択します。ベース名は、すべてのスナップショットに追加されるプレフィックスです。

◦ レプリケーション スケジュール: 有効にする頻度 (時間別、日次、週次、月次) を切り替え、有効にするスケジュールごとに保持値 (保持する複製スナップショットの数) を設定します。

- バックアップポリシー:

◦ バックアップ ポリシーのベース名: 新しい名前を入力するか、既存の名前を選択します。

◦ バックアップ スケジュール: セカンダリ ストレージのスケジュール オプションを選択し、スケジュールを有効にします。

> セカンダリ ストレージでバックアップ ロックを有効にするには、[設定] オプションを使用してバックアップの保存先を構成します。詳細については、 "設定を構成する" 。

6. *追加*を選択します。

SnapCenterまたは **Backup and Recovery** によって管理されている既存のスナップショットおよびバックアップ ポリシーを使用して、ワークロードに検出ポリシーを追加します。

ランサムウェア耐性により、他のNetApp製品またはサービスで管理されている既存のスナップショットおよびバックアップ保護を使用して、ワークロードに検出ポリシーまたは保護ポリシーのいずれかを割り当てることができます。 Backup and Recovery やSnapCenterなどの他のサービスでは、スナップショット、セカンダ

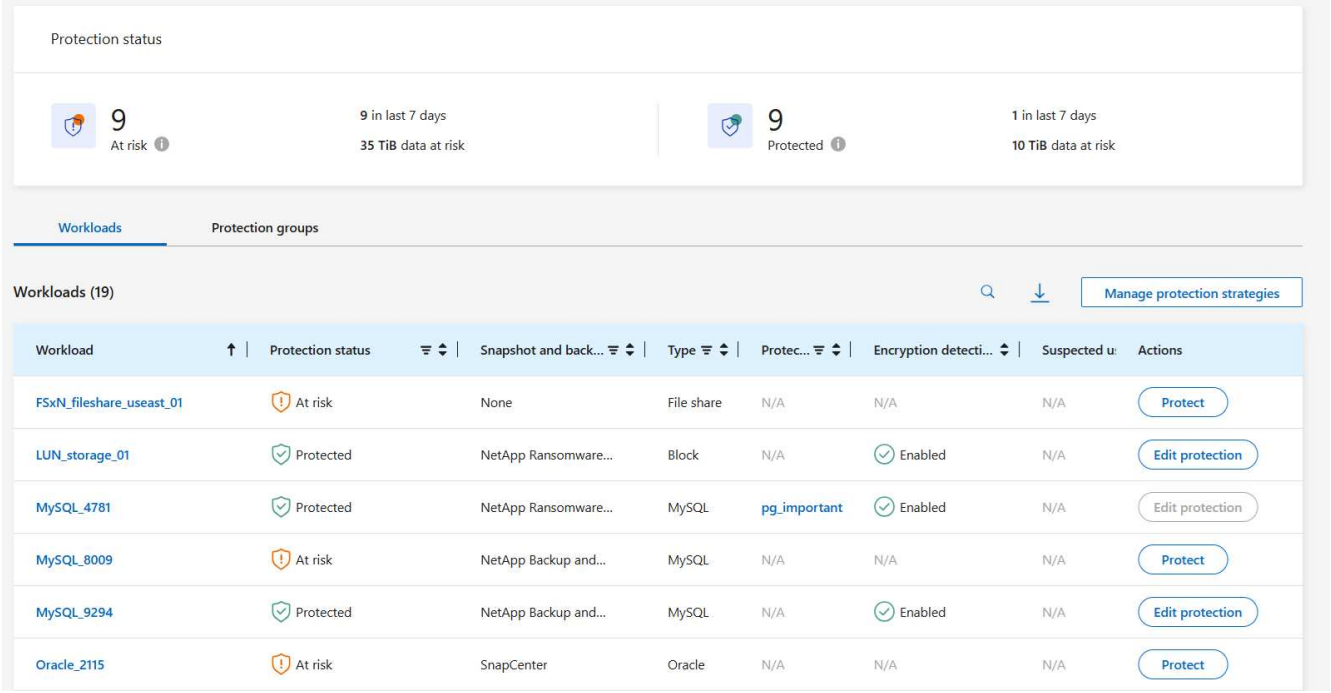
リ ストレージへのレプリケーション、またはオブジェクト ストレージへのバックアップを管理するポリシーを使用します。

既存のバックアップまたはスナップショット ポリシーを持つワークロードに検出ポリシーを追加する

Backup and Recovery またはSnapCenterで既存のスナップショットまたはバックアップ ポリシーがある場合は、ランサムウェア攻撃を検出するポリシーを追加できます。ランサムウェア耐性による保護と検出を管理するには、以下を参照してください。ランサムウェア耐性で保護 。

手順

1. ランサムウェア耐性メニューから、*保護*を選択します。



2. [保護] ページでワークロードを選択し、[保護] を選択します。
3. Ransomware Resilience は、アクティブなSnapCenterまたはバックアップとリカバリ ポリシーが存在しているかどうかを検出します。
4. 既存のバックアップとリカバリまたはSnapCenterポリシーをそのままにして、検出 ポリシーのみを適用するには、[既存のポリシーを置き換える] ボックスをオフのままにします。
5. SnapCenterポリシーの詳細を表示するには、*下矢印*を選択します。
6. 必要な検出設定を選択します：

```
*Encryption detection*
*Suspicious user behavior detection*
*Block suspicious file extensions*
```

7. 次へを選択します。
8. 検出設定として*不審なユーザー行動の検出*を選択した場合は、ユーザーアクティビティエージェントまたは"または作成する"を選択します。

ユーザー アクティビティ エージェントは新しいデータ コレクターをホストします。Ransomware Resilience は、データ コレクターを自動的に作成し、ユーザー アクティビティ イベントを Ransomware Resilience に送信して、異常なユーザー動作を検出します。

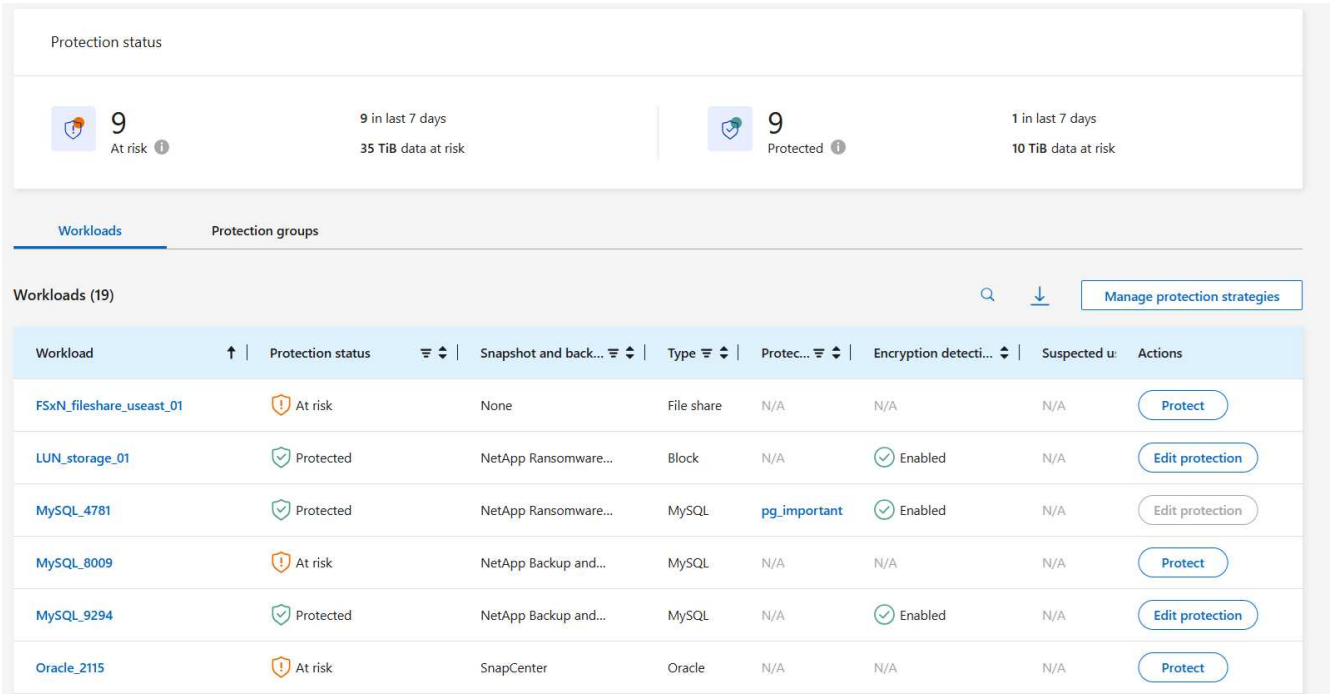
9. 次へを選択します。
10. 選択内容を確認します。検出を有効にするには、[作成] を選択します。
11. [保護] ページで、検出ステータス を確認して、検出がアクティブであることを確認します。

既存のバックアップまたはスナップショットポリシーをランサムウェア保護戦略に置き換える

既存のバックアップまたはスナップショット ポリシーをランサムウェア保護戦略に置き換えることができます。このアプローチでは、外部で管理されている保護を削除し、Ransomware Resilience で検出と保護を構成します。

手順

1. ランサムウェア耐性メニューから、*保護*を選択します。



2. [保護] ページでワークロードを選択し、[保護] を選択します。
3. Ransomware Resilience は、アクティブなバックアップとリカバリ、またはSnapCenterポリシーが既に存在するかどうかを検出します。既存のバックアップとリカバリまたはSnapCenterポリシーを置き換えるには、[既存のポリシーを置き換える] ボックスを選択します。ボックスを選択すると、Ransomware Resilience によって検出ポリシーのリストが検出ポリシーに置き換えられます。
4. 保護ポリシーを選択します。保護ポリシーが存在しない場合は、[追加] を選択して新しいポリシーを作成します。ポリシーの作成方法については、以下を参照してください。保護ポリシーを作成する 。次へを選択します。
5. 戦略にレプリケーションが含まれている場合は、宛先システム と 宛先ストレージ **VM** を選択します。次へを選択します。
6. バックアップ先を選択するか、新しいバックアップ先を作成します。次へを選択します。

a. 保護戦略にユーザー行動の検出が含まれている場合は、環境内でユーザー アクティビティ エージェントを選択して、新しいデータ コレクターをホストします。Ransomware Resilience は、データ コレクターを自動的に作成し、ユーザー アクティビティ イベントを Ransomware Resilience に送信して、異常なユーザー動作を検出します。

7. 新しい保護戦略を確認し、[保護] を選択して適用します。
8. [保護] ページで、検出ステータス を確認して、検出がアクティブであることを確認します。

別のポリシーを割り当てる

既存のポリシーを別のポリシーに置き換えることができます。

手順

1. ランサムウェア耐性メニューから、*保護*を選択します。
2. [保護] ページのワークロード行で、[保護の編集] を選択します。
3. ワークロードに、維持する既存のバックアップとリカバリまたはSnapCenterポリシーがある場合は、[既存のポリシーを置き換える] のチェックを外します。既存のポリシーを置き換えるには、[既存のポリシーを置き換える] をオンにします。
4. 「ポリシー」ページで、割り当てるポリシーの下矢印を選択して詳細を確認します。
5. 割り当てるポリシーを選択します。
6. 変更を完了するには、[保護] を選択します。

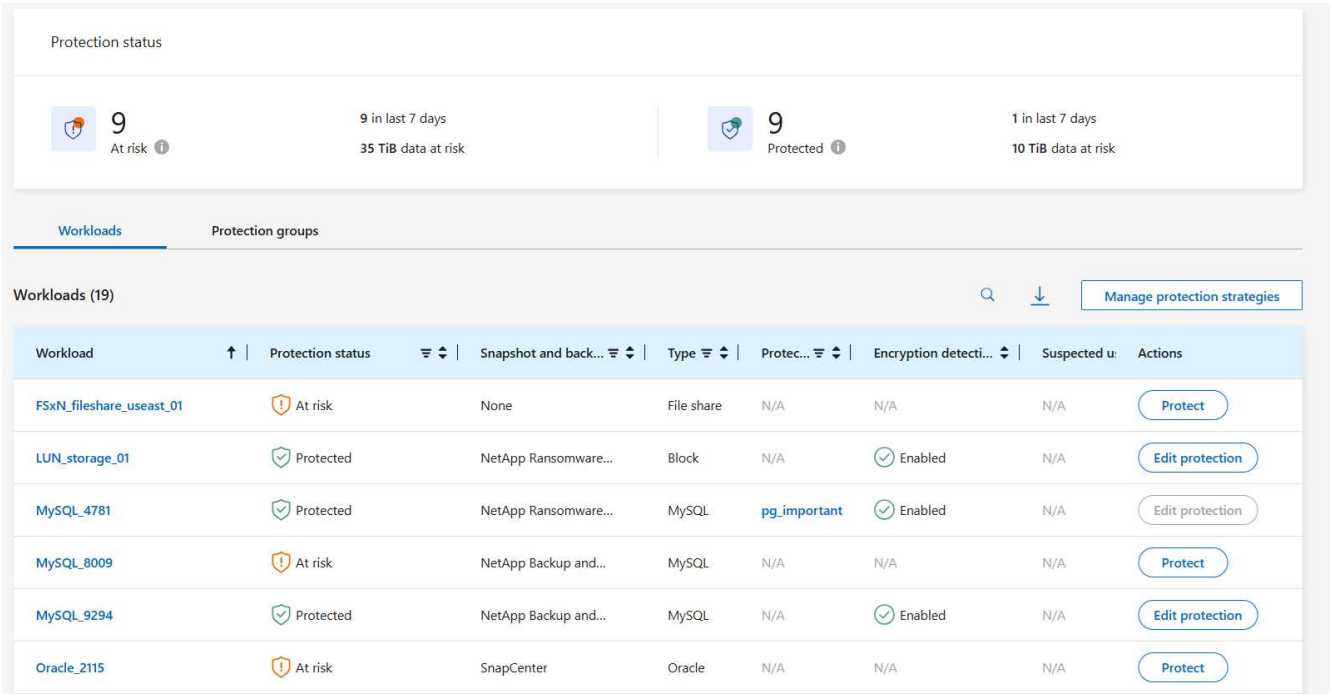
保護グループを作成する

保護グループ内のファイル共有をグループ化すると、データ資産の保護が容易になります。 Ransomware Resilience では、各ボリュームを個別に保護するのではなく、グループ内のすべてのボリュームを同時に保護できます。

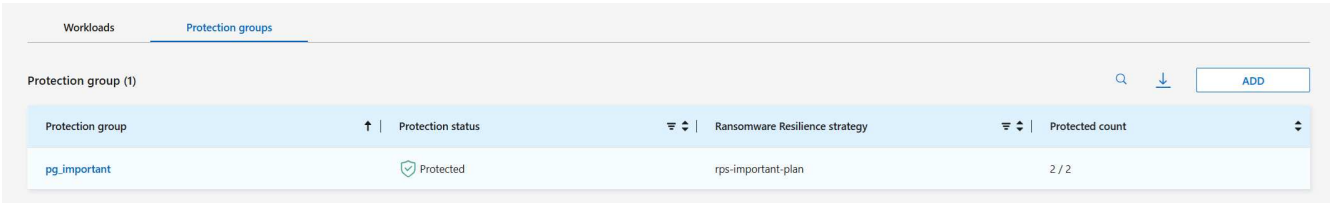
保護ステータスに関係なく (つまり、保護されていないグループと保護されているグループ)、グループを作成できます。保護グループに保護ポリシーを追加すると、 SnapCenterおよびNetApp Backup and Recoveryによって管理されるポリシーを含む既存のポリシーが新しい保護ポリシーに置き換えられます。

手順

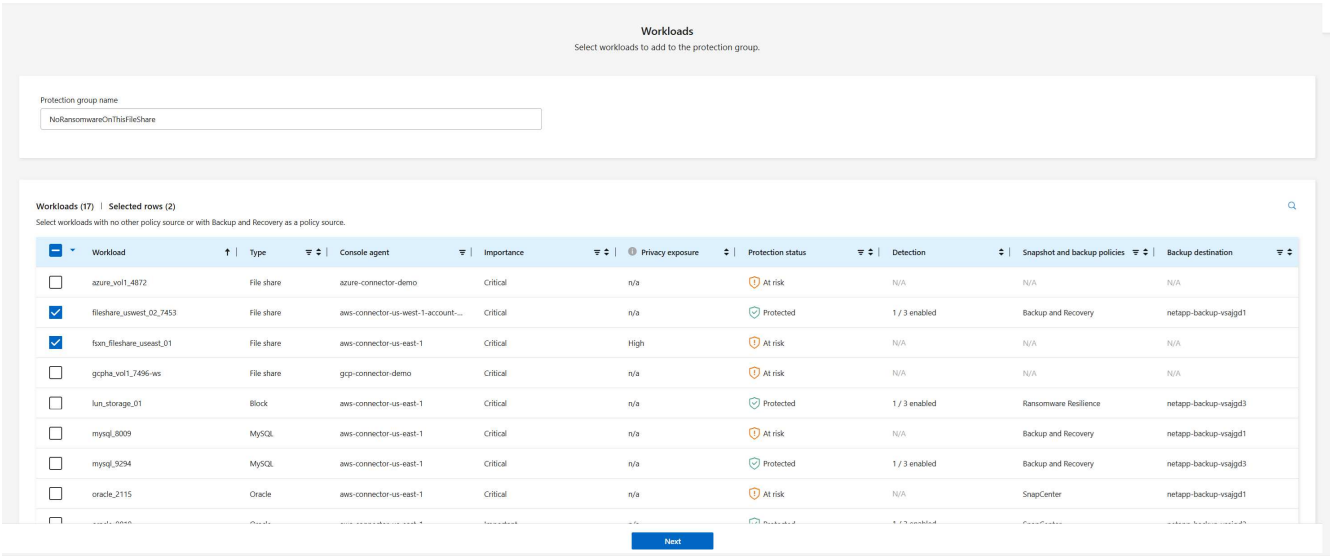
1. ランサムウェア耐性メニューから、*保護*を選択します。



2. [保護] ページで、[保護グループ] タブを選択します。



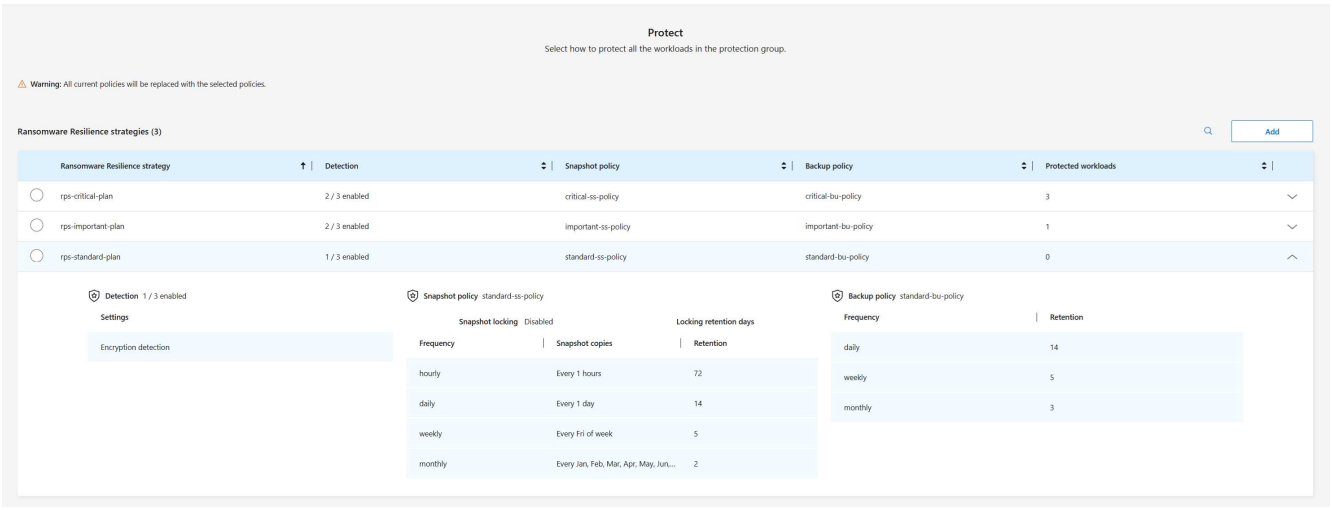
3. *追加*を選択します。



4. 保護グループの名前を入力します。
5. グループに追加するワークロードを選択します。

ワークロードの詳細を表示するには、右にスクロールします。

6. *次へ*を選択します。



7. このグループの保護を管理するポリシーを選択します。
8. 保護戦略にレプリケーションが含まれている場合は、レプリケーション設定を確認します。
   a. すべてのスナップショットを同じ宛先に複製するには、各ワークロードに同じ宛先を使用する をオンにします。コンソール エージェント セクションのワークロードに対して、宛先システム と 宛先ストレージ **VM** を選択します。+ 別の宛先を使用するには、そのボックスのチェックを外します。各コンソール エージェントの下の各ワークロードを確認し、各ワークロードに 宛先システム と 宛先ストレージ **VM** を割り当てます。次へを選択します。
9. バックアップ ポリシーを構成するには、いずれかを選択して [次へ] を選択します。
10. 検出ポリシーにユーザー行動の検出が含まれている場合は、使用するデータ コレクターを選択し、[次へ] をクリックします。
11. 保護グループの選択内容を確認します。
12. 保護グループの作成を完了するには、[追加] を選択します。

グループ保護を編集

既存のグループの検出ポリシーを変更できます。

手順

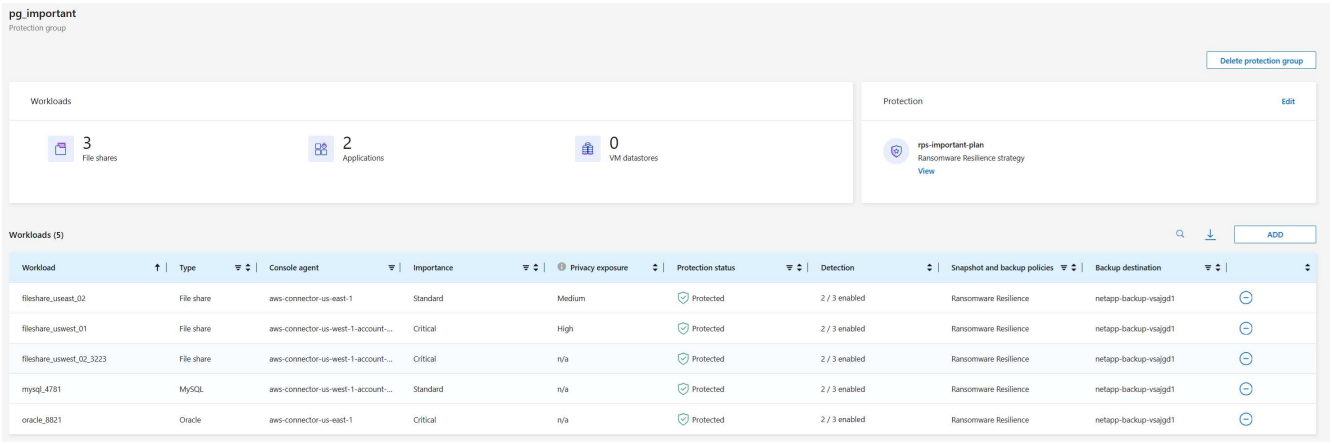
1. ランサムウェア耐性メニューから、*保護*を選択します。
2. [保護] ページで [保護グループ] タブを選択し、ポリシーを変更するグループを選択します。
3. 保護グループの概要ページで、*保護の編集*を選択します。
4. 適用する既存の保護ポリシーを選択するか、[追加] を選択して新しい保護ポリシーを作成します。保護ポリシーの追加の詳細については、以下を参照してください。保護ポリシーを作成する 。次に、[保存] を選択します。
5. バックアップ先の概要で、既存のバックアップ先を選択するか、新しいバックアップ先を追加します。
6. 変更内容を確認するには、[次へ] を選択します。

グループからワークロードを削除する

後で既存のグループからワークロードを削除する必要がある場合があります。

手順

1. ランサムウェア耐性メニューから、*保護*を選択します。
2. [保護] ページで、[保護グループ] タブを選択します。
3. 1 つ以上のワークロードを削除するグループを選択します。



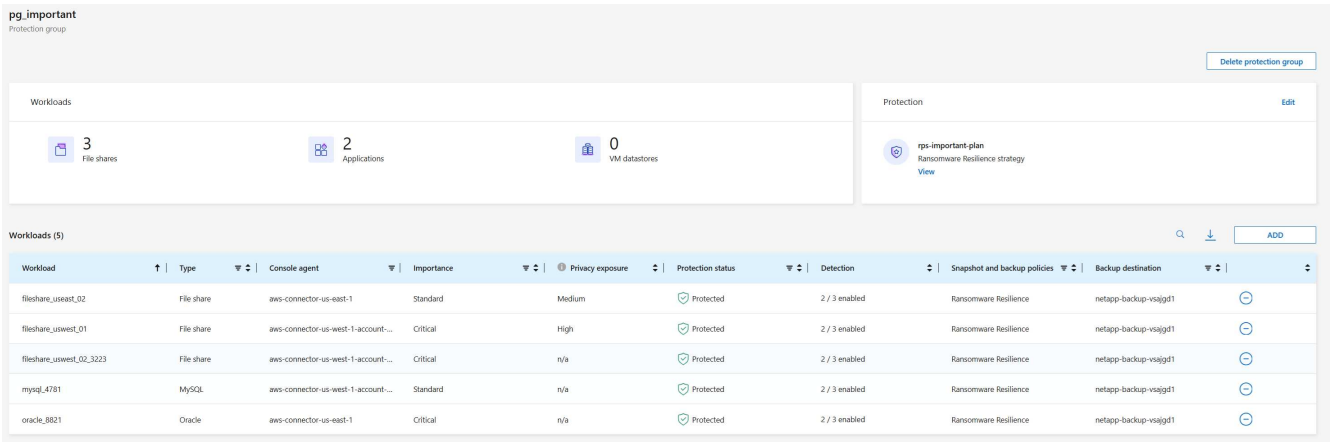
4. 選択した保護グループのページで、グループから削除するワークロードを選択し、*アクション*を選択します。 •••オプション。
5. [アクション] メニューから、[ワークロードの削除] を選択します。
6. ワークロードを削除することを確認し、[削除] を選択します。

保護グループを削除する

保護グループを削除すると、グループとその保護は削除されますが、個々のワークロードは削除されません。

手順

1. ランサムウェア耐性メニューから、*保護*を選択します。
2. [保護] ページで、[保護グループ] タブを選択します。
3. 1 つ以上のワークロードを削除するグループを選択します。



4. 選択した保護グループのページの右上にある [保護グループの削除] を選択します。
5. グループを削除することを確認し、[削除] を選択します。

ランサムウェア対策戦略の管理

ランサムウェア戦略を削除することができます。

ランサムウェア保護戦略によって保護されているワークロードを表示する

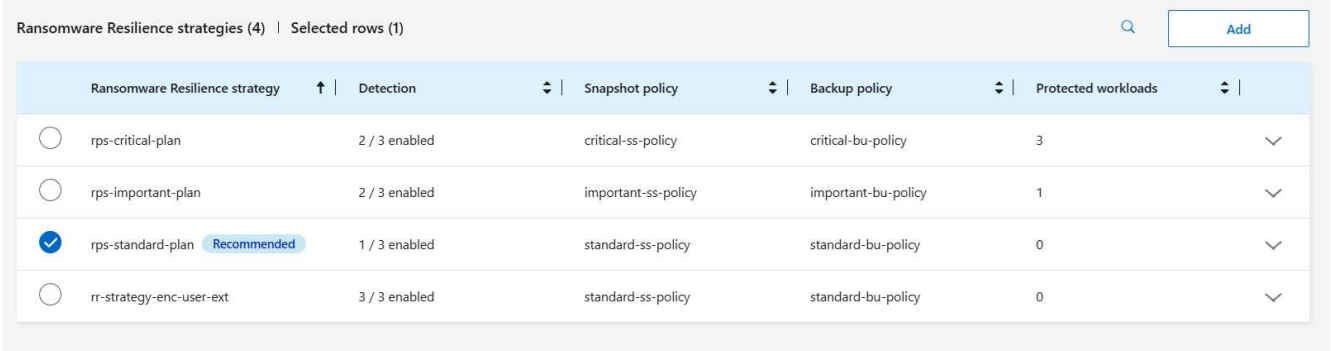
ランサムウェア保護戦略を削除する前に、その戦略によって保護されているワークロードを確認することをお勧めします。

ワークロードは、戦略のリストから、または特定の戦略を編集しているときに表示できます。

戦略を表示する手順

1. ランサムウェア耐性メニューから、*保護*を選択します。
2. [保護] ページで、[保護戦略の管理] を選択します。

   ランサムウェア保護戦略ページには、戦略のリストが表示されます。



3. 「ランサムウェア保護戦略」ページの「保護されたワークロード」列で、行の末尾にある下矢印を選択します。

ランサムウェア対策戦略を削除する

現在どのワークロードにも関連付けられていない保護戦略を削除できます。

手順

1. ランサムウェア耐性メニューから、*保護*を選択します。
2. [保護] ページで、[保護戦略の管理] を選択します。
3. 戦略管理ページで*アクション*を選択します…削除する戦略のオプションを選択します。
4. [アクション] メニューから、[ポリシーの削除] を選択します。

ランサムウェア耐性における**NetApp Data Classification**で個人を特定できる情報をスキャン

NetApp Ransomware Resilienceでは、 NetApp Data Classificationを使用して、ファイル共有ワークロード内のデータをスキャンおよび分類できます。データを分類すると、データセットに個人を特定できる情報 (PII) が含まれているかどうかを判断するのに役立ちますが、これによりセキュリティ リスクが増大する可能性があります。データ分類はNetApp Consoleのコア コンポーネントであり、追加費用なしで利用できます。

"データ分類"AI 駆動型の自然言語処理を利用してコンテキスト データの分析と分類を行い、データに関する実用的な分析情報を提供することで、コンプライアンス要件への対応、セキュリティの脆弱性の検出、コストの最適化、移行の加速を実現します。

このプロセスはワークロードの重要性に影響を与え、適切な保護が確保されるようにするのに役立ちます。

必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

データ分類でプライバシーの露出を特定する

ランサムウェア耐性におけるデータ分類を使用する前に、"データ分類を有効にしてデータをスキャンする" 。

ランサムウェア耐性の保護ページ内でデータ分類を展開できます。プライバシーの露出を特定するには、手順に従ってください。 **[露出を特定]** を選択すると、データ分類をまだ展開していない場合は、ダイアログが表示され、データ分類を有効にできます。

データ分類の詳細については、以下を参照してください。

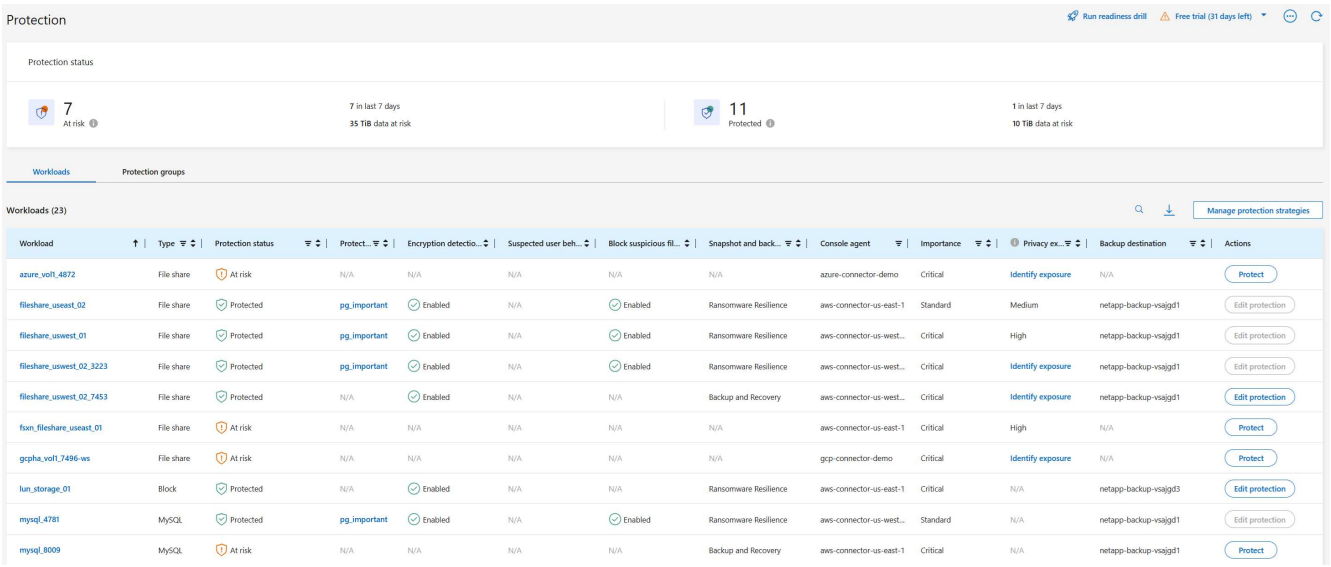
- "データ分類について学ぶ"
- "個人データのカテゴリ"
- "組織内に保存されているデータを調査する"

開始する前に

ランサムウェア耐性におけるPIIデータのスキャンは、以下の場合に利用可能です。"展開されたデータ分類" 。データ分類はコンソールの一部として追加料金なしで利用でき、オンプレミスまたは顧客のクラウドに導入できます。

手順

1. ランサムウェア耐性メニューから、*保護*を選択します。
2. [保護] ページの [ワークロード] 列で、ファイル共有ワークロードを見つけます。



3. データ分類を有効にしてデータの PII をスキャンするには、[プライバシーの露出] 列で [露出を特定] を選択します。

> データ分類を展開していない場合は、「露出を特定」を選択すると、データ分類を展開するためのダイアログが開きます。 デプロイ*を選択します。データ分類を展開した後、保護ページに戻り、「*露出の特定」を選択できます。

結果

ファイルのサイズと数によっては、スキャンに数分かかる場合があります。スキャン中、保護ページにはファイルが識別されていることが示され、ファイル数が表示されます。スキャンが完了すると、プライバシー露出列に露出レベルが「低」、「中」、「高」と評価されます。

プライバシーの露出を確認する

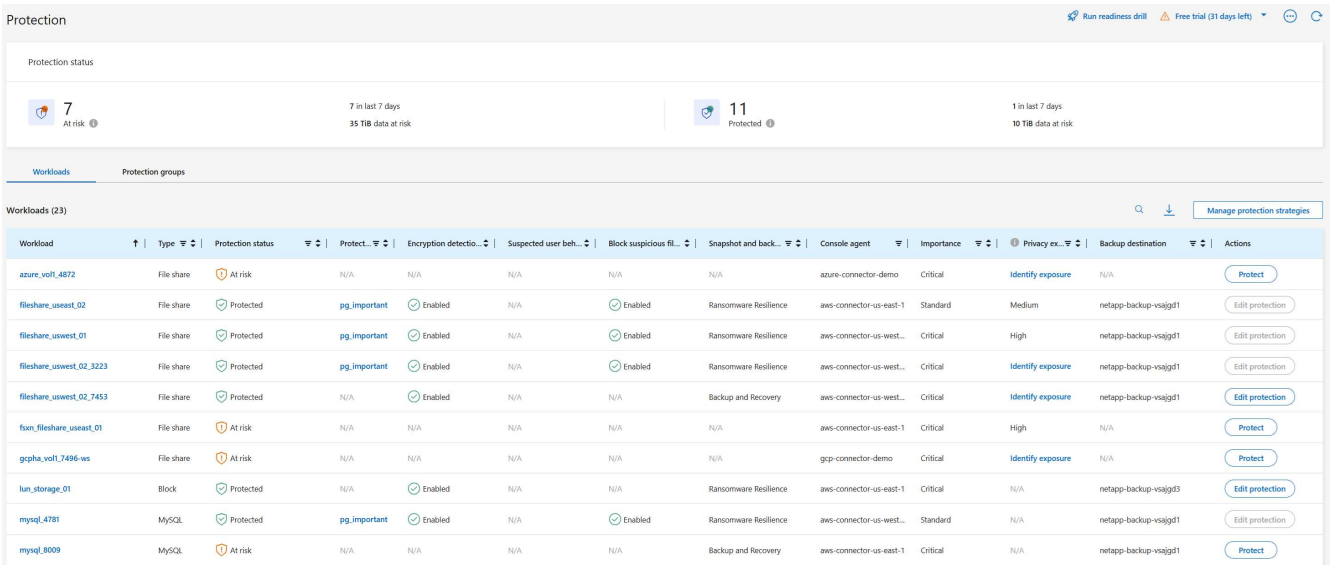
データ分類で PII をスキャンした後、リスクを評価します。

PII データは、次の 3 つの指定のいずれかに分類されます。

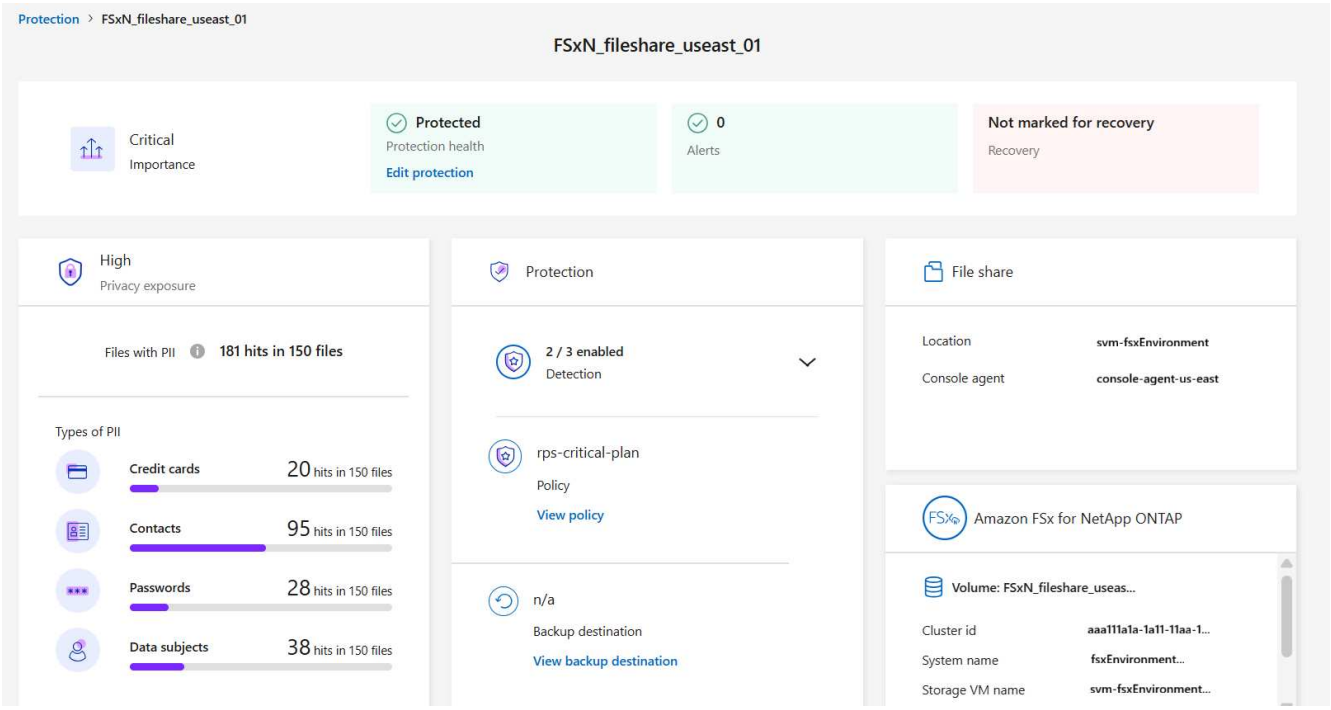
- 高: ファイルの 70% 以上に PII が含まれています
- 中: ファイルの 30% 以上 70% 未満に PII が含まれています
- 低: ファイルの 0% 以上 30% 未満に PII が含まれています

手順

1. ランサムウェア耐性メニューから、*保護*を選択します。
2. [保護] ページで、[プライバシーの公開] 列にステータスが表示されている [ワークロード] 列のファイル共有ワークロードを見つけます。



3. ワークロードの詳細を表示するには、「ワークロード」列のワークロード リンクを選択します。



4. ワークロードの詳細ページで、プライバシーの公開タイルの詳細を確認します。

プライバシーの露出がワークロードの重要性に与える影響

プライバシー露出の変化は、ワークロードの重要性に影響を及ぼす可能性があります。

プライバシーが露出した場合:	このプライバシーの露出から:	このプライバシーの露出について:	次に、ワークロードの重要度は次のようになります。
減少	高、中、低	中、低、またはなし	同じまま

プライバシーが露出した場合:	このプライバシーの露出から:	このプライバシーの露出について:	次に、ワークロードの重要度は次のようになります。
増加	なし	低	標準のまま
	低	中	標準から重要への変更
	低または中	高	標準または重要から重大への変更

詳細情報

データ分類の詳細については、データ分類のドキュメントを参照してください。

- "データ分類について学ぶ"
- "個人データのカテゴリ"
- "組織内に保存されているデータを調査する"