保護と検出

NetApp Ransomware Resilience

NetApp
April 13, 2026

目次

保護と検出

NetApp Ransomware Resilienceで保護ステータスを確認する

NetApp Ransomware Resilience の保護ダッシュボードには、ワークロードの保護ステータスと準備状況の概要が表示されます。保護ダッシュボードを使用すると、保護されているもの、保護が必要なもの、保護の範囲についての情報を得ることができます。

現在の保護の範囲を理解したら、"ランサムウェア保護戦略を作成し、ワークロードに適用できます"。

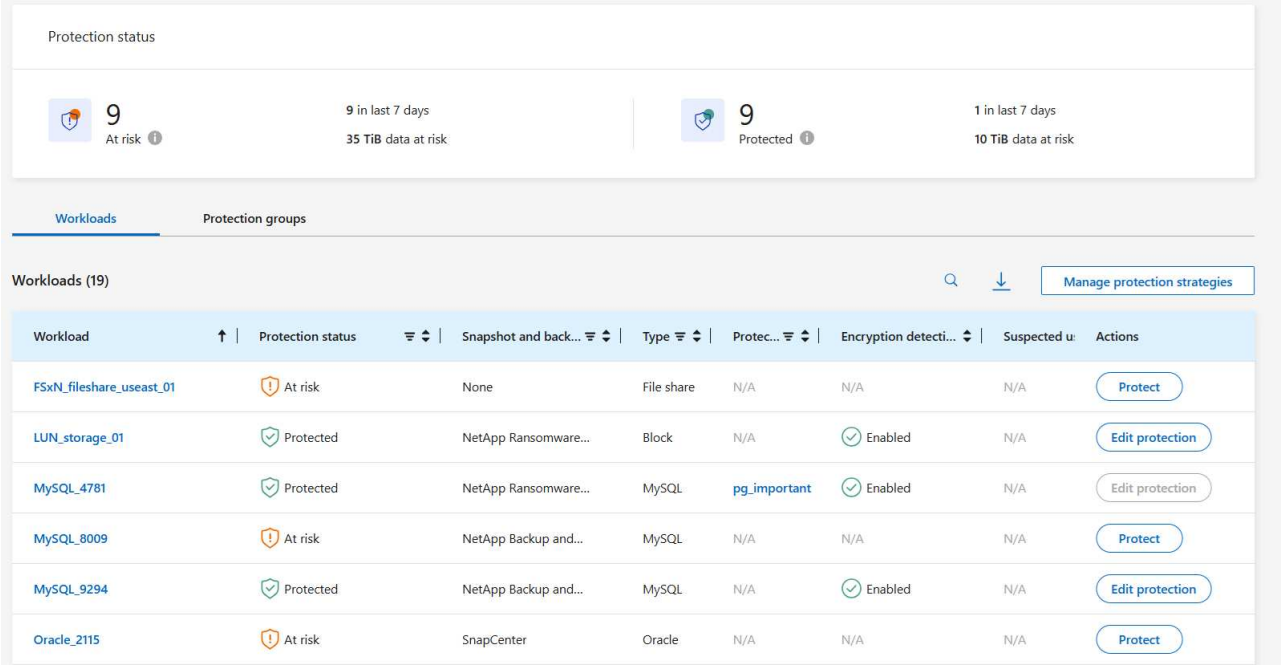
ワークロードの保護を表示する

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。

"ランサムウェア対策戦略を追加する"を参照して、Backup and Recoveryの既存の保護ポリシーがある場合にRansomware Resilienceを使用する方法を確認してください。

保護ダッシュボードについて

Ransomware Resilience の保護ダッシュボードには、保護状態に関する分析情報に加えて、ワークロードに関する詳細情報（ワークロードの名前とタイプ、Console エージェント、システム、ストレージ VM など）が表示されます。保護ダッシュボードを使用して、ワークロードのランサムウェア対策を確認および管理します。次の列は、保護体制を理解するのに特に役立ちます：

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：

+ Ransomware Resilienceは、ワークロードで設定したランサムウェア検出ポリシーの範囲に関する分析情報を提供します。次のフィールドで検出範囲を確認します。

- 暗号化検出ステータス
- 疑わしいユーザー行動の検出ステータス
- 疑わしいファイル拡張子をブロック

スナップショット、レプリケーション、およびバックアップ ポリシー：この列には、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。ポリシーがない場合、フィールドには N/A と表示されます。

重要性

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

Privacy exposure：このオプションを選択すると、"NetApp Data Classificationで個人を特定できる情報をスキャンする"。

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「N/A」と表示されます。

バックアップ先：バックアップを使用したランサムウェア保護戦略を構成している場合は、バックアップ先システムの名前がここに表示されます。

次の手順

- "ランサムウェア対策戦略でワークロードを保護する"
- "保護グループの管理"
- "個人を特定できるデータをスキャンする"

NetApp Ransomware Resilienceでバックアップ先を追加する

NetApp Ransomware Resilienceがワークロードを検出したときに、バックアップが設定されている場合、Ransomware Resilienceはバックアップの保存先を認識します。バックアップを"ランサムウェア対策戦略"の一部として使用する予定であるが、ワークロードにバックアップの保存先を設定していない場合は、サイバーレジリエンスを向上させるためにNetApp Ransomware Resilienceでバックアップの保存先を追加する必要があります。

次のいずれかのバックアップ先を選択できます：

- NetAppStorageGRID
- Amazon Web Services（AWS）
- Google Cloud Platform
- Microsoft Azure

> Amazon FSx for NetApp ONTAP および Azure NetApp Files のワークロードでは、バックアップ先を使用できません。ネイティブバックアップソリューションを使用してバックアップ操作を実行します：FSx for ONTAP バックアップサービスまたは Azure NetApp Files バックアップ。

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" 。

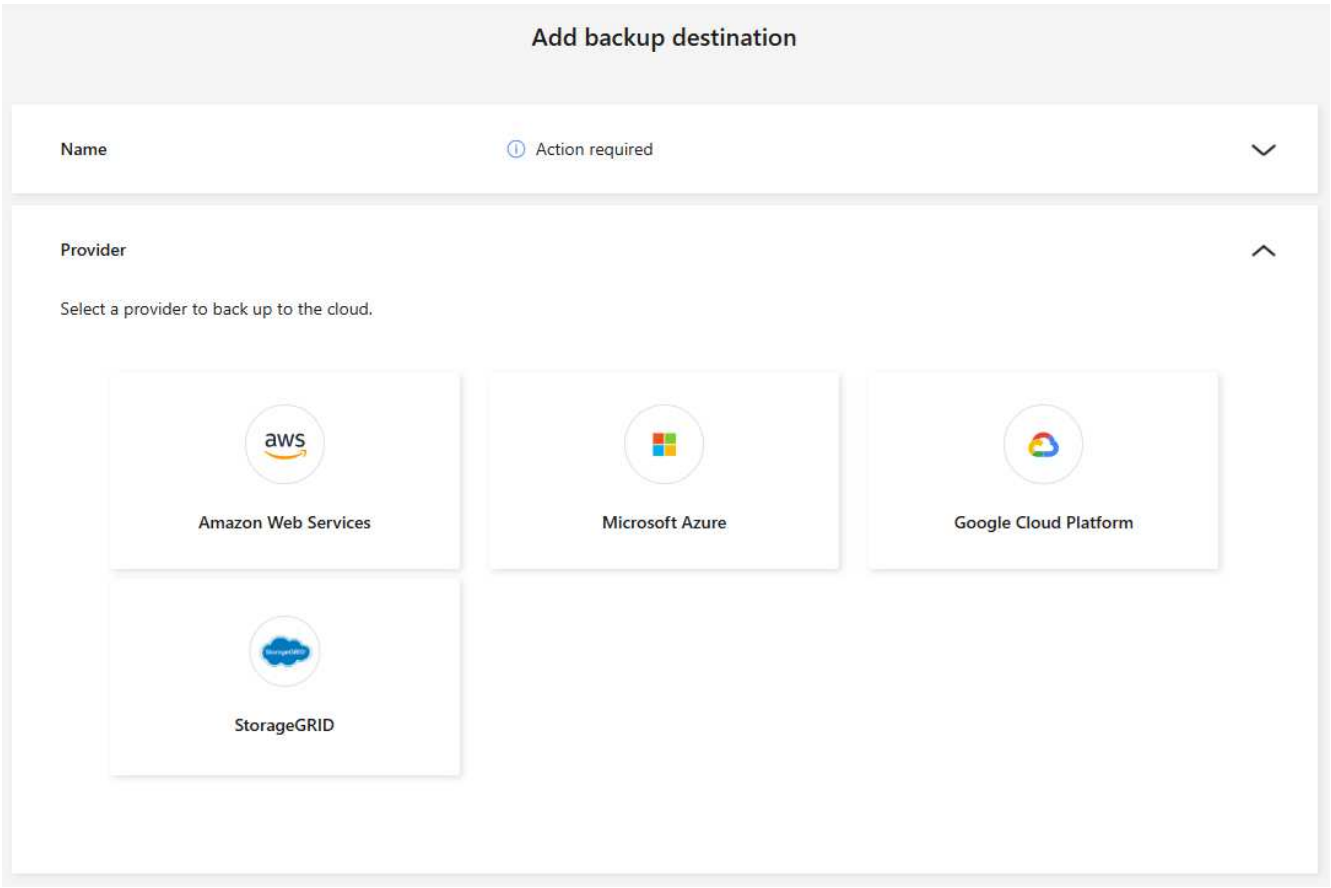
StorageGRIDをバックアップ先として追加する

NetApp StorageGRID をバックアップ先として設定するには、次の情報を入力します。

手順

1. ランサムウェア耐性で、[設定] を選択します。
2. バックアップ先タイルで、表示を選択します。
3. 追加を選択します。

4. バックアップ先の名前を入力します。

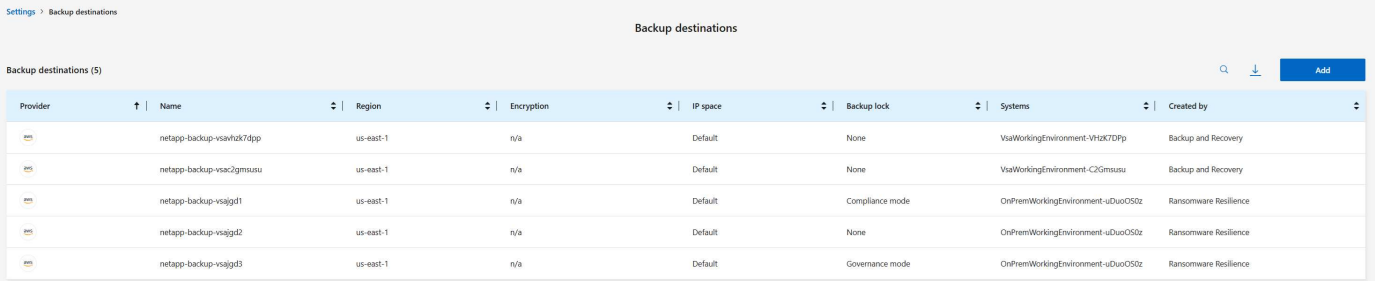


5. * StorageGRID*を選択します。
6. 各設定の横にある下矢印を選択して、必須フィールドを確認します：
   - プロバイダー設定:
     - 新しいバケットを作成するか、独自のバケットを使用するかを選択します。
     - ゲートウェイ ノードの完全修飾ドメイン名（**FQDN**） と ポート を指定します。
     - StorageGRID資格情報を入力します：アクセスキーとシークレットキー。
   - ネットワーク: IPspace を選択します。
     - IPspace は、バックアップするボリュームが存在するクラスターです。この IPspace のクラスタ間 LIF には、アウトバウンド インターネット アクセスが必要です。
   - * Backup Lock *

     バックアップロックを設定するかどうかを選択します。バックアップロックを使用すると、コピーが変更または削除されないように保護され、ランサムウェアの脅威がスキャンされます。バックアップ先の設定後は、この設定を変更できません。 バックアップロックが不要な場合は、なしを選択します。 特定の権限を持つユーザが保持期間中に保護されたバックアップファイルを上書きまたは削除できるようにするには、ガバナンスモードを選択します。 保持期間中にユーザが保護されたバックアップファイルを上書きまたは削除できないようにするには、コンプライアンスモード**を選択します。
7. *追加*を選択します。

結果

新しいバックアップ先がバックアップ先のリストに追加されます。



Amazon Web Servicesをバックアップ先として追加する

AWS をバックアップ先として設定するには、次の情報を入力します。

コンソールでAWSストレージを管理する方法の詳細については、"Amazon S3バケットを管理する"を参照してください。

手順

1. ランサムウェア耐性で、[設定] を選択します。
2. バックアップ先タイルで、表示を選択します。
3. 追加を選択します。
4. *Amazon Web Services*を選択します。
5. 各設定の横にある下矢印を選択し、値を入力または選択します。
   - プロバイダー設定:
     - 新しいバケットを作成するか、コンソールに既にバケットが存在する場合は既存のバケットを選択するか、バックアップを保存する独自のバケットを用意します。
     - AWS 認証情報の AWS アカウント、リージョン、アクセスキー、シークレットキー

       "独自のバケットを使用する場合は、「S3バケットの追加」を参照してください。" 。
   - 暗号化: 新しい S3 バケットを作成する場合は、プロバイダーから提供された暗号化キー情報を入力します。既存のバケットを選択した場合は、暗号化情報がすでに利用可能です。

     バケット内のデータは、デフォルトで AWS 管理キーで暗号化されます。 AWS 管理のキーを引き続き使用することも、独自のキーを使用してデータの暗号化を管理することもできます。
   - ネットワーク: IPspace を選択し、プライベート エンドポイントを使用するかどうかを選択します。
     - IPspace は、バックアップするボリュームが存在するクラスターです。この IPspace のクラスタ間 LIF には、アウトバウンド インターネット アクセスが必要です。
     - 必要に応じて、以前に設定した AWS プライベートエンドポイント (PrivateLink) を使用するかどうかを選択します。

       AWS PrivateLinkを使用する場合は、以下を参照してください。 "Amazon S3 用の AWS PrivateLink" 。
   - バックアップ ロック: ランサムウェア耐性により、バックアップが変更または削除されないように保

護するかどうかを選択します。このオプションはNetApp DataLock テクノロジーを使用します。各バックアップは、保持期間中、または最低 30 日間と最大 14 日間のバッファ期間にわたってロックされます。

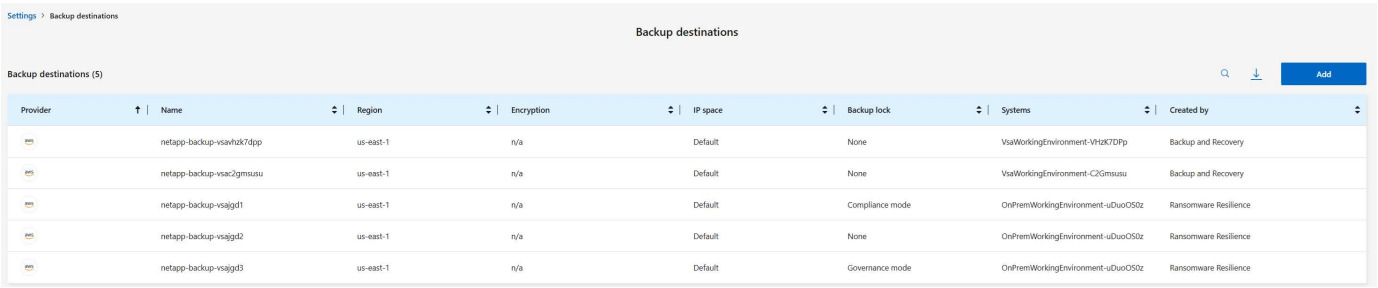
> ここでバックアップロック設定を構成すると、バックアップ先の構成後に設定を変更することはできません。

- ガバナンス モード: 特定のユーザー (s3:BypassGovernanceRetention 権限を持つ) は、保持期間中に保護されたファイルを上書きまたは削除できます。
- コンプライアンス モード: ユーザーは、保持期間中に保護されたバックアップ ファイルを上書きまたは削除することはできません。

6. *追加*を選択します。

結果

新しいバックアップ先がバックアップ先のリストに追加されます。



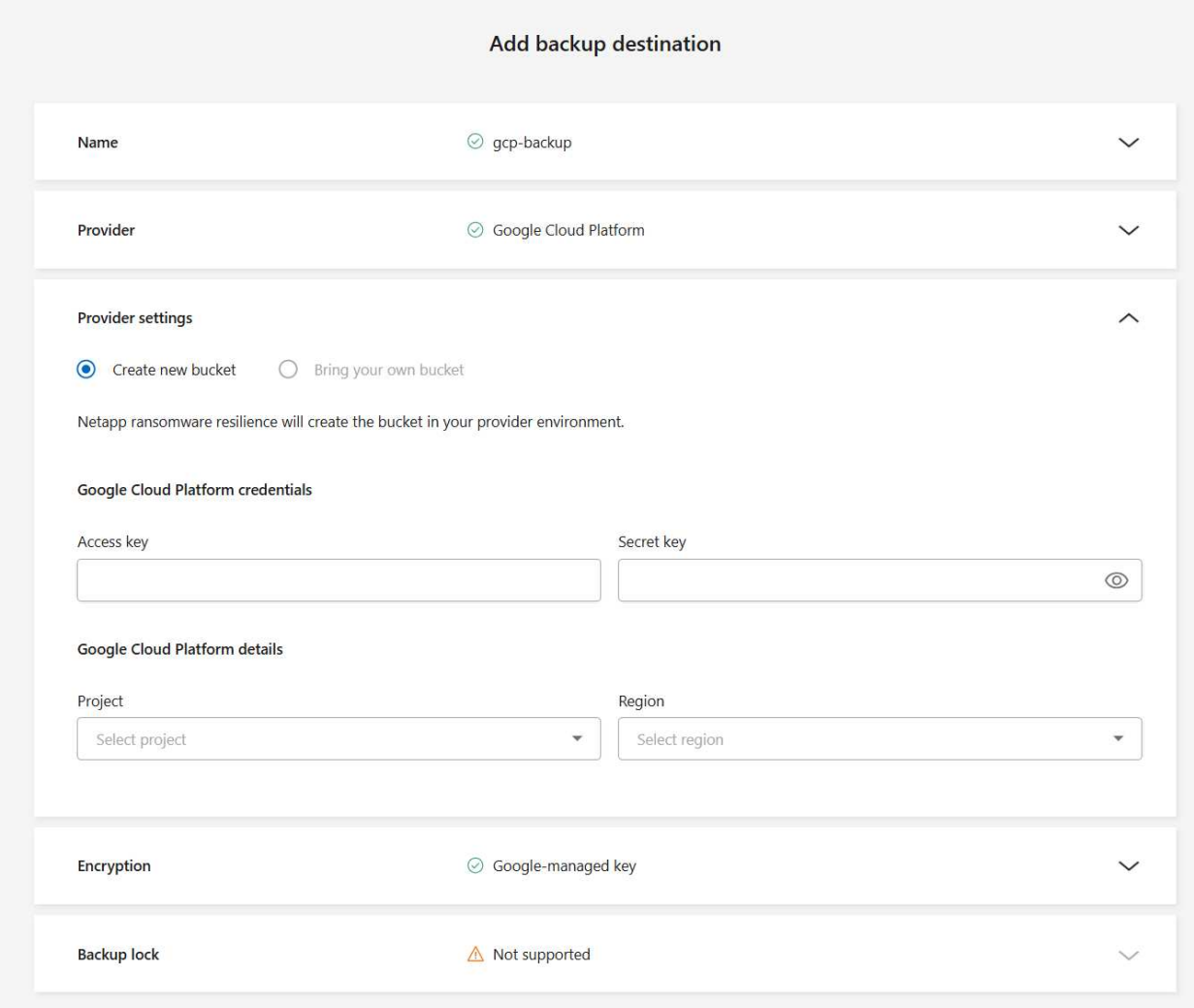
Google Cloud Platform をバックアップ先として追加する

Google Cloud Platform (GCP) をバックアップ先として設定するには、次の情報を入力します。

コンソールでGCPストレージを管理する方法の詳細については、"Google Cloud のコンソール エージェントのインストール オプション"を参照してください。

手順

1. ランサムウェア耐性で、[設定] を選択します。
2. バックアップ先タイルで、表示を選択します。
3. 追加を選択します。
4. バックアップ先の名前を入力します。
5. **Google Cloud Platform** を選択します。
6. 各設定の横にある下矢印を選択し、値を入力または選択します。
   - プロバイダー設定:
     - 新しいバケットを作成するか、独自のバケットを使用するかを選択します。
     - Google Cloud Platform の認証情報（**Access key** と **Secret key**）を入力します。
     - プロジェクト とそれが存在する リージョン を選択します。



- 暗号化: 新しいバケットを作成する場合は、プロバイダーから提供された暗号化キー情報を入力します。既存のバケットを選択した場合は、暗号化情報がすでに利用可能です。

  バケット内のデータは、デフォルトで Google 管理のキーで暗号化されます。**Google** 管理のキーを選択してデフォルト設定を続行するか、顧客管理のキーを使用することができます。

7. *追加*を選択します。

結果

新しいバックアップ先がバックアップ先のリストに追加されます。

バックアップ先として **Microsoft Azure** を追加する

Azure をバックアップ先として設定するには、次の情報を入力します。

コンソールでAzure資格情報とマーケットプレイスサブスクリプションを管理する方法の詳細については、以下を参照してください。 "Azure 資格情報とマーケットプレイスのサブスクリプションを管理する" 。

手順

1. ランサムウェア耐性で、[設定] を選択します。
2. バックアップ先タイルで、表示を選択します。

3. 追加を選択します。
4. **Azure** を選択します。
5. 各設定の横にある下矢印を選択し、値を入力または選択します。
   - プロバイダー設定:
     - 新しいストレージ アカウントを作成するか、コンソールに既に存在する場合は既存のアカウントを選択するか、バックアップを保存する独自のストレージ アカウントを使用します。
     - アプリケーション（クライアント）ID、クライアントシークレット、およびディレクトリ（テナント）IDを指定します。認証を選択します。
     - Azure サブスクリプション、リージョン、および Azure サブスクリプションのリソースグループを選択します。

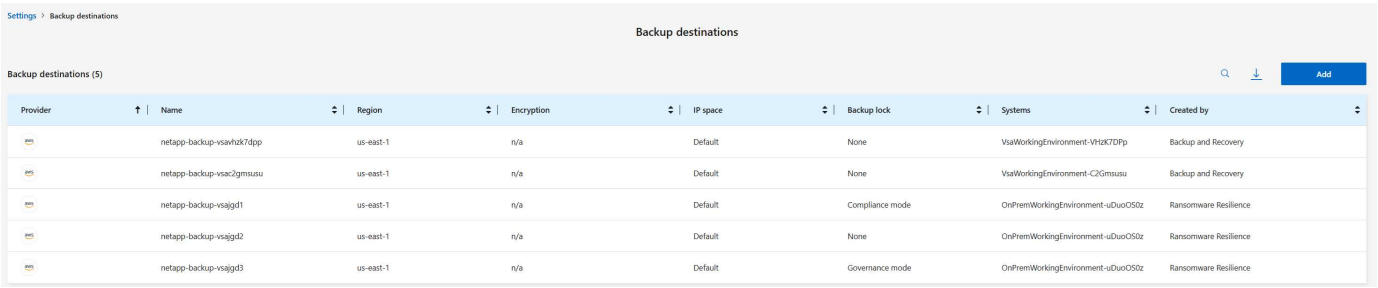
       "独自のストレージ アカウントを使用する場合は、「Azure Blob ストレージ アカウントの追加」を参照してください。" 。
   - 暗号化：デフォルトでは、データは Microsoft が管理するキーで暗号化されます。このオプションを維持するには、**Microsoft** が管理するキーを選択します。または、暗号化に独自のキーを使用するには、顧客が管理するキーを選択します。
   - ネットワーク: IPspace を選択し、プライベート エンドポイントを使用するかどうかを選択します。
     - IPspace は、バックアップするボリュームが存在するクラスターです。この IPspace のクラスタ間 LIF には、アウトバウンド インターネット アクセスが必要です。
     - 必要に応じて、以前に構成した Azure プライベート エンドポイントを使用するかどうかを選択します。

       Azure PrivateLink を使用する場合は、以下を参照してください。 "Azure プライベートリンク" 。
   - * Backup Lock *

     バックアップロックを設定するかどうかを選択します。バックアップロックを使用すると、コピーが変更または削除されないように保護され、ランサムウェアの脅威がスキャンされます。バックアップ先の設定後は、この設定を変更できません。 バックアップロックが不要な場合は、なしを選択します。 特定の権限を持つユーザが保持期間中に保護されたバックアップファイルを上書きまたは削除できるようにするには、ガバナンスモードを選択します。 保持期間中にユーザが保護されたバックアップファイルを上書きまたは削除できないようにするには、コンプライアンスモード**を選択します。
6. *追加*を選択します。

結果

新しいバックアップ先がバックアップ先のリストに追加されます。



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

ランサムウェア対策戦略は、NetApp Ransomware Resilienceの主要な機能です。検出、保護、複製をサポートします。保護戦略は、サイバーセキュリティ体制の重要な要素です。

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、"グループのワークロード"を作成して、1つの戦略の下でボリュームをまとめて保護できます。

他の**NetApp**マネージド サービスとの保護ポリシー

NetApp Ransomware Resilience以外にも、NetApp Backup and Recoveryを使用して、ファイル共有、VMファイル共有の保護を管理できます。

NetApp Backup and Recoveryサービスからの保護情報は、NetApp Ransomware Resilienceに表示されます。NetApp 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。NetApp Ransomware Resilienceで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NetApp Backup and RecoveryまたはNetApp Ransomware Resilience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環としてスナップショットが取得され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。

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

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
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
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

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
- **Backup and Recovery**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"。

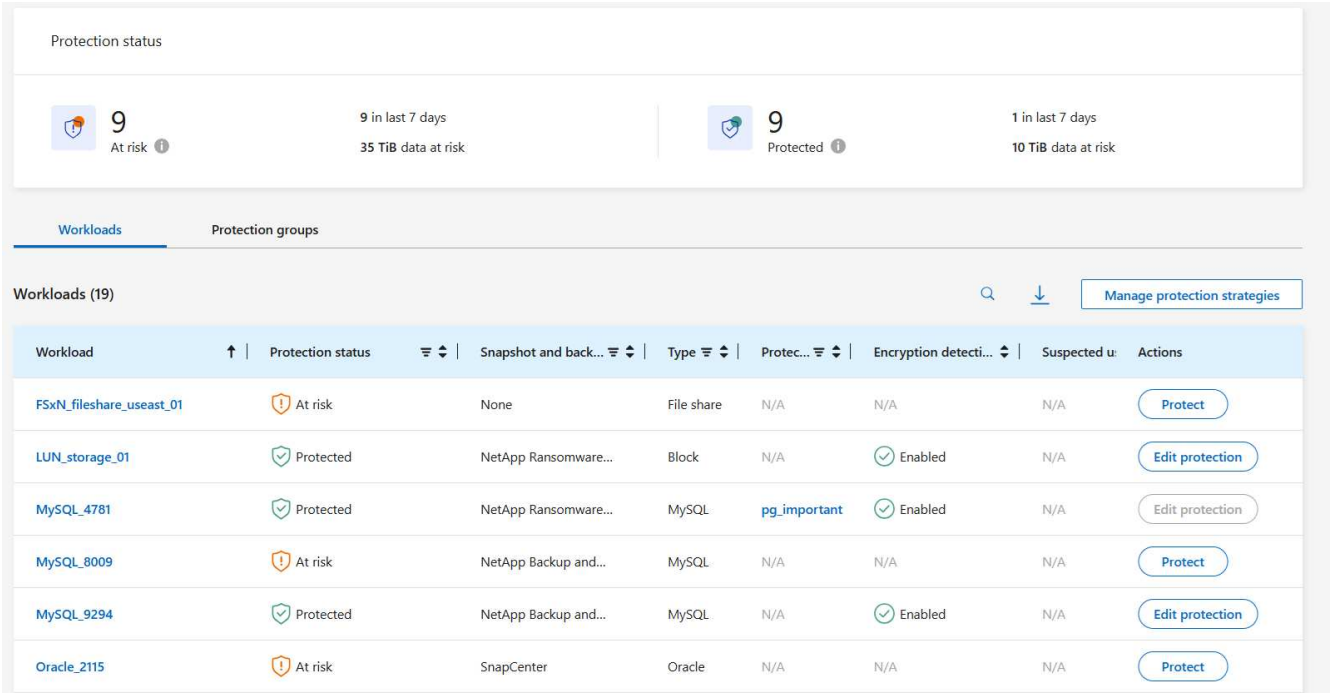
ランサムウェア対策戦略を作成する（スナップショットやバックアップポリシーがない場合）

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。

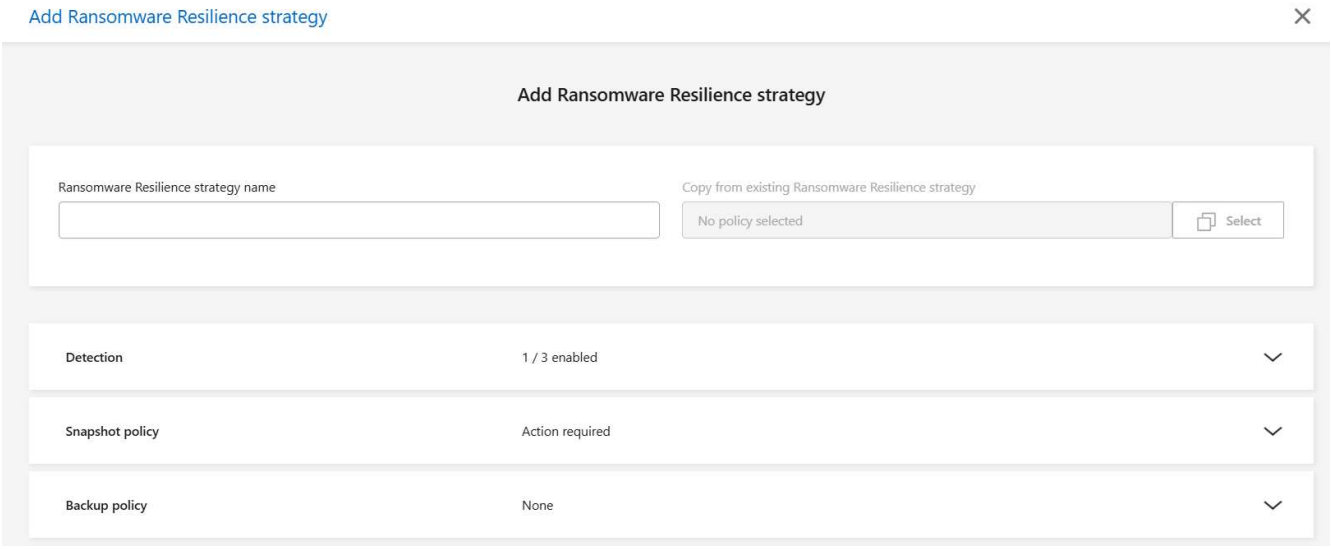
- スナップショットポリシー
- バックアップ ポリシー
- ランサムウェア検出ポリシー
- ONTAPへのセカンダリレプリケーション

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、*Settings*オプションを使用してバックアップの保存先を設定します。詳細については、"設定を構成する"を参照してください。

6. *追加*を選択します。

Backup and Recoveryで管理されている既存の**Snapshot**ポリシーとバックアップポリシーを使用しているワークロードに検出ポリシーを追加

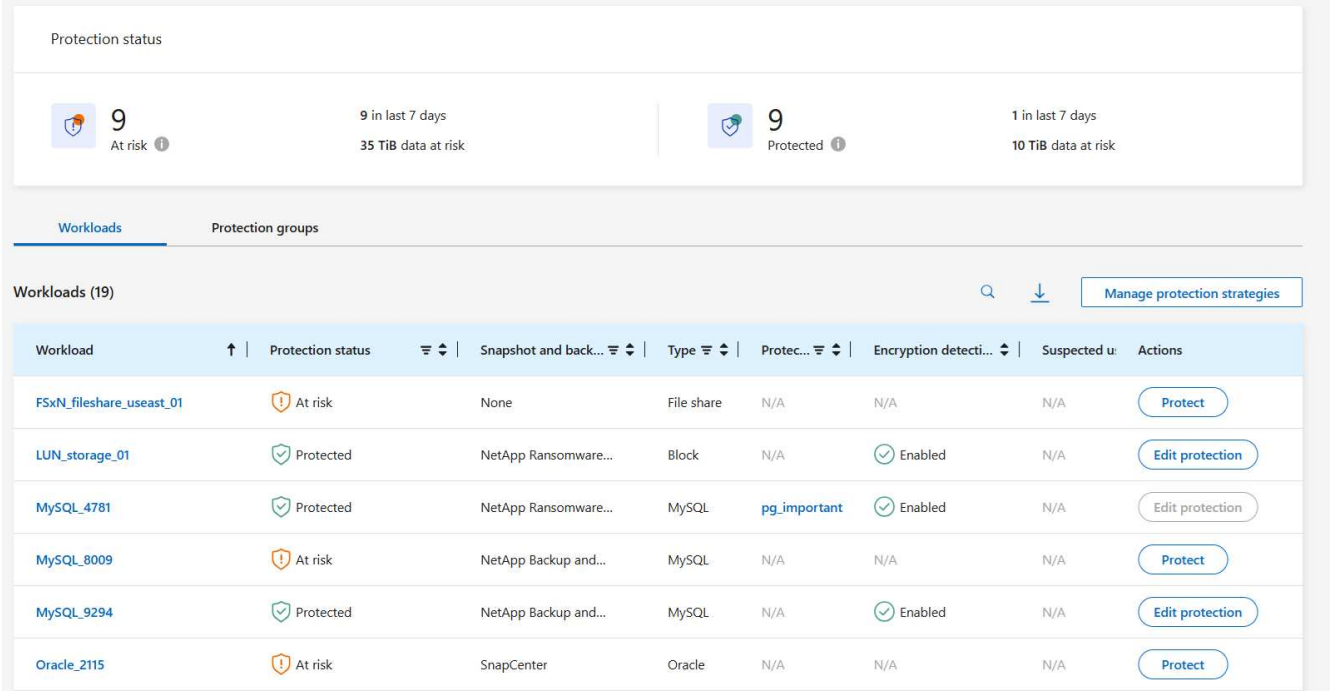
Ransomware Resilienceでは、他のNetApp製品またはサービスで管理されている既存のスナップショットおよびバックアップ保護を使用するワークロードに、検出ポリシーまたは保護ポリシーを割り当てることができます。Backup and Recoveryでは、スナップショット、セカンダリストレージへのレプリケーション、またはオブジェクトストレージへのバックアップを管理するポリシーを使用します。

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で既存のSnapshot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。Ransomware Resilienceによる保護と検出を管理するには、ランサムウェア耐性で保護を参照してください。

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 NetApp Backup and Recovery 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NetApp Backup and Recovery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] ボックスのチェックを外しておきます。
5. 必要な検出設定を選択します：
   - 暗号化検出
   - 不審なユーザー行動の検出
   - 疑わしいファイル拡張子をブロック
6. 次へを選択します。
7. 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。

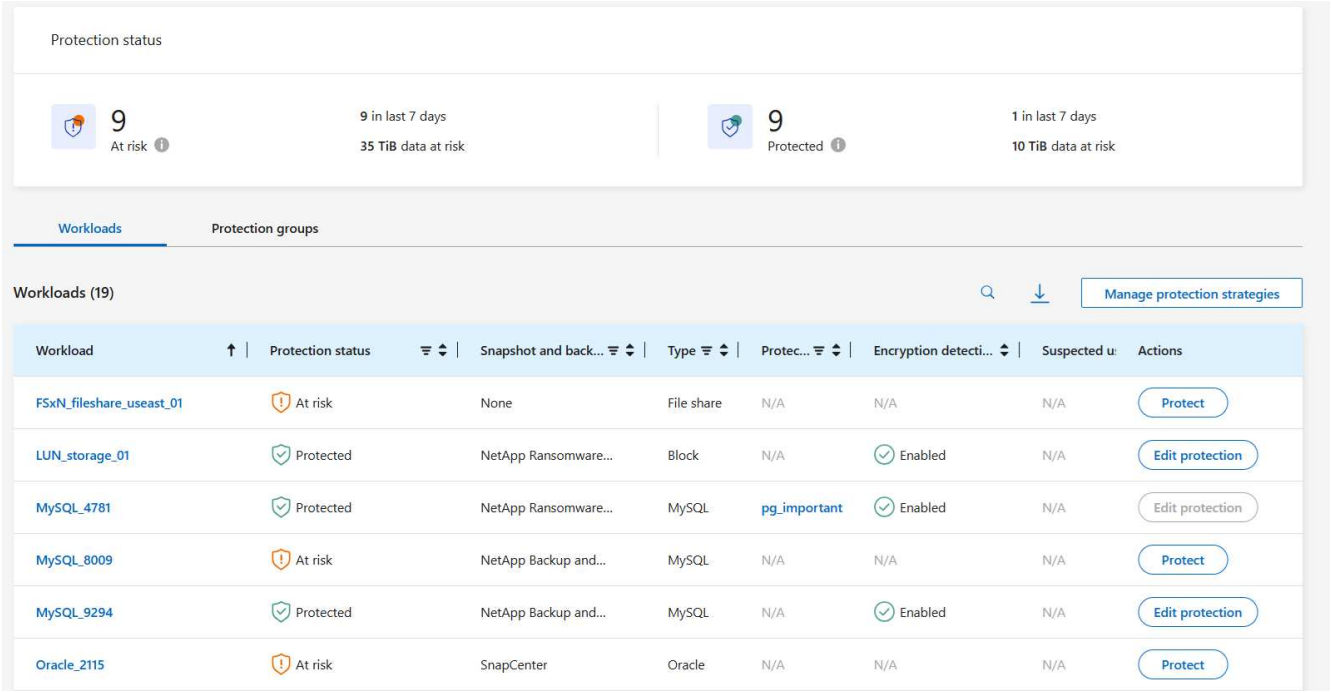
   ユーザー アクティビティ エージェントは新しいデータ コレクターをホストします。Ransomware Resilience は、データ コレクターを自動的に作成し、ユーザー アクティビティ イベントを Ransomware Resilience に送信して、異常なユーザー動作を検出します。
8. 次へを選択します。
9. 選択内容を確認します。検出を有効にするには、[作成] を選択します。
10. [保護] ページで、検出ステータス を確認して、検出がアクティブであることを確認します。

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. NetApp Ransomware Resilience は、アクティブな NetApp Backup and Recovery ポリシーが存在しているかどうかを検出します。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ボックスを選択します。ボックスを選択すると、NetApp 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NetApp Backup and Recovery保護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。

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

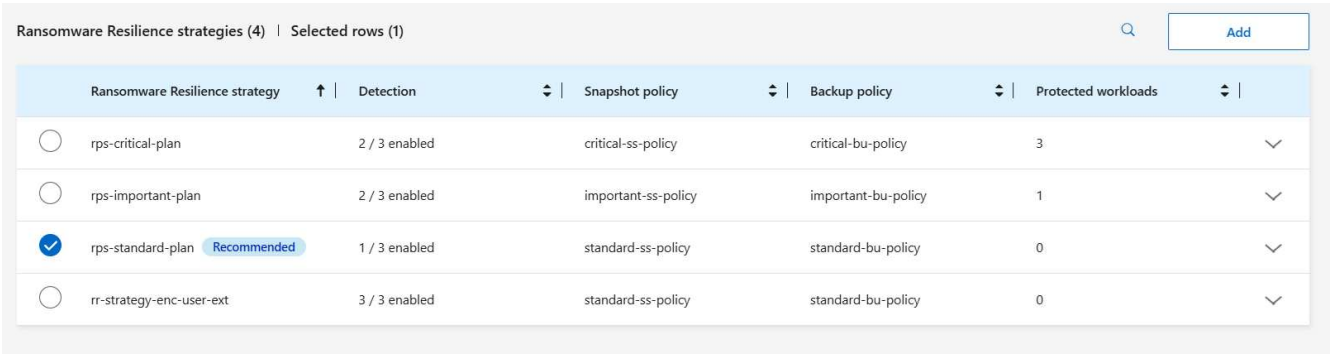
ランサムウェア保護戦略を削除する前に、その戦略によって保護されているワークロードを確認することをお勧めします。

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。

ユーザーアクティビティ検出を設定する

NetApp Ransomware Resilienceのユーザーアクティビティ検出について学ぶ

ユーザーアクティビティ検出機能により、NetApp Ransomware Resilienceにより、ユーザー レベルでランサムウェア イベントに対処し、データ侵害や大規模な削除などのイベントを阻止できます。

NetApp Ransomware Resilience は、疑わしいユーザーアクティビティを監視することで、AI を活用したデータ侵害検出を実現します。読み取りアクティビティの急激な増加と読み取りアクティビティのアクセスパターンを使用して、悪意のある意図を判断します。検出されると、Ransomware Resilience は NetApp Console 、Eメール、および構成された任意のセキュリティエコシステム（SIEM など）で自動的にアラートを生成します。

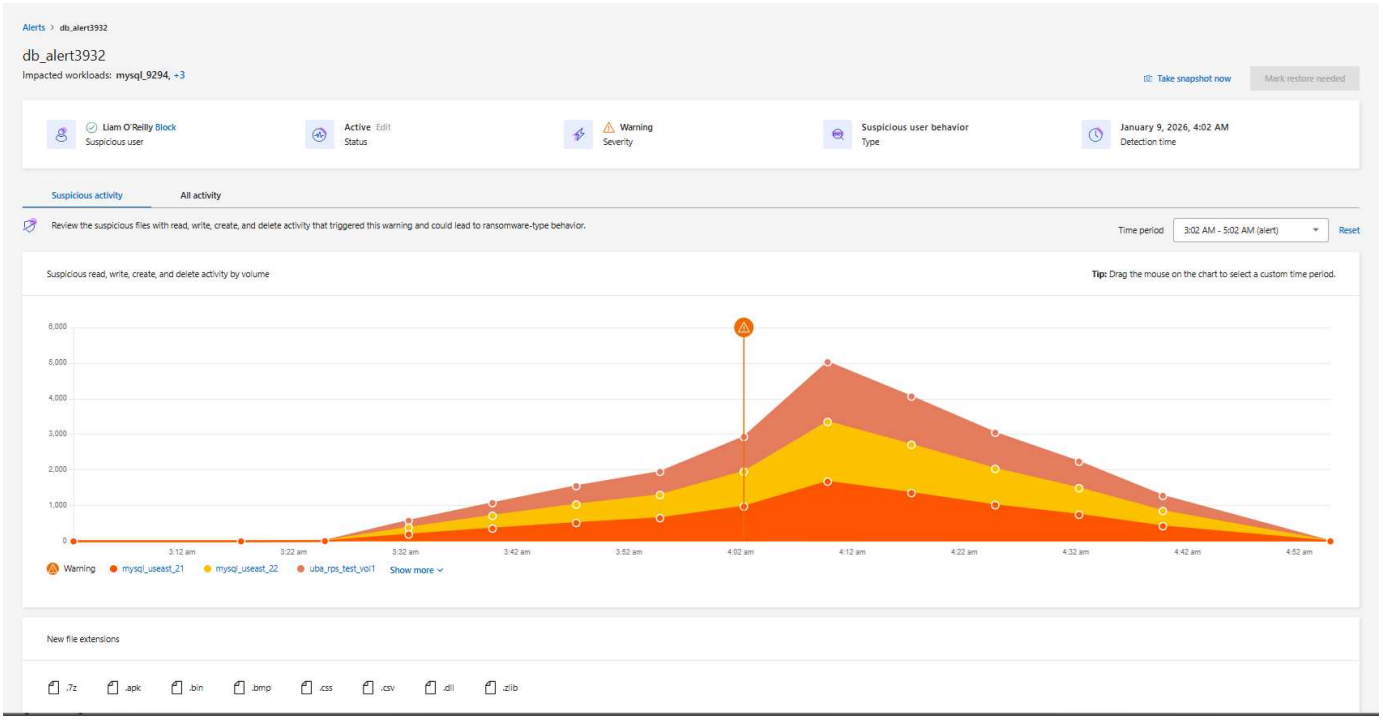
疑わしいユーザーの行動を検出して警告する NetApp Ransomware Resilience は、疑わしいと思われるデータ侵害や破壊の試みやパターンについて警告します。各アラートで、NetApp Ransomware Resilience はブロックできるユーザーを識別します。

Ransomware Resilience は、 ONTAPの FPolicy によって生成されたユーザー アクティビティ イベントを分析して、疑わしいユーザー アクティビティを検出します。ユーザー アクティビティ データを収集するには、1 つ以上のユーザー アクティビティ エージェントを展開する必要があります。エージェントは、テナント上のデバイスに接続できる Linux サーバーまたは VM です。

ユーザーアクティビティの検出は現在、SANワークロードではサポートされていません。Amazon FSxN for ONTAP、Cloud Volumes ONTAP、ONTAPのNASワークロードでユーザーアクティビティ検出を使用できます。

疑わしいユーザーアクティビティのフォレンジック

Ransomware Resilience は、ユーザーの行動に関するフォレンジックを提供します（疑わしいアクティビティが発生したときや通知が送信されたときを示すリストとグラフ）。これらは、ファイル、ディレクトリ、ボリューム、ワークロードにおける疑わしいアクティビティの頻度を経時的に詳細に示し、イベントのグラフ化に役立ちます。新しいファイル拡張子の出現も確認できます。



o

疑わしいアクティビティをすべてのアクティビティのビューと比較できます。すべてのアクティビティビューでは、アクセスの変更やアクセス拒否のイベントに加えて、読み取り、書き込み、名前の変更、移動、作成、削除のイベントを観察できます。

o

コンポーネント

NetApp Ransomware Resilience の疑わしいユーザー行動アクティビティ検出には、3 つの主要コンポーネントがあります。

- ユーザーアクティビティエージェントは、データコレクター用の実行可能環境です。ユーザーアクティビティエージェントを設定する必要があります。

- データコレクタは、ユーザーアクティビティイベントをRansomware Resilienceと共有します。データコレクタは、"疑わしいユーザアクティビティの検出によるランサムウェア保護戦略を有効化"ときに自動的に作成されます。
- ユーザーディレクトリコネクタを使用すると、ユーザー名とユーザーID間のマッピングが可能になり、疑わしいユーザーの行動への対応がより明確になります。ユーザーディレクトリコネクタを設定する必要があります。

ランサムウェア耐性と**Data Infrastructure Insights**

Ransomware Resilienceの疑わしいユーザー行動検出は、Data Infrastructure Insights（DII）Workload Securityとの統合であり、"DIIエンドポイント"を使用します。Ransomware Resilienceでユーザー行動検出を有効にするために、DII構成は必要ありません。ユーザー行動検出を有効にするには、"必要なエージェントとコレクターを作成し、適切なランサムウェア保護戦略を有効にする"。

すでにNetApp Data Infrastructure Insights（DII）Workload Security を使用している場合は、Ransomware Resilience に同じ Workload Security エージェントを使用することをお勧めします。Ransomware Resilience 用に個別の Workload Security エージェントを展開する必要はありませんが、同じ Workload Security エージェントを使用するには、Ransomware Resilience Console 組織と DII Storage Workload Security テナント間のペアリング関係が必要です。このペアリングを有効にするには、アカウント担当者にお問い合わせください。

次の手順

- "ユーザー行動アクティビティ検出の要件"
- "ユーザー行動アクティビティエージェントと検出器を設定する"

NetApp Ransomware Resilienceのユーザーアクティビティ検出要件

NetApp Ransomware Resilienceユーザー行動検出により、ユーザーレベルのランサムウェア イベントに対応できるようになります。ユーザーの動作検出を有効にするには、エージェントのセットを作成する必要があります。検出を有効にする前に、Ransomware Resilienceがイベントを適切に検出して報告できるように、概説されているオペレーティング システム、サーバー、およびネットワークの要件を満たしていることを確認する必要があります。

クラウドプロバイダのサポート

疑わしいユーザーアクティビティ データは、次のリージョンの AWS および Azure に保存される可能性があります。

クラウド プロバイダ	リージョン
AWS	• アジア太平洋（シドニー）（ap-southeast-2） • ヨーロッパ (フランクフルト) (eu-central-1) • 米国東部（バージニア北部）（us-east-1）
Azure	米国東部

オペレーティング システム要件

疑わしいユーザー行動の検出は、次のオペレーティングシステムでサポートされています：

オペレーティング システム	サポート対象のバージョン
アルマリナックス	9.4 (64 ビット) から 9.5 (64 ビット)、および 10 (64 ビット) (SELinux を含む)
CentOS	CentOS Stream 9 (64 ビット)
Debian	11 (64 ビット)、12 (64 ビット)、SELinux を含む
OpenSUSE リープ	15.3 (64 ビット) から 15.6 (64 ビット)
Oracle Linux	8.10 (64 ビット)、および 9.1 (64 ビット) から 9.6 (64 ビット) (SELinux を含む)
Red Hat	8.10 (64 ビット)、9.1 (64 ビット) から 9.6 (64 ビット)、および 10 (64 ビット) (SELinux を含む)
ロッキー	Rocky 9.4 (64 ビット) から 9.6 (64 ビット)、SELinux を含む
SUSEエンタープライズLinux	15 SP4 (64 ビット) から 15 SP6 (64 ビット) 、SELinux を含む
Ubuntu	20.04 LTS (64 ビット)、22.04 LTS (64 ビット) 、24.04 LTS (64 ビット)

ユーザー アクティビティ エージェントに使用するマシンは、他のアプリケーションレベルのソフトウェアを実行しないでください。専用サーバーをお勧めします。

その `unzip` インストールにはコマンドが必要です。その `sudo su -` インストール、スクリプトの実行、アンインストールにはコマンドが必要です。

サーバー要件

サーバーは次の最小要件を満たしている必要があります。

- **CPU**: 4コア
- **RAM**: 16GB RAM
- ディスク容量: 36 GB の空きディスク容量

サーバーの推奨事項

- ファイルシステムの作成を可能にするために追加のディスク領域を割り当てます。ファイルシステムに少なくとも 35 GB の空き領域があることを確認します。+ もし `/opt` NAS ストレージからマウントされたフォルダーであるため、ローカル ユーザーはこのフォルダーにアクセスできる必要があります。ローカル ユーザーに必要な権限がない場合、ユーザー アクティビティ エージェントの作成が失敗する可能性があります。
- ユーザーアクティビティエージェントは、Ransomware Resilienceとは別のシステムにインストールすることを推奨します。同じマシンにインストールする場合は、50～55 GBのディスク容量を確保する必要があります。Linuxの場合は、 `/opt/netapp`に25～30 GBのスペースを割り当て、 `var/log/netapp`に25 GBを割り当てます。

- Network Time Protocol (NTP) または Simple Network Time Protocol (SNTP) を使用して、 ONTAPシステムとユーザー アクティビティ エージェント マシンの両方の時刻を同期することをお勧めします。

クラウドネットワークアクセスルール

関連する地域 (アジア太平洋、ヨーロッパ、または米国) のクラウド ネットワーク アクセス ルールを確認します。

初期インストール時に、 `<site_name>`をワイルドカード（*`）権限に置き換えます。エージェントがアクティブ化され、完全に動作可能になったら、権限をサイト名に置き換えることができます。サイト名については、NetAppの担当者にお問い合わせください。

ユーザアクティビティエージェントはNetApp Data Infrastructure Insightsテクノロジを使用するため、 `cloudinsights`エンドポイントを使用します。詳細については、次を参照してください。

APACベースのユーザーアクティビティエージェントの導入

プロトコル	ポート	ソース	デスティネーション	説明
HTTPS（TCP）	443	ユーザーアクティビティエージェント	• <site_name>.cs01-ap-1.cloudinsights.netapp.com • <site_name>.c01-ap-1.cloudinsights.netapp.com • <site_name>.c02-ap-1.cloudinsights.netapp.com • gentlogin.cs01-ap-1.cloudinsights.netapp.com	ランサムウェア耐性へのアクセス

ヨーロッパを拠点とするユーザーアクティビティエージェントの導入

プロトコル	ポート	ソース	デスティネーション	説明
HTTPS（TCP）	443	ユーザーアクティビティエージェント	• <site_name>.cs01-eu-1.cloudinsights.netapp.com • <site_name>.c01-eu-1.cloudinsights.netapp.com • <site_name>.c02-eu-1.cloudinsights.netapp.com • agentlogin.cs01-eu-1.cloudinsights.netapp.com	ランサムウェア耐性へのアクセス

米国ベースのユーザアクティビティエージェントの導入

プロトコル	ポート	ソース	デスティネーション	説明
HTTPS（TCP）	443	ユーザーアクティビティエージェント	• <site_name>.cs01.cloudinsights.netapp.com • <site_name>.c01.cloudinsights.netapp.com • <site_name>.c02.cloudinsights.netapp.com • agentlogin.cs01.cloudinsights.netapp.com	ランサムウェア耐性へのアクセス

ネットワーク内ルール

プロトコル	ポート	ソース	デスティネーション	説明
TCP	389(LDAP) 636 (LDAP / start-tls)	ユーザーアクティビティエージェント	LDAP Server URL	LDAPに接続する
HTTPS（TCP）	443	ユーザーアクティビティエージェント	クラスタまたは SVM 管理 IP アドレス (SVM コレクターの構成によって異なります)	ONTAPとのAPI通信

プロトコル	ポート	ソース	デスティネーション	説明
TCP	35000 - 55000	SVMデータLIF IPアドレス	ユーザーアクティビティエージェント	Fpolicy イベントに関するONTAPからユーザー アクティビティ エージェントへの通信。ONTAP がイベントをユーザー アクティビティ エージェントに送信するには、ユーザー アクティビティ エージェントに対してこれらのポートを開く必要があります。これには、ユーザー アクティビティ エージェント自体のファイアウォール（存在する場合）も含まれます。+ 注意: これらのポートをすべて予約する必要はありませんが、予約するポートはこの範囲内である必要があります。まずは 100 個のポートを予約し、必要に応じて増やすことをお勧めします。

プロトコル	ポート	ソース	デスティネーション	説明
TCP	35000-55000	クラスタ管理IP	ユーザーアクティビティエージェント	ONTAPクラスタ管理 IP から **EMS** イベント のユーザ アクティビティ エージェントへの通信。ONTAP がEMSイベントを送信するには、ユーザ アクティビティ エージェント自体のファイアウォールも含めて、これらのポートをユーザ アクティビティ エージェントに対して開く必要があります。+ 注意: これらのポートをすべて予約する必要はありませんが、予約するポートはこの範囲内である必要があります。まずは 100 個のポートを予約し、必要に応じて増やすことをお勧めします。
SSH	22	ユーザーアクティビティエージェント	クラスタ管理	CIFS/SMB ユーザーのブロックに必要です。

次のステップ

- "ユーザアクティビティエージェントとコレクタを設定する"

NetApp Ransomware Resilienceでユーザーアクティビティ検出を設定する

NetApp Ransomware Resilience ユーザー アクティビティ検出は、ユーザー レベルのランサムウェア イベントを防ぐのに役立ちます。Ransomware Resilience で疑わしいユーザー動作の検出を有効にするには、少なくとも 1 つのユーザー アクティビティ エージェントをインストールする必要があります。これにより、ランサムウェア イベントに類似する異常なパターンがないかユーザー動作を監視するデータ収集環境が作成されます。

ユーザー アクティビティ エージェントは、データ コレクターとユーザー ディレクトリ コネクタをホストします。これらの両方がデータを分析のために SaaS の場所に送信します。

- データコレクタは、ONTAPからユーザーアクティビティデータを収集します。ユーザー行動検出を含む保護戦略を作成すると、データコレクタが自動的に作成されます。
- ユーザー ディレクトリ コネクタ はディレクトリに接続して、ユーザー ID をユーザー名にマッピングします。ユーザー ディレクトリ コネクタを設定する必要があります。

ユーザー アクティビティ エージェント、データ コレクター、ユーザー ディレクトリ コネクタはすべて、Ransomware Resilience 設定ダッシュボードから管理できます。

> すでにNetApp Data Infrastructure Insights（DII）Workload Security を使用している場合は、Ransomware Resilience に同じ Workload Security エージェントを使用することをお勧めします。Ransomware Resilience 用に個別の Workload Security エージェントを展開する必要はありませんが、同じ Workload Security エージェントを使用するには、Ransomware Resilience Console 組織と DII Storage Workload Security テナント間のペアリング関係が必要です。このペアリングを有効にするには、アカウント担当者にお問い合わせください。

+ DII を使用して_いない_場合は、ここでの設定手順に進みます。

開始する前に

- "オペレーティングシステム、サーバ、およびネットワークの要件"を満たしていることを確認してください。

必須のコンソールロール 疑わしいユーザーアクティビティの検出を有効にするには、**Organization admin role**が必要です。その後の疑わしいユーザーアクティビティの設定には、**Ransomware Resilience user behavior admin role**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"。

各ロールが組織レベルで適用されていることを確認します。

ユーザーアクティビティエージェントを作成する

ユーザーアクティビティエージェントは、"データコレクタ"の実行可能な環境です。データコレクターは、ユーザーアクティビティイベントをNetApp Ransomware Resilienceと共有します。疑わしいユーザーアクティビティの検出を有効にするには、少なくとも1つのユーザーアクティビティエージェントを作成する必要があります。

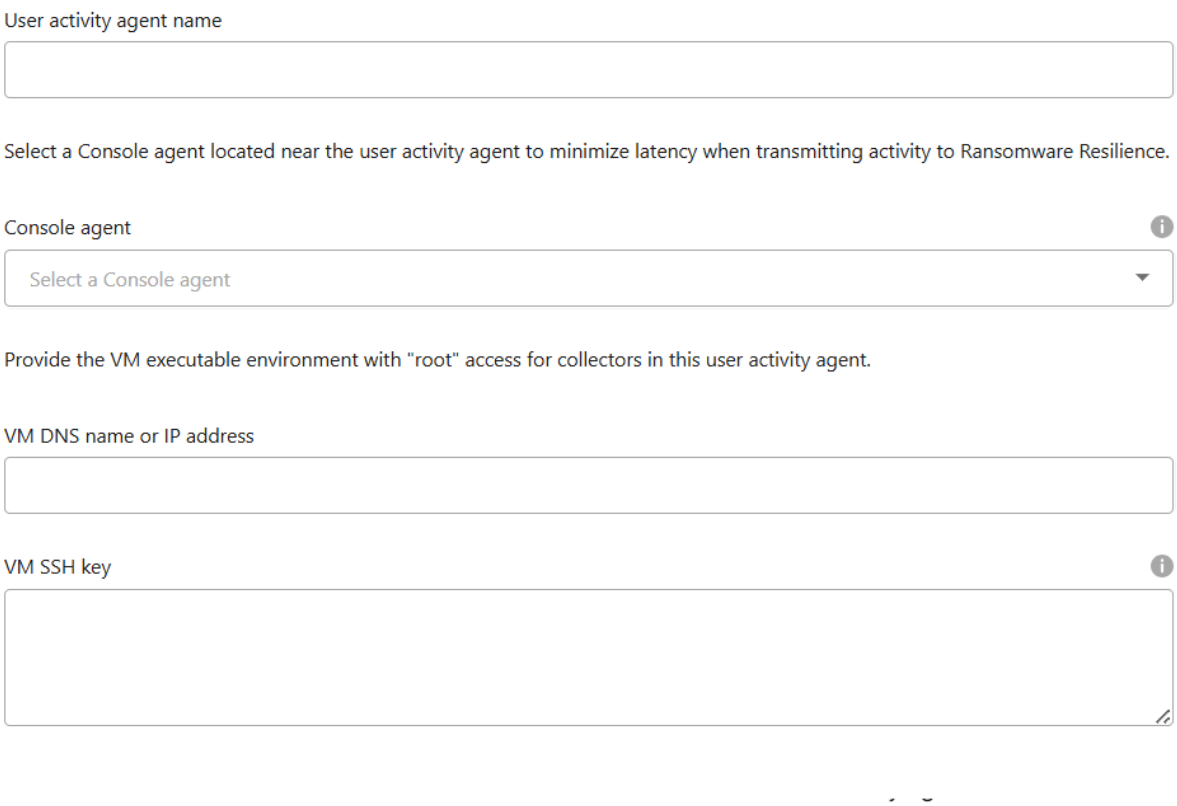
手順

1. ユーザー アクティビティ エージェントを初めて作成する場合は、ダッシュボード に移動してください。ユーザー アクティビティ タイルで、アクティブ化 を選択します。

   追加のユーザー アクティビティ エージェントを追加する場合は、[設定] に移動し、[ユーザー アクティビティ] タイルを見つけて、[管理] を選択します。[ユーザー アクティビティ] 画面で、[ユーザー アクティビティ エージェント] タブを選択し、[追加] を選択します。

2. クラウド プロバイダー を選択し、次に リージョン を選択します。次へを選択します。
3. ユーザー アクティビティ エージェントの詳細を入力します。
   - ユーザーアクティビティエージェント名
   - コンソール エージェント - コンソール エージェントは、ユーザー アクティビティ エージェントと同じネットワーク内に存在し、ユーザー アクティビティ エージェントの IP アドレスに SSH 接続できる必要があります。
   - **VM DNS**名または**IP**アドレス
   - **VM SSH** キー - 次の形式で SSH キーを入力します：

```
-----BEGIN OPENSSH PRIVATE KEY-----
private-key-contents
-----END OPENSSH PRIVATE KEY-----
```



4. 次へを選択します。
5. 設定を確認してください。*アクティブ化*を選択して、ユーザー アクティビティ エージェントの追加を完了します。
6. ユーザーアクティビティエージェントが正常に作成されたことを確認します。ユーザーアクティビティタイルでは、デプロイメントが成功すると 実行中 と表示されます。

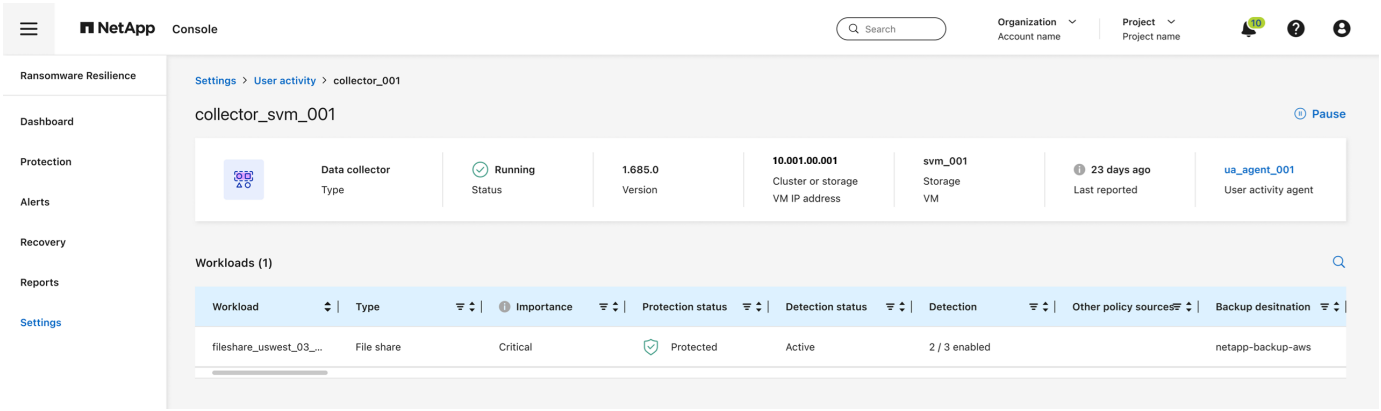
結果

ユーザーアクティビティエージェントが正常に作成されたら、設定メニューに戻り、ユーザーアクティビティタイルで管理を選択します。ユーザーアクティビティエージェントタブを選択し、ユーザーアクティビティエージェントを選択して、データコレクターやユーザーディレクトリコネクタなどの詳細を表示します。

データコレクターを追加する

疑わしいユーザー アクティビティの検出を含むランサムウェア保護戦略を有効にすると、データ コレクターが自動的に作成されます。詳細については、"検出ポリシーを追加する"を参照してください。

データコレクターの詳細を表示できます。[設定] から、[ユーザー アクティビティ] タイルの [管理] を選択します。データ コレクター タブを選択し、データ コレクターを選択して詳細を表示するか、一時停止します。



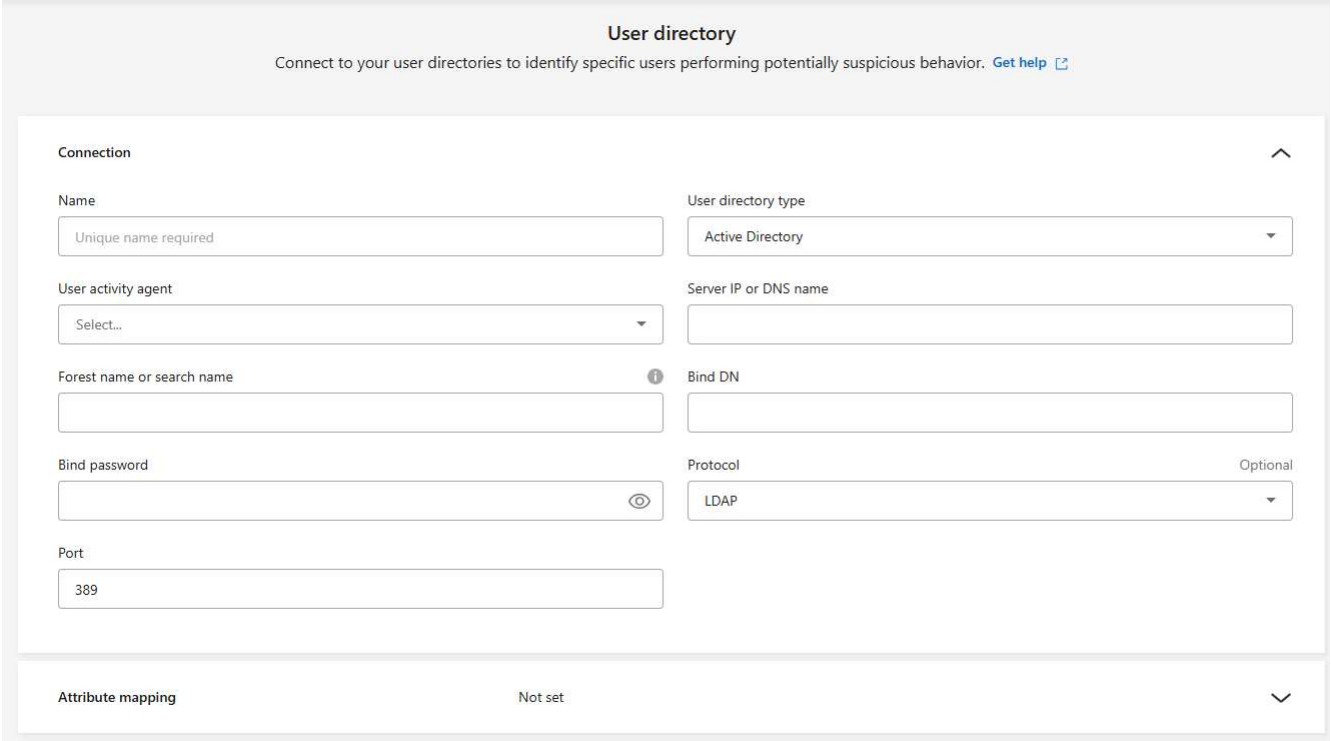
ユーザーディレクトリコネクタを作成する

ユーザー ID をユーザー名にマップするには、ユーザー ディレクトリ コネクタを作成する必要があります。

手順

1. Ransomware Resilience で、[設定] に移動します。
2. ユーザー アクティビティ タイルで、管理 を選択します。
3. ユーザー ディレクトリ コネクタ タブを選択し、追加 を選択します。
4. 接続を構成します。各フィールドに必要な情報を入力します。

フィールド	説明
名前	ユーザーディレクトリコネクタの一意の名前を入力します
ユーザーディレクトリの種類	ディレクトリタイプ
サーバーの**IP**アドレスまたはドメイン名	接続をホストするサーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN)
フォレスト名または検索名	ディレクトリ構造のフォレストレベルを直接ドメイン名として指定することができます（例： `unit.company.com`) または相対識別名のセット (例: `DC=unit,DC=company,DC=com`）。また、 `OU` 組織単位または `CN` 特定のユーザーに限定する（例： `CN=user,OU=engineering,DC=unit,DC=company,DC=com`）。
バインド**DN**	BIND DN は、user@domain.com など、ディレクトリの検索が許可されたユーザー アカウントです。ユーザーにはドメイン読み取り専用権限が必要です。
BINDパスワード	BIND DNで指定されたユーザーのパスワード
プロトコル	プロトコル フィールドはオプションです。LDAP、LDAPS、または LDAP over StartTLS を使用できます。
ポート	選択したポート番号を入力してください



属性マッピングの詳細を指定します。

- 表示名
- **SID** (LDAP を使用している場合)
- ユーザー名
- **Unix ID** (NFS を使用している場合)
- オプションの属性を含める*を選択した場合は、電子メール アドレス、電話番号、役割、州、国、部門、写真、マネージャー **DN**、またはグループも追加できます。オプションの検索クエリを追加するには、**[***詳細] を選択します。

5. 追加を選択します。
6. ユーザー ディレクトリ コネクタ タブに戻り、ユーザー ディレクトリ コネクタのステータスを確認します。正常に作成されると、ユーザー ディレクトリ コネクタのステータスは 実行中 と表示されます。

ユーザーディレクトリコネクタを削除する

手順

1. Ransomware Resilience で、[設定] に移動します。
2. ユーザー アクティビティ タイルを見つけて、[管理] を選択します。
3. ユーザー ディレクトリ コネクタ タブを選択します。
4. 削除するユーザー ディレクトリ コネクタを特定します。行末のアクションメニューで、3つの点を選択します。 `…`次に削除します。
5. ポップアップダイアログで、削除を選択して確認します。

特定の信頼できるユーザーの行動によってユーザー行動アラートがトリガーされる可能性がある場合は、そのユーザーをアラートから除外できます。

手順

1. ランサムウェア耐性で、[設定] を選択します。
2. 設定ダッシュボードで、ユーザーアクティビティカードを見つけて、管理を選択します。
3. 除外ユーザータブを選択します。
4. UI で個々のユーザーを確認するには、手動で選択を選択します。除外されたユーザーのリストをアップロードするには、アップロードを選択します。

   a. 手動で選択を選択した場合は、除外する特定のユーザーの名前の横にあるチェックボックスをオンにします。

   b. **Upload** を選択した場合は、すべてのユーザーのリストが含まれる CSV または JSON ファイルをダウンロードします。リストにアクセスするには、**Download** を選択します。

      ローカルマシンでファイルを確認します。検出を維持するすべてのユーザーの名前を削除します。検出から除外するユーザーの名前のみがリストに含まれたら、保存します。

   Ransomware Resilienceで、**Upload**を選択します。ファイルを見つけてアップロードします。

5. 除外リストへのユーザーの追加を完了するには、**[追加]** を選択します。
6. 除外ユーザータブでは、ユーザー行動検出アラートから削除されたユーザーの名前がダッシュボードに表示されるようになりました。

アラートからユーザーを直接除外することもできます。詳細については、"ランサムウェアの警告に応答する"を参照してください。

除外ユーザーリストからユーザーを削除する

後からユーザーを検出対象に再度追加することができます。

手順

1. 設定ダッシュボードで、ユーザーアクティビティカードを見つけて、管理を選択します。
2. 除外ユーザータブを選択します。
3. 追加を選択します。
4. UI から個々のユーザーを除外するには、手動で選択を選択します。
5. 除外ユーザーの選択から削除するユーザーの名前を見つけます。ユーザー名の行にあるアクションメニュー（(...）を選択し、削除を選択します。
6. ダイアログで、削除を選択して、選択したユーザーを削除することを確認します。

不審なユーザーアクティビティアラートに応答する

疑わしいユーザーアクティビティの検出を構成すると、アラートページでイベントを監視できます。詳細については、"悪意のあるアクティビティや疑わしいユーザーの行動を検出する"を参照してください。

NetApp Ransomware Resilience で保護グループを管理する

NetApp Ransomware Resilienceは、データ資産の管理を容易にするために保護グループを提供します。保護グループは、ワークロードを論理的にまとめたグループです。Ransomware Resilienceは、1つの保護戦略で保護グループ内のすべてのボリュームを同時に保護できるため、各ワークロードごとに戦略を適用する手間が省けます。

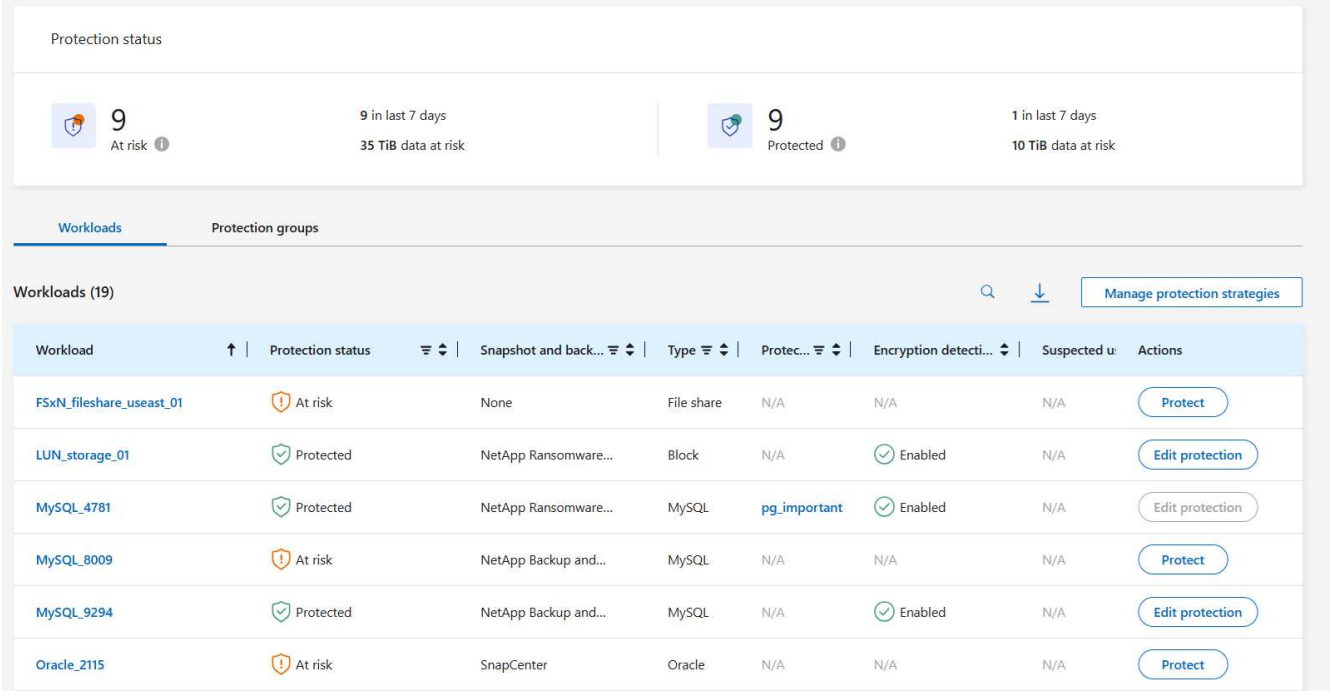
必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

保護グループを作成する

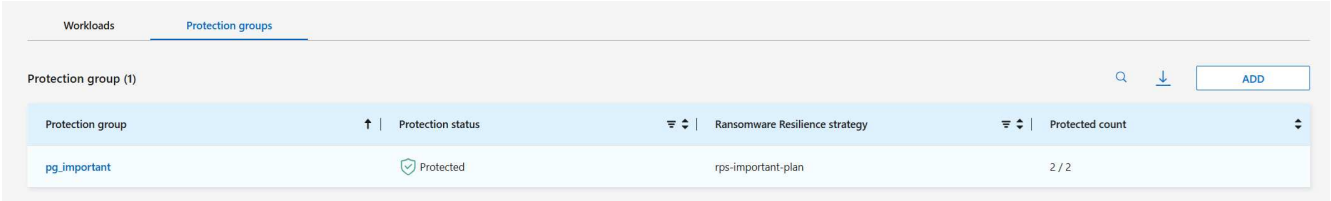
保護ステータスに関係なく（つまり、保護されていないグループと保護されているグループ）、グループを作成できます。保護グループに保護ポリシーを追加すると、新しい保護ポリシーは、NetApp Backup and Recoveryで管理されているポリシーを含む既存のポリシーをすべて置き換えます。

手順

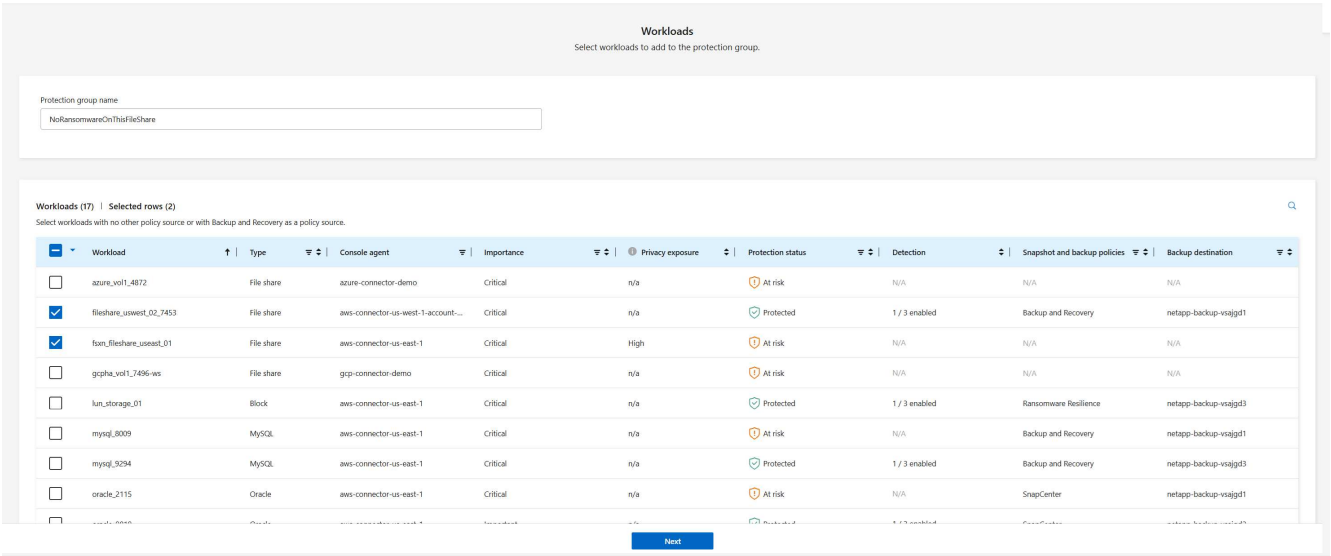
1. ランサムウェア耐性メニューから、*保護*を選択します。



2. 保護ダッシュボードから、*保護グループ*タブを選択します。



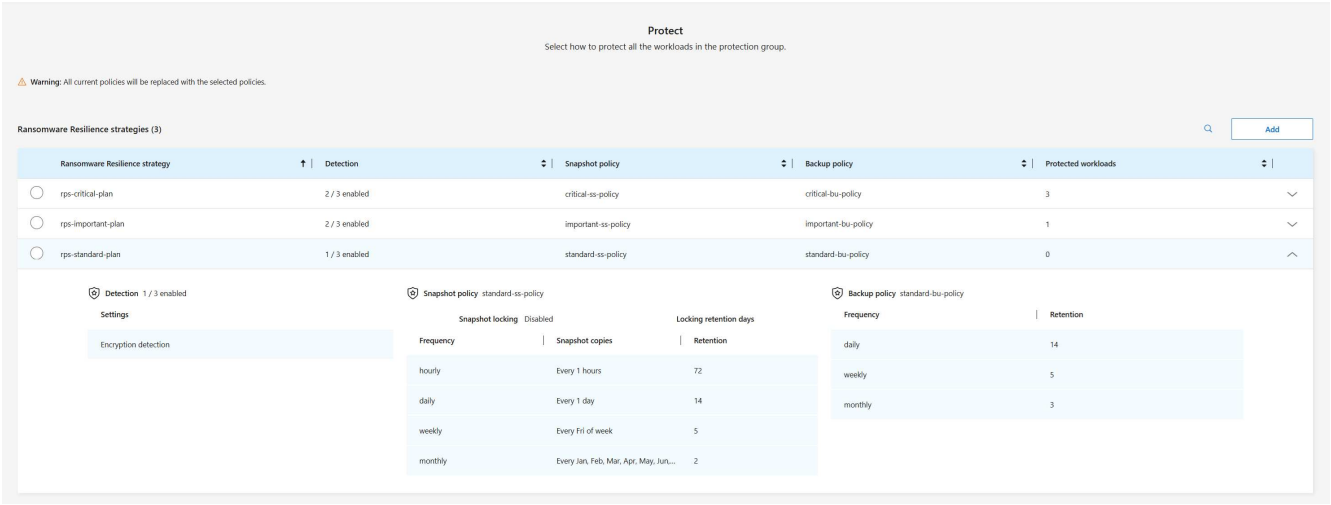
3. *追加*を選択します。



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. グループの保護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. 保護グループを確定するには、*追加*を選択します。

Ransomware Resilience の保護ダッシュボードを確認するときに、保護グループごとにワークロードを並べ替えることができます。

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

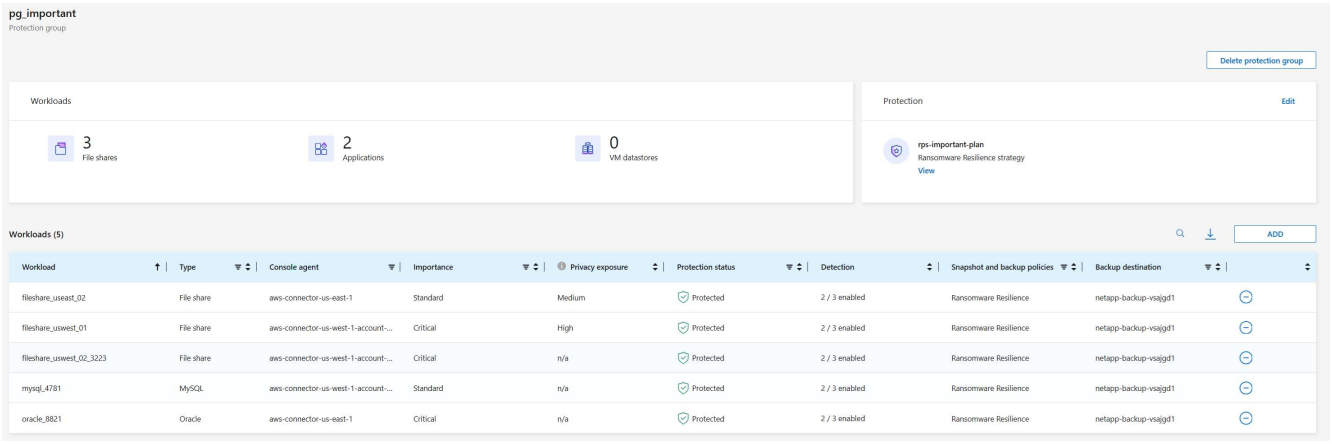
1. ランサムウェア耐性メニューから、*保護*を選択します。
2. [保護] ページで [保護グループ] タブを選択し、ポリシーを変更するグループを選択します。
3. 保護グループの概要ページで、*保護の編集*を選択します。
4. 既存の保護ポリシーを選択して適用するか、追加を選択して新しい保護ポリシーを作成します。保護ポリシーの追加の詳細については、"保護ポリシーを作成する"を参照してください。次に、保存を選択します。
5. バックアップ先の概要で、既存のバックアップ先を選択するか、新しいバックアップ先を追加します。
6. 変更内容を確認するには、[次へ] を選択します。

保護グループからワークロードを削除する

後で既存の保護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. 保護グループページで、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 ••• オプションを選択します。
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。

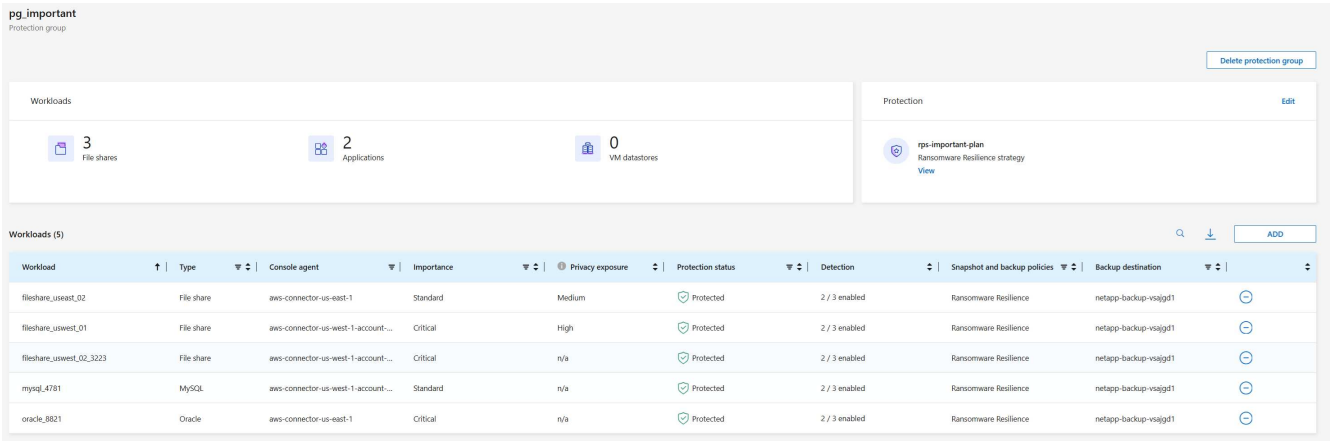
6. ワークロードを削除することを確認し、[削除] を選択します。

保護グループを削除する

保護グループを削除すると、NetApp Ransomware Resilienceによってグループとワークロードの保護戦略が削除されます。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。

NetApp Ransomware Resilienceでプライバシー侵害を特定

NetApp Ransomware Resilience内で、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。データを分類することで、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でき、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"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。

Data Classificationは、NetApp Consoleの中核コンポーネントです。Data Classificationを使用するのにライセンスは必要ありません。設定によっては、Data Classificationを構成するとコストが発生する可能性がありますが、これはRansomware Resilienceによって請求されません。詳細については、"データ分類について学ぶ"を参照してください。

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。

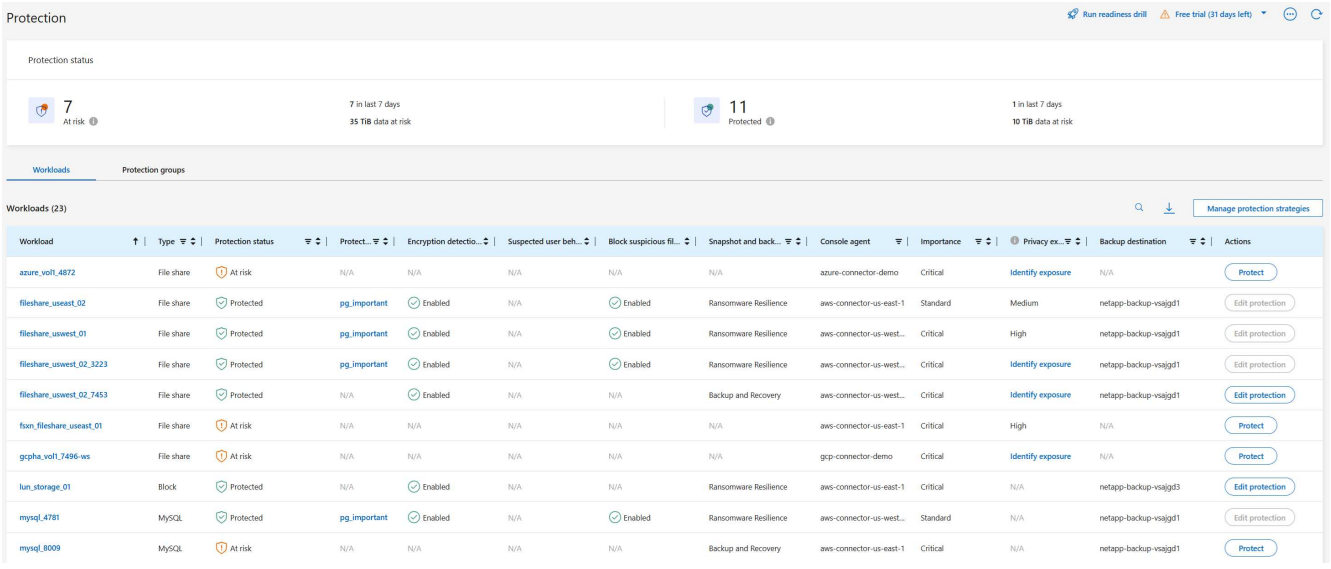
- "データ分類について学ぶ"
- "個人データのカテゴリ"
- "組織内に保存されているデータを調査する"

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

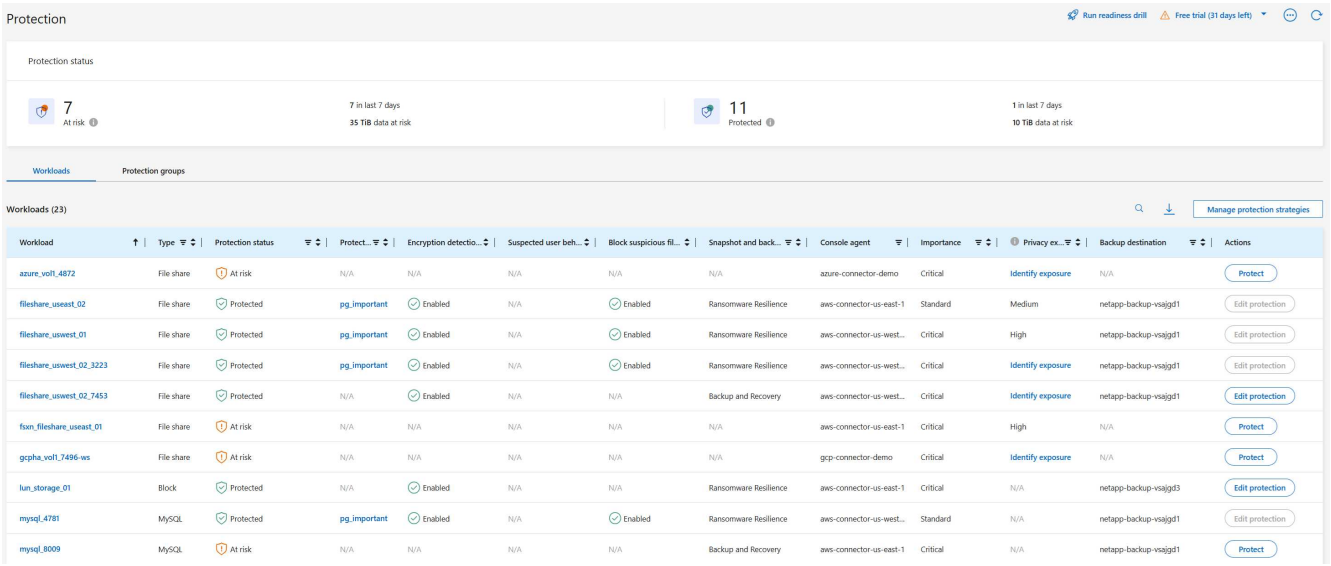
データ分類で PII をスキャンした後、リスクを評価します。

PII データは、次の 3 つの指定のいずれかに分類されます。

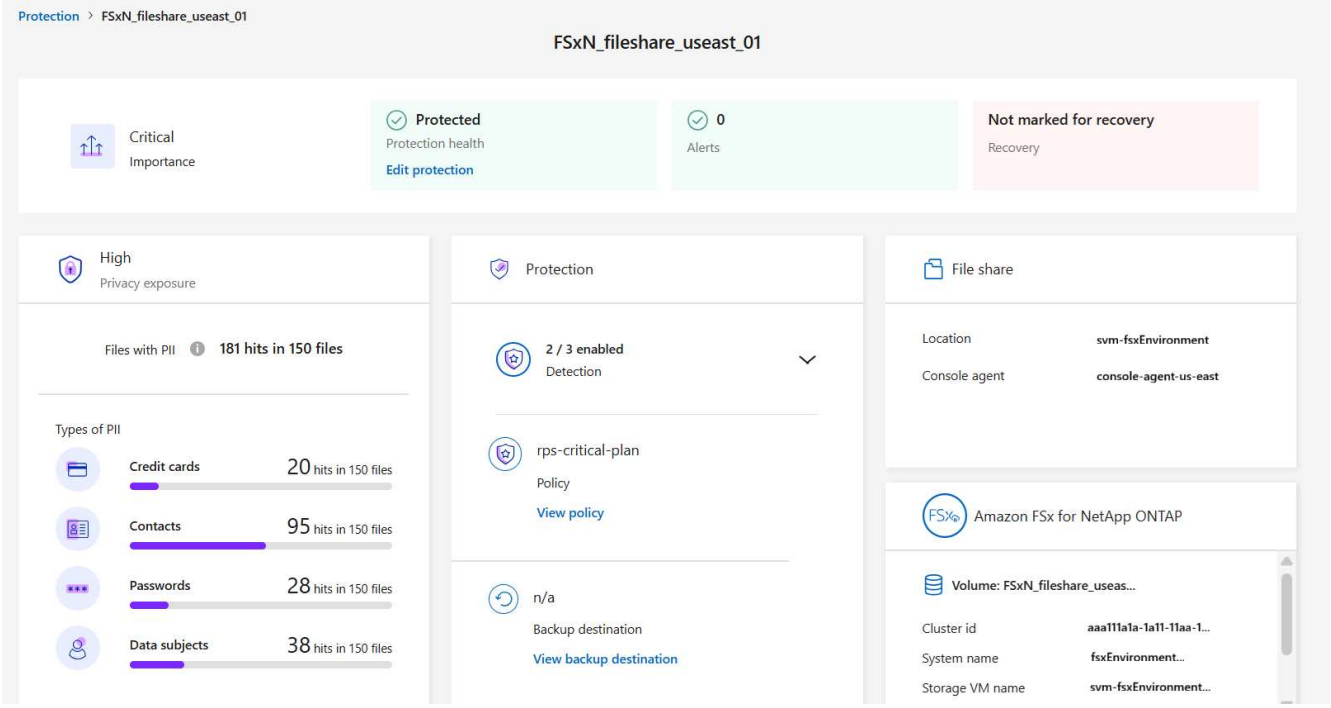
- 高: ファイルの 70% 以上に PII が含まれています
- 中: ファイルの 30% 以上 70% 未満に PII が含まれています
- 低: ファイルの 0% 以上 30% 未満に PII が含まれています

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
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"

著作権に関する情報

商標に関する情報