



ワーク LOAD を保護する NetApp Ransomware Resilience

NetApp
February 17, 2026

目次

ワーカークロードを保護する	1
NetApp Ransomware Resilience保護戦略でワーカ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
ワーカ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カ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。

The screenshot shows the 'Protection status' section of the NetApp SnapCenter interface. It displays two groups of workloads: 'At risk' (9 workloads, 35 TiB data at risk) and 'Protected' (9 workloads, 10 TiB data at risk). Below this, the 'Workloads' tab is selected, showing a list of 19 workloads with columns for Workload, Protection status, Snapshot and backup, Type, Protection, Encryption detection, Suspected ransomware, and Actions. The workloads listed include FSxN_fileshare_useast_01, LUN_storage_01, MySQL_4781, MySQL_8009, MySQL_9294, and Oracle_2115, each with its specific details and protection status.

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 but 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
重要なワークフロー 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
重要なワークフロー 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 のワークコ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。

ワークコ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。

Protection status

Workloads

Workloads (19)

Workload	Protection status	Snapshot and back...	Type	Protect...	Encryption detecti...	Suspected u...	Actions
FSxN_fileshare_useast_01	⚠️ At risk	None	File share	N/A	N/A	N/A	<button>Protect</button>
LUN_storage_01	🛡️ Protected	NetApp Ransomware...	Block	N/A	✅ Enabled	N/A	<button>Edit protection</button>
MySQL_4781	🛡️ Protected	NetApp Ransomware...	MySQL	pg_important	✅ Enabled	N/A	<button>Edit protection</button>
MySQL_8009	⚠️ At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	<button>Protect</button>
MySQL_9294	🛡️ Protected	NetApp Backup and...	MySQL	N/A	✅ Enabled	N/A	<button>Edit protection</button>
Oracle_2115	⚠️ At risk	SnapCenter	Oracle	N/A	N/A	N/A	<button>Protect</button>

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。

Add Ransomware Resilience strategy X

Add Ransomware Resilience strategy

Ransomware Resilience strategy name Copy from existing Ransomware Resilience strategy No policy selected

Detection 1 / 3 enabled

Snapshot policy Action required

Backup policy None

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、_不变ストレージ_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、ワーカ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、ワーカ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

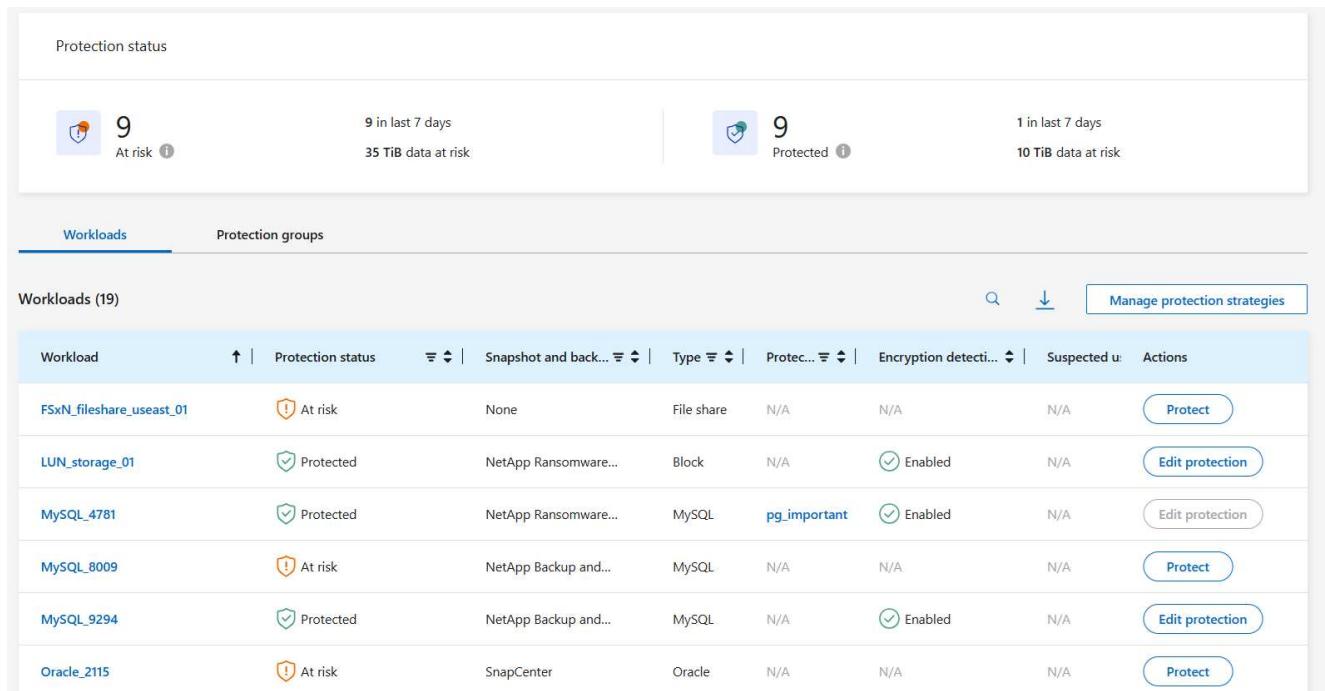
リストレージへのレプリケーション、またはオブジェクトストレージへのバックアップを管理するポリシーを使用します。

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。



Workload	Protection status	Snapshot and back...	Type	Protect...	Encryption detecti...	Suspected u...	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

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。

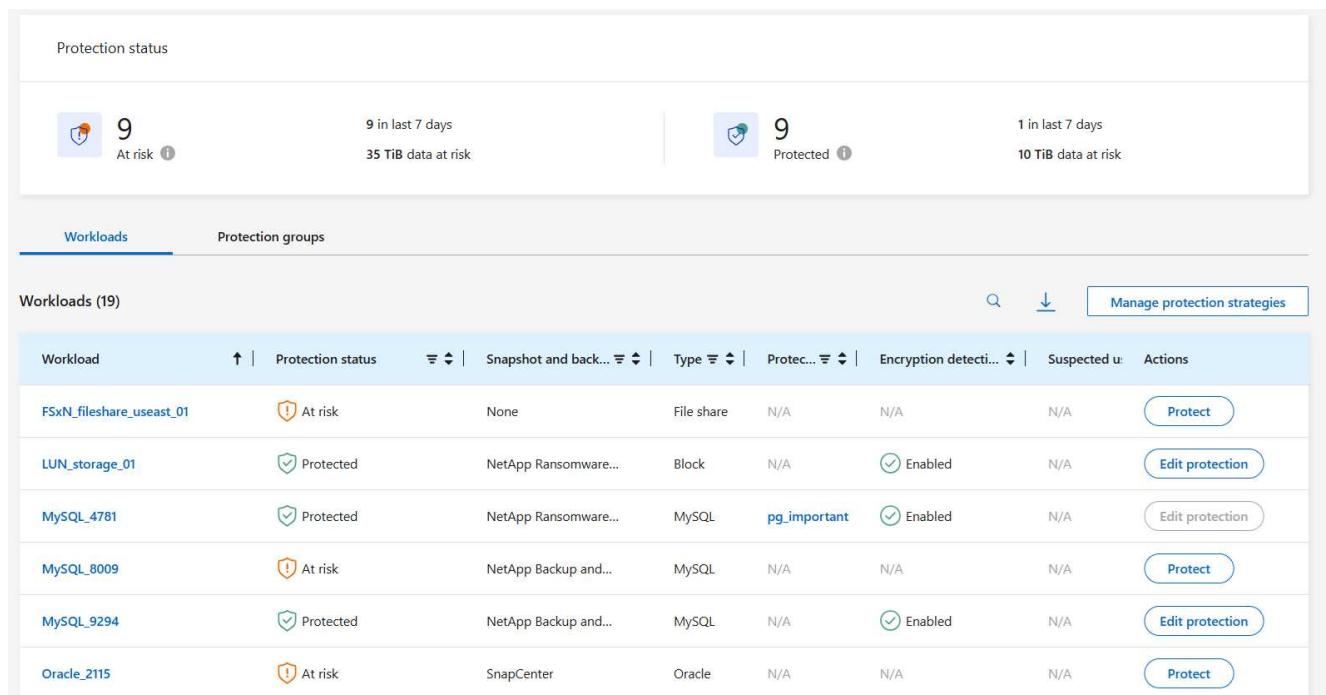
9. 次へを選択します。
10. 選択内容を確認します。検出を有効にするには、[作成] を選択します。
11. [保護] ページで、検出ステータスを確認して、検出がアクティブであることを確認します。

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。



The screenshot shows the 'Protection status' page. At the top, there are two sections: 'At risk' (9 items in last 7 days, 35 TiB data at risk) and 'Protected' (1 item in last 7 days, 10 TiB data at risk). Below this, there are tabs for 'Workloads' and 'Protection groups', with 'Workloads (19)' selected. The main table lists workloads with columns for name, protection status (e.g., At risk, Protected), snapshot and backup type, type, protection level, encryption detection, and suspected user. Actions like 'Protect', 'Edit protection', and 'Delete' are available for each row.

Workload	Protection status	Snapshot and back...	Type	Protect...	Encryption detecti...	Suspected u...	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	<button>Protect</button>
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	<button>Edit protection</button>
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	<button>Edit protection</button>
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	<button>Protect</button>
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	<button>Edit protection</button>
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	<button>Protect</button>

2. [保護] ページでワークフローを選択し、[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] ページのワークフロー行で、[保護の編集] を選択します。
3. ワークフローに、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。

Protection status


9
At risk

9 in last 7 days
35 TiB data at risk


9
Protected

1 in last 7 days
10 TiB data at risk

Workloads **Protection groups**

Workloads (19)

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u...	Actions
FSxN_fileshare_useast_01	⚠ At risk	None	File share	N/A	N/A	N/A	<button>Protect</button>
LUN_storage_01	🛡 Protected	NetApp Ransomware...	Block	N/A	✅ Enabled	N/A	<button>Edit protection</button>
MySQL_4781	🛡 Protected	NetApp Ransomware...	MySQL	pg_important	✅ Enabled	N/A	<button>Edit protection</button>
MySQL_8009	⚠ At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	<button>Protect</button>
MySQL_9294	🛡 Protected	NetApp Backup and...	MySQL	N/A	✅ Enabled	N/A	<button>Edit protection</button>
Oracle_2115	⚠ At risk	SnapCenter	Oracle	N/A	N/A	N/A	<button>Protect</button>

2. [保護] ページで、[保護グループ] タブを選択します。

Workloads **Protection groups**

Protection group (1)

Protection group	Protection status	Ransomware Resilience strategy	Protected count
pg_important	🛡 Protected	rps-important-plan	2 / 2

3. *追加*を選択します。

Workloads

Select workloads to add to the protection group.

Protection group name
NoRansomwareOnThisFileShare

Workloads (17) | Selected rows (2)

Select workloads with no other policy source or with Backup and Recovery as a policy source.

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection	Snapshot and backup policies	Backup destination
azure_voli_4872	File share	azure-connector-demo	Critical	n/a	⚠ At risk	N/A	N/A	N/A
<input checked="" type="checkbox"/> filesshare_useast_02_7453	File share	aws-connector-us-west-1-account-...	Critical	n/a	🛡 Protected	1 / 3 enabled	Backup and Recovery	netapp-backup-vsajgd1
<input checked="" type="checkbox"/> fom_fileshare_useast_01	File share	aws-connector-us-east-1	Critical	High	⚠ At risk	N/A	N/A	N/A
gcpfile_voli_1_496-aw	File share	gcp-connector-demo	Critical	n/a	⚠ At risk	N/A	N/A	N/A
lun_storage_01	Block	aws-connector-us-east-1	Critical	n/a	🛡 Protected	1 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd3
mysql_8009	MySQL	aws-connector-us-east-1	Critical	n/a	⚠ At risk	N/A	Backup and Recovery	netapp-backup-vsajgd1
mysql_9294	MySQL	aws-connector-us-east-1	Critical	n/a	🛡 Protected	1 / 3 enabled	Backup and Recovery	netapp-backup-vsajgd3
oracle_2115	Oracle	aws-connector-us-east-1	Critical	n/a	⚠ At risk	N/A	SnapCenter	netapp-backup-vsajgd1

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。

The screenshot shows the 'Protect' configuration page. At the top, it says 'Protect' and 'Select how to protect all the workloads in the protection group.' A warning message states 'Warning: All current policies will be replaced with the selected policies.' Below this is a table titled 'Ransomware Resilience strategies (3)'. The table has columns for 'Ransomware Resilience strategy', 'Detection', 'Snapshot policy', 'Backup policy', and 'Protected workloads'. There are three rows: 'rps-critical-plan' (2/3 enabled, critical-ss-policy, critical-bu-policy, 3), 'rps-important-plan' (2/3 enabled, important-ss-policy, important-bu-policy, 1), and 'rps-standard-plan' (1/3 enabled, standard-ss-policy, standard-bu-policy, 0). Below the table, there are three tabs: 'Encryption detection' (selected), 'Snapshot policy standard-ss-policy' (disabled, with frequency, snapshot copies, and retention settings), and 'Backup policy standard-bu-policy' (with frequency and retention settings).

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。

- 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

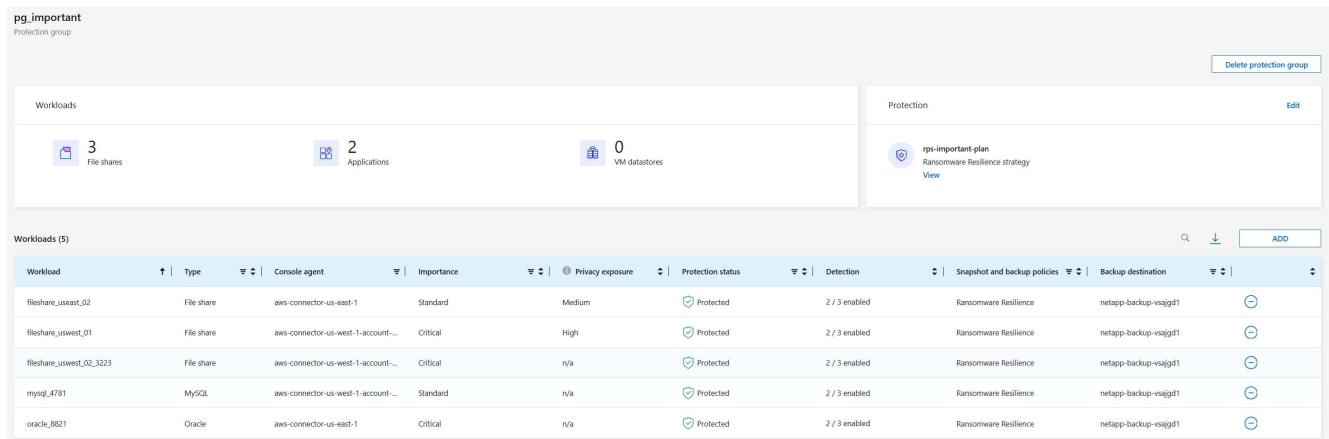
- ランサムウェア耐性メニューから、*保護*を選択します。
- [保護] ページで [保護グループ] タブを選択し、ポリシーを変更するグループを選択します。
- 保護グループの概要ページで、*保護の編集*を選択します。
- 適用する既存の保護ポリシーを選択するか、[追加] を選択して新しい保護ポリシーを作成します。保護ポリシーの追加の詳細については、以下を参照してください。[保護ポリシーを作成する](#)。次に、[保存] を選択します。
- バックアップ先の概要で、既存のバックアップ先を選択するか、新しいバックアップ先を追加します。
- 変更内容を確認するには、[次へ] を選択します。

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。



The screenshot shows the 'Protection group' page with the following details:

Workloads (5):

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection	Snapshot and backup policies	Backup destination
fileshare_uswest_02	File share	aws-connector-us-east-1	Standard	Medium	Protected	2/3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
fileshare_uswest_01	File share	aws-connector-us-west-1-account-...	Critical	High	Protected	2/3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
fileshare_uswest_02_3223	File share	aws-connector-us-west-1-account-...	Critical	n/a	Protected	2/3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
mysql_4781	MySQL	aws-connector-us-west-1-account-...	Standard	n/a	Protected	2/3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
oracle_8821	Oracle	aws-connector-us-east-1	Critical	n/a	Protected	2/3 enabled	Ransomware Resilience	netapp-backup-vsajgd1

Protection

- rps-important-plan (Ransomware Resilience strategy)

Buttons: Delete protection group, Edit, ADD.

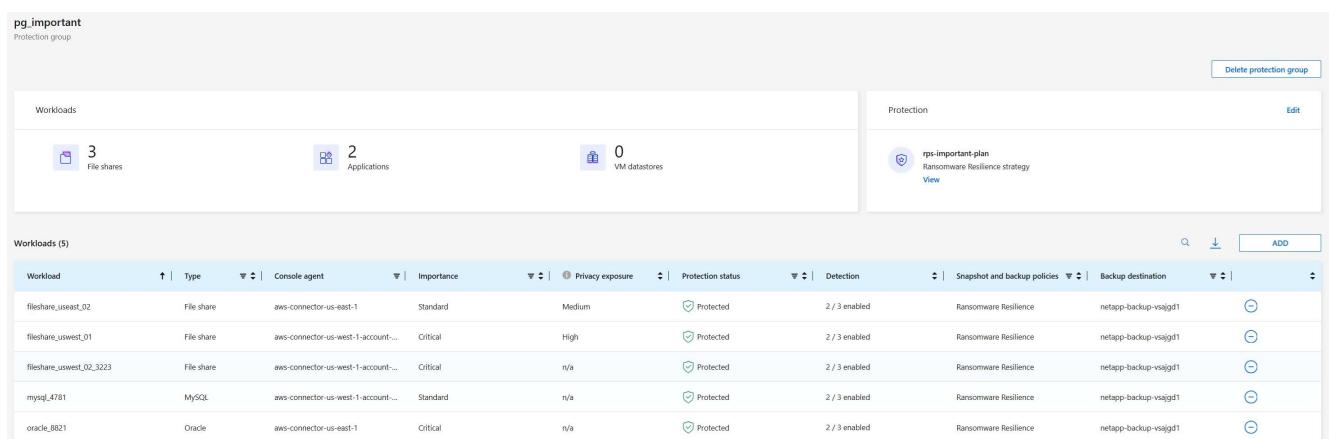
4. 選択した保護グループのページで、グループから削除するワークロードを選択し、*アクション*を選択します。...オプション。
5. [アクション] メニューから、[ワークロードの削除] を選択します。
6. ワークロードを削除することを確認し、[削除] を選択します。

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。



The screenshot shows the 'Protection group' page with the following details:

Workloads (5):

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection	Snapshot and backup policies	Backup destination
fileshare_uswest_02	File share	aws-connector-us-east-1	Standard	Medium	Protected	2/3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
fileshare_uswest_01	File share	aws-connector-us-west-1-account-...	Critical	High	Protected	2/3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
fileshare_uswest_02_3223	File share	aws-connector-us-west-1-account-...	Critical	n/a	Protected	2/3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
mysql_4781	MySQL	aws-connector-us-west-1-account-...	Standard	n/a	Protected	2/3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
oracle_8821	Oracle	aws-connector-us-east-1	Critical	n/a	Protected	2/3 enabled	Ransomware Resilience	netapp-backup-vsajgd1

Protection

- rps-important-plan (Ransomware Resilience strategy)

Buttons: Delete protection group, Edit, ADD.

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。

Ransomware Resilience strategies (4) Selected rows (1)						
Ransomware Resilience strategy	Detection	Snapshot policy	Backup policy	Protected workloads		
<input type="radio"/> rps-critical-plan	2 / 3 enabled	critical-ss-policy	critical-bu-policy	3		
<input type="radio"/> rps-important-plan	2 / 3 enabled	important-ss-policy	important-bu-policy	1		
<input checked="" type="radio"/> rps-standard-plan Recommended	1 / 3 enabled	standard-ss-policy	standard-bu-policy	0		
<input type="radio"/> rr-strategy-enc-user-ext	3 / 3 enabled	standard-ss-policy	standard-bu-policy	0		

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ために役立ちます。

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。

Protection status

7 in last 7 days
35 TiB data at risk

11 Protected
1 in last 7 days
10 TiB data at risk

Workloads (23)

Workload	Type	Protection status	pg_important	Enabled	Suspected user beh...	Block suspicious fil...	Snapshot and back...	Console agent	Importance	Privacy ex...	Backup destination	Actions
azure_voh_4672	File share	At risk	N/A	N/A	N/A	N/A	aws-connector-demo	Critical	Identify exposure	N/A	<button>Protect</button>	
fileshare_uswest_02	File share	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-east-1	Standard	Medium	netapp-backup-vsajgd1	<button>Edit protection</button>
fileshare_uswest_01	File share	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-west...	Critical	High	netapp-backup-vsajgd1	<button>Edit protection</button>
fileshare_uswest_02_3223	File share	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-west...	Critical	Identify exposure	netapp-backup-vsajgd1	<button>Edit protection</button>
fileshare_uswest_02_7453	File share	Protected	N/A	Enabled	N/A	N/A	Backup and Recovery	aws-connector-us-west...	Critical	Identify exposure	netapp-backup-vsajgd1	<button>Edit protection</button>
fsnx_fileshare_useast_01	File share	At risk	N/A	N/A	N/A	N/A	aws-connector-us-east-1	Critical	High	N/A	<button>Protect</button>	
gcpfa_volt_7496-ws	File share	At risk	N/A	N/A	N/A	N/A	gcp-connector-demo	Critical	Identify exposure	N/A	<button>Protect</button>	
lun_storage_01	Block	Protected	N/A	Enabled	N/A	N/A	Ransomware Resilience	aws-connector-us-east-1	Critical	N/A	netapp-backup-vsajgd3	<button>Edit protection</button>
mysql_4781	MySQL	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-west...	Standard	N/A	netapp-backup-vsajgd1	<button>Edit protection</button>
mysql_8009	MySQL	At risk	N/A	N/A	N/A	N/A	Backup and Recovery	aws-connector-us-east-1	Critical	N/A	netapp-backup-vsajgd1	<button>Protect</button>

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

- ランサムウェア耐性メニューから、*保護*を選択します。
- [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。

The screenshot shows the AWS Backup Protection dashboard. At the top, there are three summary cards: 'At risk' (7), 'Protected' (11), and 'Data at risk' (10 TiB). Below these are sections for 'Workloads' and 'Protection groups'. The 'Workloads' section lists 23 items, including 'azure_voh_4672', 'fileshare_useast_02', 'fileshare_useast_01', etc., with columns for Workload, Type, Protection status, and various protection settings like Encryption detection, Suspected user behavior, and Block suspicious files. The 'Protection groups' section is currently empty.

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。

The screenshot shows the detailed view for the 'FSxN_fileshare_useast_01' workload. The top navigation bar shows 'Protection > FSxN_fileshare_useast_01'. The main header is 'FSxN_fileshare_useast_01'. The top section displays 'Protected' status with '0' alerts and a note 'Not marked for recovery'. Below this, there are three main panels: 'Privacy exposure' (High, 181 hits in 150 files, types: Credit cards, Contacts, Passwords, Data subjects), 'Protection' (2/3 enabled, Detection policy: rps-critical-plan, Backup destination: n/a), and 'File share' (Location: svm-fsxEnvironment, Console agent: console-agent-us-east, Volume: FSxN_fileshare_useast_01, Cluster id: aea111a1a-1a11-11aa-1, System name: fsxEnvironment, Storage VM name: svm-fsxEnvironment).

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、ワーカロードの重要度は次のようにになります。
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"

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を隨時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5225.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。