ランサムウェア耐性を活用する
NetApp Ransomware Resilience

NetApp
February 27, 2026

目次

ランサムウェア耐性を活用する

NetApp Ransomware Resilienceにアクセス

NetApp Ransomware Resilienceにアクセスするには、NetApp Consoleからログインする必要があります。

コンソールにログインするには、 NetAppサポート サイトの認証情報を使用するか、電子メールとパスワードを使用してNetAppクラウド ログインにサインアップすることができます。 "ログインについて詳しくはこちら" 。

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、ランサムウェア レジリエンス管理者、またはランサムウェア レジリエンス ビューアー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" 。

手順

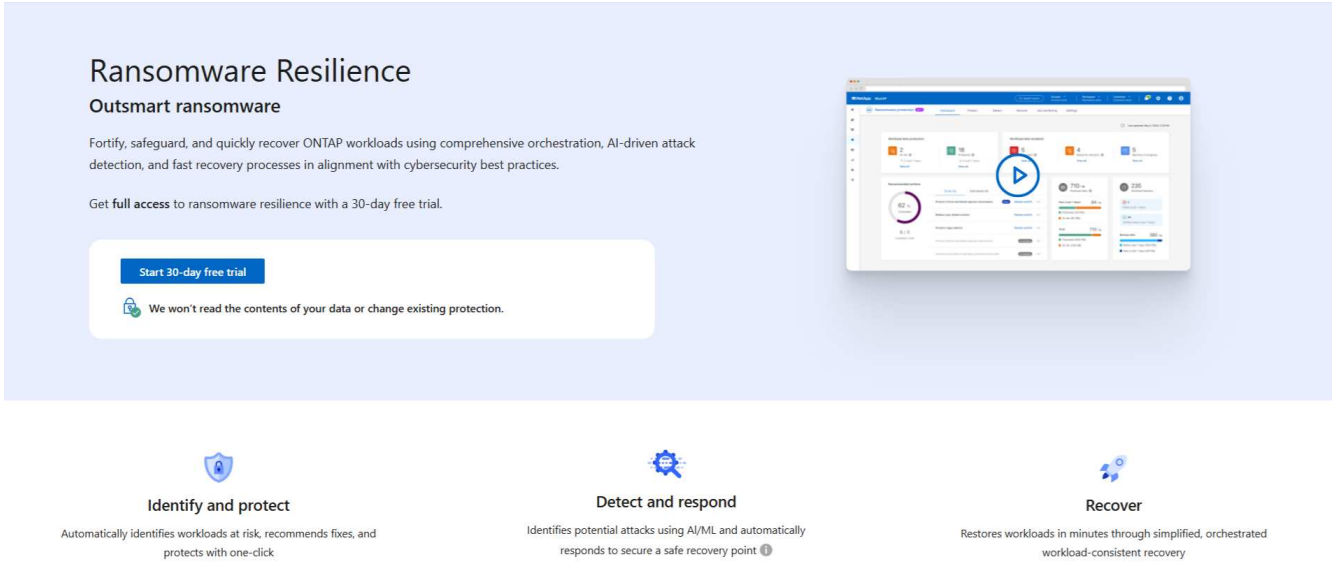
1. ウェブブラウザを開いて"コンソール"。

   コンソールのログイン ページが表示されます。

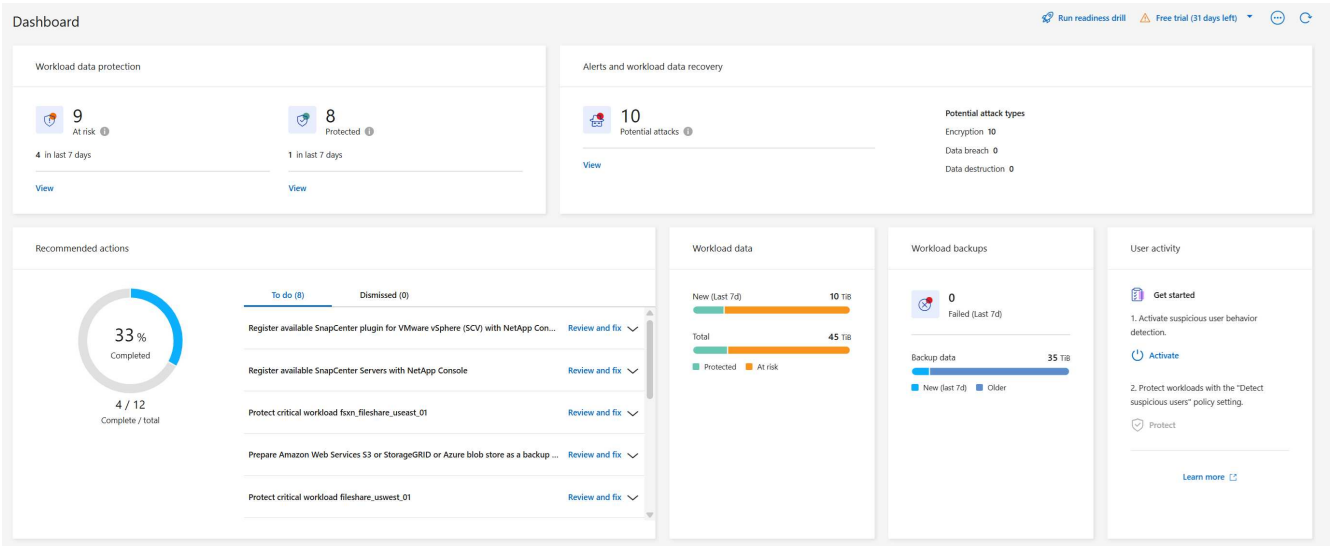
2. コンソールにログインします。
3. コンソールの左側のナビゲーションから、保護 > *ランサムウェア耐性*を選択します。

   このサービスに初めてログインする場合は、ランディング ページが表示されます。

   コンソール エージェントがない場合、またはこのサービス用のエージェントではない場合は、コンソール エージェントを展開する必要があります。"コンソールエージェントの設定方法を学ぶ" 。



それ以外の場合は、ランサムウェア耐性ダッシュボードが表示されます。



4. まだ行っていない場合は、[ワークロードの検出] オプションを選択します。

。 "ワークロードの検出" 。

NetApp Ransomware Resilienceでワークロードの健全性を監視する

NetApp Ransomware Resilienceダッシュボードでは、ワークロードの保護の健全性に関する情報が一目でわかります。危険にさらされているワークロードや保護されているワークロードを迅速に判断し、インシデントの影響を受けているワークロードや回復中のワークロードを識別し、保護されているストレージや危険にさらされているストレージの量を確認して保護の範囲を評価できます。

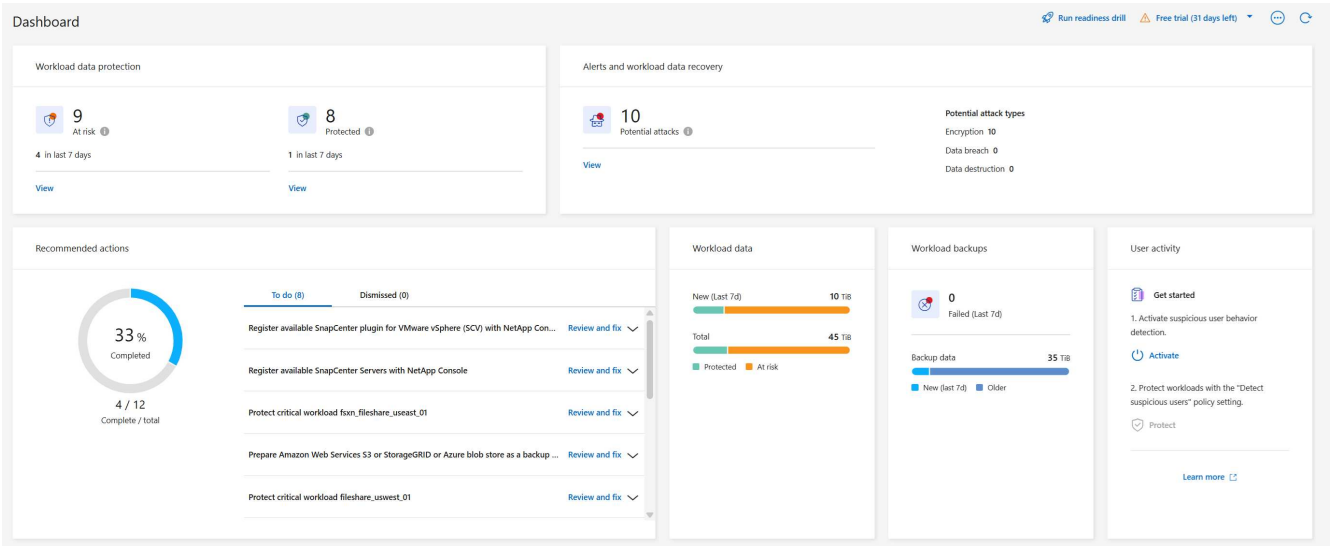
ダッシュボードを使用して、保護の提案を確認したり、設定を変更したり、レポートをダウンロードしたりできます。

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、ランサムウェア レジリエンス管理者、またはランサムウェア レジリエンス ビューアー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" 。

ダッシュボードを使用してワークロードの健全性を確認する

手順

1. コンソールがワークロードを検出すると、ランサムウェア耐性ダッシュボードにワークロード データ保護の健全性が表示されます。



ページ"]

2. ダッシュボードから、各ペインで次のアクションを実行できます：

   - ワークロード データ保護: [保護] ページで、危険にさらされている、または保護されているすべてのワークロードを表示するには、[すべて表示] を選択します。保護レベルが保護ポリシーと一致しない場合、ワークロードは危険にさらされます。。 "ワークロードを保護する" 。

     このデータに関するヒントを表示するには、「i」ツールヒントを選択します。ワークロード制限を増やすには、このｉノート内の ワークロード制限を増やす を選択します。これを選択すると、コンソール サポート ページに移動し、ケース チケットを作成できます。

   - アラートとワークロード データの回復: [すべて表示] を選択すると、ワークロードに影響を与えたアクティブなインシデント、インシデントが解決された後に回復の準備ができているアクティブなインシデント、または回復中のアクティブなインシデントが表示されます。。 "検出されたアラートに応答する" 。

     - インシデントは次のいずれかの状態に分類されます。
       - 新規
       - 却下済み
       - 却下
       - 解決済み
     - アラートのステータスは次のいずれかになります。
       - 新規
       - 非アクティブ
     - ワークロードの復元ステータスは次のいずれかになります。
       - 復元が必要
       - 実行中
       - 復元
       - 失敗

- 推奨されるアクション: 保護を強化するには、各推奨事項を確認し、[確認して修正] を選択します。

  "ダッシュボードで保護の提案を確認する"または"ワークロードを保護する"を参照してください。

  Ransomware Resilienceでは、ダッシュボードに最後にアクセスしてから24時間、新しい推奨事項が「新規」タグ付きで表示されます。アクションは優先度順に表示され、最も重要なアクションが一番上に表示されます。各推奨事項を確認し、それに基づいて対応したり、却下したりします。

アクションの合計数には、却下したアクションは含まれません。

- ワークロード データ: 過去 7 日間の保護範囲の変化を監視します。
- ワークロード バックアップ: 過去 7 日間に失敗または正常に完了した、Ransomware Resilience によって作成されたワークロード バックアップの変更を監視します。

ダッシュボードで保護の推奨事項を確認する

ランサムウェア耐性は、ワークロードの保護を評価し、その保護を改善するためのアクションを推奨します。

推奨事項を確認して対応することで、推奨事項のステータスが「完了」に変わります。または、後で対応したい場合は、無視することもできます。アクションを却下すると、推奨事項は却下されたアクションのリストに移動され、後で確認できるようになります。

以下は、Ransomware Resilience が提供する推奨事項の一部です。

推奨事項	説明	解決方法
ランサムウェア保護ポリシーを追加します。	ワークロードは現在保護されていません。	ワークロードにポリシーを割り当てます。。 "ランサムウェア攻撃からワークロードを保護する" 。
脅威レポートのために SIEM に接続します。	脅威の分析と検出のために、データをセキュリティおよびイベント管理システム (SIEM) に送信します。	脅威検出を有効にするには、SIEM/XDR サーバーの詳細を入力します。"SIEMに接続する"を参照してください。
システムのセキュリティ体制の改善	NetApp Digital Advisor は、少なくとも 1 つの高または重大なセキュリティ リスクを特定しました。	NetApp Digital Advisorですべてのセキュリティ リスクを確認します。参照 "Digital Advisorのドキュメント"。
政策をさらに強化します。	一部のワークロードでは十分な保護が得られない可能性があります。ポリシーを使用してワークロードの保護を強化します。	保持期間の延長、バックアップの追加、不変のバックアップの強制、疑わしいファイル拡張子のブロック、セカンダリ ストレージでの検出の有効化など。。 "ランサムウェア攻撃からワークロードを保護する" 。
ワークロード データをバックアップするためのバックアップ先として <バックアップ プロバイダー> を準備します。	現在、ワークロードにはバックアップ先がありません。	このワークロードを保護するには、バックアップ先を追加します。"バックアップ先を追加する"を参照してください。

推奨事項	説明	解決方法
重要な、または非常に重要なアプリケーションのワークロードをランサムウェアから保護します。	[保護] ページには、保護されていない重要な、または非常に重要な (割り当てられた優先度レベルに基づく) アプリケーション ワークロードが表示されます。	これらのワークロードにポリシーを割り当てます。。 "ランサムウェア攻撃からワークロードを保護する" 。
重要な、または非常に重要なファイル共有ワークロードをランサムウェアから保護します。	[保護] ページには、保護されていないファイル共有またはデータストア タイプの重要なワークロードまたは非常に重要なワークロードが表示されます。	各ワークロードにポリシーを割り当てます。"ランサムウェア攻撃からワークロードを保護する"を参照してください。"ランサムウェア攻撃からワークロードを保護する"を参照してください。"ランサムウェア攻撃からワークロードを保護する"を参照してください。
新しいアラートを確認します。	新しいアラートが存在します。	新しいアラートを確認します。。 "検出されたランサムウェアアラートに応答する" 。

手順

1. ランサムウェア耐性の「推奨アクション」ペインから推奨事項を選択し、「確認して修正」します。
2. 後でアクションを閉じるには、[閉じる] を選択します。

   推奨事項は To Do リストから消去され、却下リストに表示されます。

   後で、却下した項目を To Do 項目に変更できます。アイテムを完了としてマークするか、却下したアイテムを To Do アクションに変更すると、アクションの合計が 1 つ増加します。

3. 推奨事項に基づいて行動する方法に関する情報を確認するには、*情報*アイコンを選択します。

保護データを**CSV**ファイルにエクスポートする

データをエクスポートし、保護、アラート、回復の詳細を示す CSV ファイルをダウンロードできます。

メイン メニュー オプションのいずれかから CSV ファイルをダウンロードできます。

- 保護: ランサムウェア耐性によって保護または危険とマークされたワークロードの合計数など、すべてのワークロードのステータスと詳細が含まれます。
- アラート: アラートの合計数や自動スナップショットなど、すべてのアラートのステータスと詳細が含まれます。
- 回復: 復元が必要なすべてのワークロードのステータスと詳細が含まれます。これには、Ransomware Resilience によって「復元が必要」、「進行中」、「復元に失敗しました」、「正常に復元されました」とマークされたワークロードの合計数が含まれます。

ページから CSV ファイルをダウンロードすると、そのページのデータのみが含まれます。

CSV ファイルには、すべてのコンソール システム上のすべてのワークロードのデータが含まれます。

手順

1. ランサムウェア耐性ダッシュボードから*更新*を選択します。  右上のオプションを選択すると、ファイルに表示されるデータが更新されます。
2. 次のいずれかを実行します。
   - ページから*ダウンロード*を選択します  オプション。
   - ランサムウェア耐性メニューから、*レポート*を選択します。
3. レポート オプションを選択した場合は、事前設定された名前付きファイルの 1 つを選択し、ダウンロード **(CSV)** または ダウンロード **(JSON)** を選択します。

技術文書にアクセスする

ランサムウェア耐性に関する技術文書は以下からアクセスできます。"docs.netapp.com"または、ランサムウェア耐性の内部から。

手順

1. ランサムウェア耐性ダッシュボードから、垂直の*アクション*を選択します。  オプション。
2. 次のいずれかのオプションを選択します。
   - 新機能 では、リリース ノートの現在のリリースまたは以前のリリースの機能に関する情報を表示します。
   - ドキュメント ランサムウェア耐性ドキュメントのホームページとこのドキュメントを表示します。

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

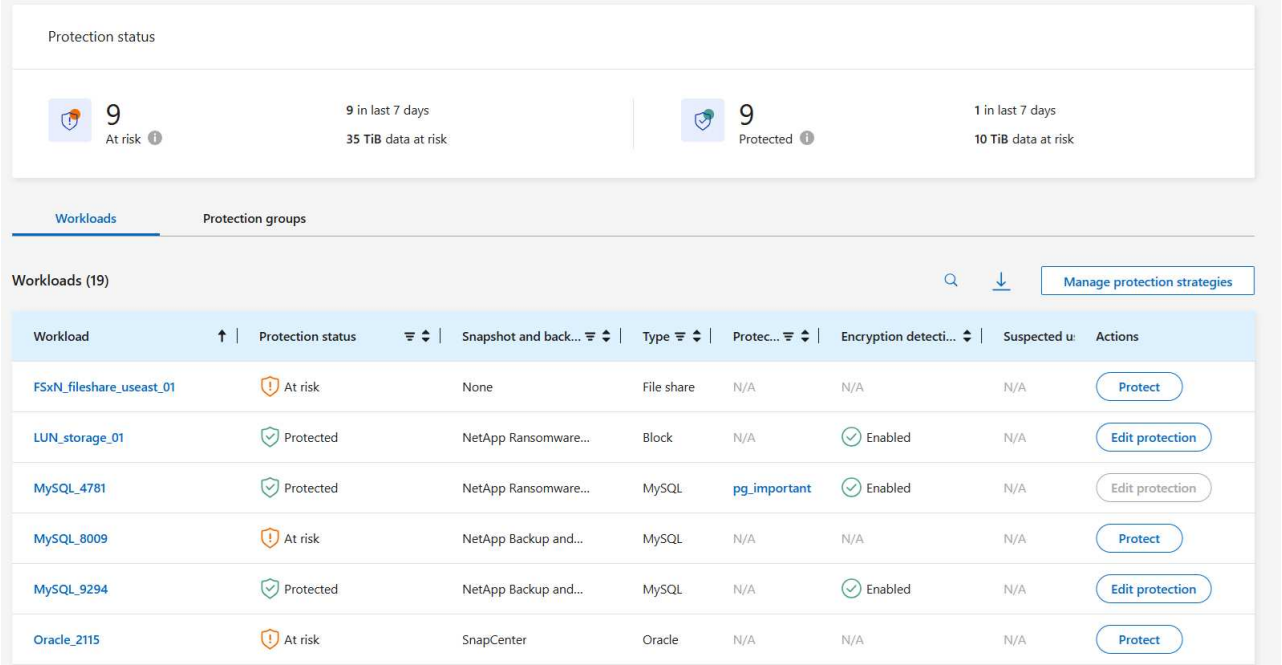
ワークロードを保護するための最初のステップの 1 つは、現在のワークロードとその保護ステータスを確認することです。次の種類のワークロードを確認できます。

- 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。

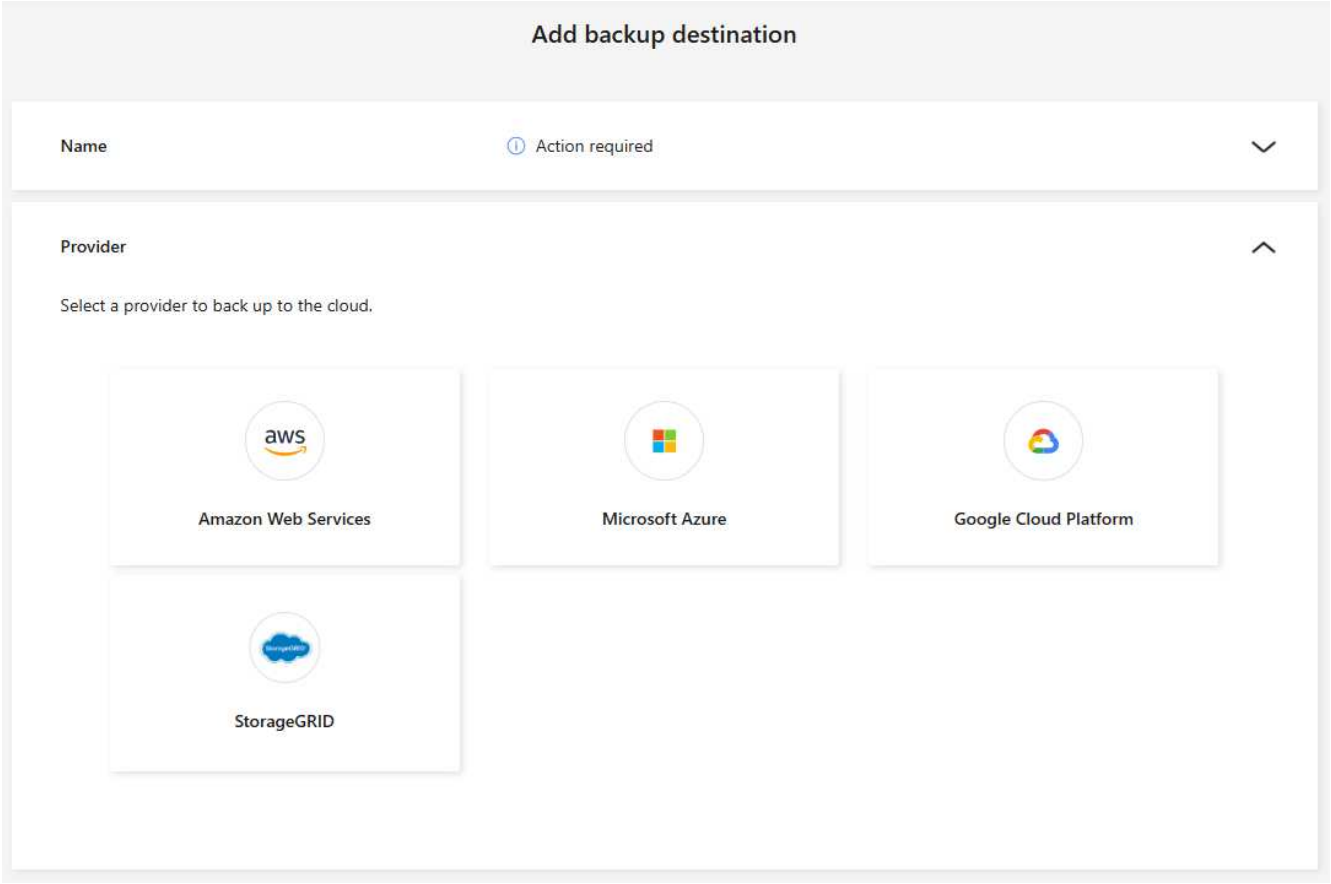
必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

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。



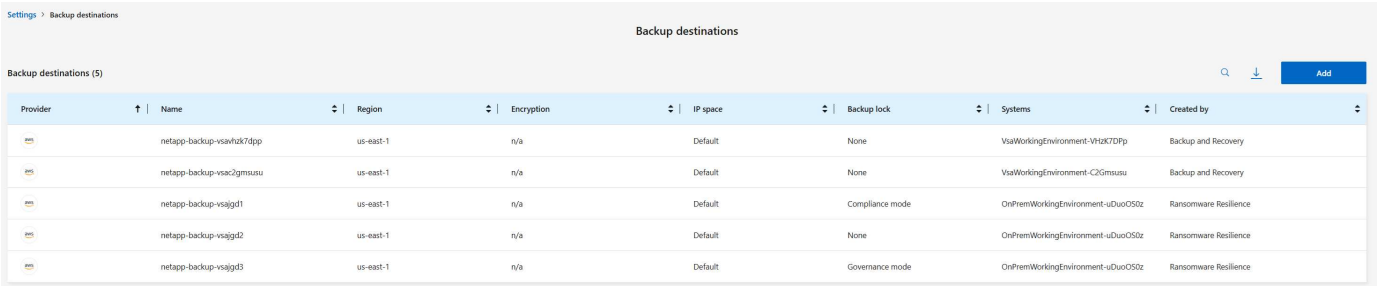
5. * StorageGRID*を選択します。

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。

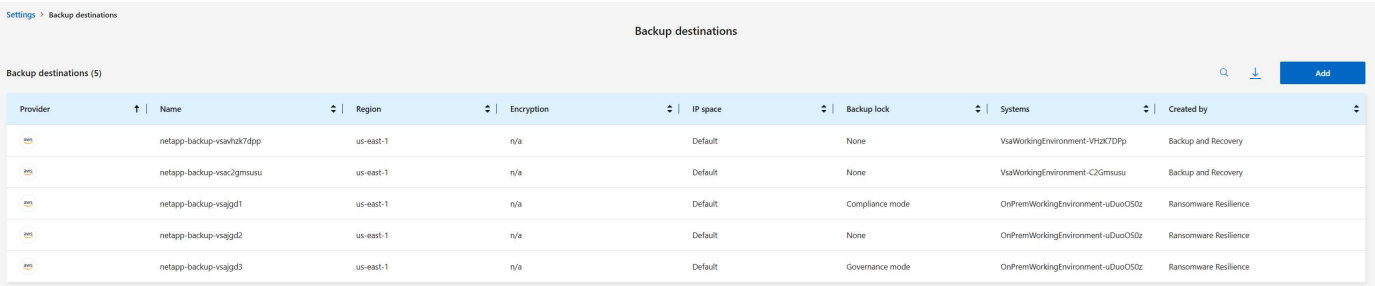
> ここでバックアップロック設定を構成すると、バックアップ先の構成後に設定を変更することはできません。

- 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。



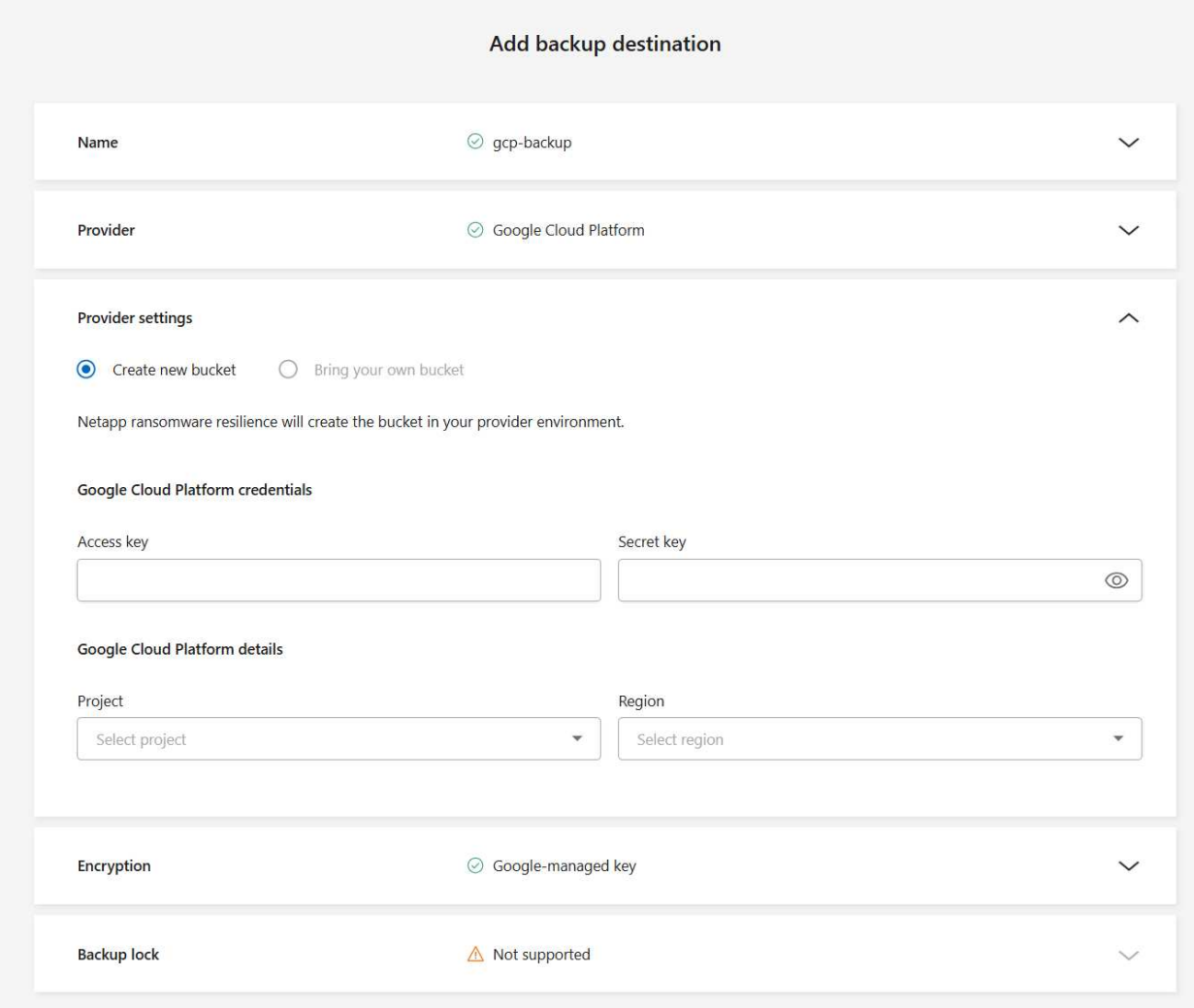
Google Cloud Platform をバックアップ先として追加する

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。

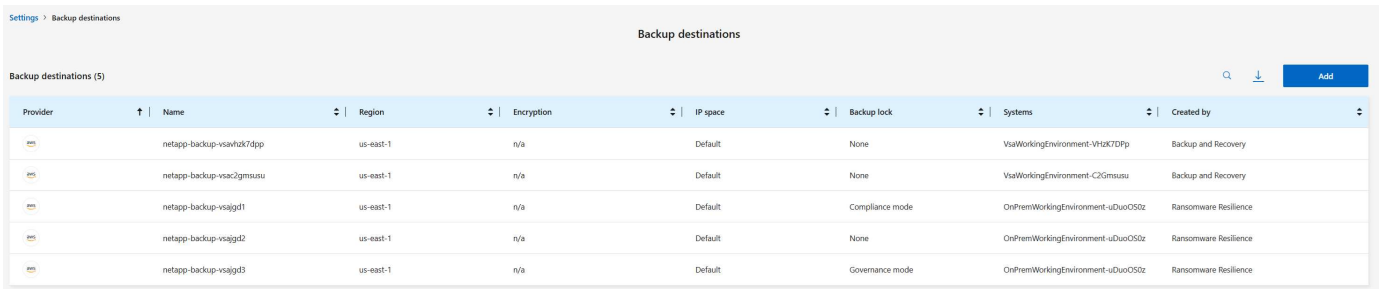
       "独自のストレージ アカウントを使用する場合は、「Azure Blob ストレージ アカウントの追加」を参照してください。" 。
   - 暗号化：デフォルトでは、データは Microsoft が管理するキーで暗号化されます。このオプションを維持するには、**Microsoft** が管理するキーを選択します。または、暗号化に独自のキーを使用するには、顧客が管理するキーを選択します。
   - ネットワーク: IPspace を選択し、プライベート エンドポイントを使用するかどうかを選択します。
     - IPspace は、バックアップするボリュームが存在するクラスターです。この IPspace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

Ransomware Resilienceは、VMデータストア用のSnapCenter for VMwareおよびOracle用のSnapCenterから保護ポリシーも検出します。これらのサービスを使用してRansomware Resilienceでリストアすることはできません。

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"。

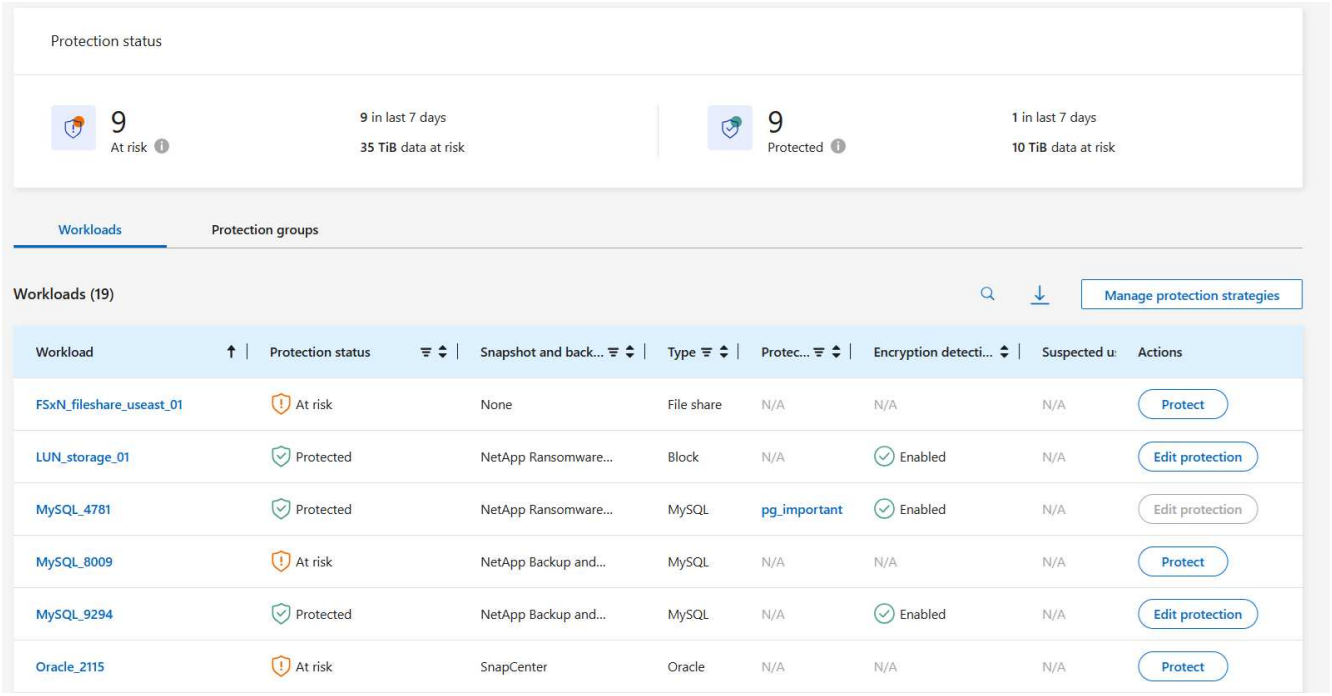
ランサムウェア対策戦略を作成する（スナップショットやバックアップポリシーがない場合）

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。

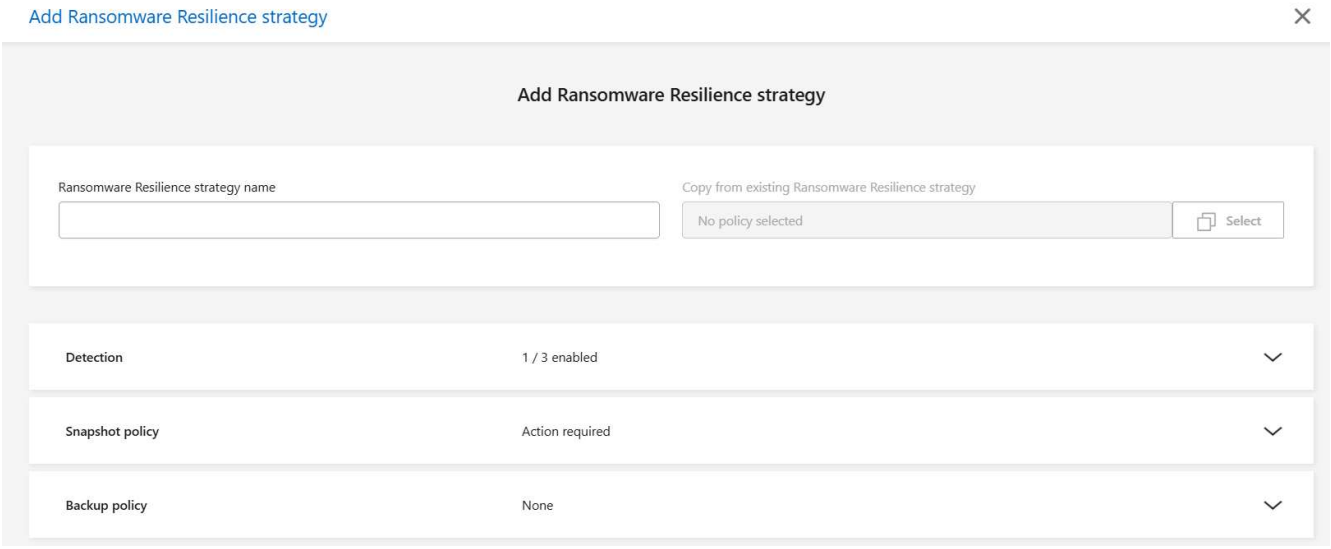
- スナップショットポリシー
- バックアップ ポリシー
- ランサムウェア検出ポリシー
- ONTAPへのセカンダリレプリケーション

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

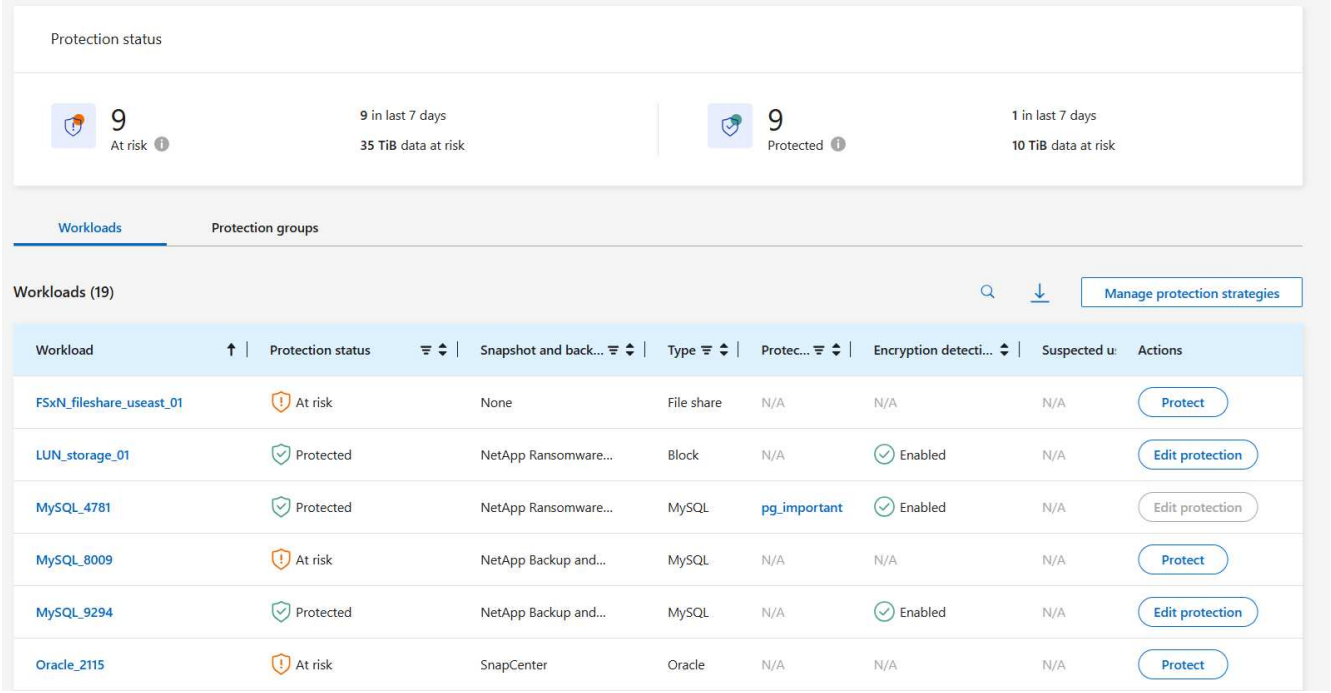
Ransomware Resilienceでは、他のNetApp製品またはサービスで管理されている既存のスナップショットおよびバックアップ保護を使用するワークロードに、検出ポリシーまたは保護ポリシーを割り当てることができます。Backup and Recoveryでは、スナップショット、セカンダリストレージへのレプリケーション、またはオブジェクトストレージへのバックアップを管理するポリシーを使用します。

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。

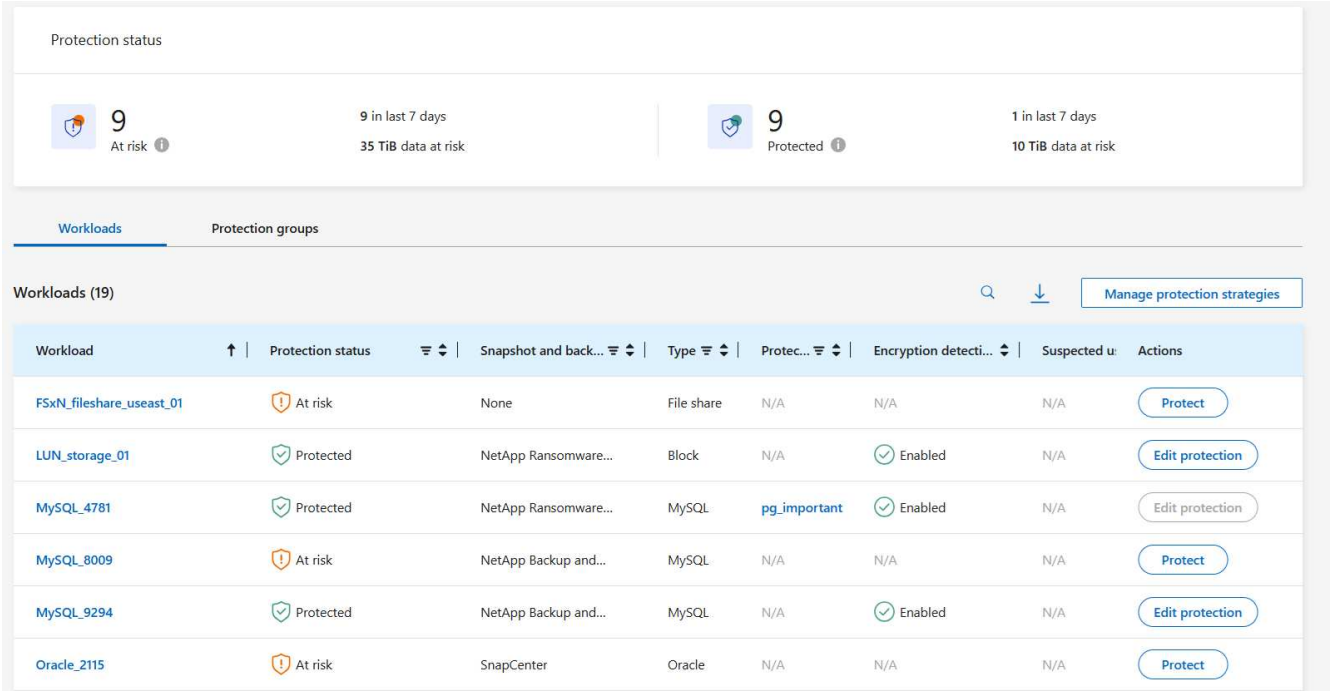
   ユーザー アクティビティ エージェントは新しいデータ コレクターをホストします。Ransomware Resilience は、データ コレクターを自動的に作成し、ユーザー アクティビティ イベントを Ransomware Resilience に送信して、異常なユーザー動作を検出します。
8. 次へを選択します。
9. 選択内容を確認します。検出を有効にするには、[作成] を選択します。
10. [保護] ページで、検出ステータス を確認して、検出がアクティブであることを確認します。

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

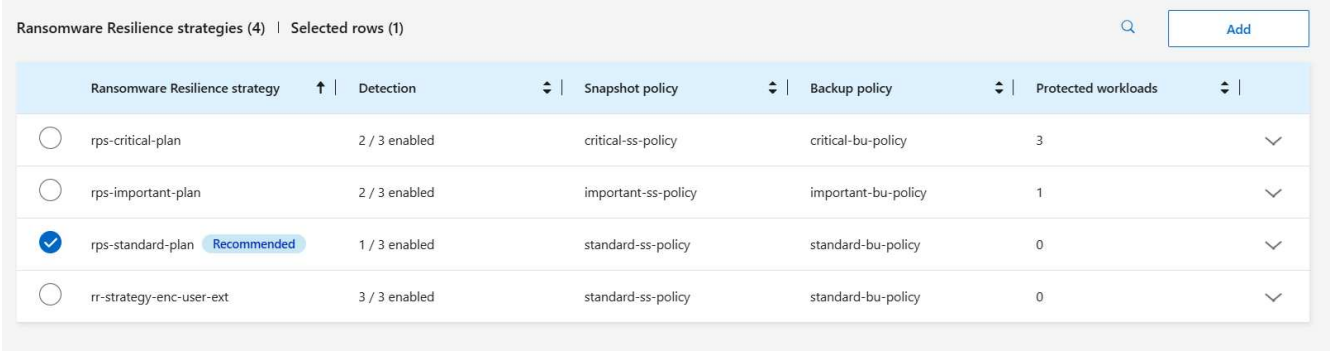
ランサムウェア保護戦略を削除する前に、その戦略によって保護されているワークロードを確認することをお勧めします。

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。

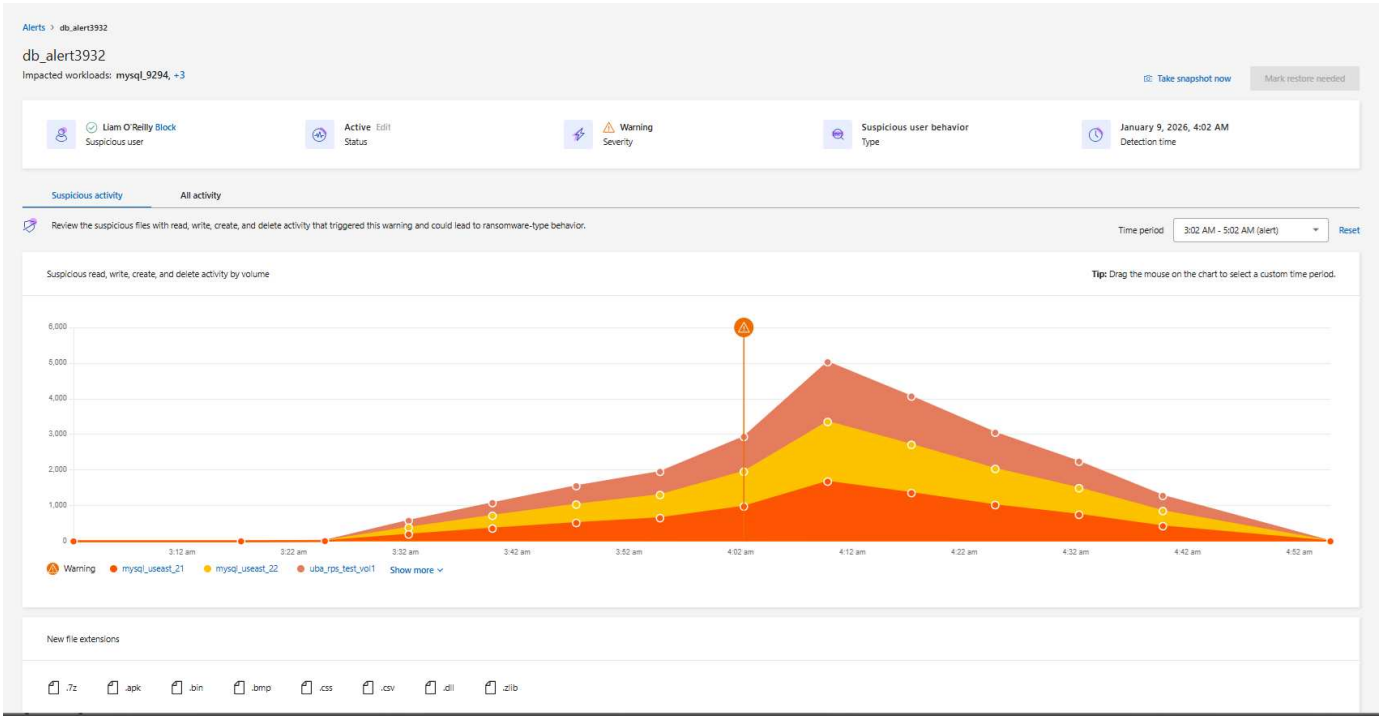
疑わしいユーザーの行動を検出して警告する NetApp Ransomware Resilience は、疑わしいと思われるデータ侵害や破壊の試みやパターンについて警告します。各アラートで、NetApp Ransomware Resilience はブロックできるユーザーを識別します。

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。

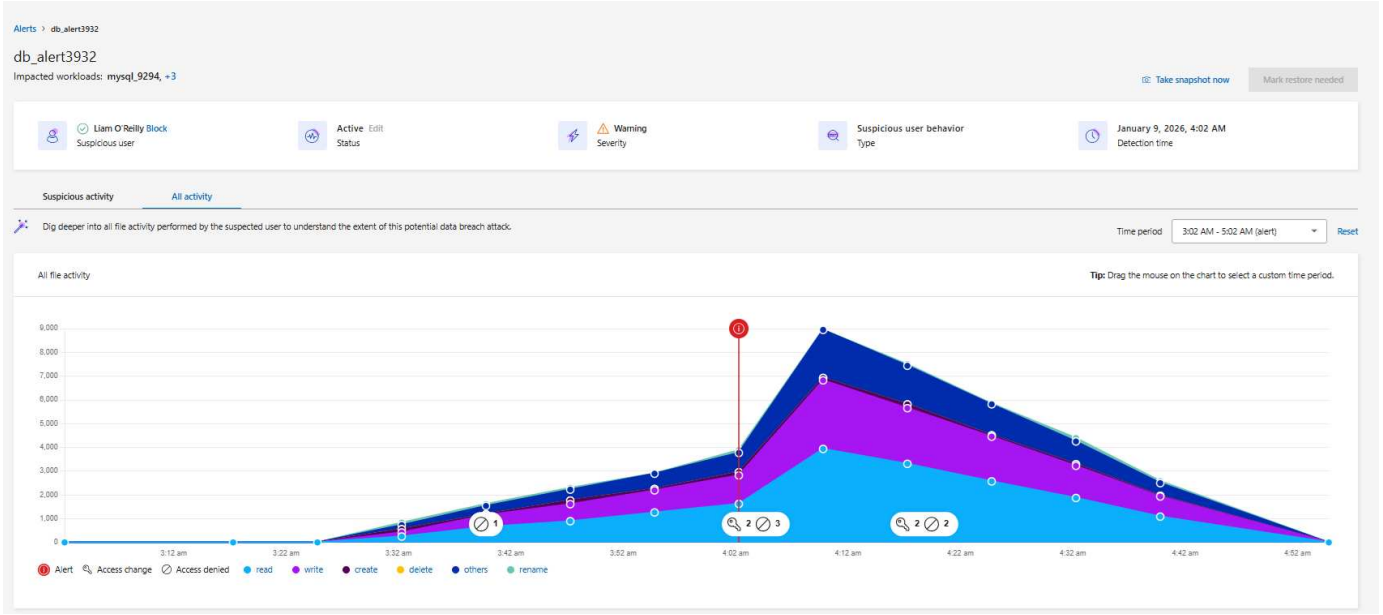
疑わしいユーザーアクティビティのフォレンジック

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。



◦

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。



◦

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 におけるユーザー行動検出の要件

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でユーザアクティビティ検出用のエージェントとコレクタを設定

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。

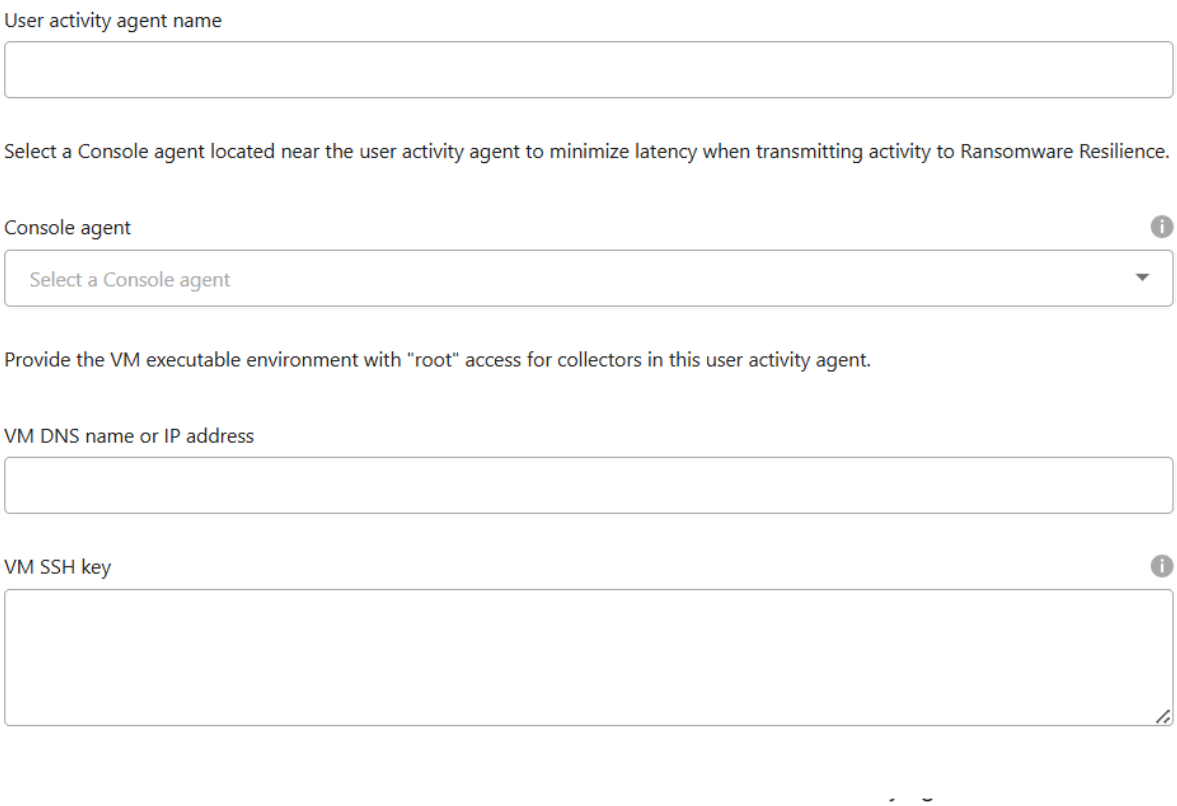
手順

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。

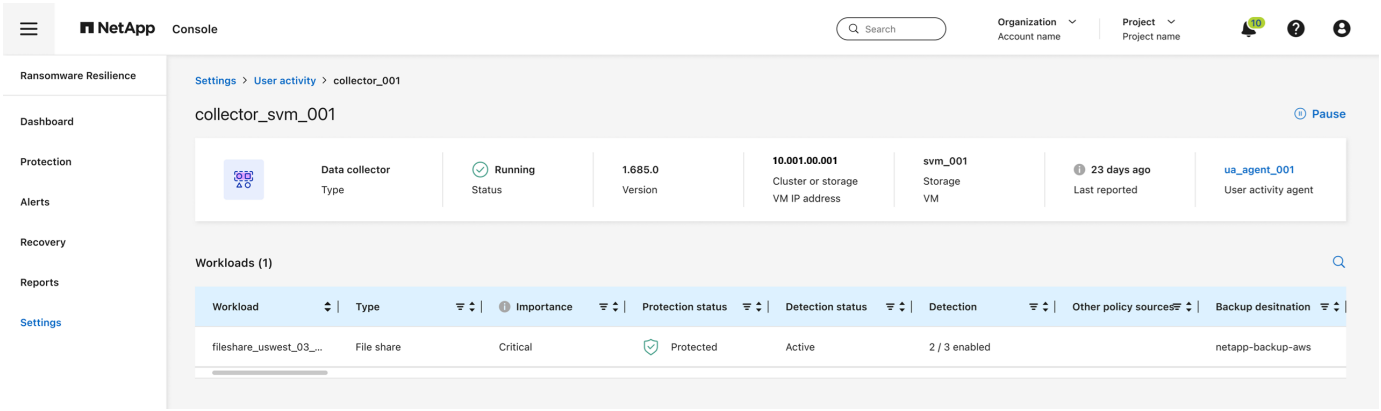
結果

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。



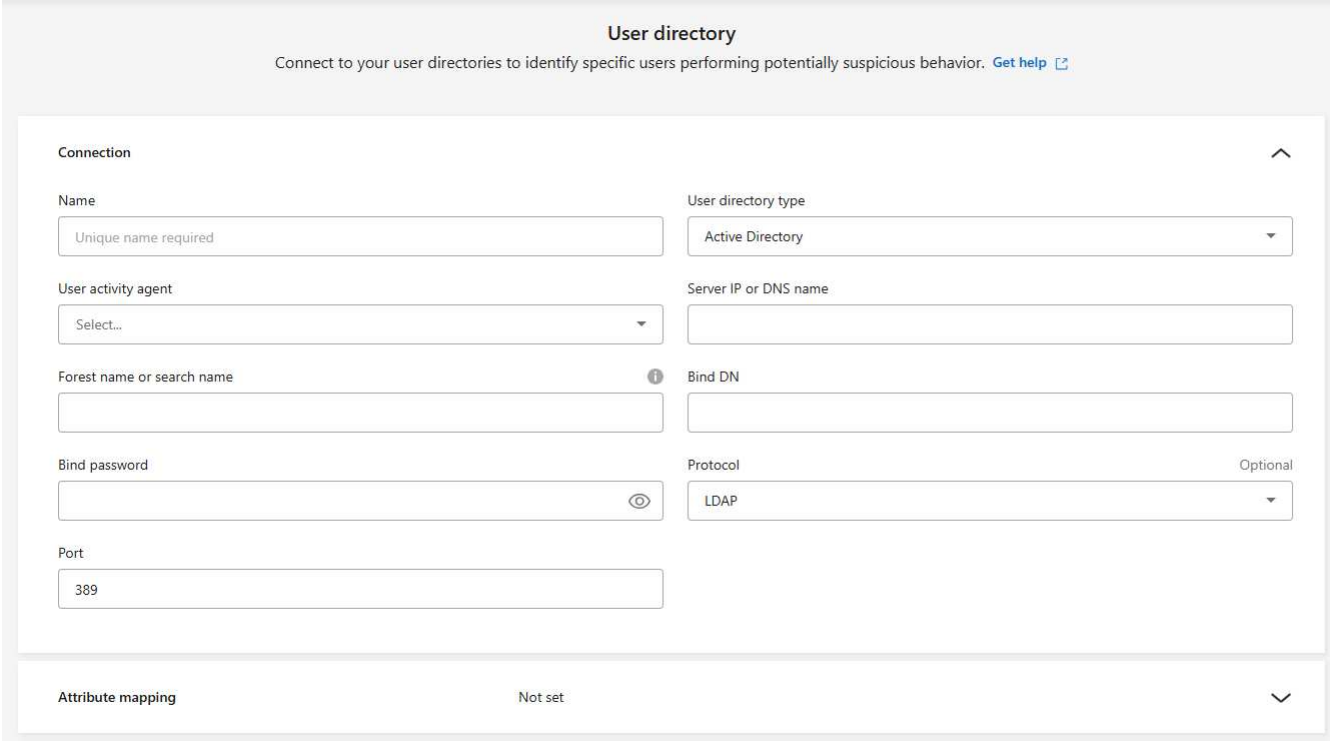
ユーザーディレクトリコネクタを作成する

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。

アラートからユーザーを除外する

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. アップロード を選択した場合は、まずすべてのユーザーのリストが含まれる CSV ファイルをダウンロードする必要があります。リストにアクセスするには、ダウンロード を選択します。

      CSV 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。アップロードを選択してファイルを見つけ、選択します。
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. 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。
4. 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。

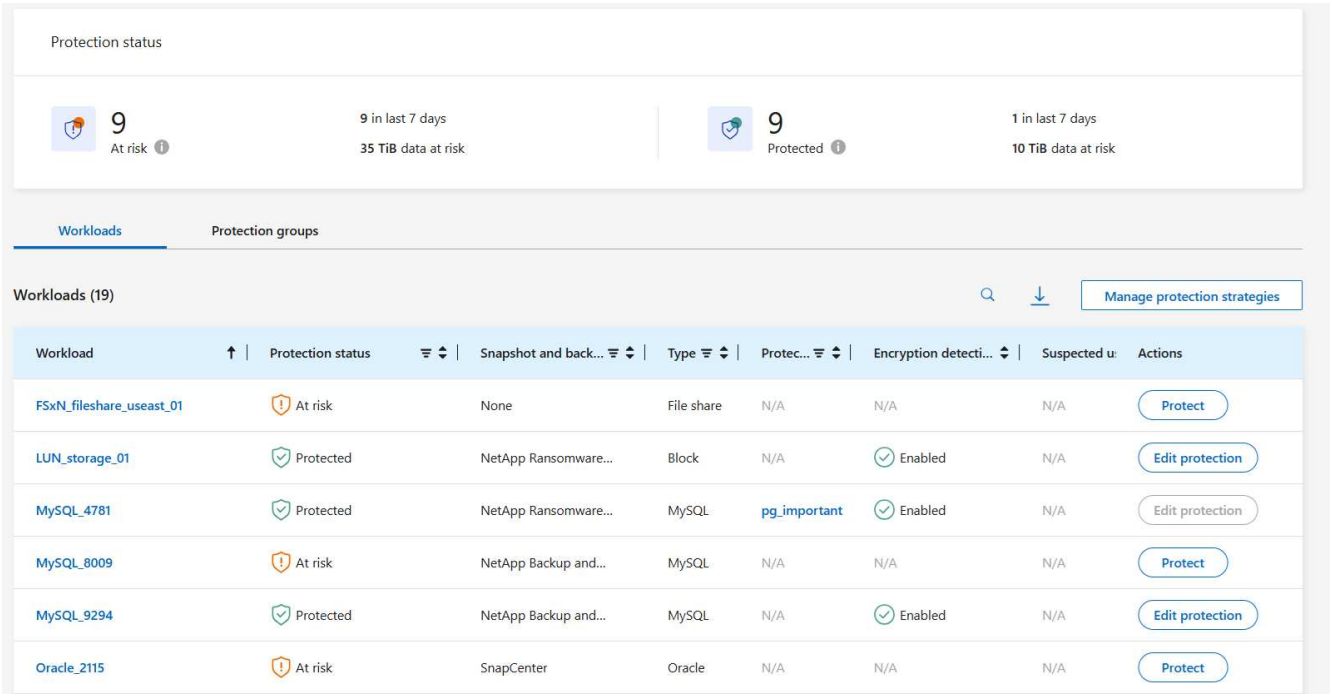
必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

保護グループを作成する

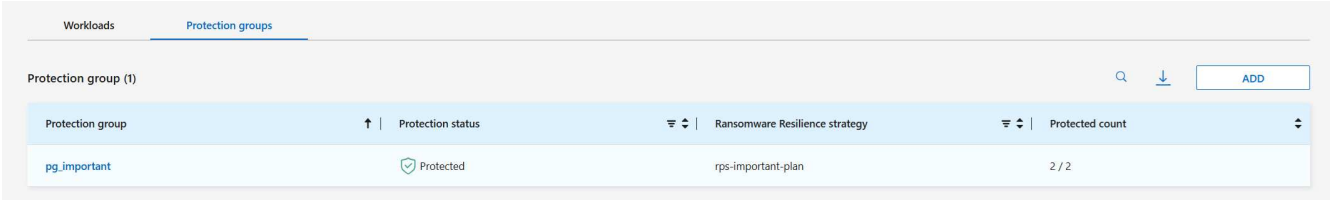
保護ステータスに関係なく（つまり、保護されていないグループと保護されているグループ）、グループを作成できます。保護グループに保護ポリシーを追加すると、新しい保護ポリシーは、NetApp Backup and Recoveryで管理されているポリシーを含む既存のポリシーをすべて置き換えます。

手順

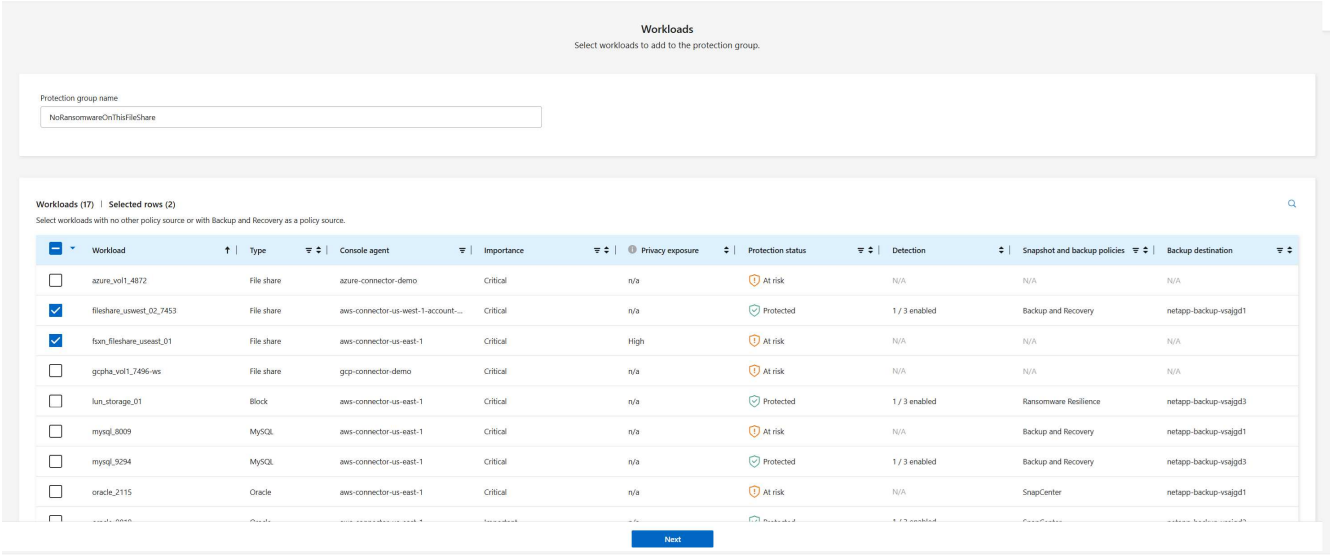
1. ランサムウェア耐性メニューから、*保護*を選択します。



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。



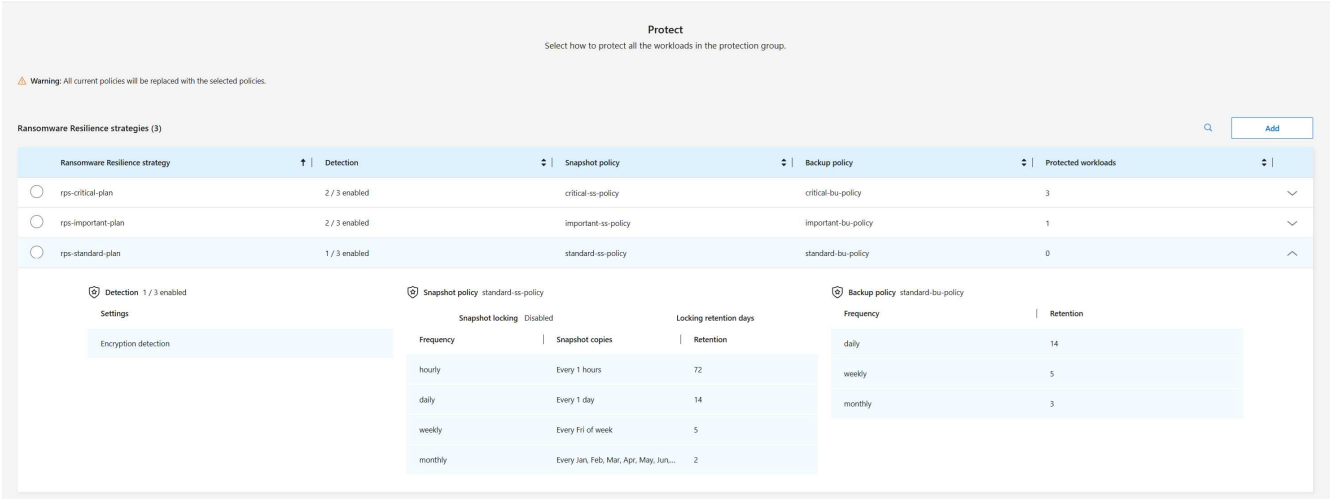
3. *追加*を選択します。



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

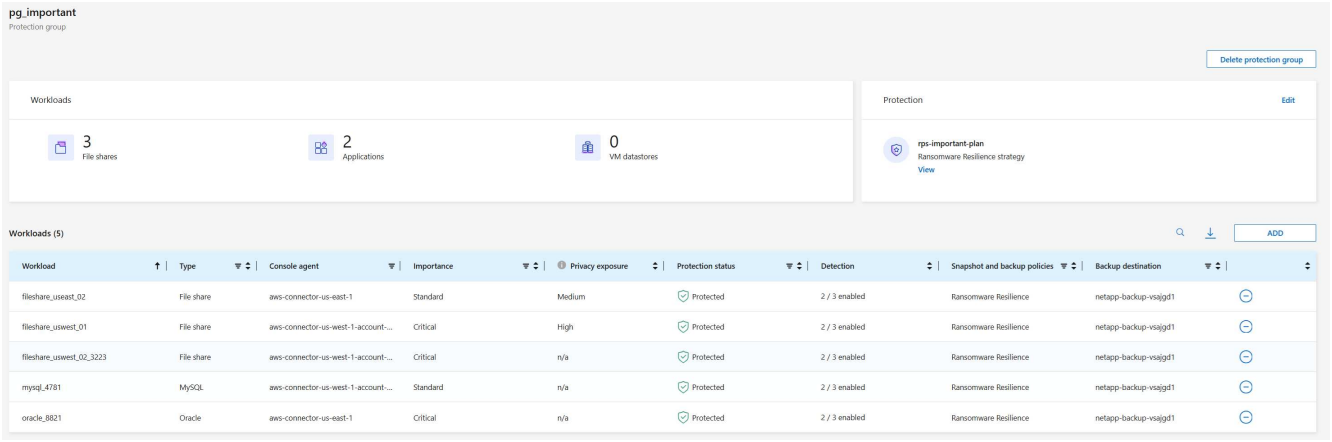
1. ランサムウェア耐性メニューから、*保護*を選択します。
2. [保護] ページで [保護グループ] タブを選択し、ポリシーを変更するグループを選択します。
3. 保護グループの概要ページで、*保護の編集*を選択します。
4. 既存の保護ポリシーを選択して適用するか、追加を選択して新しい保護ポリシーを作成します。保護ポリシーの追加の詳細については、"保護ポリシーを作成する"を参照してください。次に、保存を選択します。
5. バックアップ先の概要で、既存のバックアップ先を選択するか、新しいバックアップ先を追加します。
6. 変更内容を確認するには、[次へ] を選択します。

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。

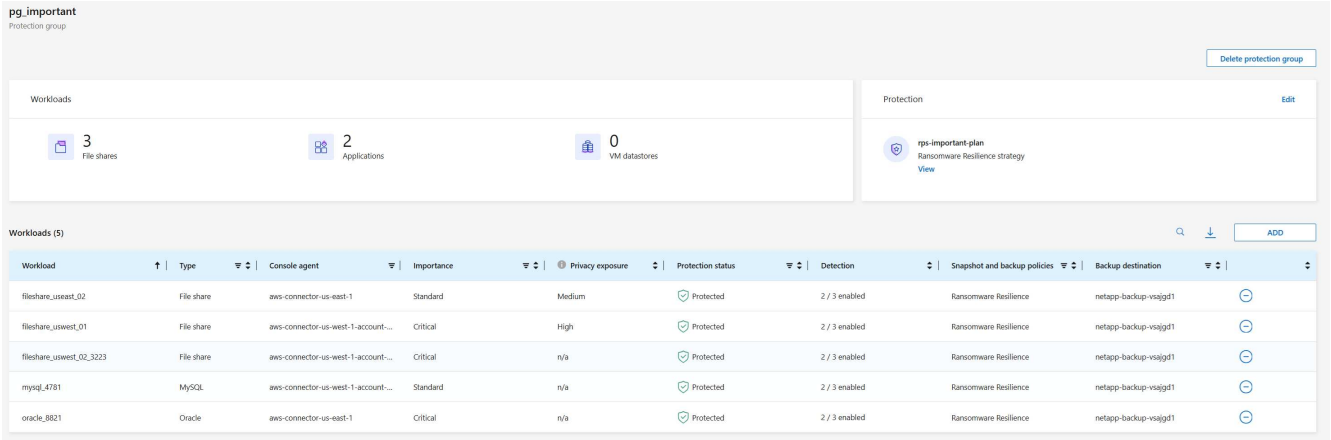
6. ワークロードを削除することを確認し、[削除] を選択します。

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。

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。

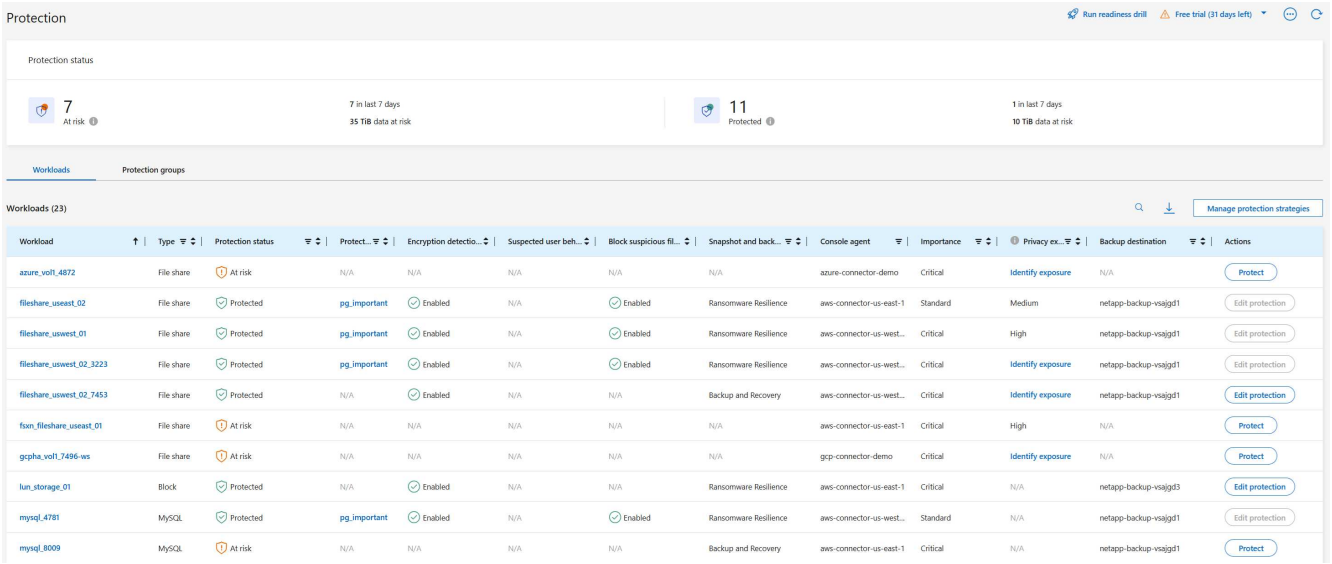
- "データ分類について学ぶ"
- "個人データのカテゴリ"
- "組織内に保存されているデータを調査する"

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

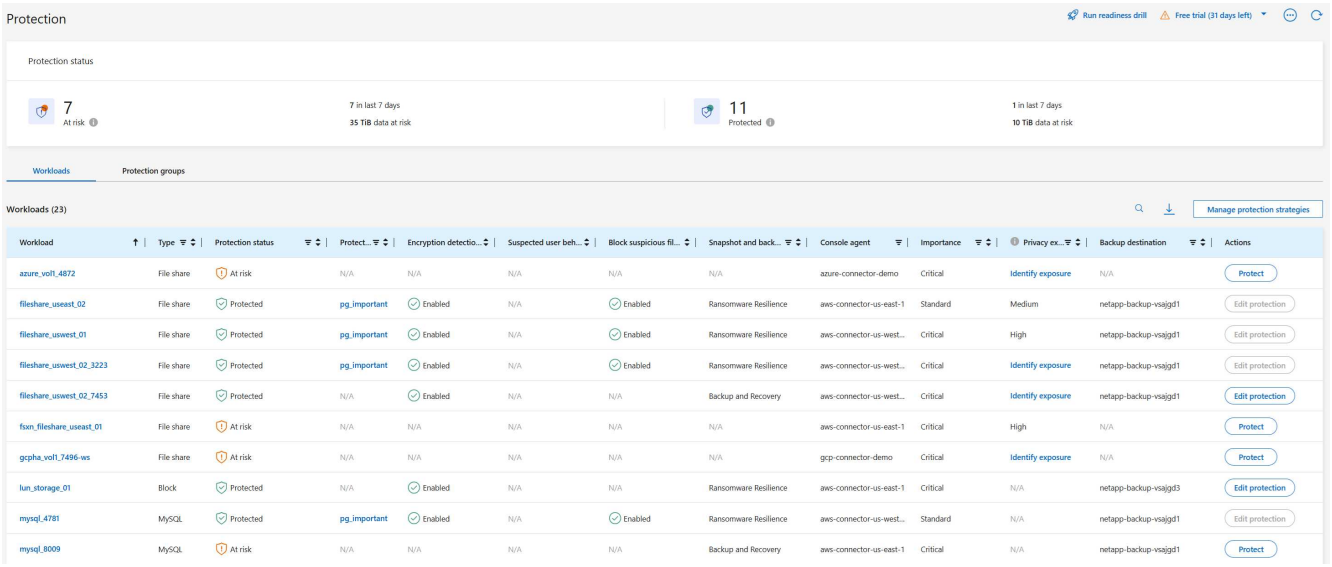
データ分類で PII をスキャンした後、リスクを評価します。

PII データは、次の 3 つの指定のいずれかに分類されます。

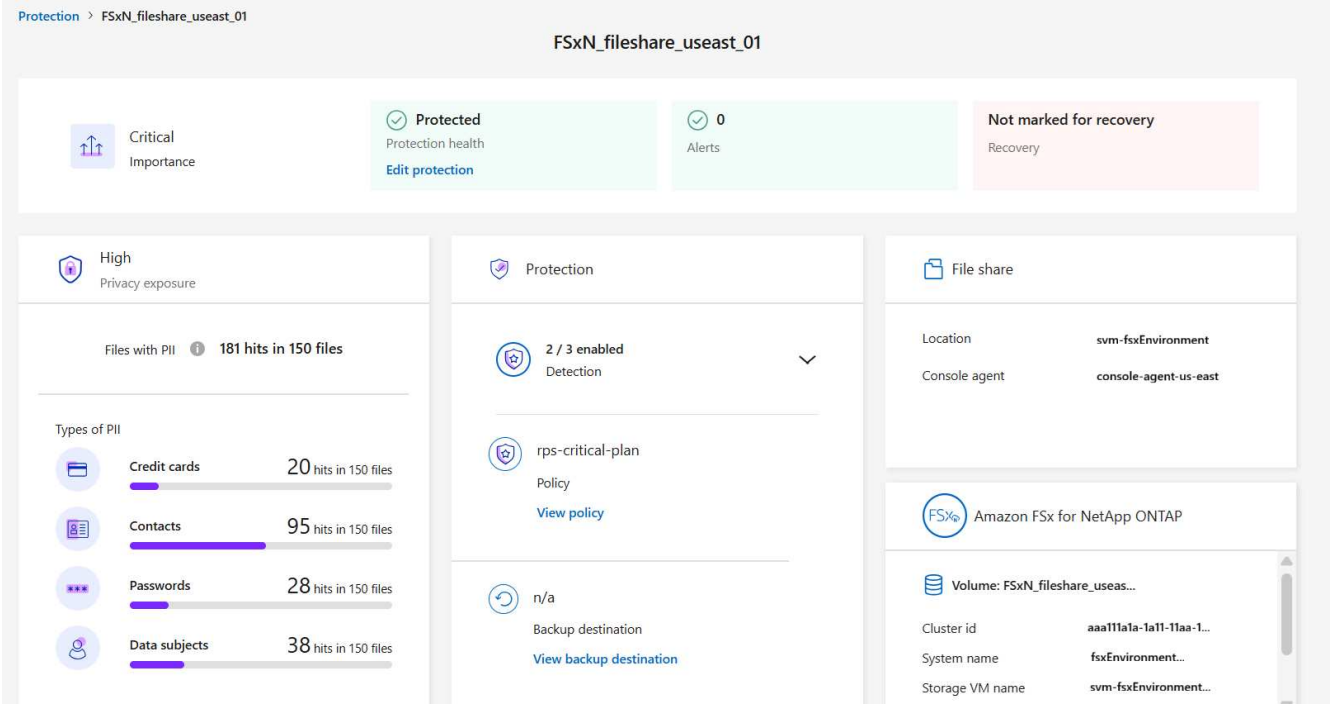
- 高: ファイルの 70% 以上に PII が含まれています
- 中: ファイルの 30% 以上 70% 未満に PII が含まれています
- 低: ファイルの 0% 以上 30% 未満に PII が含まれています

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
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"

対応と回復

NetApp Ransomware Resilienceのアラートを管理する

NetApp Ransomware Resilienceは、攻撃の可能性を検出すると、ダッシュボードと通知メニューに警告を表示します。Ransomware Resilienceは直ちにスナップショットを作成します。アラートを受信した場合は、Ransomware Resilienceの*アラート*タブで潜在的なリスクを確認し、データへの影響を評価して、潜在的なランサムウェア攻撃を防止します。

Ransomware Resilienceが攻撃の可能性を検知すると、NetApp Consoleの通知設定に通知が表示され、設定されたアドレスにメールが送信されます。メールには、深刻度、影響を受けるワークロード、Ransomware Resilienceの*アラート*タブにあるアラートへのリンクが含まれます。

誤検知を無視するか、すぐにデータを回復することを決定できます。

アラートを無視すると、Ransomware Resilience はこの動作を学習し、通常の操作と関連付けて、再度アラートを開始しなくなります。

データの復旧を開始するには、アラートを復旧準備完了としてマークし、ストレージ管理者が復旧プロセスを開始できるようにします。

各アラートには、さまざまなボリュームとステータスの複数のインシデントが含まれる場合があります。すべてのインシデントを確認します。

アラートの生成方法

Ransomware Resilience は、データエントロピーパターン、ファイル拡張子の種類、暗号化に関する証拠に基づいてアラートを生成します。アラートは次のイベントに基づいています：

- データ侵害
- データ破壊
- ファイル拡張子が作成または変更されました
- 検出されたレートと予想されるレートを比較したファイルの作成
- 検出された率と予想される率の比較によるファイル削除
- 疑わしいユーザー行動
- 暗号化レベルが高く、ファイル拡張子を変更しない場合

データ侵害、データ破壊、疑わしいユーザー行動のアラートについては、"ユーザーアクティビティ検出"を設定する必要があります。

アラートの種類とステータス

アラートには、*新規*または*非アクティブ*の 2 つのステータスのいずれかがあります。

アラートは次のいずれかのタイプに分類されます：

- 潜在的な攻撃：次の場合、アラートは潜在的な攻撃として分類されます：
  - Autonomous Ransomware Protectionが新しい拡張子を検出し、過去24時間に20回以上発生した場合（デフォルトの動作）。
  - データ侵害が検出されました。
  - データ破壊が検出されました。
- 警告: 次の動作に基づいて警告が発生します。
  - 新しい拡張機能の検出はこれまで確認されておらず、同じ動作が攻撃として宣言されるほど十分な回数繰り返されていません。
  - 高いエントロピーが観測されます。
  - ファイルの読み取り、書き込み、名前変更、または削除アクティビティが、通常のレベルと比較して 2 倍になりました。

SAN 環境の場合、警告は高エントロピーのみに基づきます。

証拠は、 ONTAPの Autonomous Ransomware Protection の情報に基づいています。詳細については、 "自律型ランサムウェア対策 - 概要" 。

アラート状態

アラート インシデントには、次の状態があります。

都道府県	説明
新しい	すべてのインシデントは、最初に特定されたときに「新規」としてマークされます。
レビュー中	アラートインシデントを評価するときに、手動で「レビュー中」としてマークすることができます。
却下	アクティビティがランサムウェア攻撃ではないと疑われる場合は、ステータスを「dismissed」に変更できます。+ 注意：攻撃を却下した後は、そのステータスを元に戻すことはできません。ワークロードを却下すると、潜在的なランサムウェア攻撃に応じて自動的に作成されたすべてのSnapshotコピーが完全に削除されます。
解決済み	インシデントは修正されました。
自動解決済み	優先度の低いアラートの場合、5日以内に何のアクションも取られなければ、インシデントは自動的に解決されます。

アラートを表示

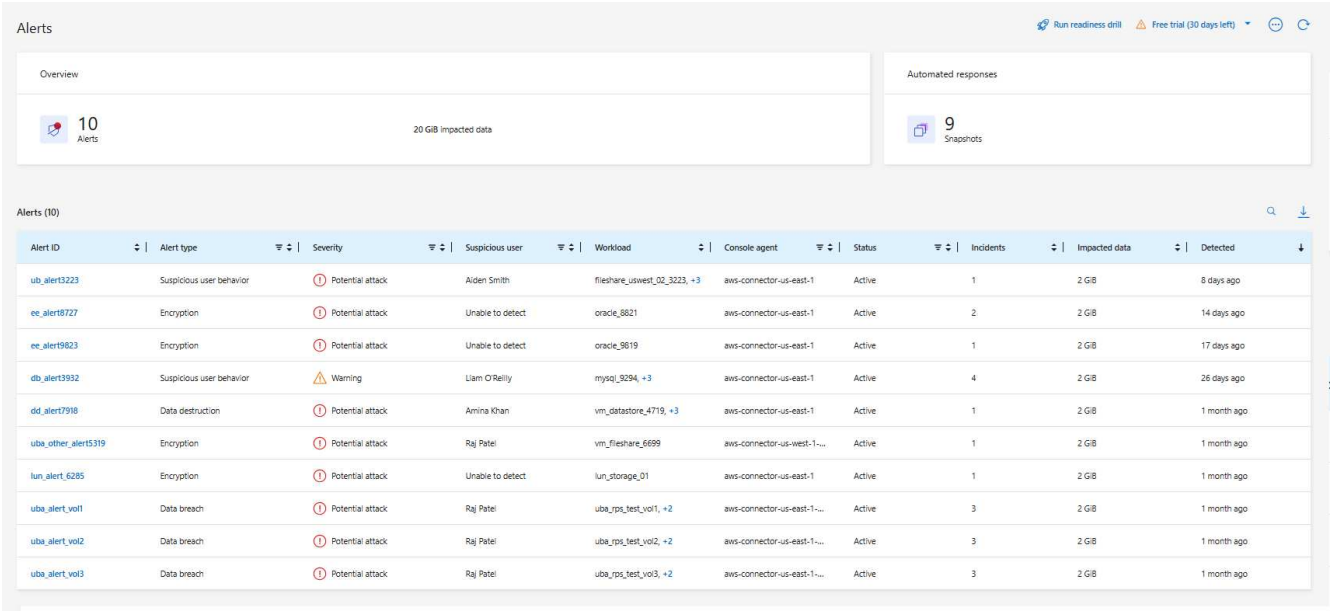
アラートには、Ransomware Resilienceダッシュボードまたは*アラート*タブからアクセスできます。

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、ランサムウェア レジリエンス管理者、またはランサムウェア レジリエンス ビューアー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" 。

手順

1. NetApp Ransomware Resilienceダッシュボードで、[アラート]ペインを確認します。
2. いずれかのステータスの下にある*すべて表示*を選択します。

3. アラートを選択して、アラートごとに各ボリュームのすべてのインシデントを確認します。
4. 追加のアラートを確認するには、左上のパンくずリストで [アラート] を選択します。
5. 「アラート」ページでアラートを確認します。



6. 次のいずれかに進みます。
   - [悪意のあるアクティビティや異常なユーザー行動を検出する] 。
   - ランサムウェア インシデントを復旧準備完了としてマークする (インシデントが中和された後) 。
   - [潜在的な攻撃ではないインシデントを無視する] 。

アラートメールに返信する

Ransomware Resilienceは潜在的な攻撃を検出すると、NetApp Console設定で設定されたサブスクリプション通知設定に基づいて、登録ユーザーにメール通知を送信します。メールには、重大度や影響を受けるリソースなど、アラートに関する情報が記載されています。

コンソールで電子メール通知を設定するには、"メール通知設定を設定する"を参照してください。

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、ランサムウェア レジリエンス管理者、またはランサムウェア レジリエンス ビューアー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" 。

手順

1. メールを表示します。
2. メールで*アラートを表示*を選択し、Ransomware Resilienceにログインします。

   アラート ページが表示されます。

3. 各アラートについて、各ボリュームのすべてのインシデントを確認します。
4. 追加のアラートを確認するには、左上のパンくずリストで [アラート] を選択します。

5. 次のいずれかに進みます。
    - [悪意のあるアクティビティや異常なユーザー行動を検出する] 。
    - ランサムウェア インシデントを復旧準備完了としてマークする (インシデントが中和された後) 。
    - [潜在的な攻撃ではないインシデントを無視する] 。

悪意のあるアクティビティや異常なユーザー行動を検出する

[アラート] タブを見ると、悪意のあるアクティビティや異常なユーザー動作があるかどうかを確認できます。

ユーザーレベルのアラートを表示するには、ユーザーアクティビティエージェントを設定し、ユーザー行動検出機能を備えた保護ポリシーを有効にする必要があります。アラートダッシュボードに「不審なユーザー」列が表示されるのは、ユーザー行動検出が有効になっている場合のみです。不審なユーザー検出を有効にするには、"不審なユーザーアクティビティ"をご覧ください。

悪意のあるアクティビティを表示する

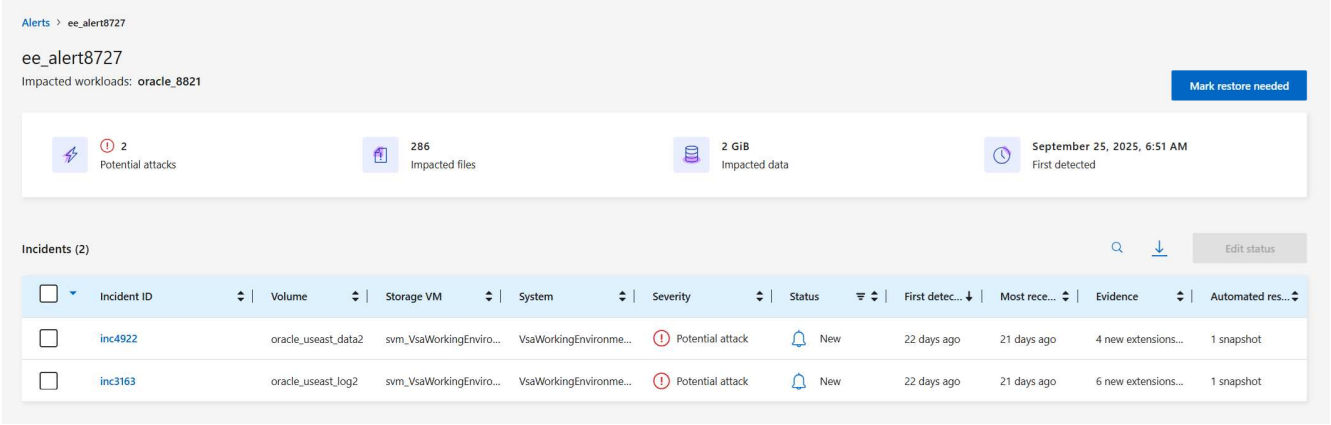
Autonomous Ransomware Protection が NetApp Ransomware Resilience でアラートをトリガーすると、次の詳細を表示できます：

- アラートがトリガーされたとき
- アクセスが変更または拒否された場合
- 受信データのエントロピー
- 新規ファイルの予想作成率と検出率の比較
- ファイルの予想削除率と検出率の比較
- 検出された率と比較したファイルの予想される名前変更率
- 影響を受けるワークロード、ボリューム、ファイル、ディレクトリ

これらの詳細は、NAS ワークロードで表示できます。 SAN 環境では、エントロピー データのみが利用可能です。

手順

1. ランサムウェア耐性メニューから、「アラート」を選択します。
2. アラートを選択します。
3. アラート内のインシデントを確認します。



4. インシデントの詳細を確認するには、インシデントを選択します。

異常なユーザー行動を表示する

異常なユーザー行動を表示するように疑わしいユーザー検出を設定している場合は、ユーザーレベルのデータを表示し、特定のユーザーをブロックできます。疑わしいユーザーの設定を有効にするには、"ユーザーアクティビティ検出用のエージェントとコレクターを設定する"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、「アラート」を選択します。
2. アラートを選択します。
3. アラート内のインシデントを確認します。
   a. 環境内の疑わしいユーザーをブロックするには、ユーザー名の横にある*ブロック*を選択します。
   b. 偽であるとわかっているアラートの対象となっている特定のユーザーに対するアラートを無効にするには、3つのドット(`…`を選択してから、このユーザーを監視から除外を選択します。ダイアログを確認し、除外を選択して確定します。

ユーザーのアラートを再度有効にするには、アラートを返します。3 つのドットを選択し、このユーザーを監視に含める を選択します。また、"ユーザーを除外する"監視から実行することもできます。

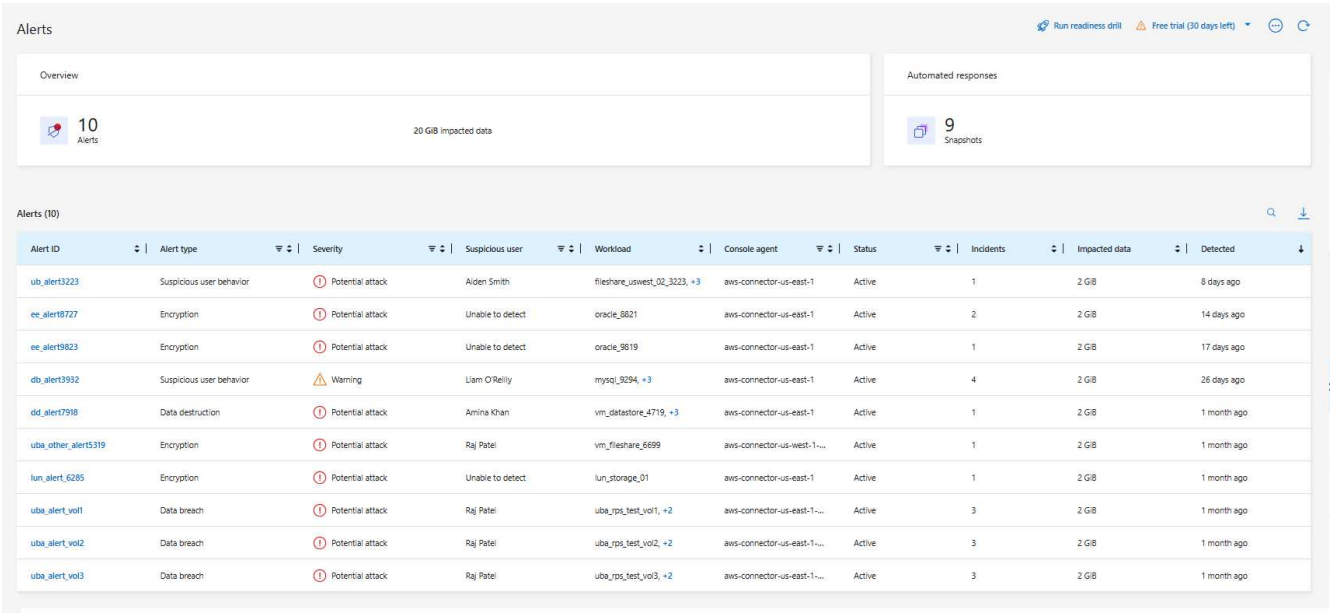
ランサムウェア インシデントを復旧準備完了としてマークする (インシデントが中和された後)

攻撃を停止した後、データの準備ができたことをストレージ管理者に通知し、リカバリプロセスを開始できるようにします。

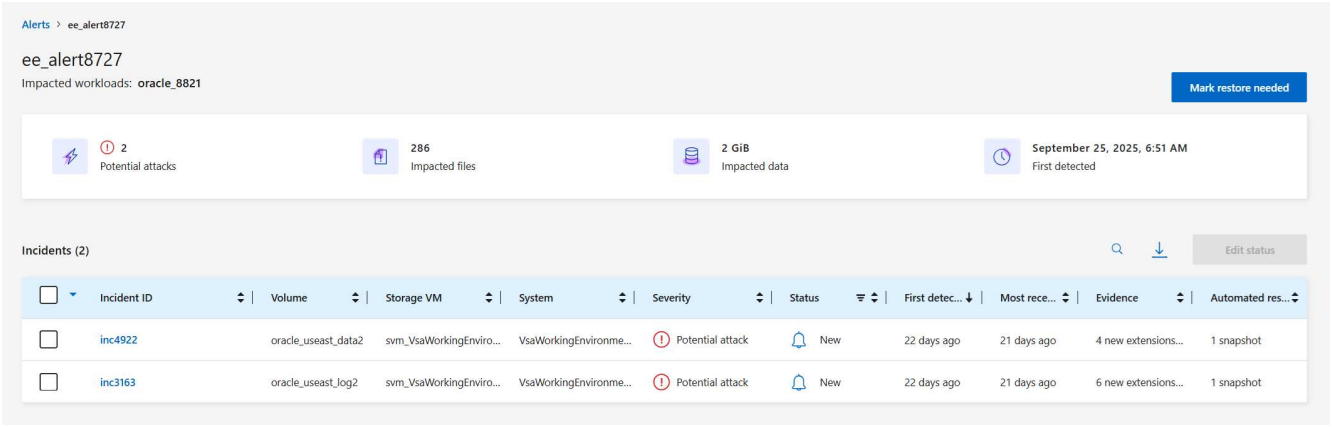
必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

手順

1. ランサムウェア耐性メニューから、「アラート」を選択します。



2. 「アラート」ページで、アラートを選択します。
3. アラート内のインシデントを確認します。



4. インシデントの回復の準備ができていると判断した場合は、「復元が必要としてマーク」を選択します。
5. アクションを確認し、「復元が必要としてマーク」を選択します。
6. ワークロードの回復を開始するには、メッセージで「ワークロードの回復」を選択するか、「回復」タブを選択します。

結果

アラートが復元対象としてマークされると、アラートは [アラート] タブから [回復] タブに移動します。

潜在的な攻撃ではないインシデントを無視する

インシデントを確認した後、そのインシデントが潜在的な攻撃であるかどうかを判断する必要があります。実際の脅威ではない場合は、無視できます。

誤検知を無視するか、すぐにデータを回復することを決定できます。アラートを無視すると、Ransomware Resilience はこの動作を学習し、通常の操作と関連付けて、そのような動作に対して再度アラートを開始しなくなります。

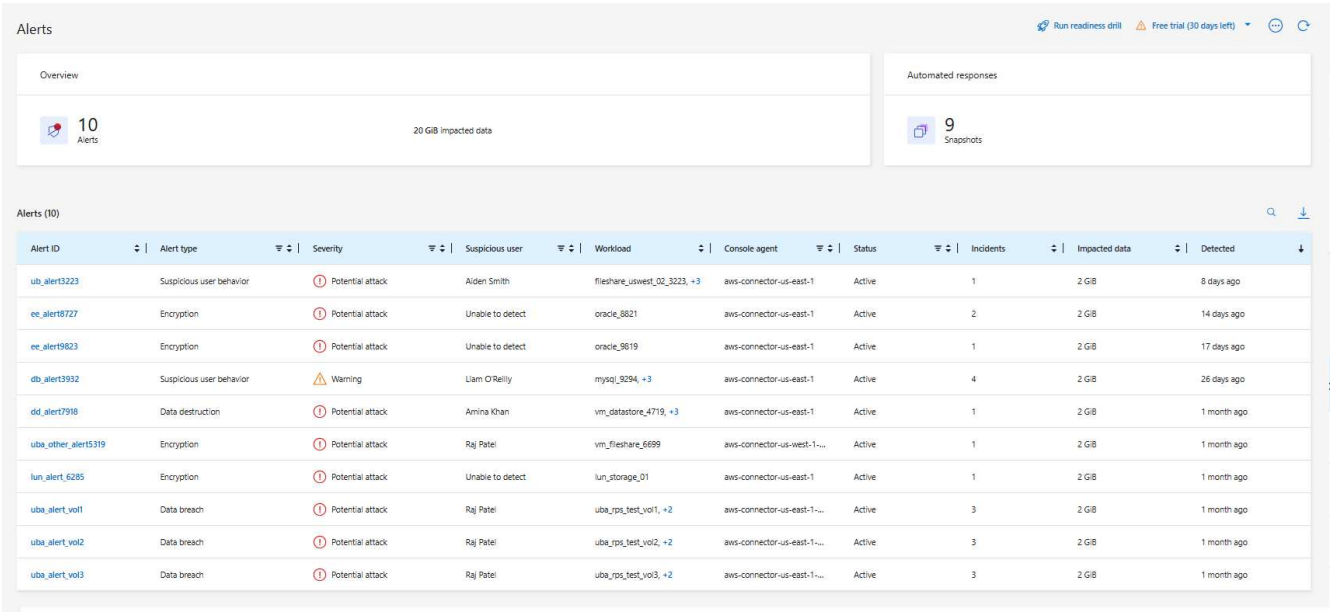
ワークロードを閉じると、潜在的なランサムウェア攻撃に応じて自動的に作成されたすべてのスナップショット コピーが完全に削除されます。

> アラートを無視した場合、そのステータスを変更したり、この変更を元に戻したりすることはできません。

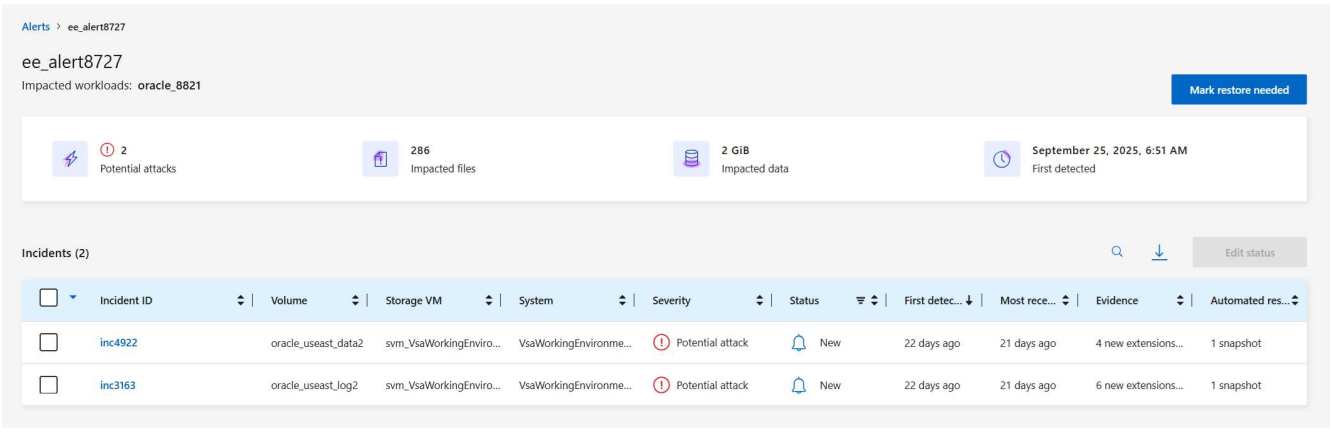
必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

手順

1. ランサムウェア耐性メニューから、「アラート」を選択します。

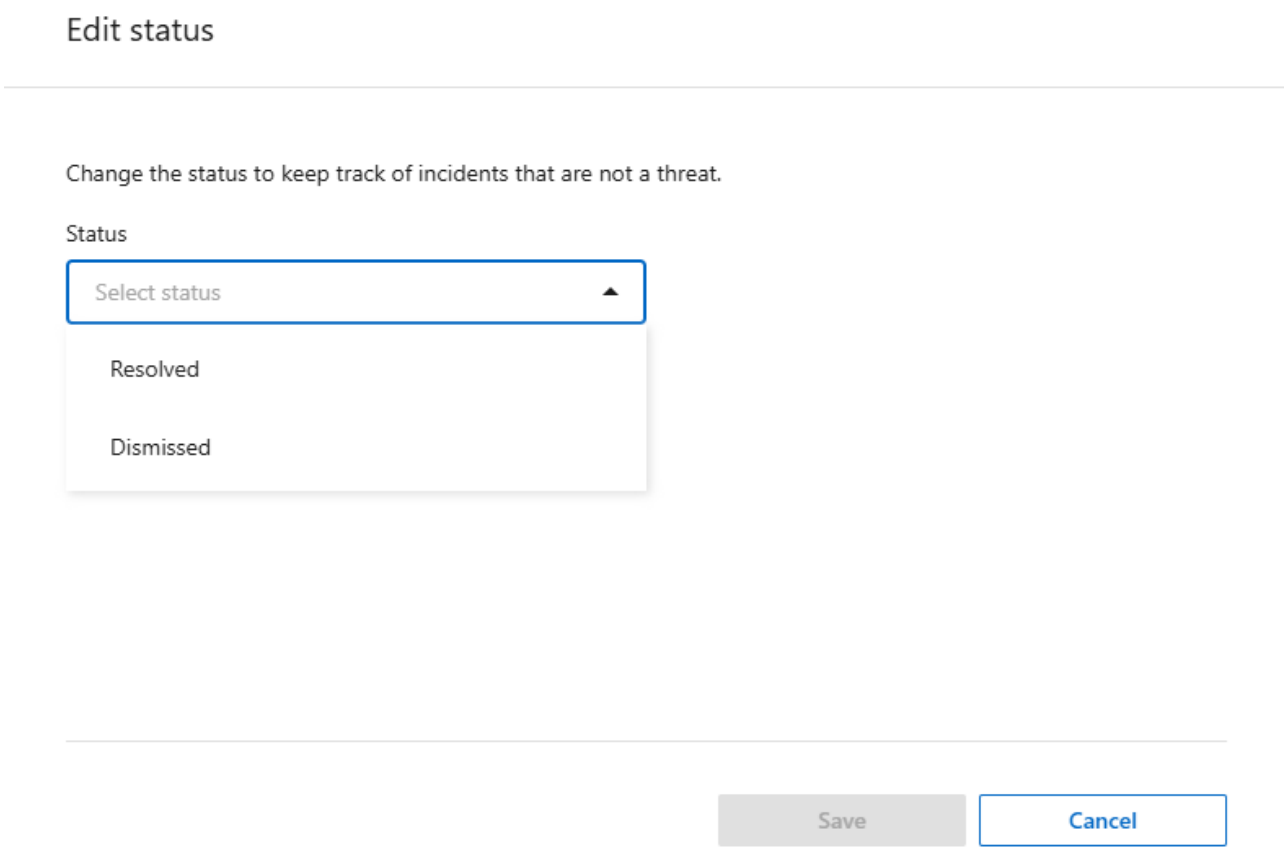


2. 「アラート」ページで、アラートを選択します。



3. 1 つ以上のインシデントを選択します。または、表の左上にあるインシデント ID ボックスを選択して、すべてのインシデントを選択します。
4. インシデントが脅威ではないと判断した場合は、誤検知として無視します。
   - インシデントを選択します。

◦ 表の上にある*ステータスの編集*ボタンを選択します。



5. [ステータスの編集] ボックスから、[却下] ステータスを選択します。

   ワークロードと削除されたスナップショット コピーに関する追加情報が表示されます。

6. *保存*を選択します。

   インシデントのステータスが「却下」に変わります。

影響を受けるファイルの一覧を表示する

アプリケーション ワークロードをファイル レベルで復元する前に、影響を受けるファイルの一覧を表示できます。影響を受けるファイルのリストをダウンロードするには、「アラート」ページにアクセスしてください。次に、「回復」ページを使用してリストをアップロードし、復元するファイルを選択します。

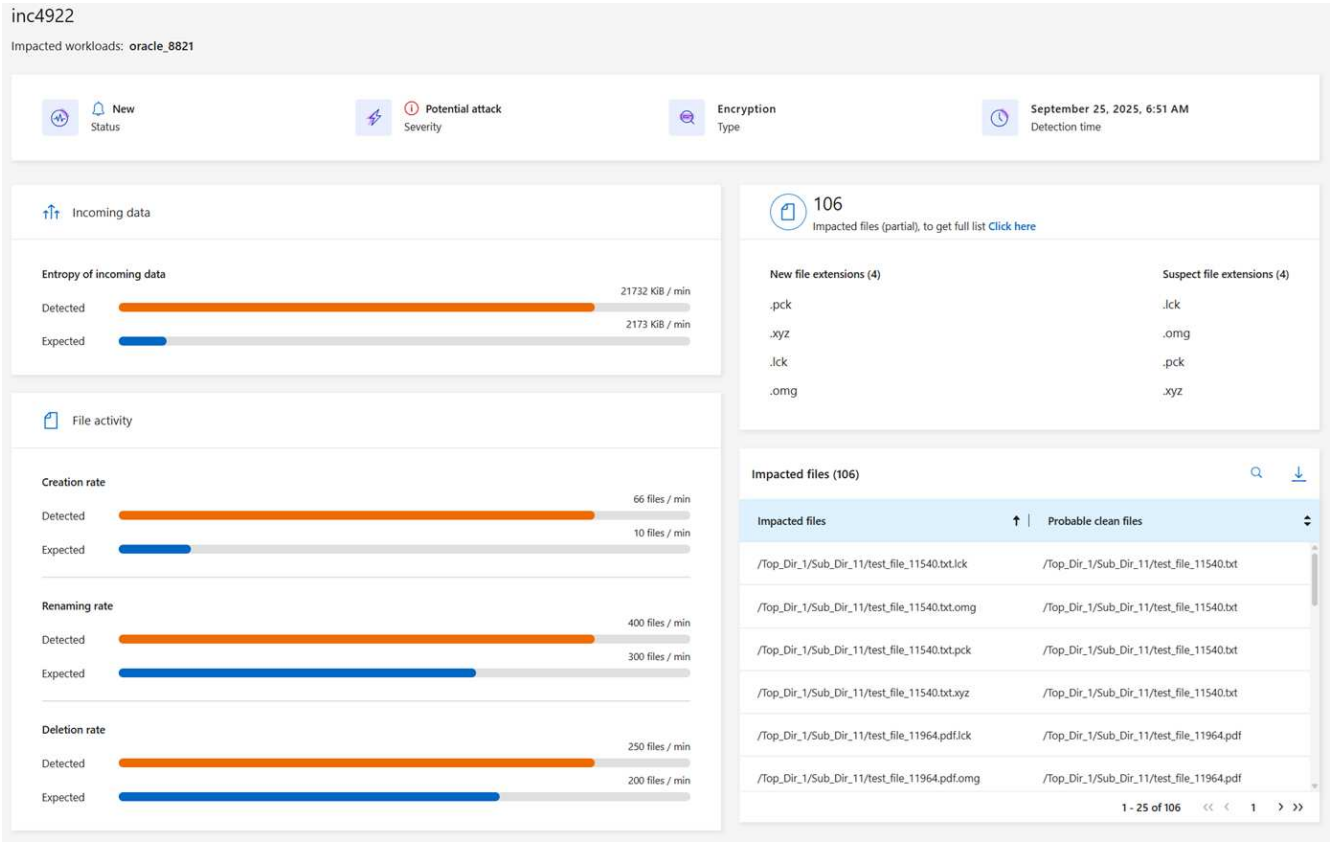
必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

手順

影響を受けるファイルのリストを取得するには、「アラート」ページを使用します。

ボリュームに複数のアラートがある場合は、アラートごとに影響を受けるファイルの CSV リストをダウンロードする必要がある場合があります。

1. ランサムウェア耐性メニューから、「アラート」を選択します。
2. [アラート] ページで、結果をワークロード別に並べ替えて、復元するアプリケーション ワークロードのアラートを表示します。
3. そのワークロードのアラートのリストから、アラートを選択します。
4. そのアラートに対して、単一のインシデントを選択します。



5. そのインシデントについては、ダウンロード アイコンを選択して、影響を受けるファイルのリストを CSV 形式でダウンロードします。

NetApp Ransomware Resilienceでランサムウェア攻撃から回復 (インシデントが中和された後)

ワークロードが「復元が必要」とマークされた後、 NetApp Ransomware Resilience は実際のリカバリポイント (RPA) を推奨し、クラッシュ耐性のあるリカバリのワークフローを調整します。

- アプリケーションやVMがNetApp Backup and RecoveryまたはRansomware Resilienceによって管理されている場合、Ransomware Resilienceは「crash consistent state（障害など予期しないシャットダウン時と同様）」の状態でリストアを実行します。これは、システムがクラッシュした場合など、同じ時点でボリューム内にあったすべてのデータがリストアされることを意味します。

  すべてのボリューム、特定のボリューム、または特定のファイルを選択してワークロードを復元できま

す。

ワークロードの回復は実行中のワークロードに影響を及ぼす可能性があります。適切な関係者と連携して回復プロセスを調整する必要があります。

ワークロードの復元ステータスは次のいずれかになります。

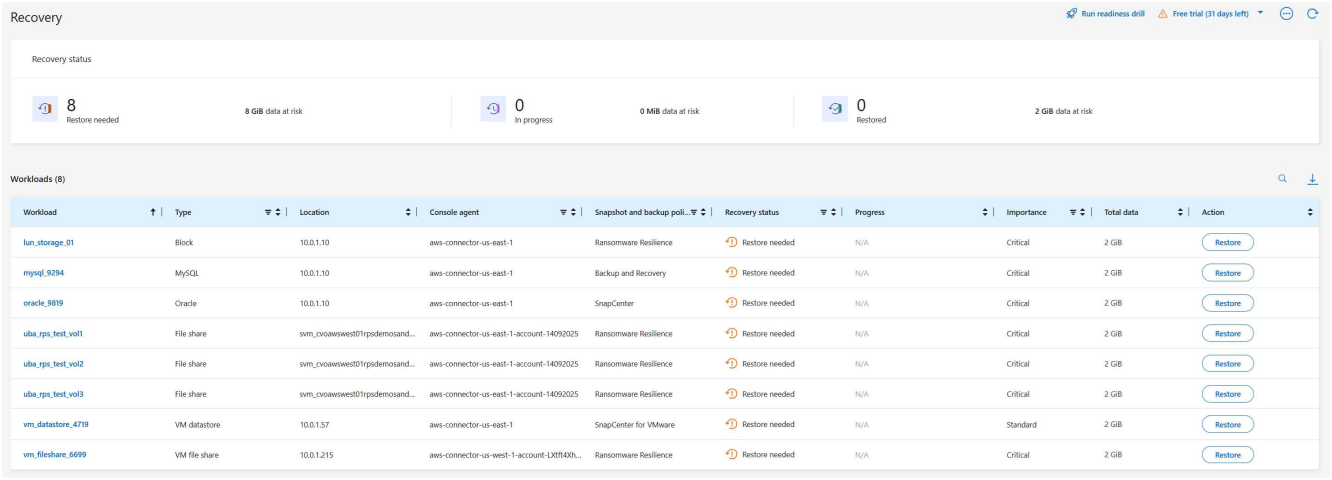
- 復元が必要です: ワークロードを復元する必要があります。
- 進行中: 復元操作が現在進行中です。
- 復元済み: ワークロードが復元されました。
- 失敗: ワークロードの復元プロセスを完了できませんでした。

復元準備が整ったワークロードを表示する

「復元が必要」の回復ステータスにあるワークロードを確認します。

手順

1. 次のいずれかを実行します。
   - ダッシュボードから、[アラート] ペインの [復元が必要] の合計を確認し、すべて表示 を選択します。
   - メニューから*回復*を選択します。
2. *回復*ページでワークロード情報を確認します。



ワークロードを復元する

Ransomware Resilience を使用すると、ストレージ管理者は、推奨される復元ポイントまたは優先復元ポイントからワークロードを復元する最適な方法を決定できます。

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" 。

セキュリティ ストレージ管理者は、さまざまなレベルでデータを回復できます。

- すべてのボリュームを回復
- ボリューム レベルまたはファイルとフォルダー レベルでアプリケーションを回復します。
- ボリューム レベル、ディレクトリ レベル、またはファイル/フォルダー レベルでファイル共有を回復します。
- VM レベルでデータストアから回復します。

プロセスはワークロードの種類によって異なります。

手順

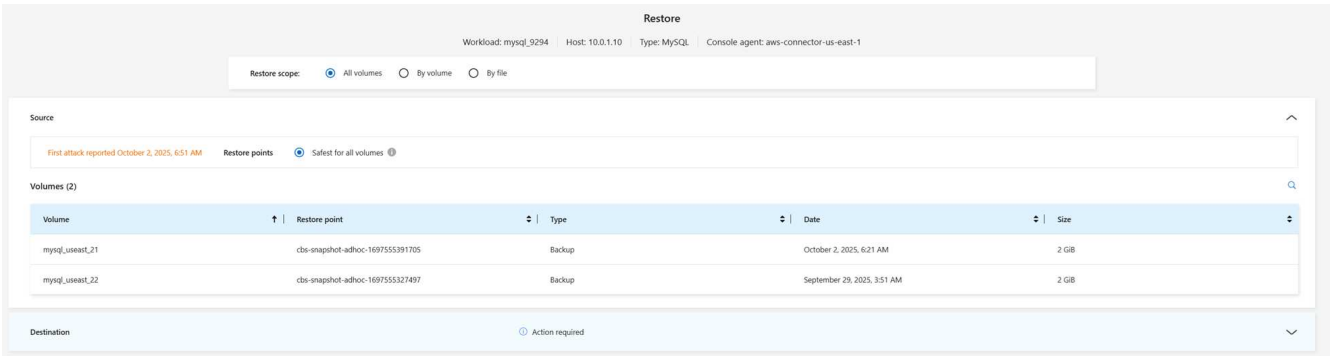
1. ランサムウェア耐性メニューから、「回復」を選択します。
2. *回復*ページでワークロード情報を確認します。
3. 「復元が必要」状態にあるワークロードを選択します。
4. 復元するには、[復元] を選択します。
5. 復元範囲: 実行する復元の種類を選択します。
    - 全巻
    - 量別
    - ファイル別: 復元するフォルダーまたは単一のファイルを指定できます。

    SAN ワークロードの場合、ワークロードごとにのみ復元できます。

    最大 100 個のファイルまたは 1 つのフォルダーを選択できます。
6. アプリケーション、ボリューム、またはファイルのいずれを選択したかに応じて、次のいずれかの手順を続行します。

すべてのボリュームを復元する

1. ランサムウェア耐性メニューから、「回復」を選択します。
2. 「復元が必要」状態にあるワークロードを選択します。
3. 復元するには、[復元] を選択します。
4. [復元] ページの [復元範囲] で、[すべてのボリューム] を選択します。



5. ソース: 詳細を表示するには、[ソース] の横にある下矢印を選択します。

a. データを復元するために使用する復元ポイントを選択します。

> ランサムウェア耐性は、インシデント発生直前の最新のバックアップを最適な復元ポイントとして識別し、「すべてのボリュームに対して最も安全」という表示を表示します。これは、最初に検出されたボリュームへの最初の攻撃の前に、すべてのボリュームがコピーに復元されることを意味します。

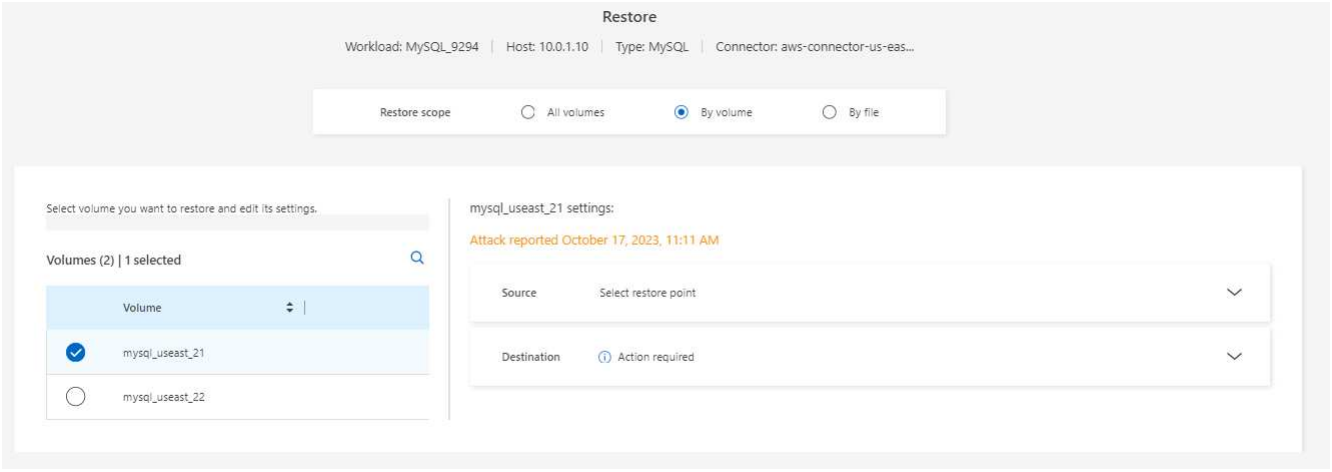
6. 目的地: 詳細を表示するには、目的地の横にある下矢印を選択します。
   a. システムを選択します。
   b. ストレージ VM を選択します。
   c. 集計を選択します。
   d. すべての新しいボリューム 先頭に追加されるボリューム プレフィックスを変更します。

> 新しいボリューム名は、プレフィックス + 元のボリューム名 + バックアップ名 + バックアップ日付として表示されます。

7. *保存*を選択します。
8. *次へ*を選択します。
9. 選択内容を確認します。
10. *復元*を選択します。
11. 上部のメニューから [リカバリ] を選択し、[リカバリ] ページでワークロードを確認します。ここでは、操作のステータスがさまざまな状態を遷移します。

ボリュームレベルでアプリケーションワークロードを復元する

1. ランサムウェア耐性メニューから、「回復」を選択します。
2. 「復元が必要」状態にあるアプリケーション ワークロードを選択します。
3. 復元するには、[復元] を選択します。
4. [復元] ページの [復元範囲] で、[ボリューム別] を選択します。



5. ボリュームのリストで、復元するボリュームを選択します。

6. ソース: 詳細を表示するには、[ソース] の横にある下矢印を選択します。
   a. データを復元するために使用する復元ポイントを選択します。

   ランサムウェア耐性は、インシデント発生直前の最新のバックアップを最適な復元ポイントとして識別し、「推奨」表示を表示します。

7. 目的地: 詳細を表示するには、目的地の横にある下矢印を選択します。
   a. システムを選択します。
   b. ストレージ VM を選択します。
   c. 集計を選択します。
   d. 新しいボリューム名を確認します。

   新しいボリューム名は、元のボリューム名 + バックアップ名 + バックアップ日付として表示されます。

8. *保存*を選択します。
9. *次へ*を選択します。
10. 選択内容を確認します。
11. *復元*を選択します。
12. 上部のメニューから [リカバリ] を選択し、[リカバリ] ページでワークロードを確認します。ここでは、操作のステータスがさまざまな状態を遷移します。

ファイルレベルでアプリケーションのワークロードを復元する

アプリケーション ワークロードをファイル レベルで復元する前に、影響を受けるファイルの一覧を表示できます。影響を受けるファイルのリストをダウンロードするには、「アラート」ページにアクセスしてください。次に、「回復」ページを使用してリストをアップロードし、復元するファイルを選択します。

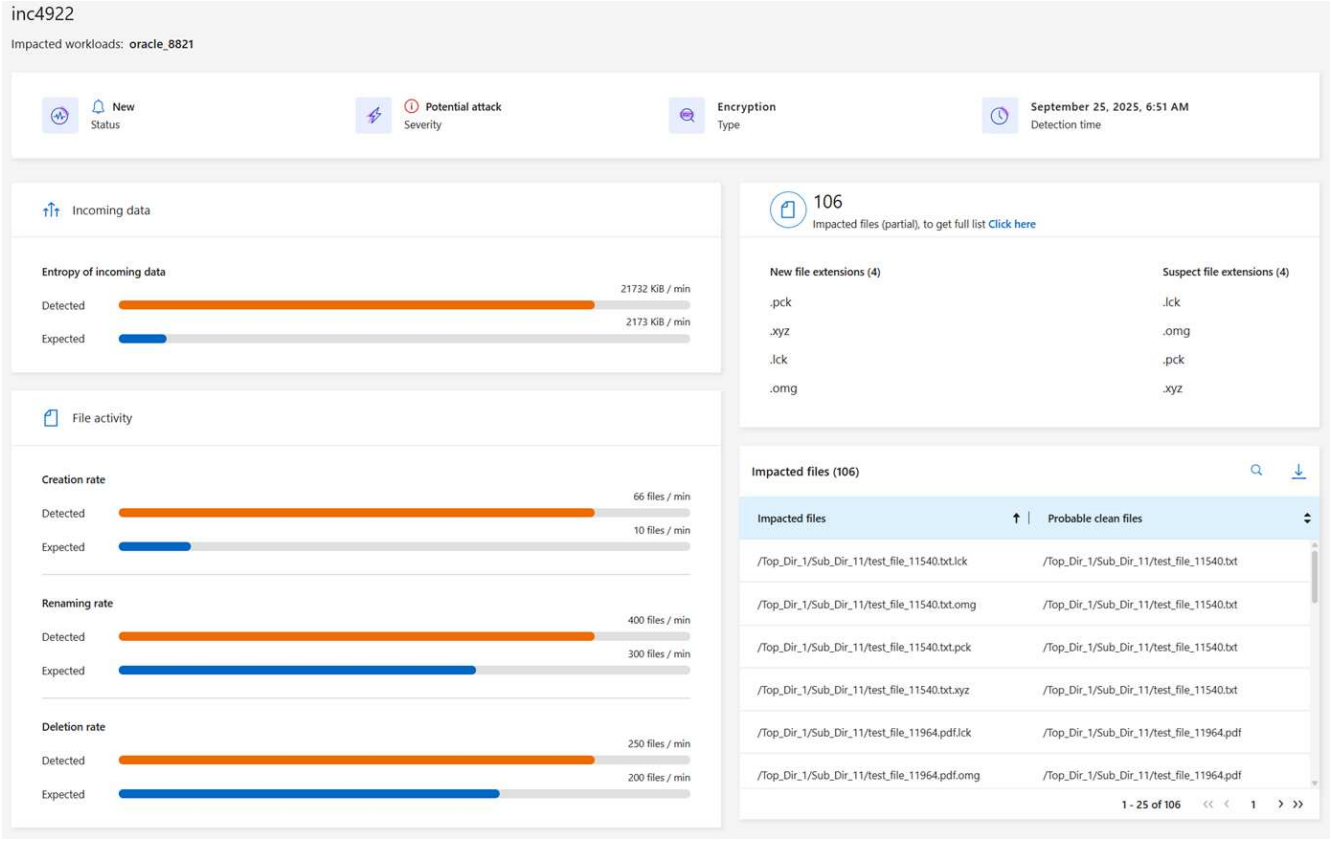
アプリケーション ワークロードをファイル レベルで同じシステムまたは別のシステムに復元できます。

影響を受けるファイルのリストを取得する手順

影響を受けるファイルのリストを取得するには、「アラート」ページを使用します。

ボリュームに複数のアラートがある場合は、アラートごとに影響を受けるファイルの CSV リストをダウンロードする必要があります。

1. ランサムウェア耐性メニューから、「アラート」を選択します。
2. [アラート] ページで、結果をワークロード別に並べ替えて、復元するアプリケーション ワークロードのアラートを表示します。
3. そのワークロードのアラートのリストから、アラートを選択します。
4. そのアラートに対して、単一のインシデントを選択します。



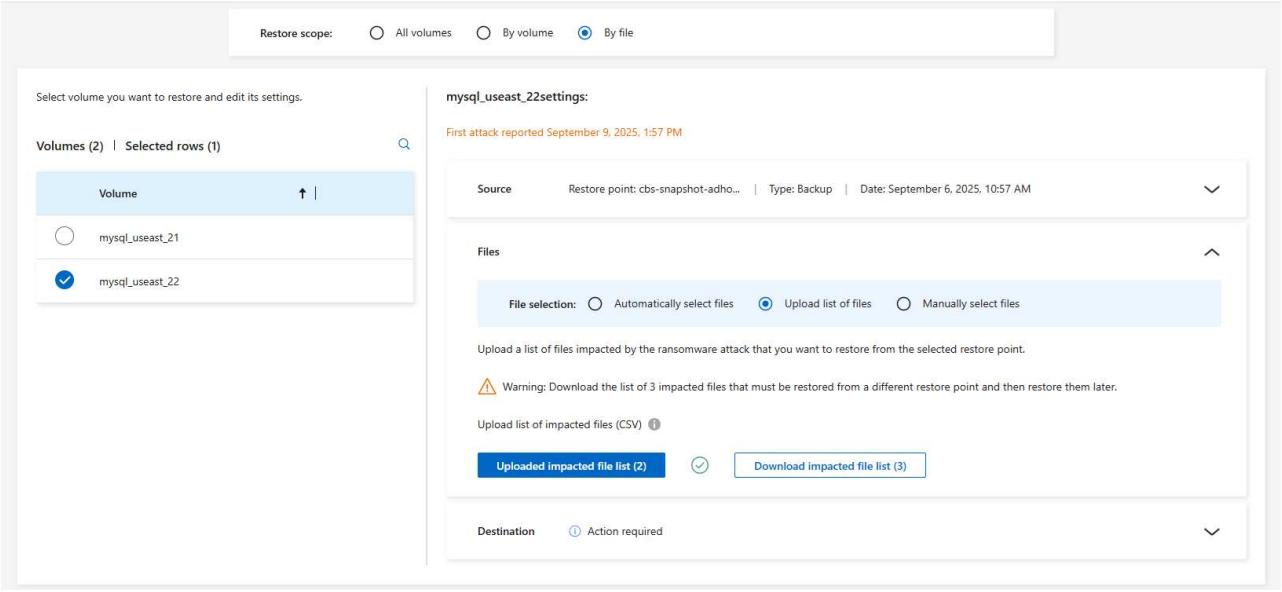
5. ファイルの完全なリストを表示するには、[影響を受けるファイル] ペインの上部にある [ここをクリック] を選択します。
6. そのインシデントについては、ダウンロード アイコンを選択し、影響を受けるファイルのリストを CSV 形式でダウンロードします。

これらのファイルを復元する手順

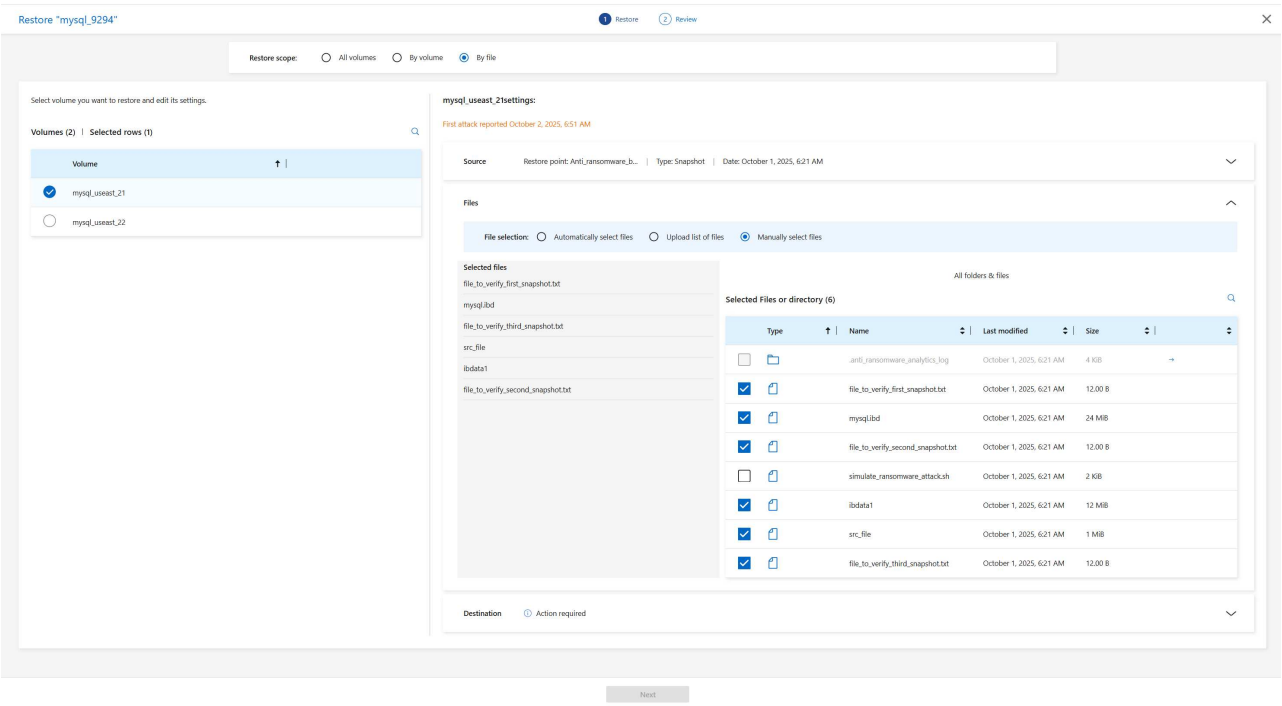
1. ランサムウェア耐性メニューから、「回復」を選択します。
2. 「復元が必要」状態にあるアプリケーション ワークロードを選択します。
3. 復元するには、[復元] を選択します。
4. [復元] ページの [復元範囲] で、[ファイル別] を選択します。
5. ボリュームのリストで、復元するファイルが含まれているボリュームを選択します。
6. 復元ポイント: 詳細を表示するには、*復元ポイント*の横にある下矢印を選択します。データを復元するために使用する復元ポイントを選択します。

> [復元ポイント] ウィンドウの [理由] 列には、スナップショットまたはバックアップの理由が「スケジュール済み」または「ランサムウェア インシデントへの自動対応」として表示されます。

7. ファイル:
   - ファイルを自動的に選択: Ransomware Resilience によって復元するファイルが選択されます。
   - ファイルのリストアップロード: アラート ページから取得した、または所有している影響を受けるファイルのリストを含む CSV ファイルをアップロードします。一度に最大 10,000 個のファイルを復元できます。



- ファイルを手動で選択: 復元するファイルまたはフォルダーを最大 10,000 個選択します。



選択した復元ポイントを使用してファイルを復元できない場合は、復元できないファイルの数を示すメッセージが表示され、[影響を受けるファイルのリストをダウンロード] を選択して、それらのファイルのリストをダウンロードできます。

8. 目的地: 詳細を表示するには、目的地の横にある下矢印を選択します。
   a. データを復元する場所（元のソースの場所または指定できる別の場所）を選択します。

元のファイルまたはディレクトリは復元されたデータによって上書きされますが、新しい名前を指定しない限り、元のファイルとフォルダの名前は同じままになります。

b. システムを選択します。

c. ストレージ VM を選択します。

d. 必要に応じて、パスを入力します。

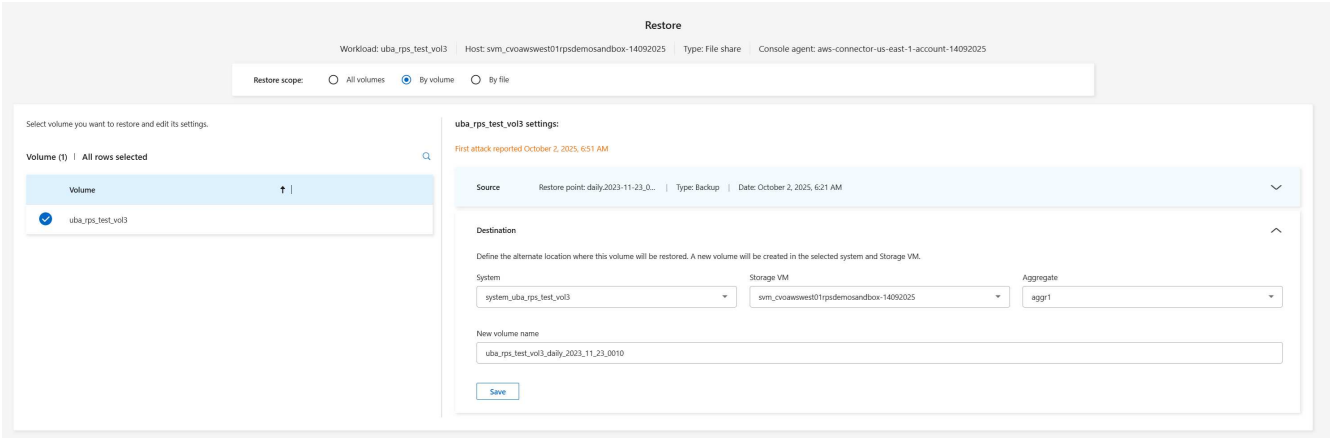
> 復元のパスを指定しない場合は、ファイルは最上位ディレクトリの新しいボリュームに復元されます。

e. 復元されたファイルまたはディレクトリの名前を現在の場所と同じ名前にするか、異なる名前にするかを選択します。

9. *次へ*を選択します。
10. 選択内容を確認します。
11. *復元*を選択します。
12. 上部のメニューから [リカバリ] を選択し、[リカバリ] ページでワークロードを確認します。ここでは、操作のステータスがさまざまな状態を遷移します。

ファイル共有またはデータストアを復元する

1. 復元するファイル共有またはデータストアを選択した後、[復元] ページの [復元範囲] で [ボリューム別] を選択します。



2. ボリュームのリストで、復元するボリュームを選択します。
3. ソース: 詳細を表示するには、[ソース] の横にある下矢印を選択します。
   a. データを復元するために使用する復元ポイントを選択します。

> ランサムウェア耐性は、インシデント発生直前の最新のバックアップを最適な復元ポイントとして識別し、「推奨」表示を表示します。

4. 目的地: 詳細を表示するには、目的地の横にある下矢印を選択します。
   a. データを復元する場所（元のソースの場所または指定できる別の場所）を選択します。

> 元のファイルまたはディレクトリは復元されたデータによって上書きされますが、新しい名前を指定しない限り、元のファイルとフォルダの名前は同じままになります。

b. システムを選択します。

c. ストレージ VM を選択します。

d. 必要に応じて、パスを入力します。

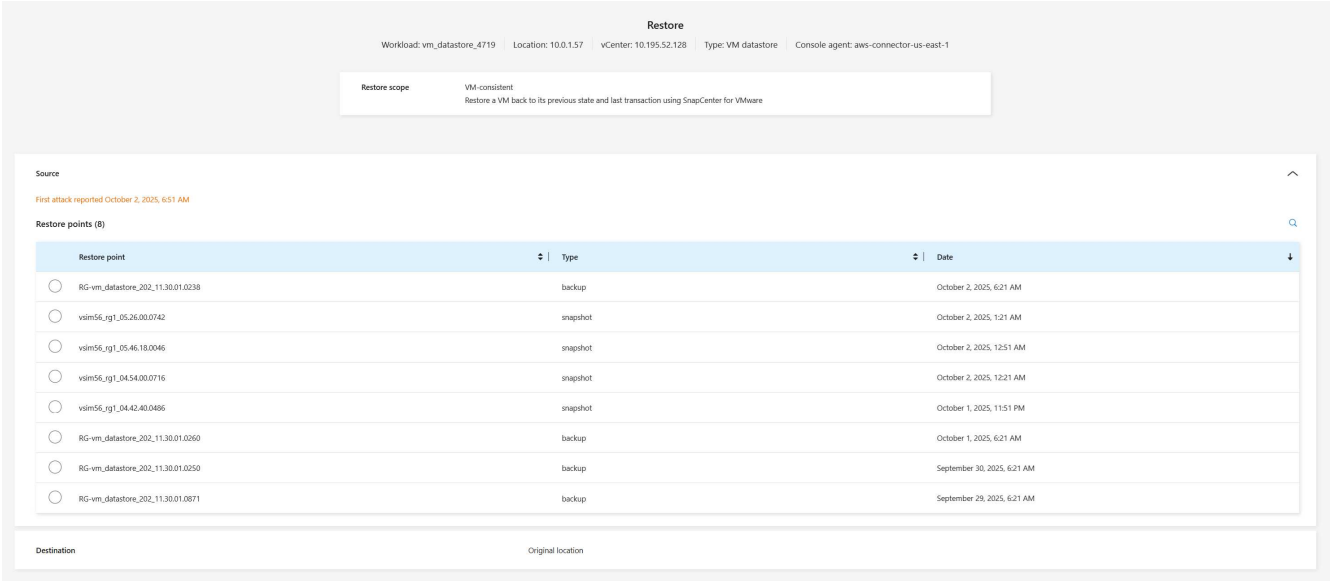
> 復元のパスを指定しない場合は、ファイルは最上位ディレクトリの新しいボリュームに復元されます。

5. *保存*を選択します。
6. 選択内容を確認します。
7. *復元*を選択します。
8. メニューから [リカバリ] を選択し、[リカバリ] ページでワークロードを確認します。ここで、操作のステータスがさまざまな状態を遷移します。

VM レベルで **VM** ファイル共有を復元する

復元する VM を選択した後、[回復] ページで次の手順を続行します。

1. ソース: 詳細を表示するには、[ソース] の横にある下矢印を選択します。



2. データを復元するために使用する復元ポイントを選択します。
3. 目的地: 元の場所へ。
4. *次へ*を選択します。
5. 選択内容を確認します。
6. *復元*を選択します。
7. メニューから [リカバリ] を選択し、[リカバリ] ページでワークロードを確認します。ここで、操作のステータスがさまざまな状態を遷移します。

NetApp Ransomware Resilienceでランサムウェア攻撃対策訓練を実施する

新しいサンプル ワークロードへの攻撃をシミュレートして、ランサムウェア攻撃の準備訓練を実行します。シミュレートされた攻撃を調査し、ワークロードを回復します。この機能を使用して、アラート通知、応答、および回復をテストします。必要に応じて何度でもドリルを実行してください。

実際のワークロード データは影響を受けません。

NFS および CIFS (SMB) ワークロードで準備ドリルを実行できます。

ランサムウェア攻撃への備えの訓練を構成する

シミュレーションを実行する前に、[設定] ページでドリルを設定します。上部メニューの「アクション」オプションから「設定」ページにアクセスします。

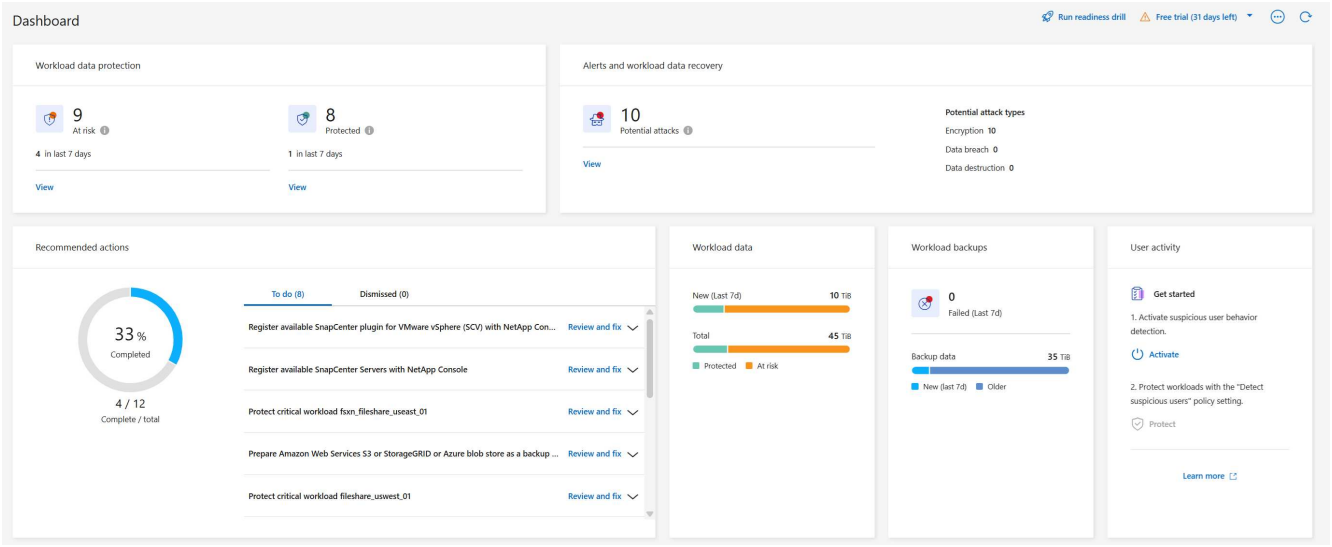
次の状況では、ユーザー名とパスワードを入力する必要があります。

- 以前に選択したストレージVMのユーザー名またはパスワードが変更された場合
- 別のCIFS（SMB）ストレージVMを選択した場合
- 別のテストワークロード名を入力する場合

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" 。

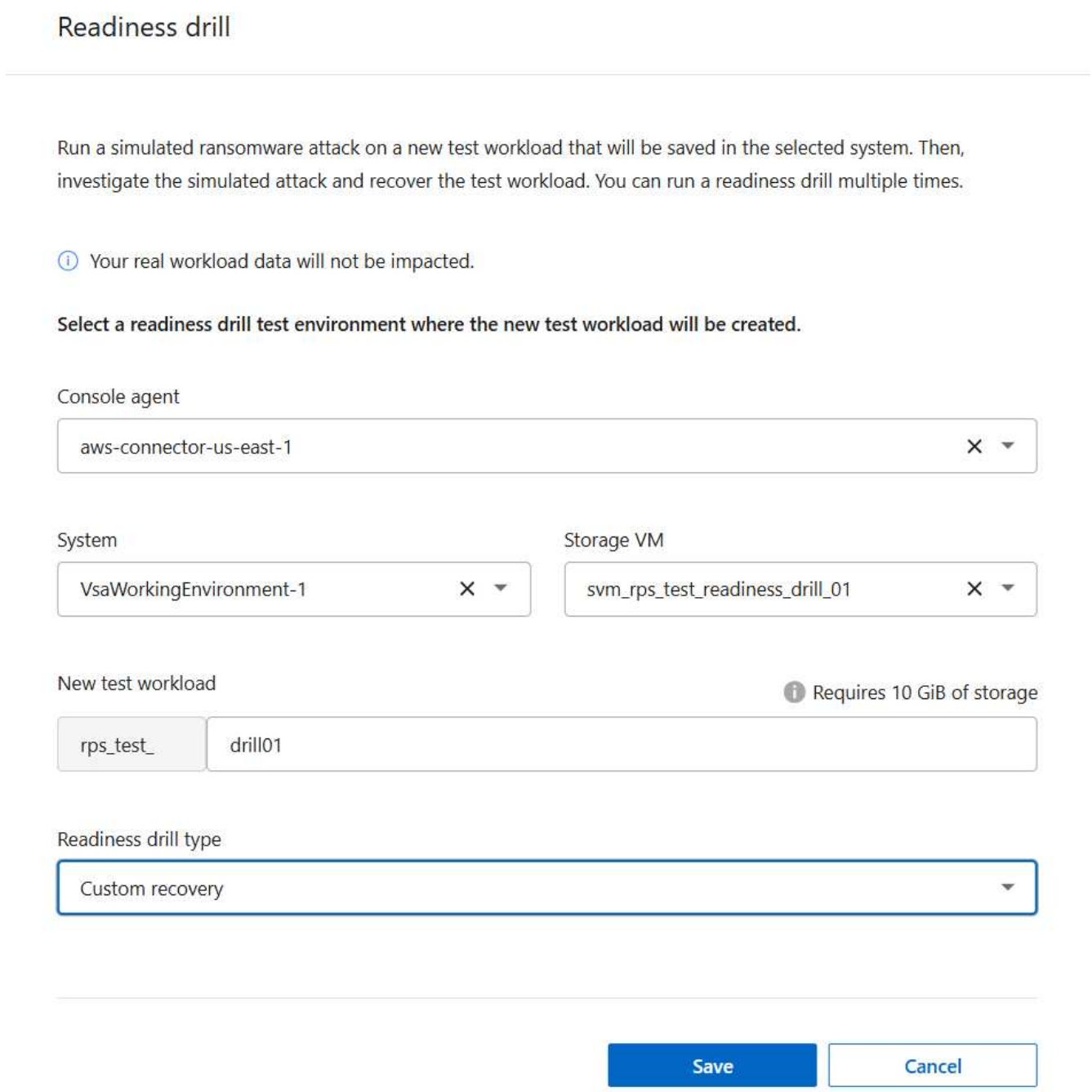
手順

1. NetApp Ransomware Resilienceメニューから、右上にある 準備ドリルの実行 ボタンを選択します。



2. [設定] ページの準備ドリル カードで、[構成] を選択します。

コンソールに準備ドリルの構成ページが表示されます。



3. 次の手順を実行します。
   a. 準備ドリルに使用するコンソール エージェントを選択します。
   b. テスト システムを選択します。
   c. テスト ストレージ SVM を選択します。
   d. CIFS (SMB) ストレージ VM を選択した場合は、ユーザー名 フィールドと パスワード フィールドが表示されます。ストレージ VM のユーザー名とパスワードを入力します。
   e. 準備訓練の種類を選択します。暗号化データ侵害から手動で回復する場合は、カスタム回復 を選択し

ます。疑わしいユーザーアクティビティからの回復には、データ侵害 を選択します。

f. 作成する新しいテスト ワークロードの名前を入力します。名前にダッシュを含めないでください。

4. *保存*を選択します。

準備ドリルの構成は、後で設定ページを使用して編集できます。

準備訓練を開始する

準備ドリルを構成したら、ドリルを開始できます。

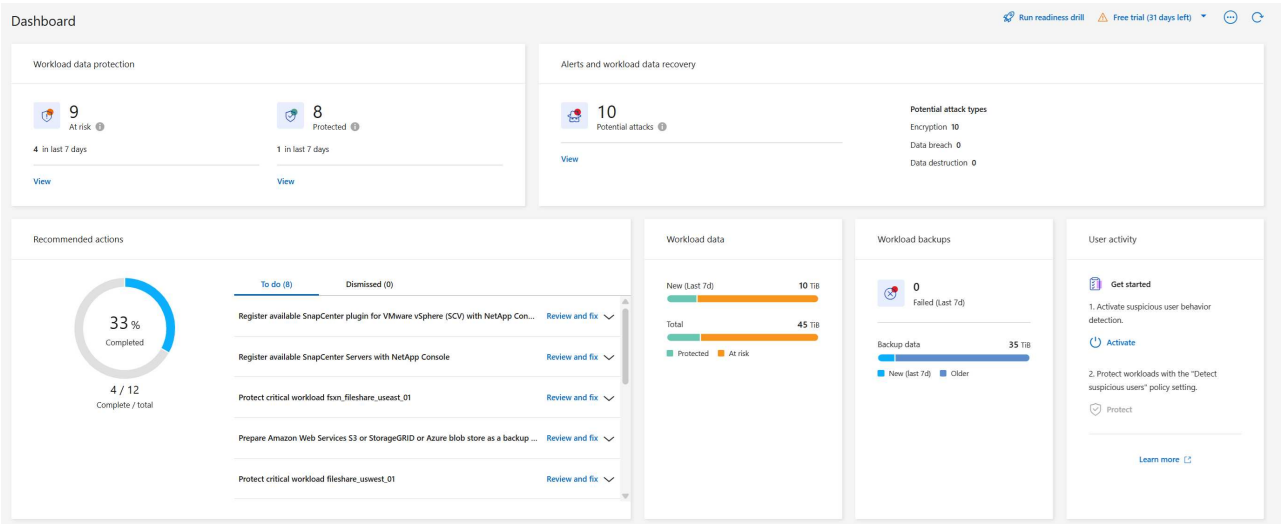
必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

準備ドリルを開始すると、Ransomware Resilience は学習モードをスキップし、アクティブ モードでドリルを開始します。ワークロードの検出ステータスはアクティブです。

検出ポリシーが最近割り当てられ、Ransomware Resilience がワークロードをスキャンすると、ワークロードはランサムウェア検出の 学習モード ステータスになることがあります。

手順

1. 次のいずれかを実行します。
   - ランサムウェア耐性メニューから、右上にある*準備ドリルを実行*ボタンを選択します。



   - または、[設定] ページの準備ドリル カードで [開始] を選択します。

ドリルの実行中は、準備ドリルの構成を編集することはできません。ドリルをリセットして停止し、設定を変更することができます。

即応訓練の警報に応答する

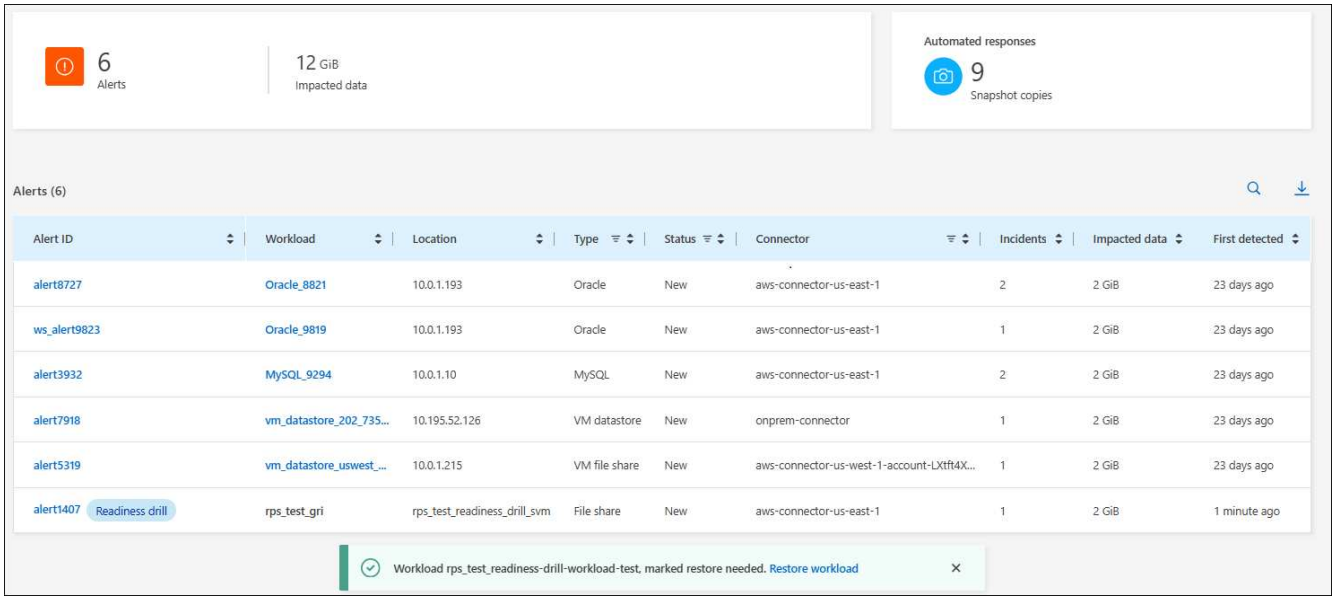
準備訓練アラートに応答して準備状況をテストします。

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" 。

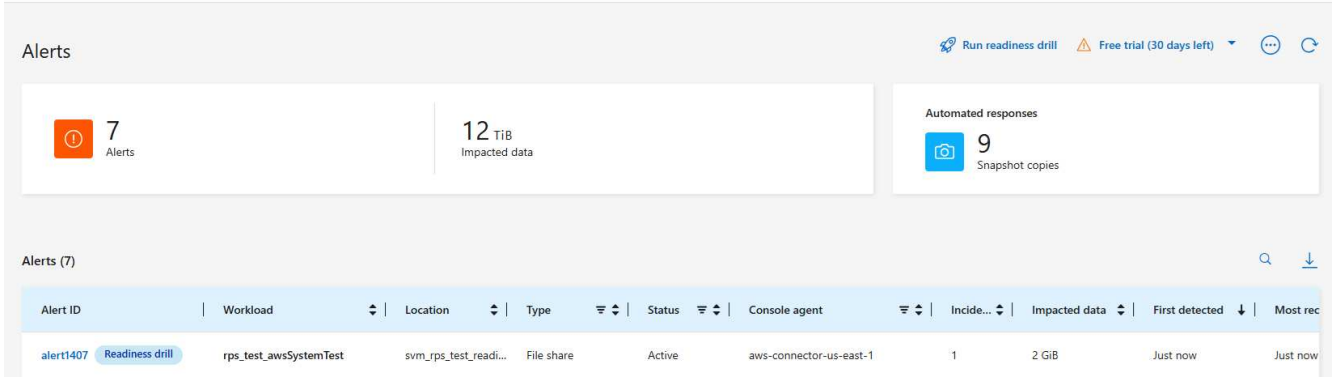
手順

1. ランサムウェア耐性メニューから、「アラート」を選択します。

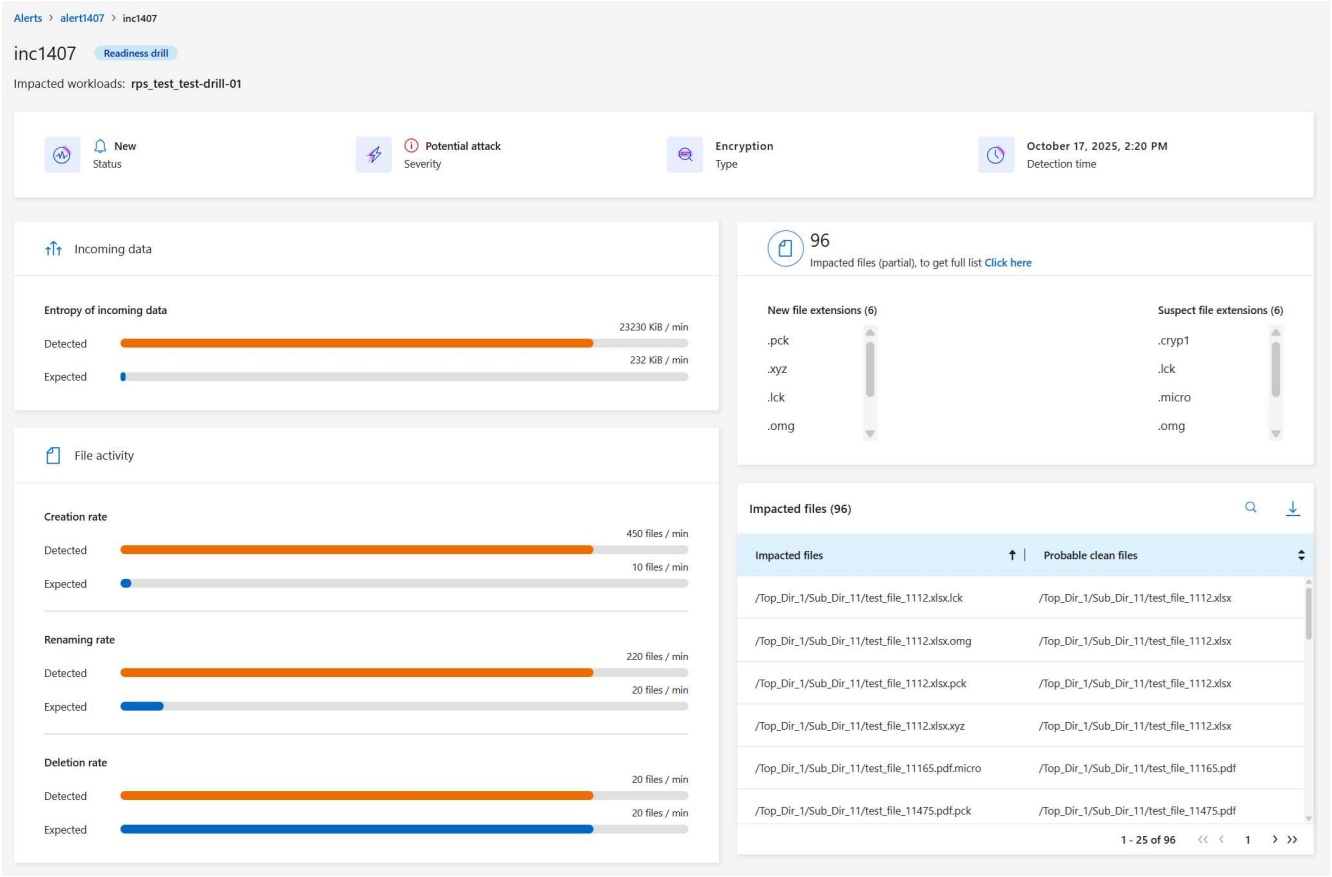
   コンソールにアラート ページが表示されます。アラート ID 列の ID の横に「準備ドリル」が表示されます。



2. 「準備訓練」の表示があるアラートを選択します。アラートの詳細ページにインシデント アラートのリストが表示されます。



3. アラート インシデントを確認します。
4. アラート インシデントを選択します。



注目すべき点は次のとおりです:

- 潜在的な攻撃の重大度を確認します。

  重大度により、ユーザーが悪意のあるアクティビティを行っている疑いがあることが示されている場合は、ユーザー名を確認します。また、"ユーザーをブロックします。"

- ファイルアクティビティと疑わしいプロセスを確認します。
  - 受信した検出されたデータを予想されるデータと比較してみます。
  - 検出されたファイルの作成率を予想される率と比較して確認します。
  - 検出されたファイル名変更率を予想される率と比較してみます。
  - 削除率を予想率と比較してみます。
- 影響を受けるファイルのリストを確認します。攻撃の原因となっている可能性のある拡張機能を確認します。
- 影響を受けるファイルとディレクトリの数を確認して、攻撃の影響と範囲を判断します。

テストワークロードを復元する

準備ドリルアラートを確認した後、必要に応じてテストのワークロードを復元します。

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" 。

手順

1. アラートの詳細ページに戻ります。
2. テスト ワークロードを復元する必要がある場合は、次の手順を実行します。
   - *復元が必要としてマーク*を選択します。
   - 確認内容を確認し、確認ボックスで「復元が必要としてマーク」を選択します。
     - ランサムウェア耐性メニューから、「回復」を選択します。
     - 復元する「準備ドリル」とマークされたテスト ワークロードを選択します。
     - *復元*を選択します。
     - 「復元」ページで、復元に関する情報を入力します。
   - ソース スナップショットのコピーを選択します。
   - 宛先ボリュームを選択します。
3. 復元のレビューページで、[復元] を選択します。

   コンソールの [回復] ページに、準備ドリル復元のステータスが「進行中」として表示されます。

   復元が完了すると、コンソールはワークロードのステータスを「復元済み」に変更します。

4. 復元されたワークロードを確認します。

復元プロセスの詳細については、"ランサムウェア攻撃からの回復（インシデントが中和された後）"。

準備訓練後にアラートのステータスを変更する

準備ドリルアラートを確認し、ワークロードを復元した後、必要に応じてアラートのステータスを変更します。

コンソールの役割が必要です 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。 "すべてのサービスのコンソールアクセスロールについて学習します"。

手順

1. アラートの詳細ページに戻ります。
2. アラートをもう一度選択します。
3. ステータスの編集 を選択してステータスを指定し、次のいずれかのステータスに変更します。
   - 却下: アクティビティがランサムウェア攻撃ではないと疑われる場合は、ステータスを「却下」に変更します。

     攻撃を却下した後は、元に戻すことはできません。ワークロードを破棄すると、潜在的なランサムウェア攻撃に応じて自動的に作成されたすべてのスナップショット コピーが完全に削除されます。アラートを無視すると、準備訓練は完了したとみなされます。

   - 解決済み: インシデントは軽減されました。

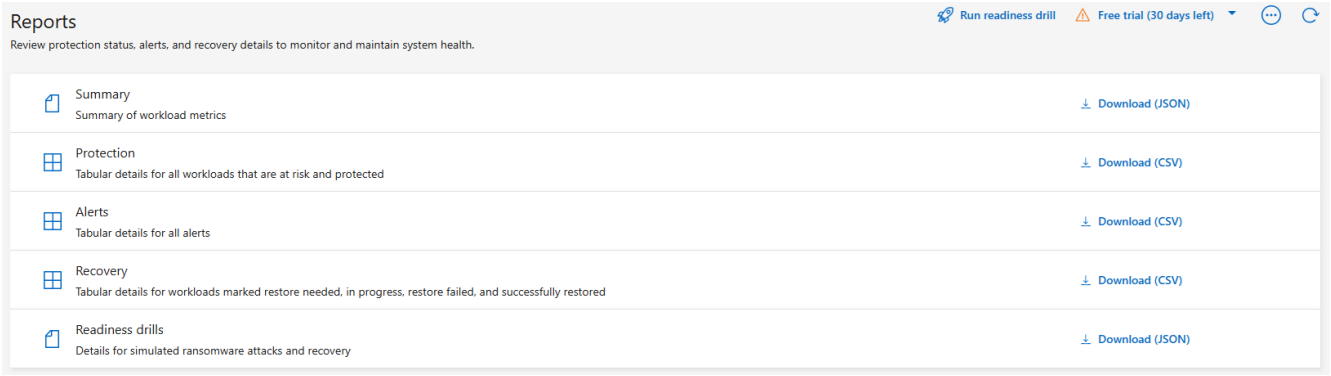
即応訓練に関する報告書を確認する

準備訓練が完了したら、訓練に関するレポートを確認して保存することをお勧めします。

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、ランサムウェア レジリエンス管理者、またはランサムウェア レジリエンス ビューアー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" 。

手順

1. ランサムウェア耐性メニューから、*レポート*を選択します。



2. 準備ドリルレポートをダウンロードするには、[準備ドリル] と [ダウンロード] を選択します。

NetApp Ransomware ResilienceをセキュリティおよびイベントSIEM管理システム（SIEM）に接続し、脅威の分析と検出を行う

セキュリティおよびイベント管理システム（SIEM）は、ログとイベント データを一元管理して、セキュリティ イベントとコンプライアンスに関する分析情報を提供します。NetApp Ransomware Resilienceは、脅威の分析と検出を効率化するために、SIEMにデータを自動的に送信することをサポートします。

NetApp Ransomware Resilience は次の SIEM をサポートしています：

- AWS Security Hub
- Microsoft Sentinel
- Splunk Cloud

Ransomware Resilience で SIEM を有効にする前に、SIEM システムを構成する必要があります。

SIEMに送信されるイベントデータ

Ransomware Resilience は、次のイベント データを SIEM システムに送信できます。

- コンテクスト：
  - **os**: これはONTAPの値を持つ定数です。
  - **os_version**: システムで実行されているONTAPのバージョン。

- **connector_id**: システムを管理するコンソールエージェントの ID。
- **cluster_id**: システムのONTAPによって報告されたクラスタ ID。
- **svm_name**: アラートが見つかった SVM の名前。
- **volume_name**: アラートが見つかったボリュームの名前。
- **volume_id**: システムのONTAPによって報告されたボリュームの ID。

- 事件：
  - **incident_id**: Ransomware Resilience で攻撃を受けているボリュームに対して Ransomware Resilience によって生成されたインシデント ID。
  - **alert_id**: ワークロードに対して Ransomware Resilience によって生成された ID。
  - 重大度: 次のアラート レベルのいずれか: 「CRITICAL」、「HIGH」、「MEDIUM」、「LOW」。
  - 説明: 検出されたアラートの詳細。例: 「ワークロード arp_learning_mode_test_2630 で潜在的なランサムウェア攻撃が検出されました」

脅威検出用に **AWS Security Hub** を構成する

Ransomware Resilience で AWS Security Hub を有効にする前に、AWS Security Hub で次の大まかな手順を実行する必要があります：

- AWS Security Hub で権限を設定します。
- AWS Security Hub で認証アクセスキーとシークレットキーを設定します。 (これらの手順はここでは説明しません。)

AWS Security Hubで権限を設定する手順

1. **AWS IAM** コンソール に移動します。
2. *ポリシー*を選択します。
3. 次の JSON 形式のコードを使用してポリシーを作成します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "NetAppSecurityHubFindings",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchImportFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource": [
        "arn:aws:securityhub:*:*:product/*/default",
        "arn:aws:securityhub:*:*:hub/default"
      ]
    }
  ]
}
```

脅威検出用に **Microsoft Sentinel** を構成する

Ransomware Resilience で Microsoft Sentinel を有効にする前に、Microsoft Sentinel で次の大まかな手順を実行する必要があります。

- 前提条件
  - Microsoft Sentinel を有効にします。
  - Microsoft Sentinel でカスタム ロールを作成します。
- 登録
  - Microsoft Sentinel からイベントを受信するには、Ransomware Resilience を登録します。
  - 登録用のシークレットを作成します。
- 権限: アプリケーションに権限を割り当てます。
- 認証: アプリケーションの認証資格情報を入力します。

Microsoft Sentinelを有効にする手順

1. Microsoft Sentinel にアクセスします。
2. **Log Analytics** ワークスペース を作成します。
3. 作成した Log Analytics ワークスペースを Microsoft Sentinel で使用できるようにします。

Microsoft Sentinelでカスタムロールを作成する手順

1. Microsoft Sentinel にアクセスします。
2. サブスクリプション > アクセス制御 **(IAM)** を選択します。
3. カスタム ロール名を入力します。 **Ransomware Resilience Sentinel Configurator** という名前を使用し

ます。

4. 次の JSON をコピーして、**JSON** タブに貼り付けます。

```
{
  "roleName": "Ransomware Resilience Sentinel Configurator",
  "description": "",
  "assignableScopes":["/subscriptions/{subscription_id}"],
  "permissions": [

  ]
}
```

5. 設定を確認して保存します。

Microsoft Sentinelからイベントを受信するために**Ransomware Resilience**を登録する手順

1. Microsoft Sentinel にアクセスします。
2. **Entra ID** > アプリケーション > *アプリ登録*を選択します。
3. アプリケーションの*表示名*に「**Ransomware Resilience**」と入力します。
4. サポートされているアカウントの種類 フィールドで、この組織ディレクトリ内のアカウントのみ を選択します。
5. イベントがプッシュされる*デフォルト インデックス*を選択します。
6. *レビュー*を選択します。
7. 設定を保存するには、[登録] を選択します。

   登録後、Microsoft Entra 管理センターにアプリケーションの概要ペインが表示されます。

登録用のシークレットを作成する手順

1. Microsoft Sentinel にアクセスします。
2. 証明書とシークレット > クライアント シークレット > *新しいクライアント シークレット*を選択します。
3. アプリケーション シークレットの説明を追加します。
4. シークレットの*有効期限*を選択するか、カスタム有効期間を指定します。

   クライアント シークレットの有効期間は 2 年 (24 か月) 以下に制限されます。 Microsoft では、有効期限を 12 か月未満に設定することをお勧めします。

5. シークレットを作成するには、[追加] を選択します。
6. 認証手順で使用するシークレットを記録します。このページを離れた後、秘密は再び表示されることはありません。

アプリケーションに権限を割り当てる手順

1. Microsoft Sentinel にアクセスします。

2. サブスクリプション > アクセス制御 **(IAM)** を選択します。
3. 追加 > *ロールの割り当てを追加*を選択します。
4. 特権管理者ロール フィールドで、**Ransomware Resilience Sentinel Configurator** を選択します。

これは先ほど作成したカスタム ロールです。

5. *次へ*を選択します。
6. アクセスの割り当て先 フィールドで、ユーザー、グループ、またはサービス プリンシパル を選択します。
7. メンバーを選択*を選択します。次に、「**Ransomware Resilience Sentinel Configurator**」を選択します。
8. *次へ*を選択します。
9. ユーザーが実行できる操作 フィールドで、特権管理者ロール (所有者、**UAA**、**RBAC)** を除くすべてのロールの割り当てをユーザーに許可する **(**推奨**)** を選択します。
10. *次へ*を選択します。
11. 権限を割り当てるには、[確認して割り当て] を選択します。

アプリケーションの認証資格情報を入力する手順

1. Microsoft Sentinel にアクセスします。
2. 資格情報を入力してください:
   a. テナント ID、クライアント アプリケーション ID、およびクライアント アプリケーション シークレットを入力します。
   b. **Authenticate** を選択します。

認証が成功すると、「認証済み」というメッセージが表示されます。

3. アプリケーションの Log Analytics ワークスペースの詳細を入力します。
   a. サブスクリプション ID、リソース グループ、Log Analytics ワークスペースを選択します。

脅威検出用に**Splunk Cloud**を構成する

Ransomware Resilience で Splunk Cloud を有効にする前に、Splunk Cloud で次の大まかな手順を実行する必要があります。

- Splunk Cloud の HTTP イベント コレクターを有効にして、コンソールから HTTP または HTTPS 経由でイベント データを受信します。
- Splunk Cloud でイベント コレクター トークンを作成します。

Splunkで**HTTP**イベントコレクターを有効にする手順

1. Splunk Cloud に移動します。
2. 設定 > *データ入力*を選択します。
3. **HTTP** イベント コレクター > グローバル設定 を選択します。

4. [すべてのトークン] トグルで、[有効] を選択します。
5. イベント コレクターが HTTP ではなく HTTPS 経由でリッスンして通信するようにするには、[SSL を有効にする] を選択します。
6. HTTP イベント コレクターの **HTTP** ポート番号 にポートを入力します。

Splunkでイベントコレクタートークンを作成する手順

1. Splunk Cloud に移動します。
2. 設定 > *データの追加*を選択します。
3. モニター > **HTTP** イベント コレクター を選択します。
4. トークンの名前を入力し、[次へ] を選択します。
5. イベントがプッシュされる デフォルト インデックス を選択し、レビュー を選択します。
6. エンドポイントのすべての設定が正しいことを確認し、[送信] を選択します。
7. トークンをコピーして別のドキュメントに貼り付け、認証手順の準備を整えます。

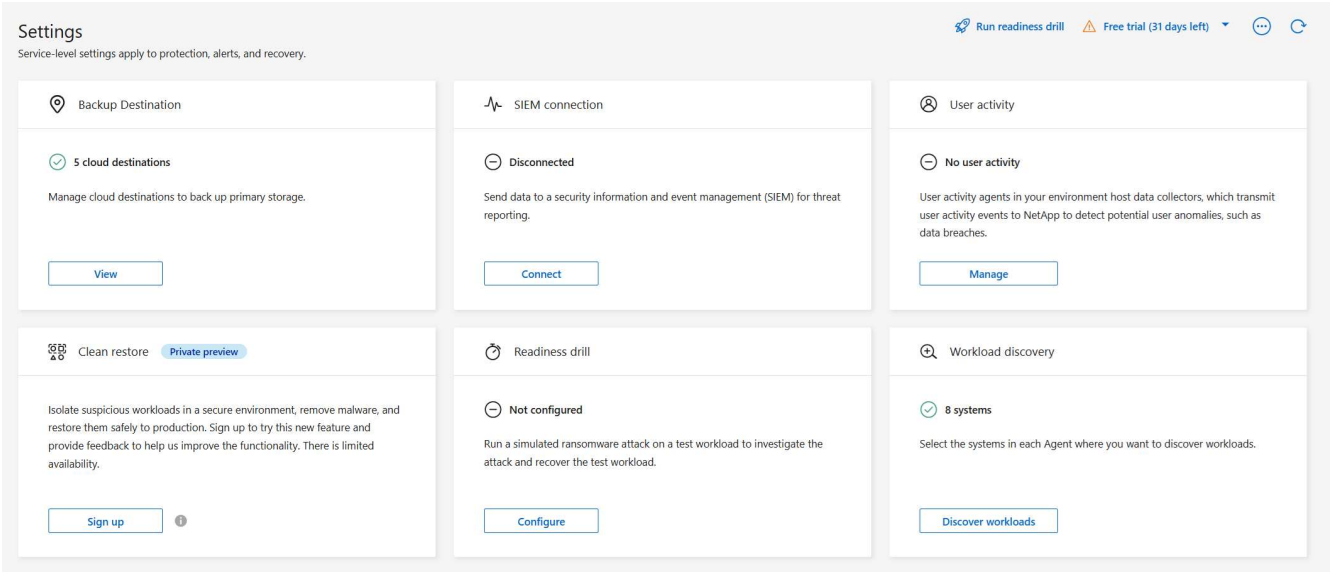
ランサムウェア耐性における**SIEM**の接続

SIEM を有効にすると、脅威の分析とレポートのために、Ransomware Resilience から SIEM サーバーにデータが送信されます。

手順

1. コンソール メニューから、保護 > ランサムウェア耐性 を選択します。
2. ランサムウェア耐性メニューから、垂直方向の … 右上のオプションをクリックします。
3. *設定*を選択します。

   設定ページが表示されます。



4. [設定] ページで、SIEM 接続タイルの [接続] を選択します。

5. SIEM システムの 1 つを選択します。
6. AWS Security Hub または Splunk Cloud で設定したトークンと認証の詳細を入力します。

   入力する情報は、選択した SIEM によって異なります。

7. *有効*を選択します。

   設定ページに「接続済み」と表示されます。

NetApp Ransomware Resilienceのレポートをダウンロード

NetApp Ransomware Resilienceは、サポートされているボリュームとサポートされていないボリューム、攻撃準備訓練、保護、アラート、リカバリの詳細を示すCSVおよびJSON形式のレポートを提供します。レポートを使用すると、訓練、保護態勢、アラート、リカバリイベントに関するオフラインレポートを保存して確認できます。

ファイルをダウンロードする前に、ダッシュボードを更新して、レポートの最新データを取得してください。

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、ランサムウェア レジリエンス管理者、またはランサムウェア レジリエンス ビューアー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" 。

*どのようなデータをダウンロードできますか?*メイン メニュー オプションのいずれかからファイルをダウンロードできます。

- 概要: サポートされているワークロードとサポートされていないワークロードのリスト、サイバーレジリエンスの体制を改善するための推奨アクション、およびランサムウェアレジリエンスダッシュボードで収集された情報が含まれています。
- 保護: 保護されているワークロードとリスクのあるワークロードの合計数など、すべてのワークロードのステータスと詳細が含まれます。
- アラート: アラートの合計数や自動スナップショットなど、すべてのアラートのステータスと詳細が含ま

れます。

- 回復: 復元が必要なすべてのワークロードのステータスと詳細が含まれます。これには、「復元が必要」、「進行中」、「復元に失敗しました」、「正常に復元されました」とマークされたワークロードの合計数も含まれます。
- レポート: どのページからでもデータをエクスポートし、ファイルをダウンロードできます。

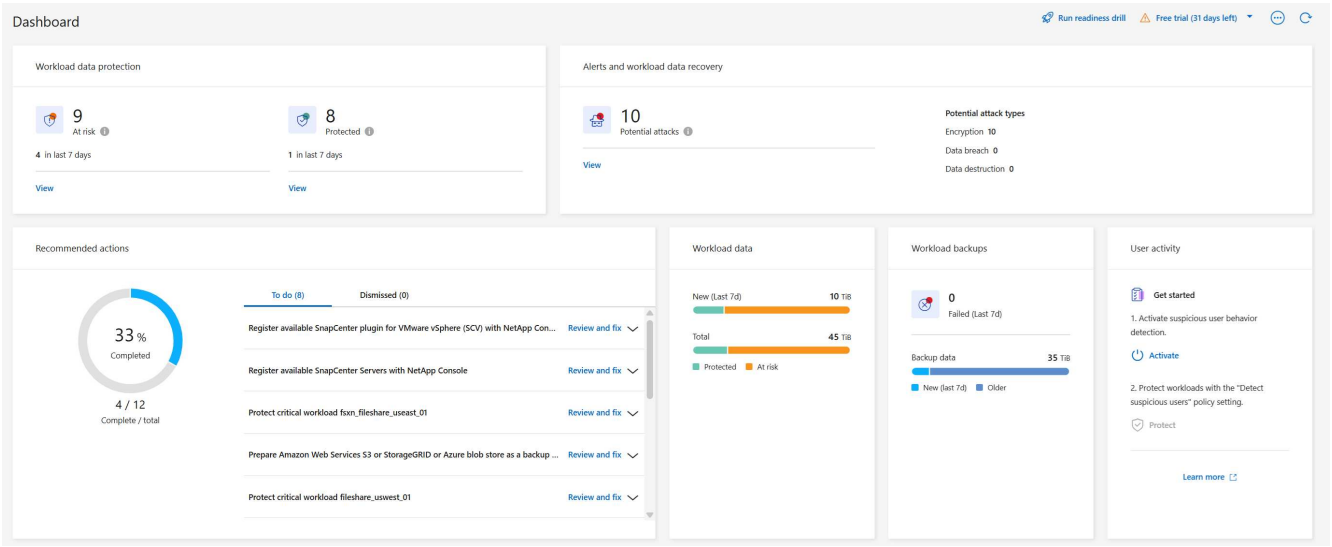
> 準備ドリルレポートは、レポート ページからのみダウンロードできます。

保護、アラート、または回復ページから CSV または JSON ファイルをダウンロードすると、そのページのデータのみが表示されます。

CSV または JSON ファイルには、すべてのコンソール システム上のすべてのワークロードのデータが含まれます。

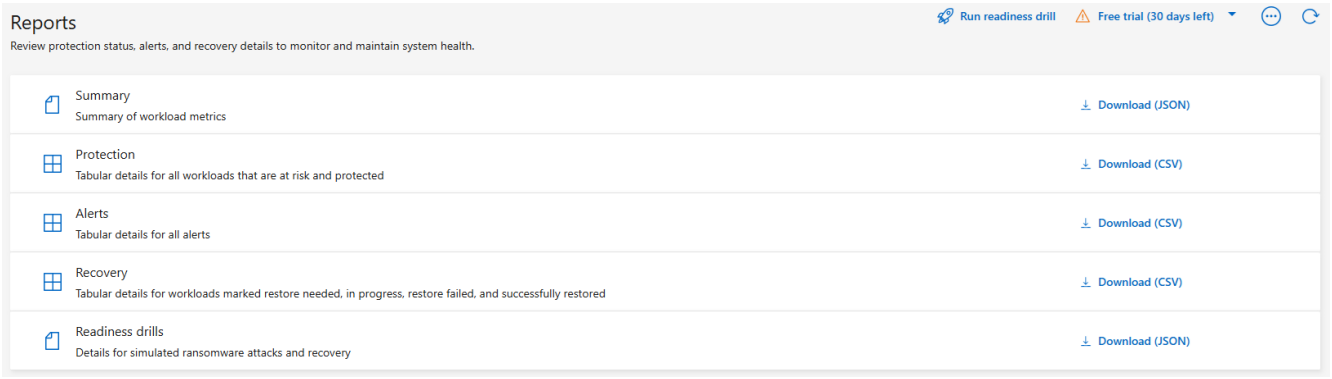
手順

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。



ページ"]

2. ダッシュボードまたは他のページから、右上の*更新* オプションを選択すると、レポートに表示されるデータが更新されます。
3. 次のいずれかを実行します。
   - ページから*ダウンロード*を選択します オプション。
   - NetApp Ransomware Resilienceメニューから、レポート を選択します。
4. レポート オプションを選択した場合は、事前設定されたファイル名の 1 つを選択し、ダウンロード を選択します。


Reports
Review protection status, alerts, and recovery details to monitor and maintain system health.
Run readiness drill
Free trial (30 days left)
Summary
Summary of workload metrics
Download (JSON)
Protection
Tabular details for all workloads that are at risk and protected
Download (CSV)
Alerts
Tabular details for all alerts
Download (CSV)
Recovery
Tabular details for workloads marked restore needed, in progress, restore failed, and successfully restored
Download (CSV)
Readiness drills
Details for simulated ransomware attacks and recovery
Download (JSON)