NetAppランサムウェア耐性ドキュメント

NetApp Ransomware Resilience

NetApp
October 06, 2025

目次

NetAppランサムウェア耐性ドキュメント 1
リリース ノート 2
NetAppランサムウェア耐性の新機能 2
2025年10月6日 2
2025年7月15日 2
2025年6月9日 3
2025年5月13日 3
2025年4月29日 4
2025年4月14日 4
2025年3月10日 5
2024年12月16日 6
2024年11月7日 6
2024年9月30日 7
2024年9月2日 7
2024年8月5日 8
2024年7月1日 8
2024年6月10日 9
2024年5月14日 9
2024年3月5日 11
2023年10月6日 12
NetApp Ransomware Resilienceの既知の制限 12
準備訓練のリセットオプションの問題 13
Amazon FSx for NetApp ONTAP の制限 13
始めましょう 14
NetAppのランサムウェア耐性について学ぶ 14
データ層におけるランサムウェア耐性 14
ランサムウェア耐性でできること 15
ランサムウェア耐性を使用するメリット 16
料金 16
ライセンス 17
NetAppコンソール 17
ランサムウェア耐性の仕組み 18
サポートされているバックアップターゲット、システム、ワークロードデータソース 20
ランサムウェア対策に役立つ用語 21
NetAppランサムウェア耐性の前提条件 21
NetAppコンソール 21
ONTAP 9.11.1以降 22
データのバックアップ用 22
ONTAPシステムで管理者以外のユーザーの権限を更新する 22

NetAppランサムウェア耐性のクイックスタート 23
NetAppランサムウェア耐性を設定する 24
バックアップ先を準備する 24
NetAppコンソールをセットアップする 24
NetAppランサムウェア耐性にアクセス 25
NetApp Ransomware Resilienceのライセンスを設定する 26
その他のライセンス 27
30日間の無料トライアルでお試しください 27
AWS Marketplace からサブスクライブする 28
Microsoft Azure Marketplace を通じてサブスクライブする 31
Google Cloud Platform Marketplace から登録する 33
ライセンス持ち込み（BYOL） 36
コンソールのライセンスが期限切れになったら更新してください 37
PAYGOサブスクリプションを終了する 37
NetApp Ransomware Resilience のワークロードを発見 38
検出して保護するワークロードを選択する 38
以前に選択したシステムに対して新しく作成されたワークロードを検出する 40
新しいシステムを発見する 40
NetApp Ransomware Resilienceでランサムウェア攻撃対策訓練を実施する 41
ランサムウェア攻撃への備えの訓練を構成する 41
準備訓練を開始する 44
即応訓練警報に応答する 44
テストワークロードを復元する 46
準備訓練後にアラートのステータスを変更する 47
即応訓練に関する報告書を確認する 47
NetApp Ransomware Resilienceで保護設定を構成する 48
設定ページに直接アクセスする 48
ランサムウェア攻撃をシミュレートする 49
ワークロード検出を構成する 49
Data Infrastructure Insights Workload Security
に接続して、疑わしい異常なユーザー行動を確認します。 49
バックアップ先を追加する 50
脅威の分析と検出のためにセキュリティおよびイベント管理システム (SIEM) に接続する 57
ランサムウェア耐性を活用する 64
NetAppのランサムウェア耐性を活用する 64
NetAPp ランサムウェア耐性ダッシュボードを使用してワークロードの健全性を監視する 64
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 64
ダッシュボードで保護の推奨事項を確認する 66
保護データをCSVファイルにエクスポートする 68
技術文書にアクセスする 68
ワークロードを保護する 68

NetAppランサムウェア耐性保護戦略でワークロードを保護する 69
ランサムウェア耐性におけるNetAppデータ分類で個人を特定できる情報をスキャン 83
NetApp Ransomware Resilience で検出されたランサムウェアアラートを処理する 87
アラートを表示 88
アラートメールに返信する 89
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 90
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) 93
潜在的な攻撃ではないインシデントを無視する 94
影響を受けるファイルの一覧を表示する 96
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) 97
復元準備が整ったワークロードを表示する 98
SnapCenterによって管理されるワークロードを復元する 98
SnapCenterで管理されていないワークロードを復元する 99
NetApp Ransomware Resilience のレポートをダウンロード 107
知識とサポート 109
サポートに登録する 109
サポート登録の概要 109
NetAppサポートのためにBlueXPを登録する 109
Cloud Volumes ONTAPサポートに NSS 認証情報を関連付ける 112
ヘルプを受ける 113
クラウドプロバイダーのファイルサービスのサポートを受ける 113
セルフサポートオプションを使用する 114
NetAppサポートでケースを作成する 114
サポートケースを管理する（プレビュー） 116
NetAppランサムウェア耐性に関するよくある質問 119
導入 119
アクセス 119
他のサービスとのやり取り 120
ワークロード 120
保護ポリシー 121

NetAppランサムウェア耐性ドキュメント

リリース ノート

NetAppランサムウェア耐性の新機能

NetApp Ransomware Resilience の新機能について学びます。

2025年10月6日

BlueXP ransomware protectionは**NetApp**ランサムウェア耐性に変わりました

BlueXPランサムウェア レプリケーションの名前がNetApp Ransomware Resilience に変更されました。

BlueXPは**NetApp**コンソールになりました

BlueXP は、データ インフラストラクチャの管理における役割をより適切に反映するために、名前が変更され、再設計されました。

NetAppコンソールは、オンプレミスとクラウド環境全体にわたるエンタープライズ グレードのストレージとデータ サービスの集中管理を提供し、リアルタイムの分析情報、ワークフローの高速化、管理の簡素化を実現します。

変更内容の詳細については、 "NetAppコンソールのリリースノート" 。

2025年7月15日

SANワークロードのサポート

このリリースには、BlueXP ransomware protectionにおける SAN ワークロードのサポートが含まれています。 NFS および CIFS ワークロードに加えて、SAN ワークロードも保護できるようになりました。

詳細については、 "BlueXP ransomware protectionの前提条件" 。

ワークロード保護の改善

このリリースでは、 SnapCenterやBlueXP backup and recoveryなどの他のNetAppツールからのスナップショットおよびバックアップ ポリシーを使用したワークロードの構成プロセスが改善されています。以前のリリースでは、 BlueXP ransomware protectionは他のツールからのポリシーを検出し、検出ポリシーの変更のみが可能でした。このリリースでは、スナップショットおよびバックアップ ポリシーをBlueXP ransomware protectionポリシーに置き換えたり、他のツールのポリシーを引き続き使用したりできるようになりました。

詳細については、"ワークロードを保護する" 。

メール通知

BlueXP ransomware protectionが攻撃の可能性を検出すると、 BlueXP通知に通知が表示され、設定した電子メール アドレスに電子メールが送信されます。

電子メールには、重大度、影響を受けるワークロード、 BlueXP ransomware protectionの アラート タブのアラートへのリンクに関する情報が含まれています。

BlueXP ransomware protectionでセキュリティおよびイベント管理 (SIEM) システムを構成した場合、サービスはアラートの詳細を SIEM システムに送信します。

詳細については、"検出されたランサムウェアアラートを処理する" 。

2025年6月9日

ランディングページの更新

このリリースには、BlueXP ransomware protectionのランディング ページの更新が含まれており、無料トライアルの開始と検出が容易になります。

準備訓練の最新情報

以前は、新しいサンプル ワークロードに対する攻撃をシミュレートすることで、ランサムウェア対策訓練を実行できました。この機能を使用すると、シミュレートされた攻撃を調査し、ワークロードを回復できます。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。必要に応じてこれらのドリルを実行し、スケジュールを設定します。

このリリースでは、 BlueXP ransomware protectionダッシュボードの新しいボタンを使用して、テスト ワークロードでランサムウェア準備ドリルを実行できるようになりました。これにより、制御された環境内でランサムウェア攻撃のシミュレート、その影響の調査、ワークロードの効率的な回復が容易になります。

NFS ワークロードに加えて、CIFS (SMB) ワークロードでも準備ドリルを実行できるようになりました。

詳細については、 "ランサムウェア攻撃への備えの訓練を実施する" 。

BlueXP classificationの更新を有効にする

BlueXP ransomware protectionサービス内でBlueXP classificationを使用する前に、 BlueXP classificationを有効にしてデータをスキャンする必要があります。データを分類すると、セキュリティ リスクを増大させる可能性のある個人を特定できる情報 (PII) を見つけるのに役立ちます。

BlueXP ransomware protection内から、ファイル共有ワークロードにBlueXP classificationを展開できます。プライバシー露出*列で、*露出の特定*オプションを選択します。分類サービスを有効にしている場合、このアクションによって露出が識別されます。それ以外の場合、このリリースでは、ダイアログ ボックスに**BlueXP classification**を展開するオプションが表示されます。 *デプロイ を選択すると、 BlueXP classificationサービスのランディング ページに移動し、そのサービスをデプロイできます。W

詳細については、 "クラウドでBlueXP classificationを展開" BlueXP ransomware protection内でサービスを利用するには、 "BlueXP classificationで個人を特定できる情報をスキャン" 。

2025年5月13日

BlueXP ransomware protectionにおけるサポートされていない作業環境の報告

検出ワークフロー中に、サポートされているワークロードまたはサポートされていないワークロードにマウスを移動すると、 BlueXP ransomware protectionによって詳細が報告されます。これにより、一部のワークロードがBlueXP ransomware protectionサービスによって検出されない理由を理解するのに役立ちます。

サービスが作業環境をサポートしない理由は多数あります。たとえば、作業環境のONTAPバージョンが必要なバージョンよりも低い可能性があります。サポートされていない作業環境にマウスを移動すると、ツールヒ

ントに理由が表示されます。

初期検出中にサポートされていない作業環境を表示でき、結果をダウンロードすることもできます。設定ページの ワークロード検出 オプションから検出結果を表示することもできます。

詳細については、 "BlueXP ransomware protectionでワークロードを発見" 。

2025年4月29日

Amazon FSx for NetApp ONTAPのサポート

このリリースでは、Amazon FSx for NetApp ONTAPがサポートされます。この機能は、BlueXP ransomware protectionを使用して FSx for ONTAPワークロードを保護するのに役立ちます。

FSx for ONTAP は、クラウドでNetApp ONTAPストレージのパワーを提供する、完全に管理されたサービスです。ネイティブ AWS サービスの俊敏性と拡張性を備え、オンプレミスで使用するのと同じ機能、パフォーマンス、管理機能を提供します。

BlueXP ransomware protectionワークフローに次の変更が加えられました。

- 検出には、FSx for ONTAP 9.15 作業環境のワークロードが含まれます。
- [保護] タブには、FSx for ONTAP環境のワークロードが表示されます。この環境では、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する必要があります。 BlueXP ransomware protectionスナップショットを使用してこれらのワークロードを復元できます。

> FSx for ONTAPで実行されているワークロードのバックアップ ポリシーは、 BlueXPでは設定できません。 Amazon FSx for NetApp ONTAPで設定されている既存のバックアップポリシーは変更されません。

- アラート インシデントには、新しい FSx for ONTAP作業環境が表示されます。

詳細については、 "BlueXP ransomware protectionと動作環境について学ぶ" 。

サポートされているオプションの詳細については、 "BlueXP ransomware protectionの制限" 。

BlueXPアクセスロールが必要

BlueXP ransomware protectionを表示、検出、または管理するには、組織管理者、フォルダーまたはプロジェクト管理者、ランサムウェア保護管理者、またはランサムウェア保護閲覧者のいずれかのアクセス ロールが必要です。

"すべてのサービスに対するBlueXPのアクセスロールについて学ぶ" 。

2025年4月14日

即応訓練報告書

このリリースでは、ランサムウェア攻撃の準備訓練レポートを確認できるようになりました。準備ドリルを使用すると、新しく作成されたサンプル ワークロードに対するランサムウェア攻撃をシミュレートできます。次に、シミュレートされた攻撃を調査し、サンプルのワークロードを回復します。この機能は、アラート通知、対応、および回復プロセスをテストすることで、実際のランサムウェア攻撃が発生した場合に備えて準備

ができていることを確認するのに役立ちます。

詳細については、 "ランサムウェア攻撃への備えの訓練を実施する" 。

新しいロールベースのアクセス制御のロールと権限

以前は、ユーザーの責任に基づいて役割と権限を割り当てることができました。これにより、 BlueXP ransomware protectionへのユーザー アクセスを管理するのに役立ちました。このリリースでは、権限が更新されたBlueXP ransomware protectionに固有の 2 つの新しいロールが追加されました。新しい役割は次のとおりです。

- ランサムウェア保護管理者
- ランサムウェア保護ビューア

権限の詳細については、 "BlueXP ransomware protection機能へのロールベースのアクセス" 。

支払いの改善

このリリースには、支払いプロセスに対するいくつかの改善が含まれています。

詳細については、 "ライセンスと支払いオプションを設定する" 。

2025年3月10日

攻撃をシミュレートして対応する

このリリースでは、ランサムウェア攻撃をシミュレートして、ランサムウェアアラートへの対応をテストします。この機能は、アラート通知、対応、および回復プロセスをテストすることで、実際のランサムウェア攻撃が発生した場合に備えて準備ができていることを確認するのに役立ちます。

詳細については、 "ランサムウェア攻撃への備えの訓練を実施する" 。

発見プロセスの強化

このリリースには、選択的検出および再検出プロセスの機能強化が含まれています。

- このリリースでは、以前に選択した作業環境に追加された新しく作成されたワークロードを検出できます。
- このリリースでは、新しい作業環境を選択することもできます。この機能は、環境に追加された新しいワークロードを保護するのに役立ちます。
- これらの検出プロセスは、検出プロセス中に最初に実行することも、設定オプション内で実行することもできます。

詳細については、 "以前に選択した作業環境に対して新しく作成されたワークロードを検出する"そして "設定オプションで機能を設定する"。

高度な暗号化が検出されるとアラートが発せられます

このリリースでは、ファイル拡張子を大幅に変更しなくても、ワークロードで高度な暗号化が検出された場合にアラートを表示できます。この機能は、 ONTAP Autonomous Ransomware Protection (ARP) AI を使用し、ランサムウェア攻撃のリスクがあるワークロードを特定するのに役立ちます。この機能を使用して、拡張子の

変更の有無にかかわらず、影響を受けるファイルのリスト全体をダウンロードします。

詳細については、 "検出されたランサムウェアアラートに応答する" 。

2024年12月16日

Data Infrastructure Insightsストレージワークロードセキュリティを使用して異常なユーザー行動を検出する

このリリースでは、 Data Infrastructure Insights Storage Workload Security を使用して、ストレージ ワークロード内の異常なユーザー動作を検出できます。この機能は、潜在的なセキュリティ脅威を特定し、悪意のある可能性のあるユーザーをブロックしてデータを保護するのに役立ちます。

詳細については、 "検出されたランサムウェアアラートに応答する" 。

Data Infrastructure Insights Storage Workload Security を使用して異常なユーザー動作を検出する前に、BlueXP ransomware protectionの*設定* オプションを使用してオプションを構成する必要があります。

参照 "BlueXP ransomware protection設定を構成する"。

検出して保護するワークロードを選択する

このリリースでは、次のことが可能になりました。

- 各コネクタ内で、ワークロードを検出する作業環境を選択します。環境内の特定のワークロードを保護し、他のワークロードは保護しない場合は、この機能が役立つ可能性があります。
- ワークロードの検出中に、コネクタごとにワークロードの自動検出を有効にすることができます。この機能を使用すると、保護するワークロードを選択できます。
- 以前に選択した作業環境に対して新しく作成されたワークロードを検出します。

参照 "ワークロードを発見する"。

2024年11月7日

データ分類を有効にし、個人を特定できる情報 **(PII)** をスキャンします

このリリースでは、 BlueXPファミリーのコア コンポーネントであるBlueXP classificationを有効にして、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、データに個人情報やプライベートな情報が含まれているかどうかを識別するのに役立ち、セキュリティ リスクが増大する可能性があります。このプロセスはワークロードの重要性にも影響を及ぼし、適切なレベルの保護でワークロードを保護していることを確認するのに役立ちます。

BlueXP ransomware protectionにおける PII データのスキャンは、 BlueXP classificationを導入したお客様には一般にご利用いただけます。 BlueXP classificationはBlueXPプラットフォーム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展開できます。

参照 "BlueXP ransomware protection設定を構成する"。

スキャンを開始するには、[保護] ページで、[プライバシーの露出] 列の [露出を特定] をクリックします。

"BlueXP classificationで個人を特定できる機密データをスキャン" 。

Microsoft Sentinel との **SIEM** 統合

Microsoft Sentinel を使用して脅威の分析と検出を行うために、データをセキュリティおよびイベント管理システム (SIEM) に送信できるようになりました。以前は、SIEM として AWS Security Hub または Splunk Cloud を選択できました。

"BlueXP ransomware protection設定の構成について詳しくは、こちらをご覧ください。" 。

今すぐ**30**日間無料トライアル

このリリースでは、 BlueXP ransomware protectionの新規導入に 30 日間の無料トライアルが提供されます。以前は、 BlueXP ransomware protectionは90 日間の無料トライアルを提供していました。すでに 90 日間の無料トライアル中の場合は、そのオファーは 90 日間継続されます。

Podman のファイルレベルでアプリケーション 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、攻撃の影響を受けた可能性のあるファイルの一覧を表示し、復元するファイルを特定できるようになりました。以前は、組織 (以前のアカウント) 内のBlueXPコネクタが Podman を使用していた場合、この機能は無効になっていました。 Podman で有効になりました。 BlueXP ransomware protectionで復元するファイルを選択したり、アラートの影響を受けたすべてのファイルをリストした CSV ファイルをアップロードしたり、復元するファイルを手動で特定したりすることができます。

"ランサムウェア攻撃からの回復について詳しくはこちら" 。

2024年9月30日

ファイル共有ワークロードのカスタムグループ化

このリリースでは、ファイル共有をグループにまとめることができるため、データ資産をより簡単に保護できるようになりました。このサービスでは、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。以前は、各ボリュームを個別に保護する必要がありました。

"ランサムウェア対策戦略におけるファイル共有ワークロードのグループ化について詳しくは、こちらをご覧ください。" 。

2024年9月2日

Digital Advisorによるセキュリティリスク評価

BlueXP ransomware protectionは、 NetApp Digital Advisorからクラスターに関連する高レベルおよび重大なセキュリティ リスクに関する情報を収集するようになりました。リスクが見つかった場合、 BlueXP ransomware protectionはダッシュボードの 推奨アクション ペインに「クラスター <name> の既知のセキュリティ脆弱性を修正する」という推奨事項を表示します。ダッシュボードの推奨事項から、[確認して修正] をクリックすると、セキュリティ リスクを解決するためにDigital Advisorと Common Vulnerability & Exposure (CVE) の記事を確認することが提案されます。セキュリティリスクが複数ある場合は、 Digital Advisorの情報を確認してください。

参照 "Digital Advisorのドキュメント"。

Google Cloud Platform へのバックアップ

このリリースでは、バックアップ先を Google Cloud Platform バケットに設定できます。以前は、バックアップ先を追加できるのはNetApp StorageGRID、Amazon Web Services、Microsoft Azure のみでした。

"BlueXP ransomware protection設定の構成について詳しくは、こちらをご覧ください。" 。

Google Cloud Platform のサポート

このサービスでは、ストレージ保護のために、Google Cloud Platform 用のCloud Volumes ONTAP をサポートするようになりました。以前は、このサービスはオンプレミスの NAS に加えて、Amazon Web Services および Microsoft Azure 向けのCloud Volumes ONTAPのみをサポートしていました。

"BlueXP ransomware protectionとサポートされているデータソース、バックアップ先、作業環境について学びます" 。

ロールベース アクセス制御

ロールベースのアクセス制御 (RBAC) を使用して、特定のアクティビティへのアクセスを制限できるようになりました。 BlueXP ransomware protectionでは、 BlueXPの 2 つのロール (BlueXPアカウント管理者と非アカウント管理者 (閲覧者)) を使用します。

各ロールが実行できるアクションの詳細については、 "ロールベースのアクセス制御権限" 。

2024年8月5日

Splunk Cloudによる脅威検出

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) に自動的に送信できます。以前のリリースでは、SIEM として AWS Security Hub のみを選択できました。このリリースでは、SIEM として AWS Security Hub または Splunk Cloud を選択できるようになりました。

"BlueXP ransomware protection設定の構成について詳しくは、こちらをご覧ください。" 。

2024年7月1日

ライセンス持ち込み（BYOL）

このリリースでは、 NetApp の営業担当者から取得したNetAppライセンス ファイル (NLF) である BYOL ライセンスを使用できます。

"ライセンスの設定について詳しくはこちら" 。

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、攻撃の影響を受けた可能性のあるファイルの一覧を表示し、復元するファイルを特定できるようになりました。 BlueXP ransomware protectionで復元するファイルを選択したり、アラートの影響を受けたすべてのファイルをリストした CSV ファイルをアップロードしたり、復元するファイルを手動で特定したりすることができます。

このリリースでは、アカウント内のすべてのBlueXPコネクタが Podman を使用していない場合でも、単一ファイルの復元機能が有効になります。それ以外の場合、そのアカウントは無効になります。

"ランサムウェア攻撃からの回復について詳しくはこちら" 。

影響を受けるファイルのリストをダウンロードする

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、[アラート] ページにアクセスして影響を受けるファイルのリストを CSV ファイルでダウンロードし、[リカバリ] ページを使用して CSV ファイルをアップロードできるようになりました。

"アプリケーションを復元する前に影響を受けるファイルをダウンロードする方法について詳しくは、こちらをご覧ください。" 。

保護プランを削除する

このリリースでは、ランサムウェア保護戦略を削除できるようになりました。

"ワークロードの保護とランサムウェア保護戦略の管理について詳しく学ぶ" 。

2024年6月10日

プライマリストレージ上のスナップショットコピーのロック

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まで到達した場合でも、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。

"ランサムウェア対策戦略におけるワークロードの保護とバックアップロックの有効化について詳しくは、こちらをご覧ください。" 。

Microsoft Azure 向け**Cloud Volumes ONTAP**のサポート

このリリースでは、Cloud Volumes ONTAP for AWS およびオンプレミスのONTAP NAS に加えて、 Cloud Volumes ONTAP for Microsoft Azure をシステムとしてサポートします。

"Azure でのCloud Volumes ONTAPのクイック スタート"

"BlueXP ransomware protectionについて学ぶ" 。

バックアップ先として **Microsoft Azure** が追加されました

AWS およびNetApp StorageGRIDに加えて、Microsoft Azure をバックアップ先として追加できるようになりました。

"保護設定を構成する方法について詳しくは、こちらをご覧ください。" 。

2024年5月14日

ライセンスの更新

90 日間の無料トライアルにご登録いただけます。まもなく、Amazon Web Services Marketplace で従量課金制サブスクリプションを購入したり、独自のNetAppライセンスを使用できるようになります。

"ライセンスの設定について詳しくはこちら" 。

CIFSプロトコル

このサービスでは、NFS プロトコルと CIFS プロトコルの両方を使用して、AWS システム内のオンプレミスのONTAPとCloud Volumes ONTAP をサポートするようになりました。以前のリリースでは、NFS プロトコルのみがサポートされていました。

ワークロードの詳細

このリリースでは、保護ページやその他のページのワークロード情報にさらに詳しい情報が提供され、ワークロード保護の評価が改善されました。ワークロードの詳細から、現在割り当てられているポリシーを確認し、構成されているバックアップ先を確認できます。

"保護ページでワークロードの詳細を表示する方法の詳細" 。

アプリケーション整合性と**VM**整合性の保護とリカバリ

NetApp SnapCenterソフトウェアによるアプリケーション整合性のある保護と、 SnapCenter Plug-in for VMware vSphereによる VM 整合性のある保護を実行できるようになりました。これにより、静止状態と整合性のある状態が実現され、後でリカバリが必要になった場合にデータ損失の可能性を回避できます。回復が必要な場合は、アプリケーションまたは VM を以前の任意の状態に復元できます。

"ワークロードの保護について詳しく見る" 。

ランサムウェア対策戦略

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、このサービスで作成する次のポリシーを含めることができるランサムウェア保護戦略を作成できます。

- スナップショットポリシー
- バックアップ ポリシー
- 検出ポリシー

"ワークロードの保護について詳しく見る" 。

脅威検出

サードパーティのセキュリティおよびイベント管理 (SIEM) システムを使用して、脅威検出を有効にできるようになりました。ダッシュボードには、「脅威検出を有効にする」という新しい推奨事項が表示されるようになりました。これは設定ページで構成できます。

"設定オプションの構成について詳しくは" 。

誤検知アラートを無視する

[アラート] タブから、誤検知を無視したり、データをすぐに回復したりできるようになりました。

"ランサムウェアアラートへの対応について詳しくはこちら" 。

検出ステータス

新しい検出ステータスが [保護] ページに表示されます。これには、ワークロードに適用されたランサムウェア検出のステータスが表示されます。

"ワークロードの保護と保護ステータスの表示について詳しくは、こちらをご覧ください。" 。

CSVファイルをダウンロード

保護、アラート、回復のページから CSV ファイル* をダウンロードできます。

"ダッシュボードやその他のページからCSVファイルをダウンロードする方法について詳しくは、こちらをご覧ください。" 。

ドキュメントリンク

ドキュメントの表示リンクが UI に含まれるようになりました。このドキュメントにはダッシュボードの「アクション」からアクセスできます。  オプション。リリース ノートの詳細を表示するには 新機能 を選択し、 BlueXP ransomware protectionドキュメントのホーム ページを表示するには ドキュメント を選択してください。

BlueXP backup and recovery

BlueXP backup and recoveryサービスをシステムで有効にしておく必要がなくなりました。見る"前提条件" 。BlueXP ransomware protectionサービスは、設定オプションを通じてバックアップの保存先を構成するのに役立ちます。見る"設定を構成する" 。

設定オプション

BlueXP ransomware protection設定でバックアップ先を設定できるようになりました。

"設定オプションの構成について詳しくは" 。

2024年3月5日

保護ポリシー管理

定義済みのポリシーを使用するだけでなく、ポリシーを作成できるようになりました。 "ポリシー管理の詳細" 。

二次ストレージの不変性（**DataLock**）

オブジェクト ストア内のNetApp DataLock テクノロジーを使用して、セカンダリ ストレージ内のバックアップを不変にできるようになりました。 "保護ポリシーの作成について詳しくは" 。

NetApp StorageGRIDへの自動バックアップ

AWS の使用に加えて、バックアップ先としてStorageGRID を選択できるようになりました。 "バックアップ先の設定について詳しくは" 。

潜在的な攻撃を調査するための追加機能

検出された潜在的な攻撃を調査するために、より詳細なフォレンジック情報を表示できるようになりました。 "検出されたランサムウェアアラートへの対応について詳しくは、こちらをご覧ください。" 。

回復プロセス

回復プロセスが強化されました。これで、ワークロードのボリュームごとに、またはすべてのボリュームを回復できるようになりました。 "ランサムウェア攻撃からの復旧（インシデントが中和された後）について詳しくは、こちらをご覧ください。" 。

"BlueXP ransomware protectionについて学ぶ" 。

2023年10月6日

BlueXP ransomware protectionサービスは、データを保護し、潜在的な攻撃を検出し、ランサムウェア攻撃からデータを回復するための SaaS ソリューションです。

プレビュー バージョンでは、このサービスは、オンプレミスの NAS ストレージ上の Oracle、MySQL、VM データストア、ファイル共有のアプリケーション ベースのワークロードと、 BlueXP組織全体の AWS 上のCloud Volumes ONTAP (NFS プロトコルを使用) を個別に保護し、データを Amazon Web Services クラウド ストレージにバックアップします。

BlueXP ransomware protectionサービスは、 NetAppの複数のテクノロジをフル活用して、データ セキュリティ管理者またはセキュリティ運用エンジニアが次の目標を達成できるようにします。

- すべてのワークロードにおけるランサムウェア保護を一目で確認できます。
- ランサムウェア対策の推奨事項を理解する
- BlueXP ransomware protectionの推奨事項に基づいて保護体制を改善します。
- ランサムウェア保護ポリシーを割り当てて、主要なワークロードと高リスクのデータをランサムウェア攻撃から保護します。
- データの異常を探しながら、ランサムウェア攻撃に対するワークロードの健全性を監視します。
- ランサムウェア インシデントがワークロードに与える影響を迅速に評価します。
- データを復元し、保存されたデータからの再感染が発生しないようにすることで、ランサムウェア インシデントからインテリジェントに回復します。

"BlueXP ransomware protectionについて学ぶ" 。

NetApp Ransomware Resilienceの既知の制限

今回のリリースでサポートされていない、または今回のリリースでは正常に機能しないプラットフォーム、デバイス、機能が記載されています。これらの制限事項をよく確認してください。

準備訓練のリセットオプションの問題

ランサムウェア攻撃対策ドリル用にONTAP 9.11.1 ボリュームを選択すると、Ransomware Resilience によってアラートが送信されます。 「ボリュームへのクローン」オプションを使用してデータを回復し、ドリルをリセットすると、リセット操作は失敗します。

Amazon FSx for NetApp ONTAP の制限

Amazon FSx for NetApp ONTAPシステムは、Ransomware Resilience でサポートされています。このシステムには次の制限が適用されます。

- Fsx for ONTAPではバックアップ ポリシーはサポートされていません。この環境では、バックアップにAmazon FSxを使用してバックアップ操作を実行する必要があります。 Ransomware Resilience を使用してこれらのワークロードを復元できます。
- 復元操作はスナップショットからのみ実行されます。

始めましょう

NetAppのランサムウェア耐性について学ぶ

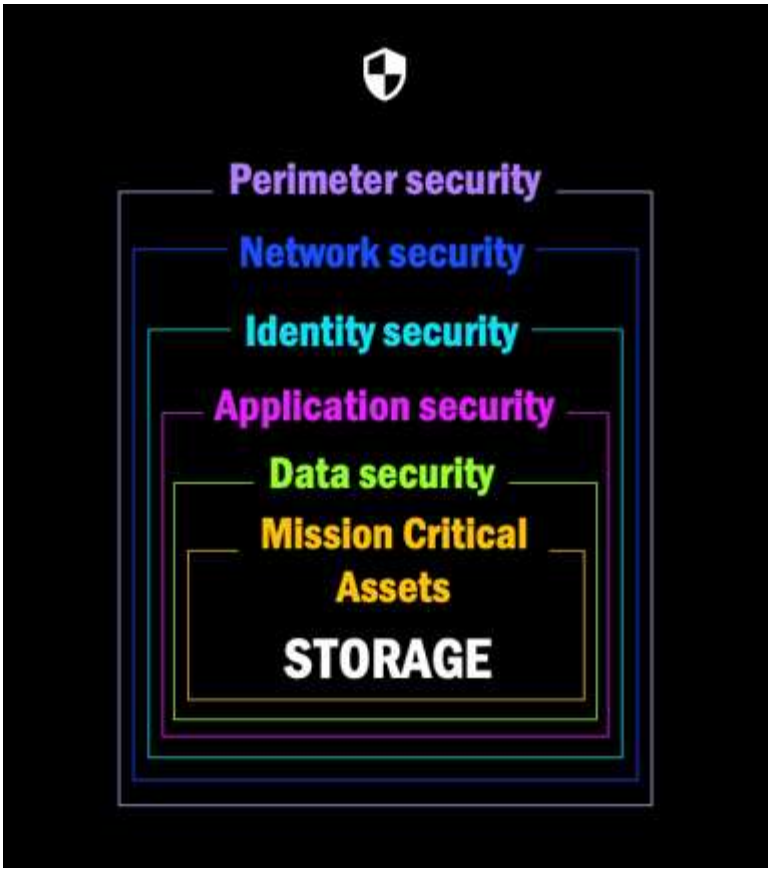
ランサムウェア攻撃によりデータへのアクセスがブロックされ、攻撃者はデータの解放や暗号化の解除と引き換えに身代金を要求する可能性があります。 IDC によれば、ランサムウェアの被害者が複数のランサムウェア攻撃を受けることは珍しくありません。この攻撃により、1 日から数週間にわたりデータへのアクセスが中断される可能性があります。

NetApp Ransomware Resilience は、ランサムウェア攻撃からデータを保護します。ランサムウェア耐性では、オンプレミスの NAS ストレージ (NFS および CIFS プロトコルを使用) と SAN ストレージ (FC、iSCSI、NVMe) 上の Oracle、MySQL、VM データストア、ファイル共有のアプリケーションベースのワークロード、および NetApp コンソール全体のCloud Volumes ONTAP for Amazon Web Services、 Cloud Volumes ONTAP for Google Cloud、 Cloud Volumes ONTAP for Microsoft Azure、 Amazon FSx for NetApp ONTAP のNetAppが利用できます。 Amazon Web Services、Google Cloud、Microsoft Azure クラウド ストレージ、NetApp StorageGRIDにデータをバックアップできます。

データ層におけるランサムウェア耐性

セキュリティ体制は通常、さまざまなサイバー脅威から保護するために複数の防御層を網羅します。

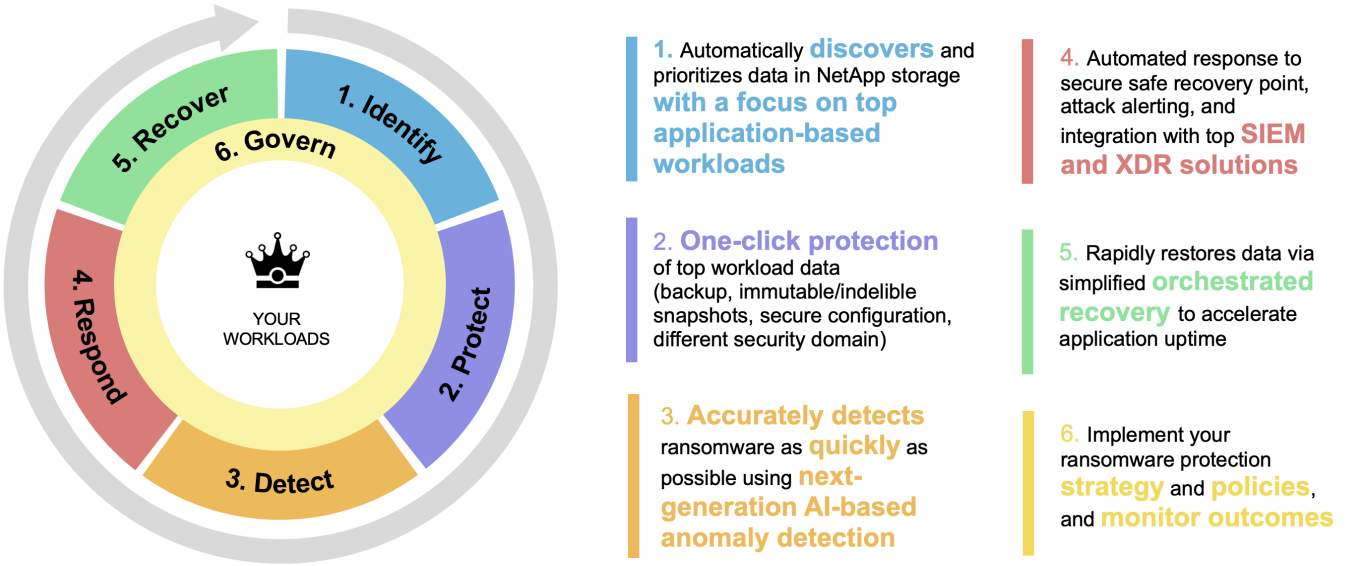
- 最外層: これは、ファイアウォール、侵入検知システム、仮想プライベート ネットワークを使用してネットワーク境界を保護する最初の防御線です。
- ネットワーク セキュリティ: このレイヤーは、ネットワークのセグメンテーション、トラフィックの監視、暗号化を基盤として構築されます。
- **ID** セキュリティ: 認証方法、アクセス制御、ID 管理を使用して、承認されたユーザーのみが機密リソースにアクセスできるようにします。
- アプリケーション セキュリティ: 安全なコーディング プラクティス、セキュリティ テスト、ランタイム アプリケーションの自己保護を使用してソフトウェア アプリケーションを保護します。
- データ セキュリティ: データ保護、バックアップ、および回復戦略によりデータを保護します。ランサムウェア耐性はこの層で動作します。



ランサムウェア耐性でできること

ランサムウェア耐性は、複数のNetAppテクノロジーをフル活用することで、ストレージ管理者、データ セキュリティ管理者、またはセキュリティ運用エンジニアが次の目標を達成できるようにします。

- NetAppコンソール、プロジェクト、コンソール エージェント全体で、 NetAppオンプレミス NAS (NFS または CIFS) および SAN (FC、iSCSI、NVMe) システム内のすべてのアプリケーションベース、ファイル共有、または VMware 管理のワークロードを 識別 します。ランサムウェア耐性は、データの優先度を分類し、ランサムウェア耐性の向上に関する推奨事項を提供します。
- データのバックアップ、スナップショット コピー、ランサムウェア保護戦略を有効にして、ワークロードを*保護*します。
- ランサムウェア攻撃の可能性がある異常を*検出*します。脚注:[攻撃が検出されない可能性もありますが、当社の調査によると、 NetApp のテクノロジにより、特定のファイル暗号化ベースのランサムウェア攻撃を高いレベルで検出できることがわかっています。]
- 不正なコピーや悪意によるコピーの削除ができないようにロックされた、改ざん防止のNetApp ONTAPスナップショットを自動的に開始することで、潜在的なランサムウェア攻撃に*対応*します。バックアップデータは変更不可能なまま、ソースと宛先の両方でランサムウェア攻撃からエンドツーエンドで保護されます。
- 複数のNetAppテクノロジーをオーケストレーションすることで、ワークロードの稼働時間を短縮し、ワークロードを 回復 します。特定のボリュームを回復することを選択できます。 Ransomware Resilience では、最適なオプションに関する推奨事項が提供されます。
- 管理: ランサムウェア保護戦略を実装し、結果を監視します。



ランサムウェア耐性を使用するメリット

ランサムウェア耐性には次のような利点があります。

- ワークロードと既存のスナップショットおよびバックアップ スケジュールを検出し、それらの相対的な重要度をランク付けします。
- ランサムウェア保護の態勢を評価し、わかりやすいダッシュボードに表示します。
- 検出と保護態勢の分析に基づいて、次のステップに関する推奨事項を提供します。
- ワンクリック アクセスで AI/ML 主導のデータ保護推奨事項を適用します。
- MySQL、Oracle、VMware データストア、ファイル共有などの主要なアプリケーションベースのワークロード内のデータを保護します。
- AI テクノロジーを使用して、プライマリ ストレージ上のデータに対するランサムウェア攻撃をリアルタイムで検出します。
- 検出された潜在的な攻撃に応じて、スナップショット コピーを作成し、異常なアクティビティに関するアラートを開始することで、自動アクションを開始します。
- RPO ポリシーを満たすようにキュレートされたリカバリを適用します。 Ransomware Resilience は、NetApp Backup and Recovery (旧称 Cloud Backup) やSnapCenterなどの複数のNetAppリカバリ サービスを使用して、ランサムウェア インシデントからのリカバリを調整します。
- ロールベースのアクセス制御 (RBAC) を使用して、機能と操作へのアクセスを管理します。

料金

NetApp は、Ransomware Resilience の試用版の使用に対して料金を請求しません。

2024 年 10 月のリリースでは、Ransomware Resilience の新規展開に 30 日間の無料トライアルが提供されます。以前、Ransomware Resilience は 90 日間の無料トライアルを提供していました。すでに 90 日間の無料トライアルに登録している場合は、そのトライアルは 90 日間有効です。

バックアップとリカバリとランサムウェア耐性の両方をお持ちの場合、両方の製品で保護されている共通データについては、ランサムウェア耐性に対してのみ課金されます。

ライセンスまたは PayGo サブスクリプションを購入した後、ランサムウェア検出ポリシー (Autonomous Ransomware Protection) が有効になっている (Ransomware Resilience によって検出または設定された) ワークロードと、少なくとも 1 つ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、Ransomware Resilience によってそのワークロードは「保護済み」に分類され、購入した容量または PayGo サブスクリプションに対してカウントされます。バックアップ ポリシーまたはスナップショット ポリシーがあっても、検出ポリシーなしでワークロードが検出された場合は、「危険」と分類され、購入した容量にはカウントされません。

保護されたワークロードは、90 日間の試用期間が終了した後、購入した容量またはサブスクリプションに対してカウントされます。ランサムウェア耐性は、効率化前の保護されたワークロードに関連付けられたデータに対して GB 単位で課金されます。

ライセンス

Ransomware Resilience では、無料トライアル、従量課金制サブスクリプション、独自のライセンスの使用など、さまざまなライセンス プランを使用できます。

Ransomware Resilience にはNetApp ONTAP One ライセンスが必要です。

Ransomware Resilience ライセンスには、追加のNetApp製品は含まれません。 Ransomware Resilience では、ライセンスがなくてもバックアップとリカバリを使用できます。

異常なユーザー行動を検出するために、Ransomware Resilience は、悪意のあるファイル アクティビティを検出するONTAP内の機械学習 (ML) モデルであるNetApp Autonomous Ransomware Protection を使用します。このモデルは、Ransomware Resilience ライセンスに含まれています。さらに、 Data Infrastructure Insights (旧称Cloud Insights) Workload Security (ライセンスが必要) を使用して、ユーザーの行動を調査し、特定のユーザーのさらなるアクティビティをブロックすることもできます。

詳細については、 "ライセンスの設定" 。

NetAppコンソール

Ransomware Resilience はNetAppコンソールからアクセスできます。

NetAppコンソールは、オンプレミスとクラウド環境全体にわたるエンタープライズ グレードのNetAppストレージとデータ サービスの集中管理を提供します。NetAppデータ サービスにアクセスして使用するには、コンソールが必要です。管理インターフェースとして、1 つのインターフェースから多数のストレージ リソースを管理できます。コンソール管理者は、企業内のすべてのシステムのストレージとサービスへのアクセスを制御できます。

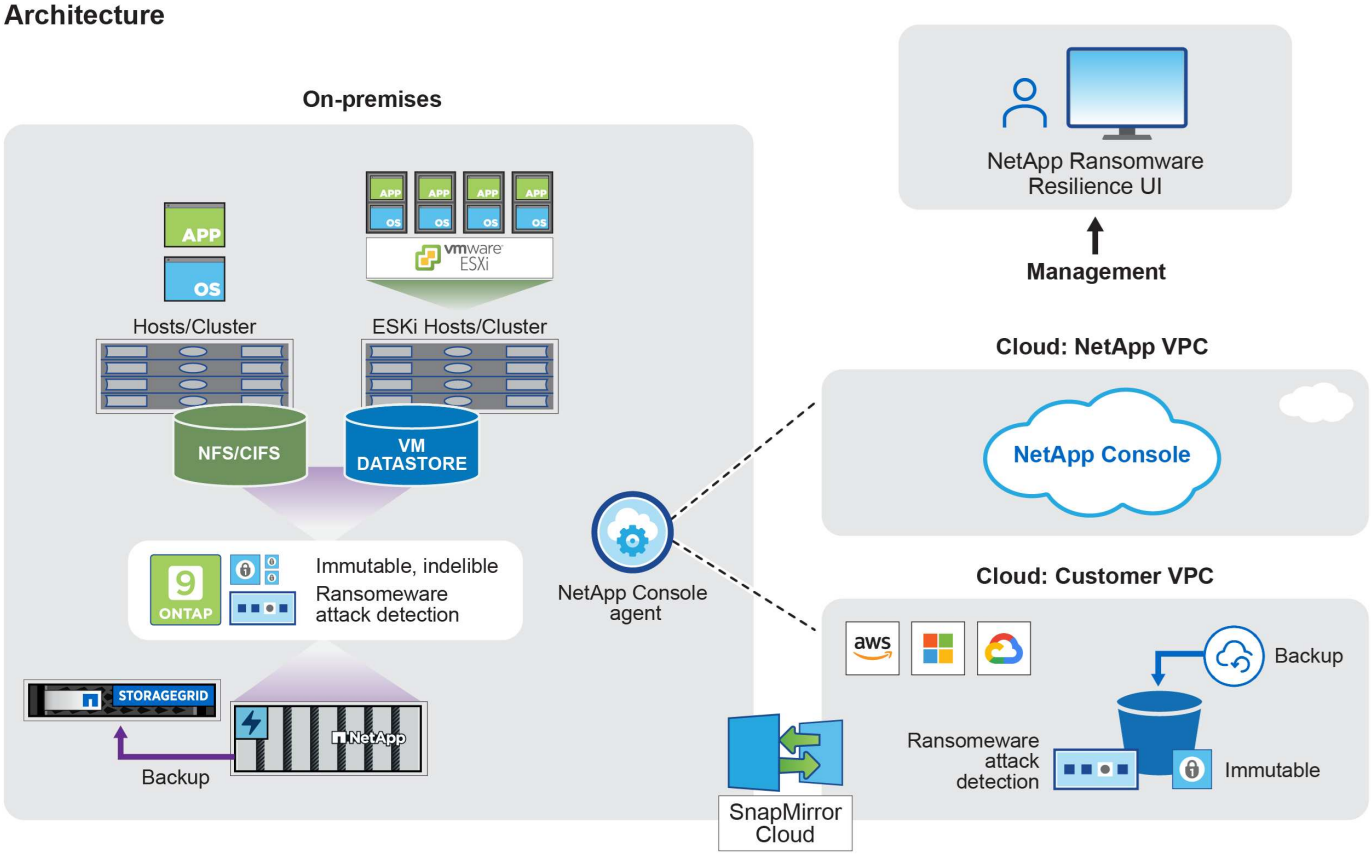
NetAppコンソールの使用を開始するためにライセンスやサブスクリプションは必要ありません。ストレージシステムまたはNetAppデータ サービスへの接続を確保するためにクラウドにコンソール エージェントを展開する必要がある場合にのみ料金が発生します。ただし、コンソールからアクセスできる一部のNetAppデータ サービスは、ライセンスまたはサブスクリプションベースです。

詳細はこちら"NetAppコンソール"。

ランサムウェア耐性の仕組み

Ransomware Resilience は、 NetApp Backup and Recovery を使用してファイル共有ワークロードのスナップショットおよびバックアップ ポリシーを検出して設定し、 SnapCenterまたはSnapCenter for VMware を使用してアプリケーションおよび VM ワークロードのスナップショットおよびバックアップ ポリシーを検出して設定します。さらに、Ransomware Resilience は、バックアップとリカバリ、およびSnapCenter / SnapCenter for VMware を使用して、ファイルとワークロードの整合性のあるリカバリを実行します。

Architecture



特徴	説明
識別する	• コンソールに接続されているすべての顧客のオンプレミス NAS (NFS および CIFS プロトコル)、SAN (FC、iSCSI、NVMe)、およびCloud Volumes ONTAPデータを検索します。 • ONTAPおよびSnapCenterサービス API から顧客データを識別し、ワークロードに関連付けます。詳細はこちら "ONTAP"そして "SnapCenterソフトウェア"。 • 各ボリュームのNetAppスナップショット コピーとバックアップ ポリシーの現在の保護レベルと、オンボックス検出機能を検出します。ランサムウェア耐性は、バックアップとリカバリ、 ONTAPサービス、および Autonomous Ransomware Protection (ONTAPのバージョンに応じて ARP または ARP/AI)、FPolicy、バックアップ ポリシー、スナップショット ポリシーなどのNetAppテクノロジーを使用して、この保護態勢をワークロードに関連付けます。詳細はこちら "自律型ランサムウェア対策"、 "NetAppバックアップとリカバリ" 、 そして "ONTAP FPolicy"。 • 自動的に検出された保護レベルに基づいて各ワークロードにビジネス優先度を割り当て、ビジネス優先度に基づいてワークロードの保護ポリシーを推奨します。ワークロードの優先順位は、ワークロードに関連付けられた各ボリュームにすでに適用されているスナップショット頻度に基づいています。
守る	• ワークロードをアクティブに監視し、識別された各ワークロードにポリシーを適用して、バックアップとリカバリ、 SnapCenter、およびONTAP API の使用を調整します。
検出する	• 潜在的に異常な暗号化とアクティビティを検出する統合機械学習 (ML) モデルを使用して、潜在的な攻撃を検出します。 • プライマリ ストレージ内の潜在的なランサムウェア攻撃を検出することから始まり、追加の自動スナップショット コピーを取得して最も近いデータ復元ポイントを作成することで異常なアクティビティに対応する、二重層検出を提供します。ランサムウェア耐性は、主要なワークロードのパフォーマンスに影響を与えることなく、より深く掘り下げて潜在的な攻撃をより正確に特定する機能を提供します。 • ONTAP、Autonomous Ransomware Protection（ ONTAPのバージョンに応じて ARP または ARP/AI）、 Data Infrastructure Insights （旧称Cloud Insights ）、Workload Security、および FPolicy テクノロジーを使用して、攻撃の疑いのある特定のファイルを特定し、関連するワークロードにマッピングします。
応答する	• ファイル アクティビティ、ユーザー アクティビティ、エントロピーなどの関連データを表示し、攻撃に関するフォレンジック レビューを完了するのに役立ちます。 • ONTAP、Autonomous Ransomware Protection (ONTAPのバージョンに応じて ARP または ARP/AI)、FPolicy などのNetApp のテクノロジと製品を使用して、クイック スナップショット コピーを開始します。
回復する	• バックアップとリカバリ、 ONTAP、自律型ランサムウェア保護 (ONTAPのバージョンに応じて ARP または ARP/AI)、および FPolicy のテクノロジとサービスを使用して、最適なスナップショットまたはバックアップを決定し、最適な RPA (実際の復旧ポイント) を推奨します。 • VM、ファイル共有、ブロック ストレージ、データベースなどのワークロードのリカバリをアプリケーションの一貫性を保ちながらオーケストレーションします。

特徴	説明
統治	• ランサムウェア対策戦略を割り当てる • 結果を監視するのに役立ちます。

サポートされているバックアップターゲット、システム、ワークロードデータソース

Ransomware Resilience は、次のバックアップ ターゲット、システム、およびデータ ソースをサポートします。

サポートされているバックアップ対象

- Amazon Web Services（AWS）S3
- Google Cloud Platform
- Microsoft Azure ブロブ
- NetAppStorageGRID

サポートされているシステム

- ONTAPバージョン 9.11.1 以降を搭載したオンプレミスのONTAP NAS (NFS および CIFS プロトコルを使用)
- ONTAPバージョン 9.17.1 以降を搭載したオンプレミスのONTAP SAN (FC、iSCSI、NVMe プロトコルを使用)
- AWS 用のCloud Volumes ONTAP 9.11.1 以上（NFS および CIFS プロトコルを使用）
- Google Cloud Platform 用のCloud Volumes ONTAP 9.11.1 以上（NFS および CIFS プロトコルを使用）
- Microsoft Azure 用のCloud Volumes ONTAP 9.12.1 以上 (NFS および CIFS プロトコルを使用)
- AWS、Google Cloud Platform、Microsoft Azure 向けのCloud Volumes ONTAP 9.17.1 以上（FC、iSCSI、NVMe プロトコルを使用）
- Amazon FSx for NetApp ONTAP は、自律型ランサムウェア保護 (ARP であり、ARP/AI ではありません) を使用します。

  ARP/AI にはONTAP 9.16 以上が必要です。

以下はサポートされていません: FlexGroupボリューム、9.11.1 より前のONTAPバージョン、マウント ポイント ボリューム、マウント パス ボリューム、オフライン ボリューム、およびデータ保護 (DP) ボリューム。

サポートされているワークロード データ ソース

ランサムウェア耐性は、プライマリ データ ボリューム上の次のアプリケーション ベースのワークロードを保護します。

- NetAppファイル共有
- ブロックストレージ

- VMwareデータストア
- データベース（MySQL および Oracle）
- 近日中にさらに追加予定

さらに、 SnapCenterまたはSnapCenter for VMware を使用している場合は、それらの製品でサポートされているすべてのワークロードも Ransomware Resilience で識別されます。ランサムウェア耐性は、ワークロードの一貫性を保ちながらこれらを保護し、回復することができます。

ランサムウェア対策に役立つ用語

ランサムウェア対策に関連するいくつかの用語を理解しておくと役立つかもしれません。

- 保護: ランサムウェア耐性における保護とは、保護ポリシーを使用して、スナップショットと不変のバックアップが別のセキュリティ ドメインに定期的に実行されるようにすることを意味します。
- ワークロード: ランサムウェア耐性のワークロードには、MySQL または Oracle データベース、VMware データストア、ファイル共有が含まれる場合があります。

NetAppランサムウェア耐性の前提条件

運用環境、ログイン、ネットワーク アクセス、Web ブラウザの準備状況を確認して、NetApp Ransomware Resilience を開始してください。

Ransomware Resilience を使用するには、前提条件を満たす必要があります。

NetAppコンソール

- リソースを検出するための組織管理者権限を持つNetAppコンソール ユーザー アカウント。
- オンプレミスのONTAPクラスターまたは AWS または Azure のCloud Volumes ONTAPに接続するアクティブなコンソールエージェントが少なくとも 1 つあるコンソール組織。
- コンソールエージェントには、 `cloudmanager-ransomware-protection`アクティブな状態のコンテナ。
- NetAppオンプレミスONTAPクラスターまたは AWS または Azure のCloud Volumes ONTAP を備えた少なくとも 1 つのコンソール システム。 Ransomware Resilience は、NAS (NFS および SMB) と SAN (iSCSI、FC、NVMe) の両方のプロトコルをサポートします。
  - ONTAP OS バージョン 9.11.1 以降のONTAPまたはCloud Volumes ONTAPクラスターがサポートされています。

    SAN ワークロードは、 ONTAP 9.17.1 以降でのみサポートされます。

  - オンプレミスのONTAPクラスターまたは AWS または Azure クラウドのCloud Volumes ONTAP がコンソールにまだオンボードされていない場合は、コンソール エージェントが必要です。

    参照 "コンソールエージェントの設定方法を学ぶ"そして "標準コンソール要件"。

単一のコンソール組織に複数のコンソール エージェントがある場合、Ransomware Resilience は、コンソール UI で現在選択されているエージェント以外のすべてのコンソール エージェントにわたってONTAPリソースをスキャンします。

ONTAP 9.11.1以降

- オンプレミスのONTAPインスタンスでONTAP One ライセンスが有効になっています。
- 使用しているONTAPのバージョンに応じて、オンプレミスのONTAPインスタンスで有効化された、Ransomware Resilience によって使用されるNetApp Autonomous Ransomware Protection のライセンス。参照 "自律型ランサムウェア対策 - 概要"。

  Ransomware Resilience の一般リリースには、プレビュー リリースとは異なり、 NetApp Autonomous Ransomware Protection テクノロジーのライセンスが含まれています。参照 "自律型ランサムウェア対策 - 概要"詳細については。

  ライセンスの詳細については、"ランサムウェア耐性について学ぶ" 。

- 保護構成（自律型ランサムウェア保護の有効化など）を適用するには、Ransomware ResilienceにONTAPクラスターに対する管理者権限が必要です。 ONTAPクラスタは、 ONTAPクラスタ管理者のユーザー認証情報のみを使用してオンボードされている必要があります。
- ONTAPクラスタが非管理者ユーザの認証情報を使用してコンソールにすでにオンボードされている場合は、このページで説明されているように、 ONTAPクラスタにログインして、非管理者ユーザの権限を必要な権限に更新する必要があります。

データのバックアップ用

- バックアップ ターゲットおよびアクセス権限セット用のNetApp StorageGRID、AWS S3、Azure Blob、または Google Cloud Platform のアカウント。

  参照 "AWS、Azure、またはS3の権限リスト"詳細については。

- システムでNetApp Backup and Recovery を有効にする必要はありません。

  Ransomware Resilience は、設定オプションを通じてバックアップ先を構成するのに役立ちます。見る" 設定を構成する" 。

ONTAPシステムで管理者以外のユーザーの権限を更新する

特定のシステムの管理者以外のユーザー権限を更新する必要がある場合は、次の手順を実行します。

1. コンソールにログインし、 ONTAPユーザー権限の更新が必要なシステムを探します。
2. 詳細を表示するにはシステムを選択してください。
3. ユーザー名を表示するには、[追加情報を表示] を選択します。
4. admin ユーザーを使用してONTAPクラスタ CLI にログインします。
5. そのユーザーの既存のロールを表示します。入力：

```
security login show -user-or-group-name <username>
```

6. ユーザーの役割を変更します。入力：

```
security login modify -user-or-group-name <username> -application
console|http|ontapi|ssh|telnet -authentication-method password -role
admin
```

7. 使用するには、ランサムウェア耐性 UI に戻ります。

NetAppランサムウェア耐性のクイックスタート

NetApp Ransomware Resilience を開始するために必要な手順の概要を以下に示します。各ステップ内のリンクをクリックすると、詳細情報を提供するページに移動します。

1 前提条件を確認する

"システムがこれらの要件を満たしていることを確認してください"。

2 ランサムウェア耐性を設定する

- "NetApp StorageGRID、Amazon Web Services、Google Cloud Platform、または Microsoft Azure をバックアップ先として準備します。"。
- "コンソールエージェントを構成する"。
- "ライセンスの設定"。
- "コンソールでワークロードを検出する"。
- "バックアップ先を設定する"。
- "オプションで脅威検出を有効にする"。
- "オプションとして、ランサムウェア攻撃準備訓練を実施する"。

3 次は何?

ランサムウェア耐性を設定したら、次に行うことは次のとおりです。

- "ダッシュボードでワークロード保護の健全性を表示する"。
- "ワークロードを保護する"。
- "潜在的なランサムウェア攻撃の検出に対応する"。
- "攻撃からの回復（インシデントが中和された後）"。

NetAppランサムウェア耐性を設定する

NetApp Ransomware Resilience を簡単に導入できます。始める前に、"前提条件"環境の準備ができていることを確認します。

バックアップ先を準備する

次のいずれかのバックアップ先を準備します。

- NetAppStorageGRID
- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure

バックアップ先自体でオプションを構成した後、後で Ransomware Resilience でバックアップ先として構成します。ランサムウェア耐性におけるバックアップ先の設定方法の詳細については、以下を参照してください。"バックアップ先を設定する" 。

StorageGRIDをバックアップ先として準備する

StorageGRIDをバックアップ先として使用する場合は、 "StorageGRIDドキュメント" StorageGRIDの詳細については、こちらをご覧ください。

AWSをバックアップ先として準備する

- AWS にアカウントを設定します。
- 設定 "AWS 権限"AWS で。

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、以下を参照してください。 "Amazon S3バケットを管理する" 。

Azure をバックアップ先として準備する

- Azure でアカウントを設定します。
- 設定 "Azure のアクセス許可"Azure で。

コンソールでAzureストレージ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 ストレージ アカウントを管理する" 。

NetAppコンソールをセットアップする

次のステップは、コンソールとランサムウェア耐性を設定することです。

レビュー "標準モードのコンソール要件"。

コンソールエージェントを作成する

このサービスを試用または使用するには、 NetApp の営業担当者にお問い合わせください。その後、コンソー

ル エージェントを使用すると、ランサムウェア耐性のための適切な機能が含まれるようになります。

ランサムウェア耐性を使用してコンソールエージェントを作成するには、コンソールエージェントを作成する権限を持つコンソール組織管理者に連絡し、説明されているドキュメントを参照してください。 "コンソールエージェントを作成する方法" 。

> コンソール エージェントが複数ある場合、Ransomware Resilience は、コンソールに現在表示されているエージェント以外のすべてのコンソール エージェントにわたってデータをスキャンします。このサービスは、この組織に関連付けられているすべてのプロジェクトとすべてのコンソール エージェントを検出します。

NetAppランサムウェア耐性にアクセス

NetAppコンソールからNetApp Ransomware Resilience にログインします。

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。 "すべてのサービスに対するBlueXPのアクセスロールについて学ぶ" 。

手順

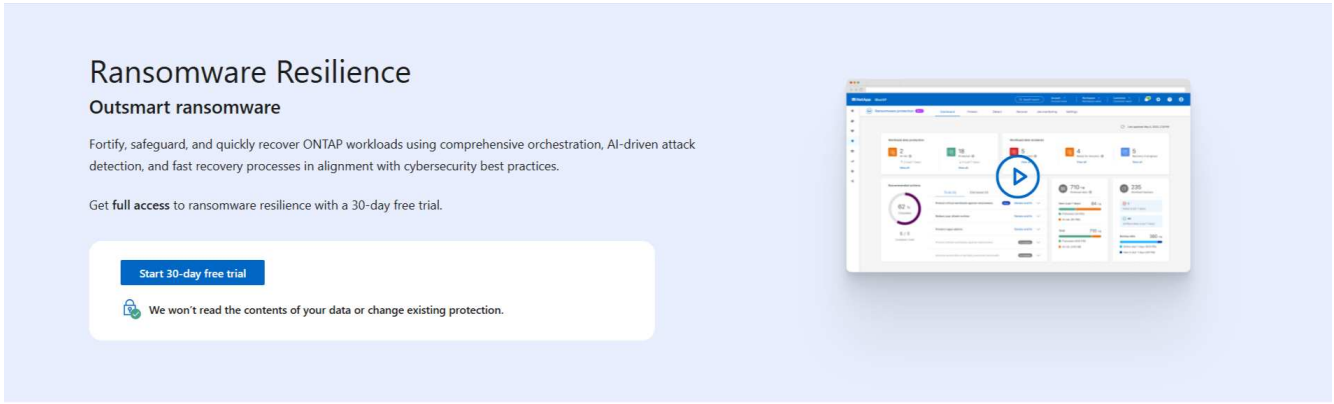
1. ウェブブラウザを開いて"コンソール"。

   コンソールのログイン ページが表示されます。

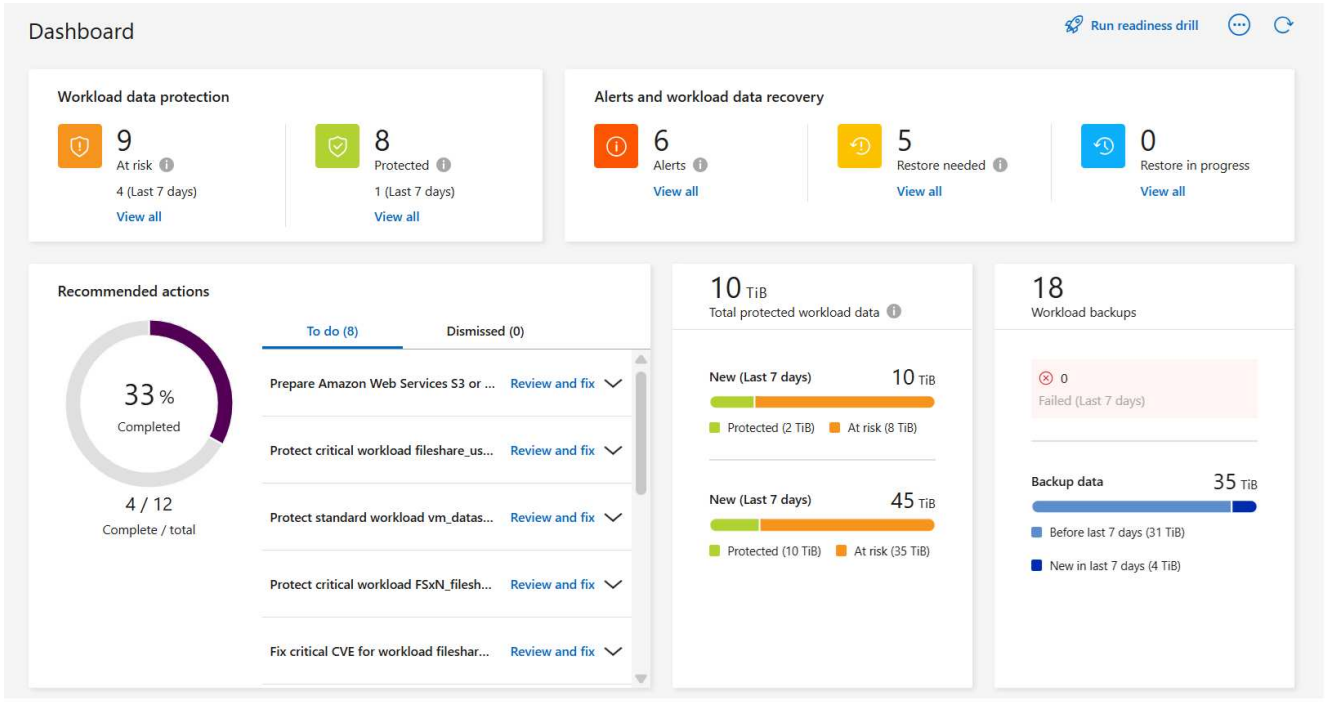
2. コンソールにログインします。
3. コンソールの左側のナビゲーションから、保護 > *ランサムウェア耐性*を選択します。

   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のライセンスを設定する

NetApp Ransomware Resilience では、さまざまなライセンス プランを使用できます。

このタスクを実行するには、組織管理者、フォルダー管理者、またはプロジェクト管理者のロールが必要です。 "コンソールアクセスロールについて学ぶ" 。

ライセンスの種類 次のライセンスの種類を使用できます。

- 30 日間の無料トライアルにサインアップしてください。
- Amazon Web Services (AWS) Marketplace、Google Cloud Marketplace、または Azure Marketplace で従量課金制 (PAYGO) サブスクリプションを購入します。
- BYOL (Bring Your Own License) は、 NetApp の営業担当者から取得したNetAppライセンス ファイル (NLF) です。ライセンス シリアル番号を使用して、コンソールで BYOL をアクティブ化できます。

BYOL を設定するか、PAYGO サブスクリプションを購入すると、コンソールの [ライセンスとサブスクリプション] セクションでライセンスを確認できます。

無料トライアルが終了した後、またはライセンスやサブスクリプションの有効期限が切れた後でも、Ransomware Resilience で次の操作を実行できます。

- ワークロードとワークロードの健全性を表示します。
- ポリシーなどのリソースを削除します。
- 試用期間中またはライセンスに基づいて作成されたすべてのスケジュールされた操作を実行します。

その他のライセンス

Ransomware Resilience ライセンスには、追加のNetApp製品は含まれません。 Ransomware Resilience では、ライセンスがなくてもNetApp Backup and Recovery を使用できます。

バックアップとリカバリとランサムウェア耐性の両方をお持ちの場合、両方の製品で保護されている共通データについては、ランサムウェア耐性に対してのみ課金されます。

Data Infrastructure Insights Workload Security を使用すると、異常なユーザー動作を表示できます。これには、Data Infrastructure Insights Workload Security のライセンスが必要であり、Ransomware Resilience でそれを有効にする必要があります。データインフラストラクチャインサイトワークロードセキュリティの概要については、 "ワークロードセキュリティについて"

Data Infrastructure Insights Workload Security のライセンスを所有しておらず、Ransomware Resilience で有効にしていない場合、異常なユーザー動作の情報は表示されません。

30日間の無料トライアルでお試しください

30 日間の無料トライアルを使用して、Ransomware Resilience を試すことができます。無料トライアルを開始するには、コンソール組織管理者である必要があります。

2024 年 10 月のリリースでは、Ransomware Resilience の新規展開に 30 日間の無料トライアルが提供されます。以前、Ransomware Resilience は 90 日間の無料トライアルを提供していました。すでに 90 日間の無料トライアル中の場合は、そのオファーは 90 日間継続されます。

トライアル期間中は容量制限は適用されません。

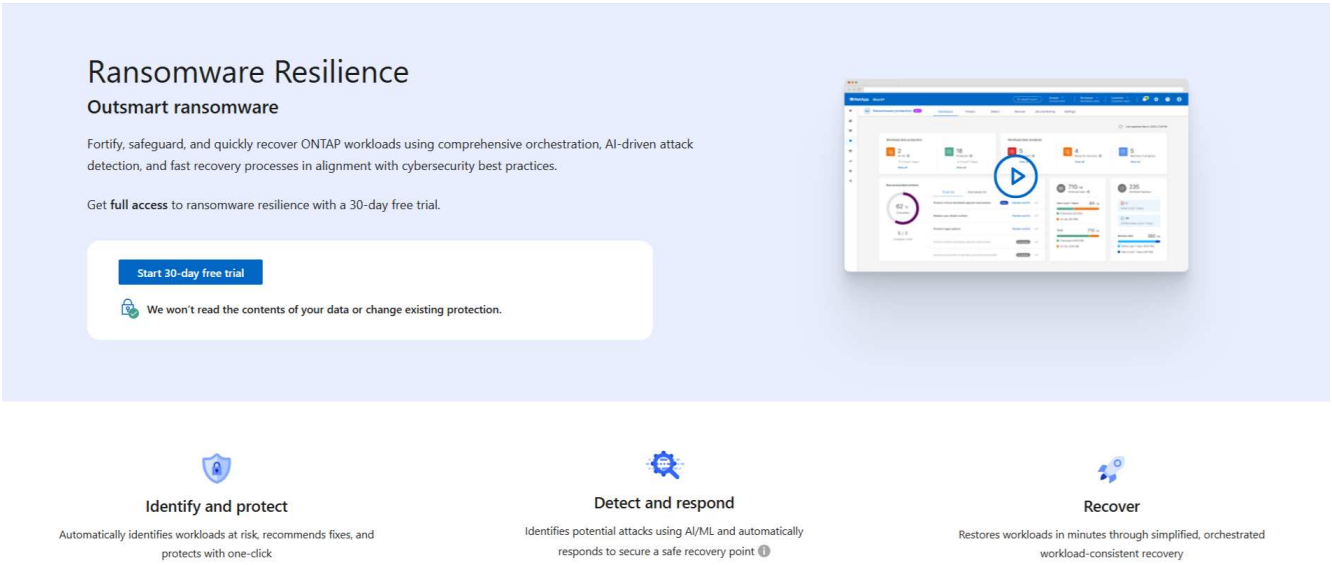
いつでもライセンスを取得したりサブスクライブしたりすることができ、30 日間の試用期間が終了するまで料金は発生しません。 30 日間の試用期間後に継続するには、BYOL ライセンスまたは PAYGO サブスクリプションを購入する必要があります。

試用期間中は、すべての機能をご利用になれます。

手順

1. アクセス "コンソール"。
2. コンソールにログインします。
3. NetAppコンソールから、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。



4. 他のサービス用のコネクタをまだ追加していない場合は、追加します。

   コンソールエージェントを追加するには、 "コンソールエージェントについて学ぶ" 。

5. コンソール エージェントを設定すると、ランサムウェア耐性ランディング ページで、コンソール エージェントを追加するためのボタンがワークロードを検出するためのボタンに変わります。 *ワークロードの検出から開始*を選択します。
6. 無料トライアルの情報を確認するには、右上のドロップダウン オプションを選択します。

試用期間が終了したら、サブスクリプションまたはライセンスを取得してください

無料トライアルが終了したら、いずれかのマーケットプレイスを通じてサブスクライブするか、 NetAppからライセンスを購入することができます。

すでに PAYGO サブスクリプションをお持ちの場合は、無料トライアル終了後にライセンスは自動的にサブスクリプションに切り替わります。

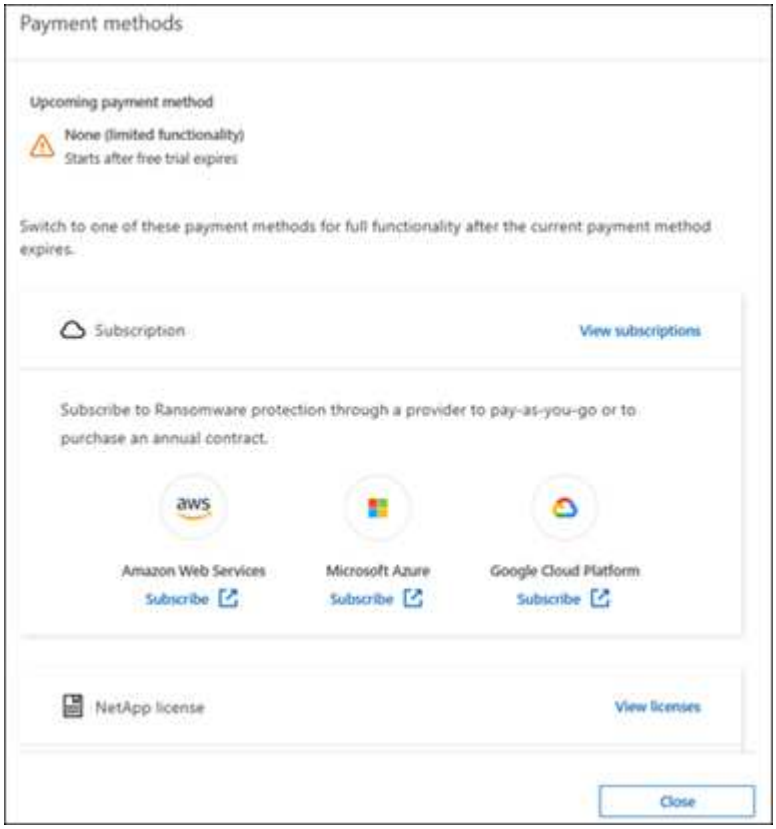
AWS Marketplace からサブスクライブする Microsoft Azure Marketplace を通じてサブスクライブする Google Cloud Platform Marketplace から登録する ライセンス持ち込み（BYOL）

AWS Marketplace からサブスクライブする

この手順では、AWS Marketplace で直接サブスクライブする方法の概要を説明します。

手順

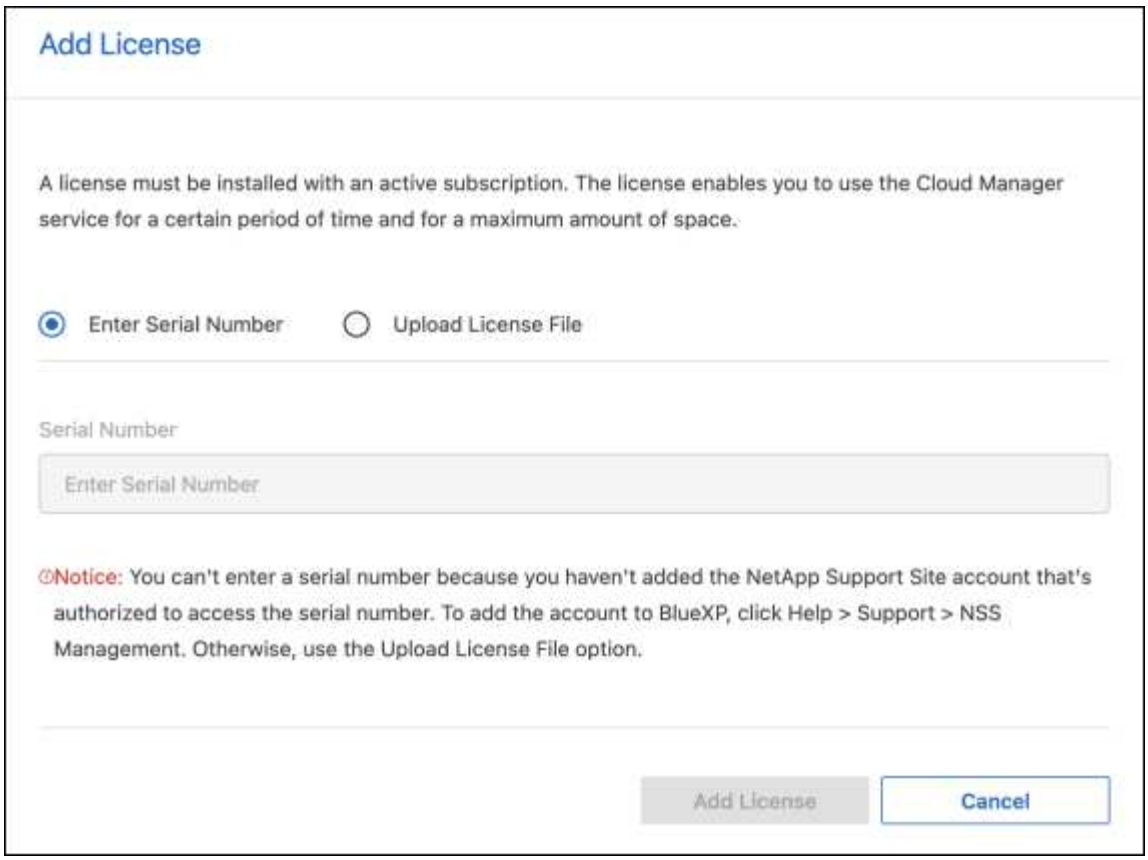
1. ランサムウェア耐性で、次のいずれかを実行します。
   - 無料トライアルの有効期限が切れるというメッセージが表示された場合は、「支払い方法の表示」を選択してください。
   - トライアルをまだ開始していない場合は、右上の*無料トライアル*通知を選択し、*お支払い方法を表示*を選択してください。



2. お支払い方法ページで、**Amazon Web Services** の サブスクライブ を選択します。
3. AWS Marketplace で、[購入オプションを表示] を選択します。
4. AWS Marketplace を使用して、* NetApp Intelligent Services* と **Ransomware Resilience** をサブスクライブします。
5. Ransomware Resilience に戻ると、登録したことを示すメッセージが表示されます。

> Ransomware Resilience のシリアル番号が記載され、Ransomware Resilience が AWS Marketplace でサブスクライブされていることを示すメールが送信されます。

6. ランサムウェア耐性の支払い方法ページに戻ります。
7. *ライセンスの追加*を選択して、コンソールにライセンスを追加します。



8. [ライセンスの追加] ページで、[シリアル番号を入力] を選択し、送信された電子メールに記載されているシリアル番号を入力して、[ライセンスの追加] を選択します。
9. ライセンスの詳細を表示するには、コンソールの左側のナビゲーションから、管理 > *ライセンスとサブスクリプション*を選択します。
   - サブスクリプション情報を表示するには、[サブスクリプション] を選択します。
   - BYOL ライセンスを表示するには、データ サービス ライセンス を選択します。

10. ランサムウェア耐性に戻ります。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。

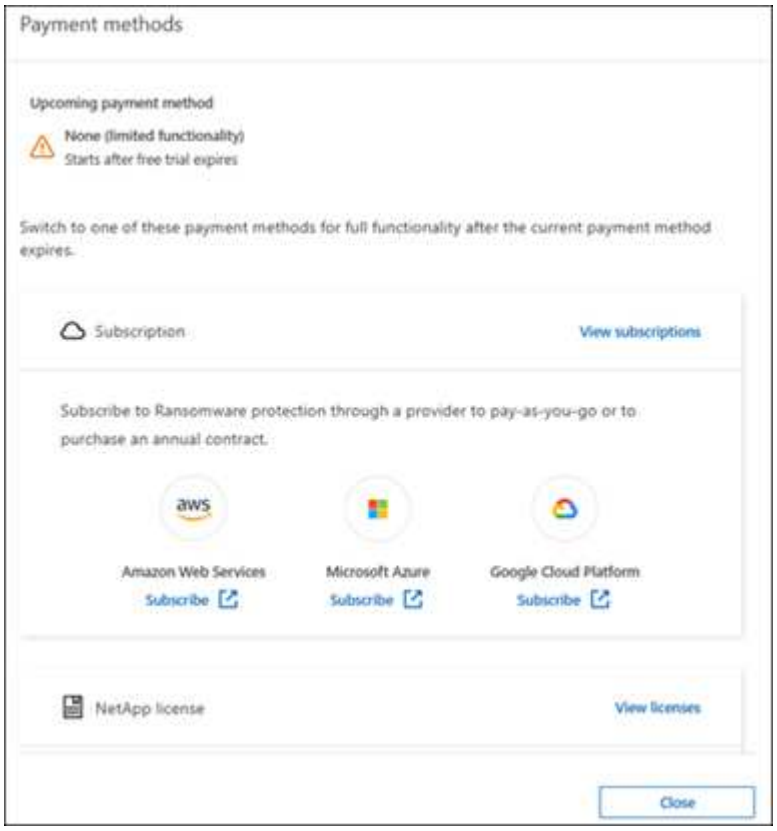
ライセンスが追加されたことを示すメッセージが表示されます。

Microsoft Azure Marketplace を通じてサブスクライブする

この手順では、Azure Marketplace で直接サブスクライブする方法の概要を説明します。

手順

1. ランサムウェア耐性で、次のいずれかを実行します。
   - 無料トライアルの有効期限が切れるというメッセージが表示された場合は、「支払い方法の表示」を選択してください。
   - トライアルをまだ開始していない場合は、右上の*無料トライアル*通知を選択し、*お支払い方法を表示*を選択してください。

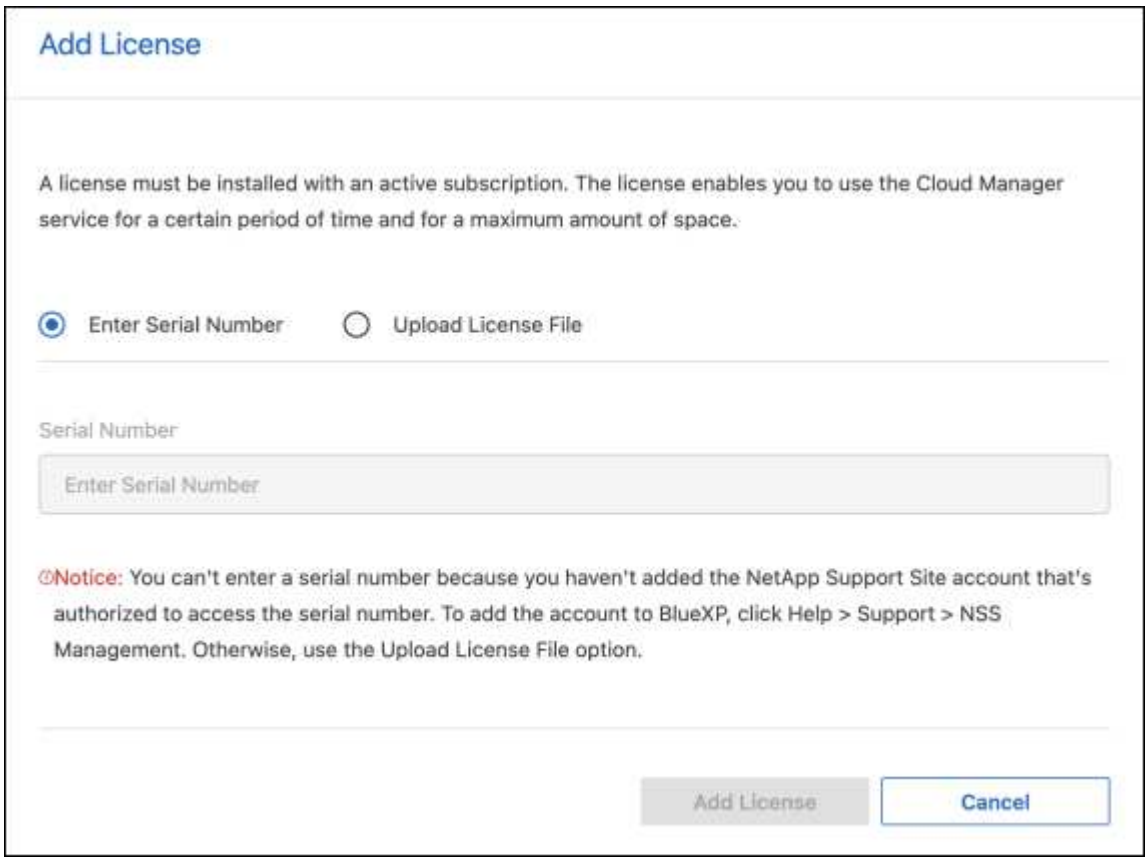


2. [支払い方法] ページで、**Microsoft Azure Marketplace** の サブスクライブ を選択します。
3. Azure Marketplace で、[購入オプションの表示] を選択します。
4. Azure Marketplace を使用して、* NetApp Intelligent Services* と **Ransomware Resilience** をサブスクライブします。
5. Ransomware Resilience に戻ると、登録したことを示すメッセージが表示されます。

> Ransomware Resilience のシリアル番号が記載され、Ransomware Resilience が Azure Marketplace でサブスクライブされていることを示す電子メールが送信されます。

6. ランサムウェア耐性支払い方法ページに戻ります。

7. ライセンスを追加するには、「ライセンスの追加」を選択します。



8. 「ライセンスの追加」ページで、「シリアル番号を入力」を選択し、送信された電子メールに記載されているシリアル番号を入力します。 *ライセンスの追加*を選択します。
9. ライセンスとサブスクリプションでライセンスの詳細を表示するには、コンソールの左側のナビゲーションから、ガバナンス > ライセンスとサブスクリプション を選択します。
   - サブスクリプション情報を表示するには、[サブスクリプション] を選択します。
   - BYOL ライセンスを表示するには、データ サービス ライセンス を選択します。

10. ランサムウェア耐性に戻ります。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。

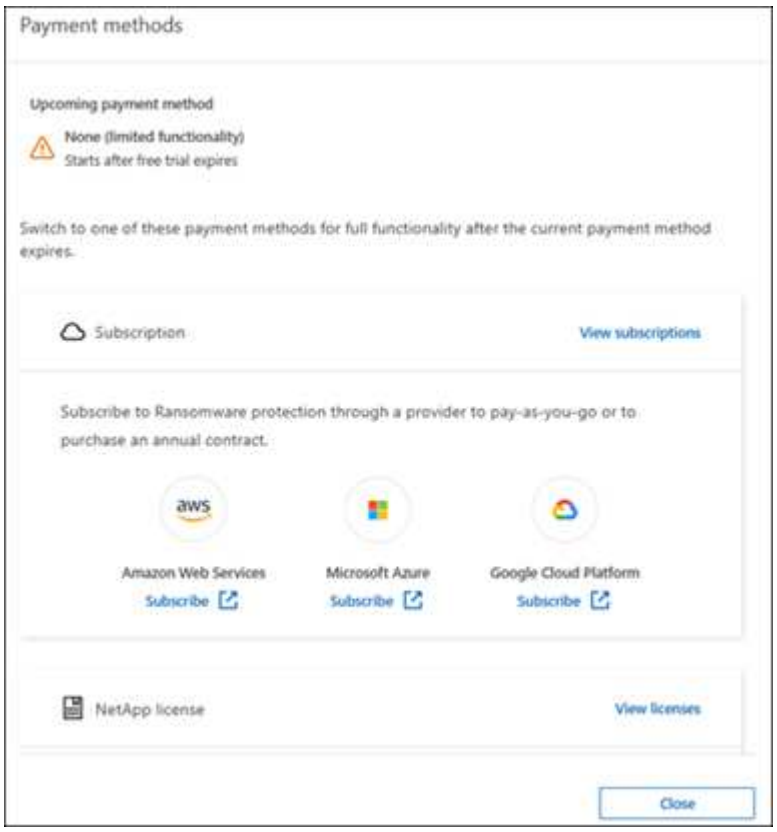
    ライセンスが追加されたことを示すメッセージが表示されます。

Google Cloud Platform Marketplace から登録する

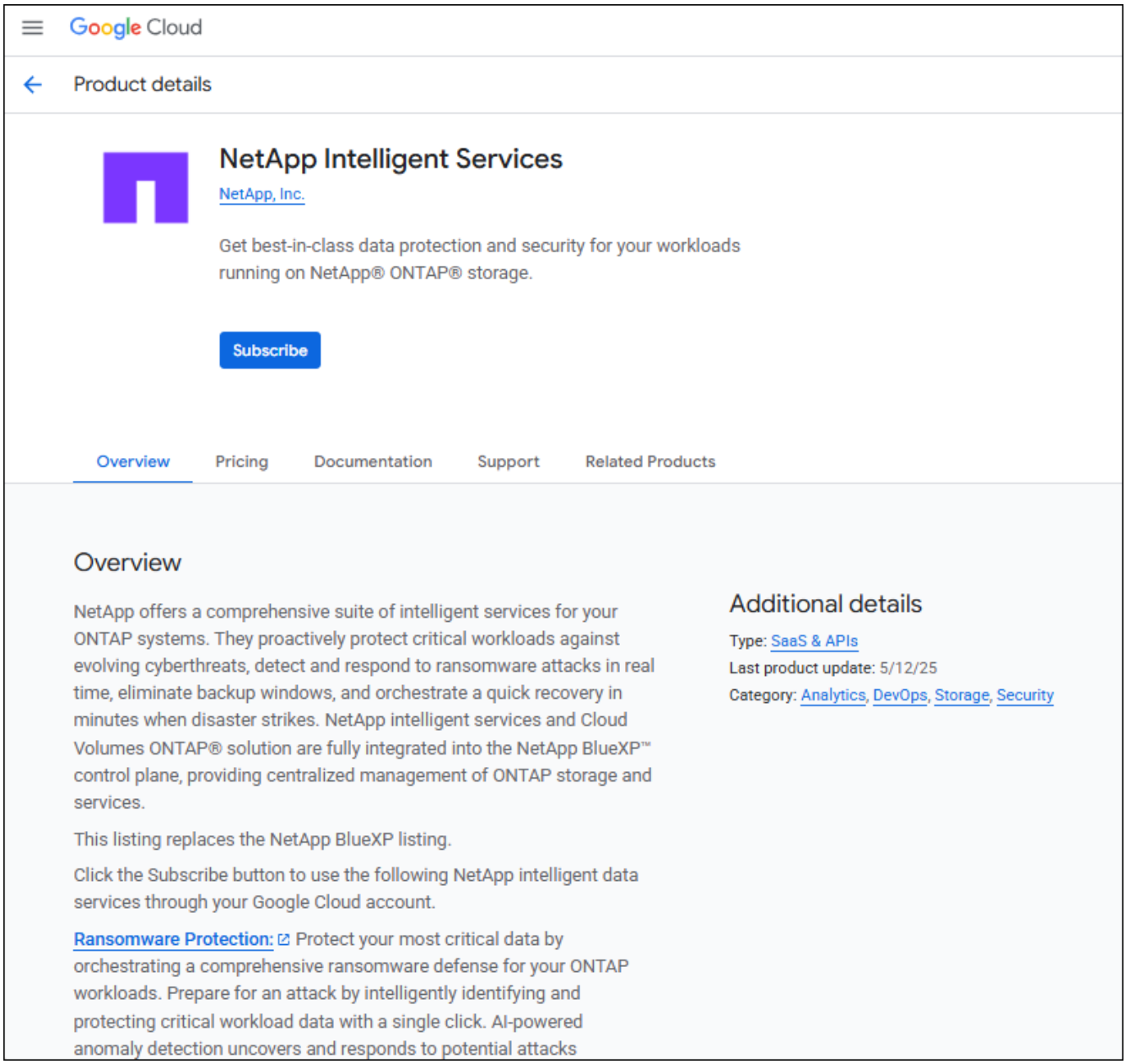
この手順では、Google Cloud Platform Marketplace で直接サブスクライブする方法の概要を説明します。

手順

1. ランサムウェア耐性で、次のいずれかを実行します。
    - 無料トライアルの有効期限が切れるというメッセージが表示された場合は、「支払い方法の表示」を選択してください。
    - トライアルをまだ開始していない場合は、右上の*無料トライアル*通知を選択し、*お支払い方法を表示*を選択してください。



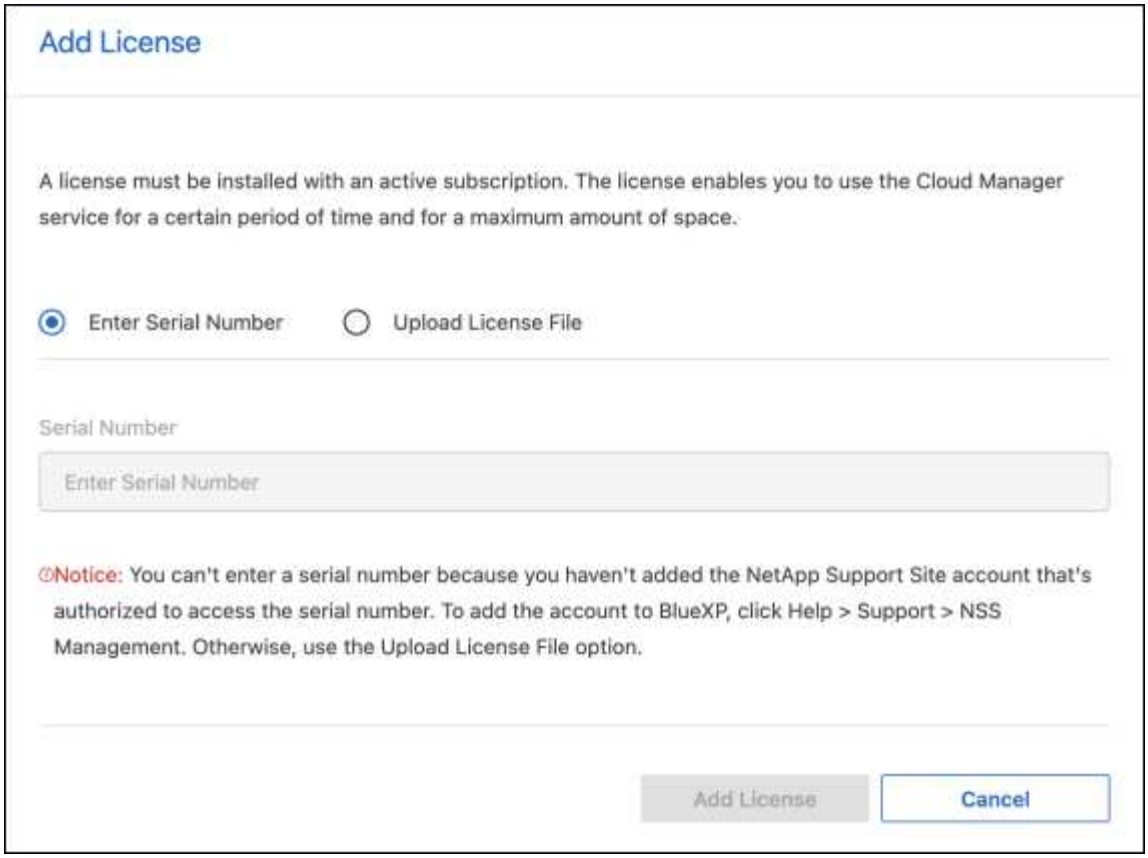
2. [お支払い方法] ページで、Google Cloud Platform Marketplace の [サブスクライブ] を選択します。
3. Google Cloud Platform Marketplace で、[**Subscribe**] を選択します。
4. Google Cloud Platform Marketplace を使用して、* NetApp Intelligent Services* と **Ransomware Resilience** をサブスクライブしま
す。



5. Ransomware Resilience に戻ると、登録したことを示すメッセージが表示されます。

> Ransomware Resilience のシリアル番号が記載され、Ransomware Resilience が Google Cloud Platform Marketplace に登録されていることを通知するメールが送信されます。

6. ランサムウェア耐性支払い方法ページに戻ります。
7. コンソールにライセンスを追加するには、[ライセンスの追加] を選択します。



8. ライセンスの追加ページで、*シリアル番号を入力*を選択します。送信されたメールに記載されているシリアル番号を入力してください。 *ライセンスの追加*を選択します。
9. ライセンスの詳細を表示するには、コンソールの左側のナビゲーションから、ガバナンス > *ライセンスとサブスクリプション*を選択します。
   - サブスクリプション情報を表示するには、[サブスクリプション] を選択します。
   - BYOL ライセンスを表示するには、データ サービス ライセンス を選択します。

10. ランサムウェア耐性に戻ります。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。

ライセンスが追加されたことを示すメッセージが表示されます。

ライセンス持ち込み（BYOL）

独自のライセンスを持ち込む (BYOL) 場合は、ライセンスを購入し、 NetAppライセンス ファイル (NLF) を取得して、コンソールにライセンスを追加する必要があります。

コンソールにライセンスファイルを追加する

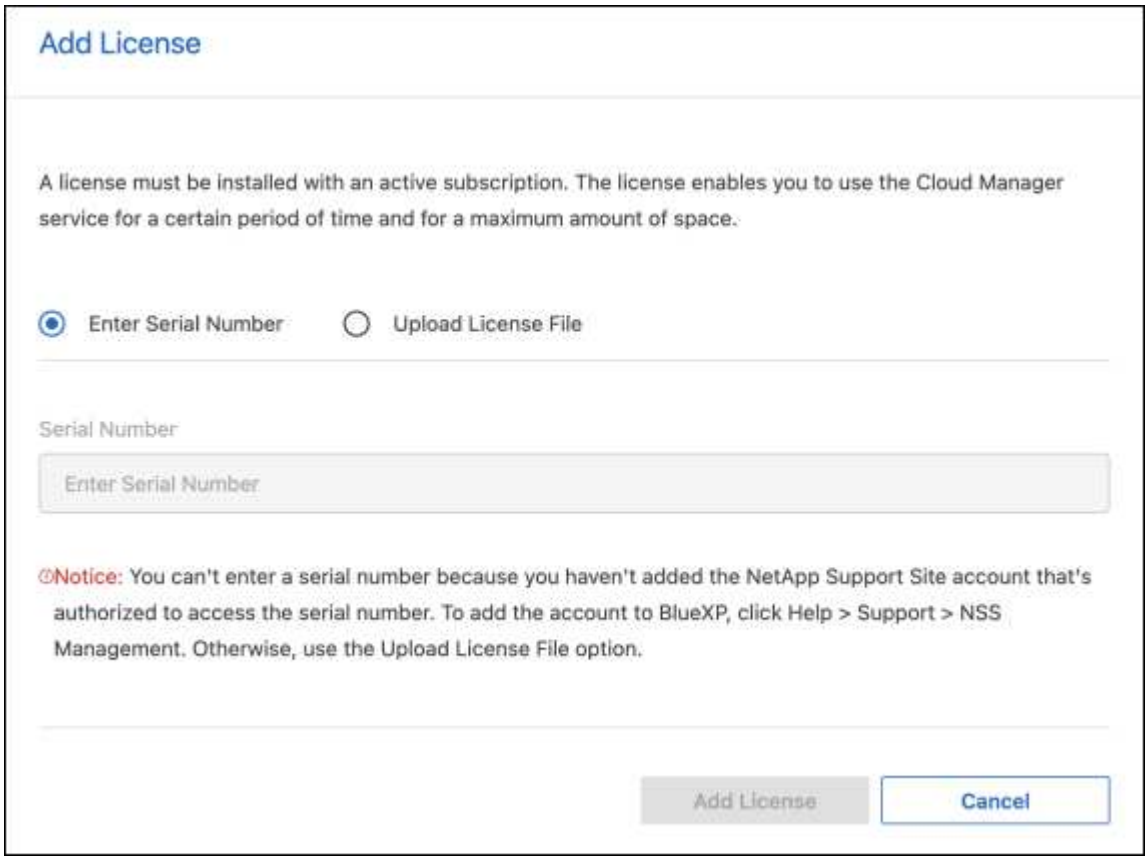
NetApp の営業担当者から Ransomware Resilience ライセンスを購入したら、Ransomware Resilience のシリアル番号とNetAppサポート サイト (NSS) のアカウント情報を入力してライセンスをアクティブ化します。

開始する前に

Ransomware Resilience のシリアル番号が必要です。この番号は販売注文書から探すか、アカウント チームに問い合わせて確認してください。

手順

1. ライセンスを取得したら、Ransomware Resilience に戻ります。右上にある*支払い方法の表示*オプションを選択します。または、無料トライアルの有効期限が切れるというメッセージで、[サブスクライブまたはライセンスを購入] を選択します。
2. ライセンスの追加 を選択して、コンソールのライセンスとサブスクリプション ページに移動します。
3. データ サービス ライセンス タブから、ライセンスの追加 を選択します。



4. 「ライセンスの追加」ページで、シリアル番号とNetAppサポート サイトのアカウント情報を入力します。

- コンソール ライセンスのシリアル番号があり、NSS アカウントがわかっている場合は、[シリアル番号を入力] オプションを選択し、その情報を入力します。

  NetAppサポートサイトのアカウントがドロップダウンリストから選択できない場合は、 "NSSアカウントをコンソールに追加する" 。

- zvondolr ライセンス ファイル (ダーク サイトにインストールする場合に必要) がある場合は、[ライセンス ファイルのアップロード] オプションを選択し、プロンプトに従ってファイルを添付します。

5. *ライセンスの追加*を選択します。

結果

「ライセンスとサブスクリプション」ページには、Ransomware Resilience にライセンスがあることが表示されます。

コンソールのライセンスが期限切れになったら更新してください

ライセンスの有効期限が近づいている場合、またはライセンス容量が制限に達した場合は、Ransomware Resilience UI で通知されます。期限が切れる前に Ransomware Resilience ライセンスを更新すれば、スキャンしたデータへのアクセスが中断されることはありません。

このメッセージはライセンスとサブスクリプションにも表示されます。 "通知設定" 。

手順

1. ライセンスの更新をリクエストするには、サポートに電子メールを送信できます。

   ライセンスの料金を支払い、ライセンスがNetAppサポート サイトに登録されると、コンソールによってライセンスが自動的に更新されます。データ サービス ライセンス ページには 5 ～ 10 分以内に変更が反映されます。

2. コンソールがライセンスを自動的に更新できない場合は、ライセンス ファイルを手動でアップロードする必要があります。
   a. ライセンス ファイルは、 NetAppサポート サイトから入手できます。
   b. コンソールで、管理 > ライセンスとサブスクリプション を選択します。
   c. データ サービス ライセンス タブを選択し、更新するシリアル番号の アクション... アイコンを選択して、ライセンスの更新 を選択します。

PAYGOサブスクリプションを終了する

PAYGO サブスクリプションを終了したい場合は、いつでも終了できます。

手順

1. 「Ransomware Resilience」の右上にあるライセンス オプションを選択します。
2. *支払い方法の表示*を選択します。
3. ドロップダウンの詳細で、[現在の支払い方法の有効期限が切れた後に使用する] ボックスのチェックを外します。
4. *保存*を選択します。

NetApp Ransomware Resilience のワークロードを発見

NetApp Ransomware Resilience を使用する前に、まずデータを検出する必要があります。検出中に、Ransomware Resilience は組織内のすべてのコンソール エージェントとプロジェクトのシステム内のすべてのボリュームとファイルを分析します。

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。"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" 。

*ランサムウェア耐性は何を検出しますか?*ランサムウェア耐性は、MySQL アプリケーション、Oracle アプリケーション、VMware データストア、ファイル共有、ブロック ストレージを評価します。

Ransomware Resilience では、 FlexGroupを使用するボリュームを持つワークロードは検出されません。

Ransomware Resilience は、サポートされているシステム構成とサポートされていないシステム構成の両方を検出し、ダッシュボードに表示します。

Ransomware Resilience は、現在のバックアップ保護、スナップショット コピー、およびNetApp Autonomous Ransomware Protection オプションをチェックします。次に、ランサムウェア保護を強化する方法を推奨します。

*ワークロードをどのように検出できますか?*次の処理を実行できます。

- 各コンソール エージェント内で、ワークロードを検出するシステムを選択します。環境内の特定のワークロードを保護し、他のワークロードは保護しない場合は、この機能が役立つ可能性があります。
- 以前選択したシステムに対して新しく作成されたワークロードを検出します。
- 新しいシステムを発見してください。

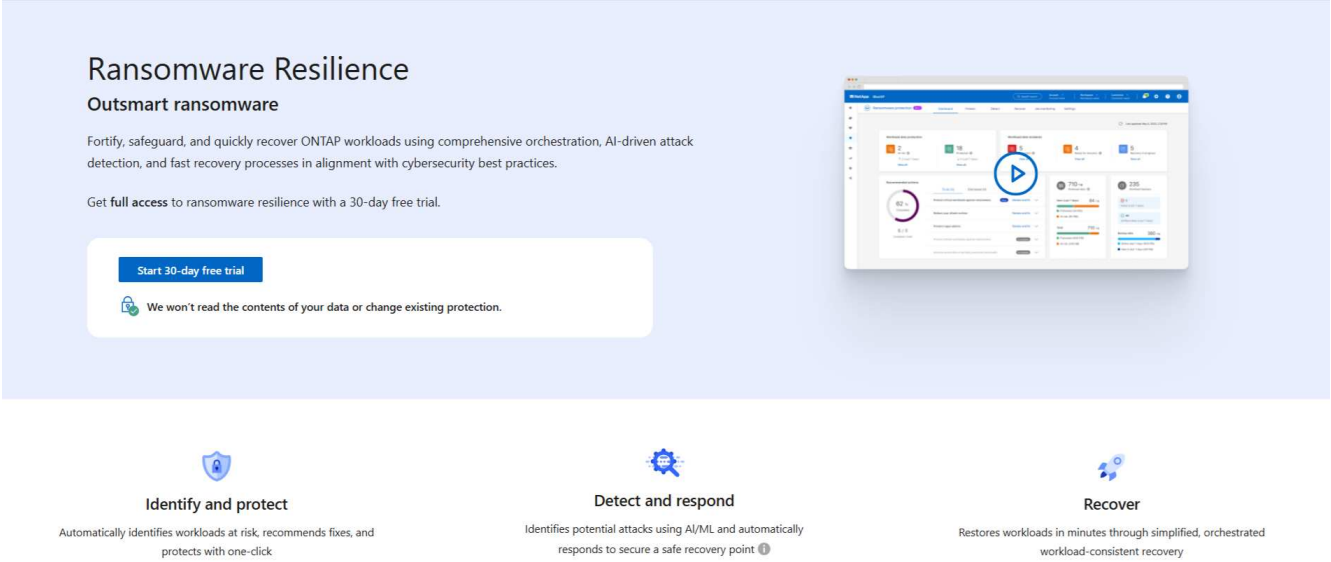
検出して保護するワークロードを選択する

各コンソール エージェント内で、ワークロードを検出するシステムを選択します。

手順

1. NetAppコンソールから、保護 > ランサムウェア保護 を選択します。

   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。



無料トライアルを開始した場合、[**30** 日間の無料トライアルを開始] ボタンのラベルが [ワークロードの検出から開始] に変わります。

2. 最初のランディング ページで、[ワークロードの検出から開始する] を選択します。

   Ransomware Resilience は、サポートされているシステムとサポートされていないシステムの両方を検出します。このプロセスには数分かかる場合があります。

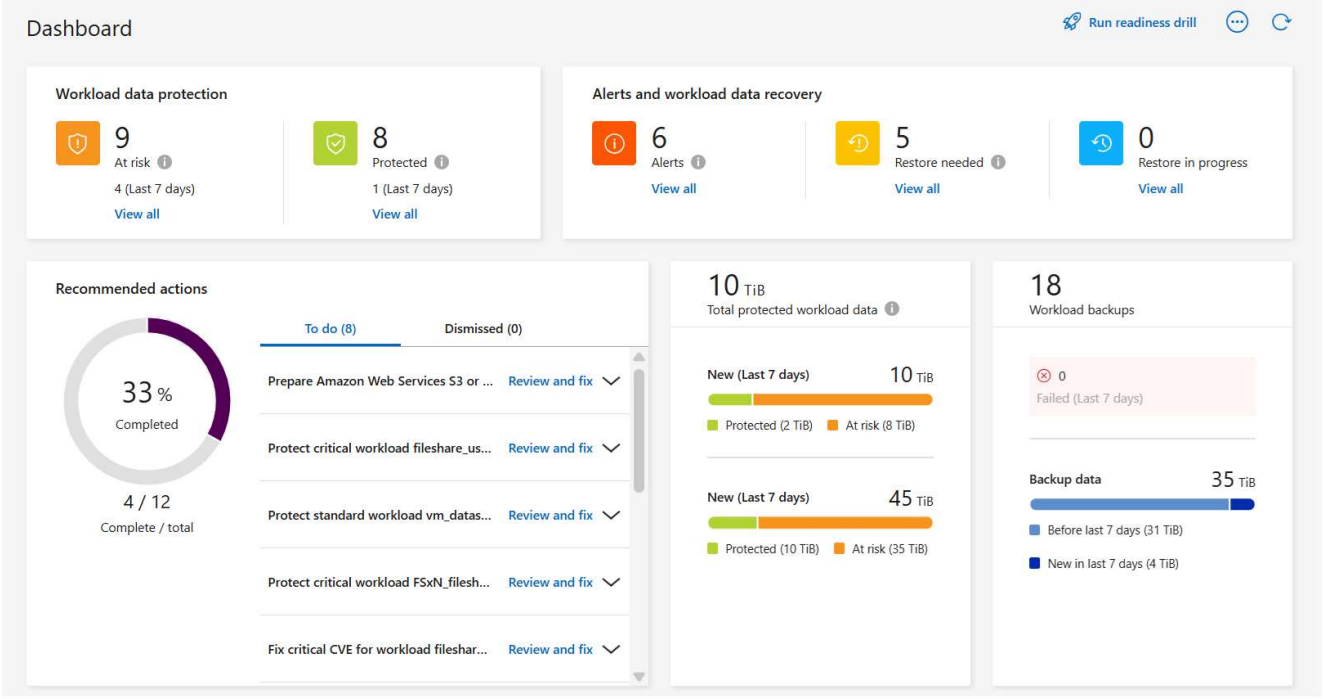
   [ワークロードの検出のスクリーンショット]

3. 特定のコンソール エージェントのワークロードを検出するには、ワークロードを検出するコンソール エージェントの横にある [システムの選択] を選択します。
4. ワークロードを検出するシステムを選択します。
5. *Discover*を選択します。

   ランサムウェア耐性は、選択されたシステムを持つコンソール エージェントのワークロード データのみを検出します。このプロセスには数分かかる場合があります。

6. 検出されたワークロードのリストをダウンロードするには、[結果のダウンロード] を選択します。
7. ランサムウェア耐性ダッシュボードを表示するには、[ダッシュボードに移動] を選択します。

   ダッシュボードにはデータ保護の健全性が表示されます。新しいワークロードが検出されると、危険にさらされているワークロードまたは保護されているワークロードの数が更新されます。



"ダッシュボードに表示される内容について説明します。"

以前に選択したシステムに対して新しく作成されたワークロードを検出する

検出対象のシステムをすでに選択している場合は、ダッシュボードからそれらの環境に対して新しく作成されたワークロードを検出できます。

手順

1. 最後の検出日を特定するには、ランサムウェア耐性ダッシュボードの右上にある 更新 アイコンの横にある日付と時刻のスタンプを確認します。
2. ダッシュボードから、更新アイコン を選択して新しいワークロードを見つけます。

新しいシステムを発見する

すでにシステムを検出している場合は、新しいシステムや以前に選択しなかったシステムを見つけることができます。

手順

1. ランサムウェア耐性メニューから、垂直方向の … 右上のオプションをクリックします。ドロップダウンメニューから*設定*を選択します。
2. ワークロード検出カードで、*ワークロードの検出*を選択します。

   このプロセスには数分かかる場合があり、読み込みアイコンに進行状況が表示されます。

3. Ransomware Resilience は、サポートされているシステムとサポートされていないシステムの両方を検出します。 ONTAPバージョンが必要なバージョンより低い場合、Ransomware Resilience はシステムをサポートしません。サポートされていないシステムにマウスを移動すると、ツールチップに理由が表示されます。ワークロードを検出するシステムを選択します。

4. *Discover*を選択します。

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。

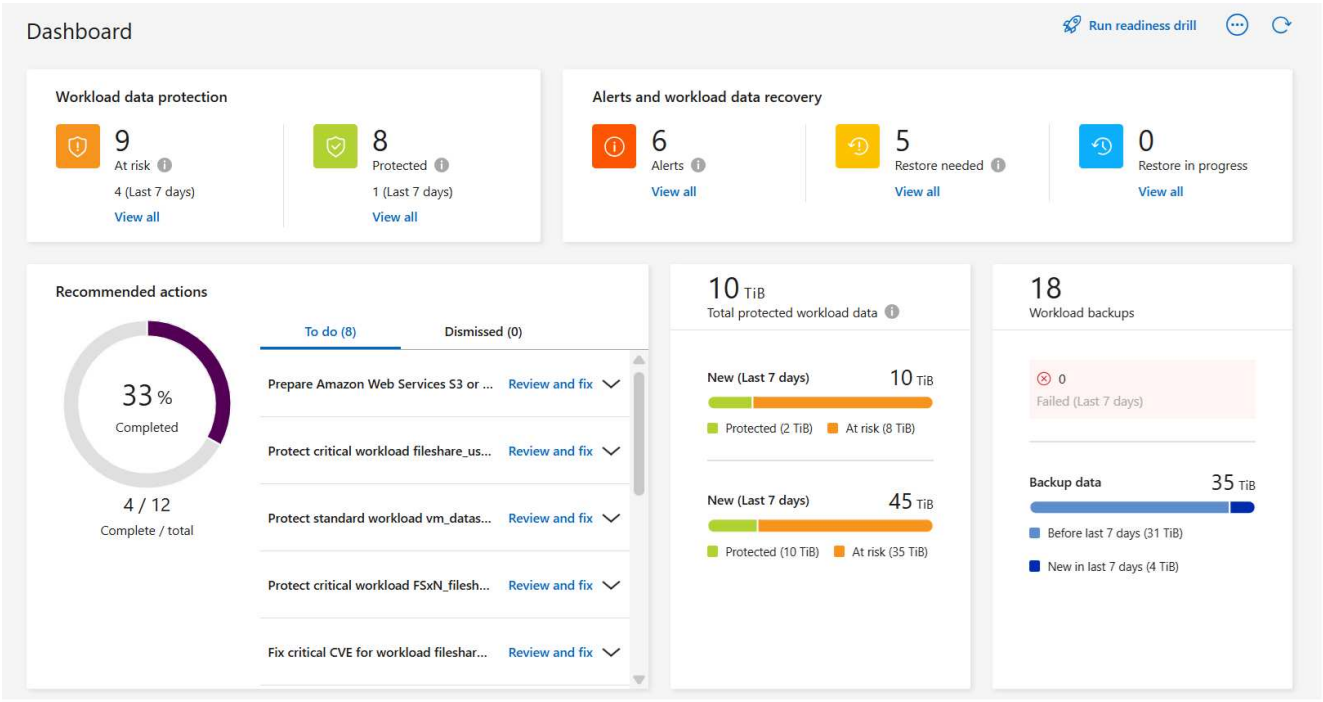
次の状況では、ユーザー名とパスワードを入力する必要があります。

- 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。"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" 。

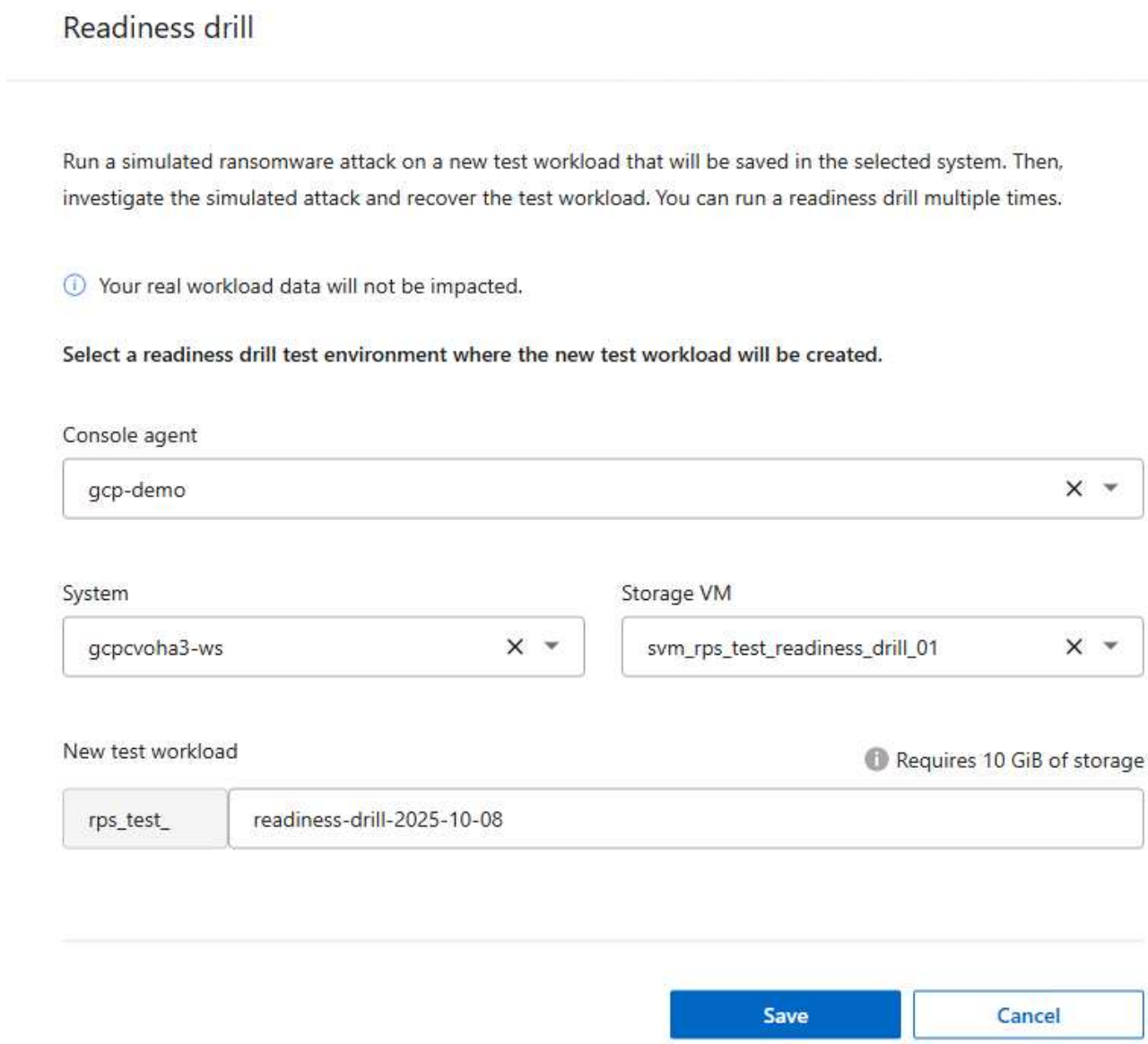
手順

1. 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. 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。

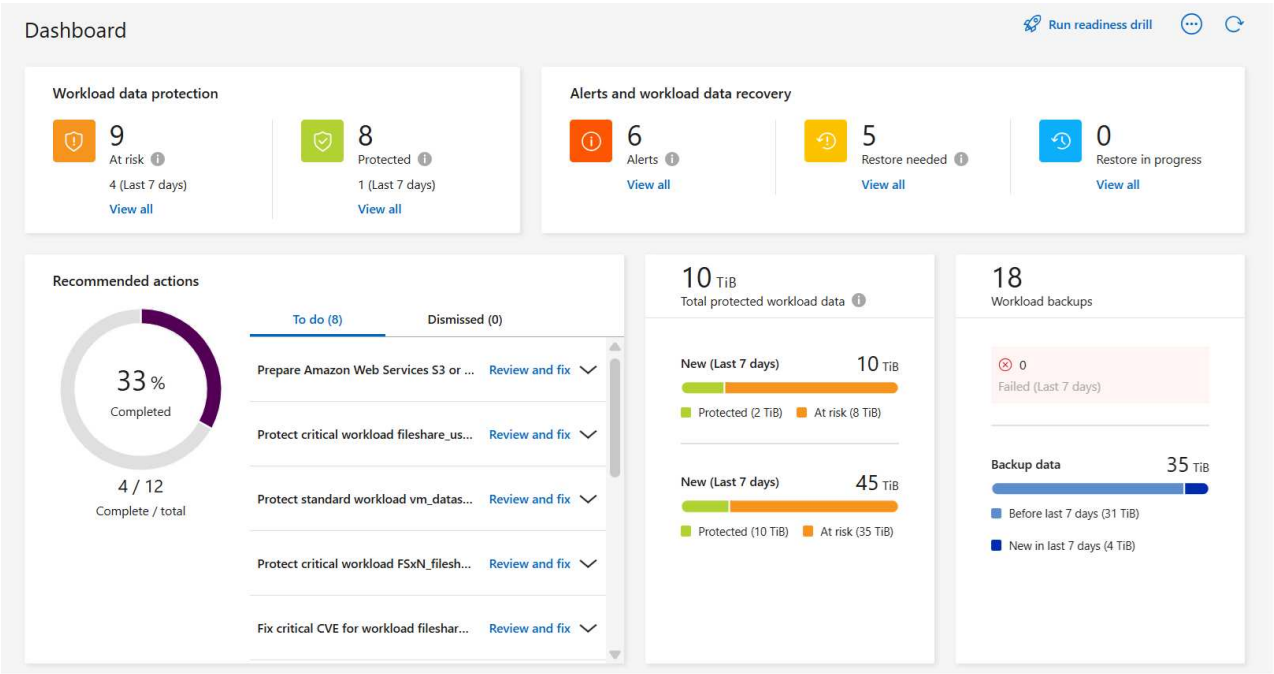
必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"すべてのサービスのコンソールアクセスロールについて学習します"。

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。
2. 準備ドリルをすでに構成している場合は、[開始] を選択すると、準備ドリルが開始されます。

ドリルが開始された後は、準備ドリルの構成を編集することはできません。リセットして再度始めることができます。

即応訓練警報に応答する

準備訓練アラートに応答して準備状況をテストします。

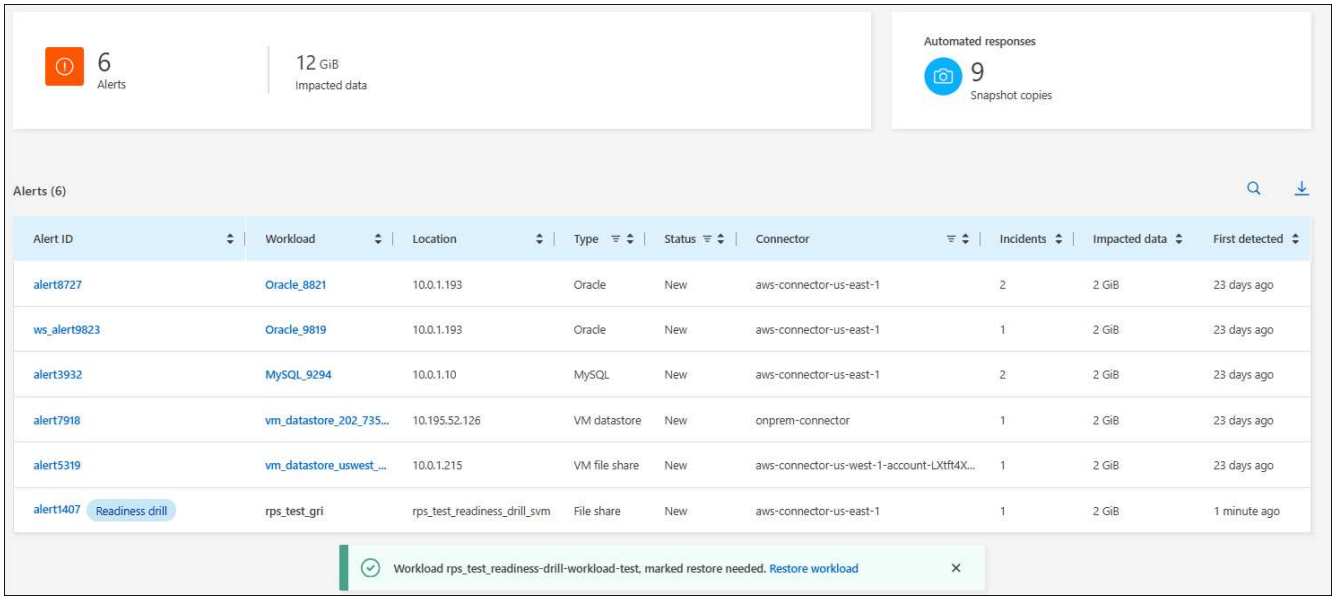
必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"すべてのサービスのコンソールアクセスロールにつ

いて学習します"。

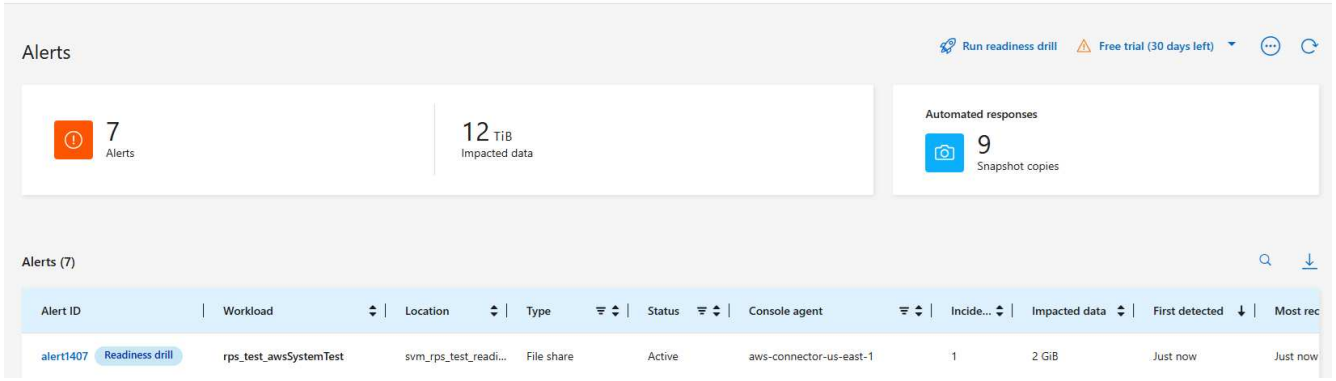
手順

1. 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。

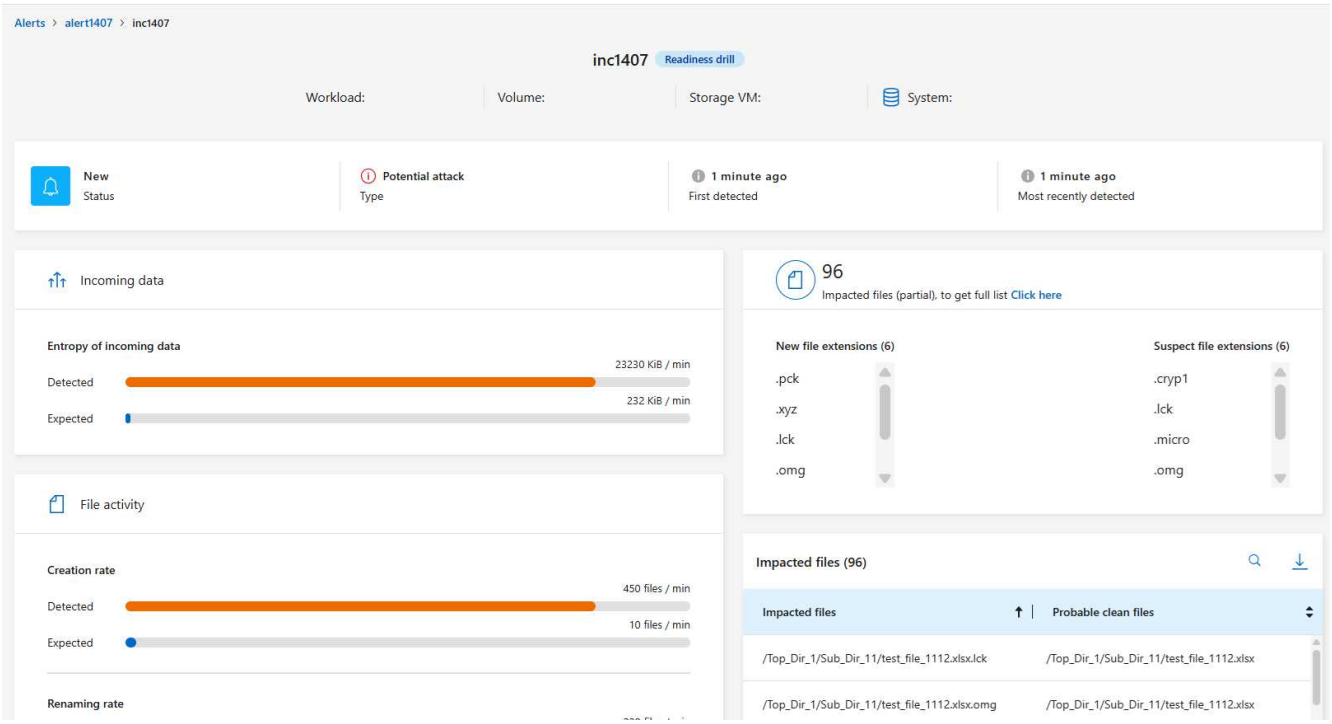
   コンソールにアラート ページが表示されます。アラート ID 列の ID の横に「準備ドリル」が表示されます。



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:

- 潜在的な攻撃タイプを確認します。

  タイプにより、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。 ワークロード セキュリティで調査 を選択して、 Data Infrastructure Insightsワークロード セキュリティでユーザーをさらに調査する必要がある場合があります。

- 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。"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. 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。

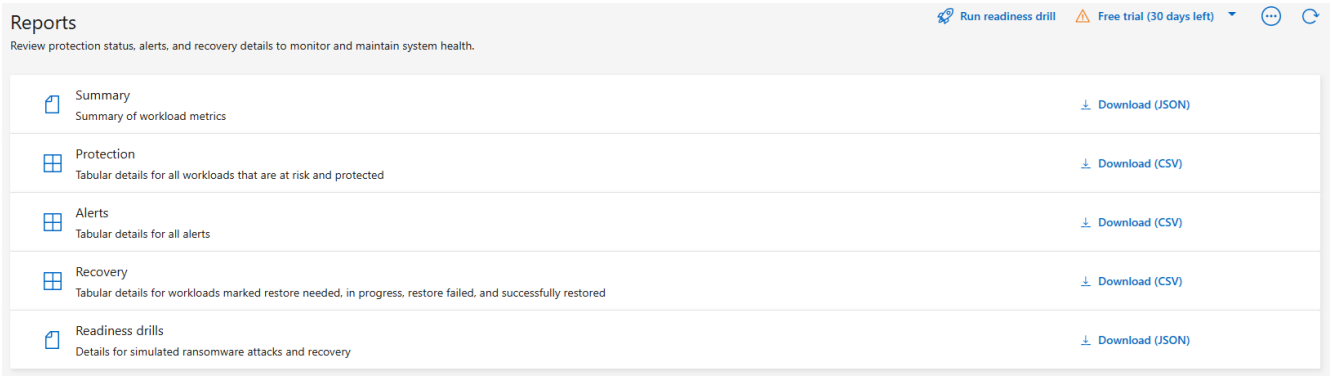
即応訓練に関する報告書を確認する

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。"すべてのサービスに対するBlueXPのアクセス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で保護設定を構成する

設定 オプションにアクセスすることで、バックアップ先を構成したり、外部のセキュリティおよびイベント管理 (SIEM) システムへデータを送信したり、攻撃準備ドリルを実施したり、ワークロード検出を構成したり、 Data Infrastructure Insights Workload Security への接続を構成したりすることができます。

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。"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" 。

設定ページで何ができますか? 「設定」ページからは、次の操作を実行できます。

- 準備訓練を実施してランサムウェア攻撃をシミュレートし、シミュレートされたランサムウェアアラートに応答します。詳細については、 "ランサムウェア攻撃への備えの訓練を実施する" 。
- ワークロード検出を構成します。
- ランサムウェアアラートで疑わしいユーザー情報を表示するには、Data Infrastructure Insights Workload Security への接続を構成します。
- バックアップ先を追加します。
- 脅威の分析と検出のために、セキュリティおよびイベント管理システム (SIEM) を接続します。脅威検出を有効にすると、脅威分析のためにデータが自動的に SIEM に送信されます。

設定ページに直接アクセスする

上部メニューの近くにある [アクション] オプションから [設定] ページに簡単にアクセスできます。

1. ランサムウェア耐性から、垂直方向を選択します … 右上のオプションをクリックします。

2. ドロップダウンメニューから*設定*を選択します。

ランサムウェア攻撃をシミュレートする

新しく作成されたサンプル ワークロードに対するランサムウェア攻撃をシミュレートして、ランサムウェア対策訓練を実施します。次に、シミュレートされた攻撃を調査し、サンプルのワークロードを回復します。この機能は、アラート通知、対応、および回復プロセスをテストすることで、実際のランサムウェア攻撃が発生した場合に備えて準備ができていることを確認するのに役立ちます。ランサムウェア対策訓練を複数回実行できます。

詳細については、"ランサムウェア攻撃への備えの訓練を実施する" 。

ワークロード検出を構成する

環境内の新しいワークロードを自動的に検出するようにワークロード検出を構成できます。

1. [設定] ページで、ワークロードの検出 タイルを見つけます。
2. *ワークロードの検出*タイルで、*ワークロードの検出*を選択します。

   このページには、以前に選択されなかったシステムを持つコンソール エージェント、新しく利用可能になったコンソール エージェント、および新しく利用可能になったシステムが表示されます。このページには、以前選択されたシステムは表示されません。

3. ワークロードを検出するコンソール エージェントを選択します。
4. システムのリストを確認します。
5. ワークロードを検出するシステムをチェックするか、テーブルの上部にあるボックスを選択して、検出されたすべてのワークロード環境でワークロードを検出します。
6. 必要に応じて他のシステムでもこれを実行してください。
7. 検出 を選択すると、選択したコンソール エージェントで Ransomware Resilience によって新しいワークロードが自動的に検出されます。

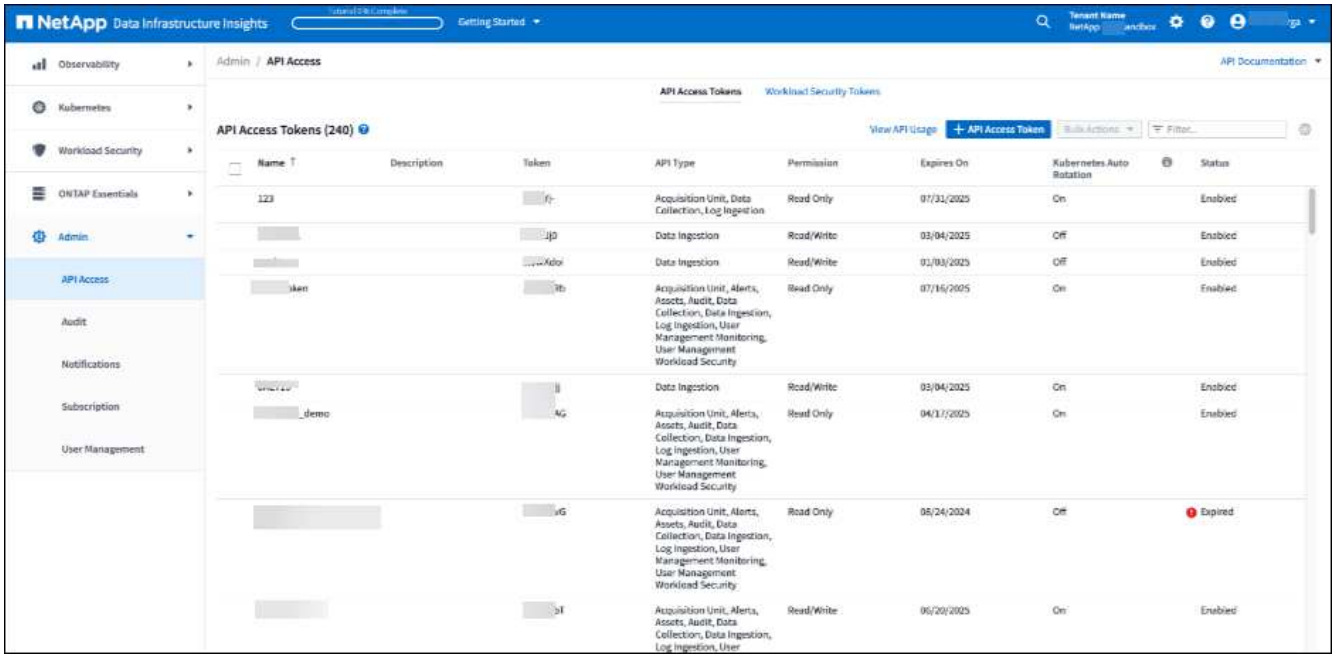
Data Infrastructure Insights Workload Security に接続して、疑わしい異常なユーザー行動を確認します。

Ransomware Resilience で異常なユーザー行動の疑いの詳細を表示するには、まず、 Data Infrastructure Insightsワークロード セキュリティ システムへの接続を構成する必要があります。

Data Infrastructure Insightsワークロード セキュリティ システムから **API** アクセス トークンを取得します。

Data Infrastructure Insightsワークロード セキュリティ システムから API アクセス トークンを取得します。

1. Data Infrastructure Insightsワークロード セキュリティ システムにログインします。
2. 左側のナビゲーションから、管理者 > **API** アクセス を選択します。



3. API アクセス トークンを作成するか、既存のトークンを使用します。
4. API アクセス トークンをコピーします。

Data Infrastructure Insightsワークロードセキュリティに接続

1. 「ランサムウェア耐性設定」メニューから、「ワークロード セキュリティ接続」タイルを見つけます。
2. *接続*を選択します。
3. データ インフラストラクチャ ワークロード セキュリティ UI の URL を入力します。
4. ワークロード セキュリティへのアクセスを提供する API アクセス トークンを入力します。
5. *接続*を選択します。

バックアップ先を追加する

Ransomware Resilience は、まだバックアップがないワークロードと、まだバックアップ先が割り当てられていないワークロードを識別できます。

これらのワークロードを保護するには、バックアップ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

バックアップ先は、Amazon FSx for NetApp ONTAP 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。

ダッシュボードから、またはメニューの [設定] オプションにアクセスして、推奨アクションに基づいてバッ

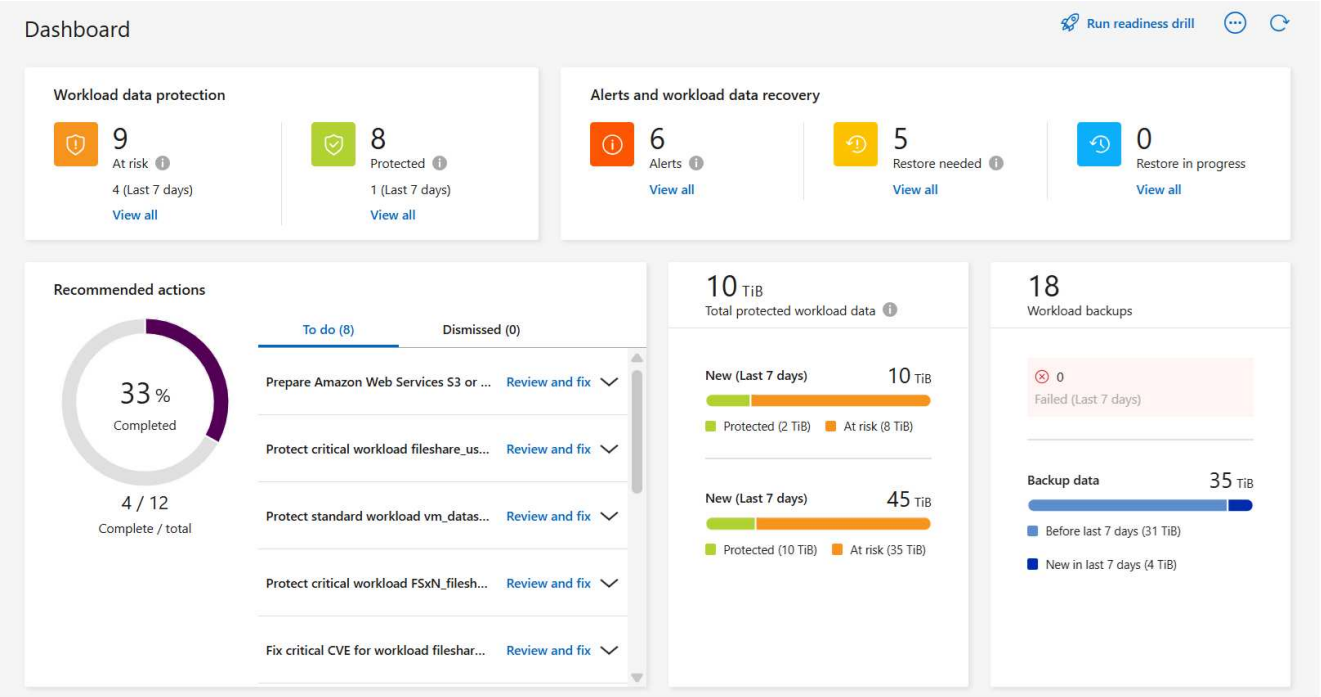
クアップ先を追加できます。

ダッシュボードの推奨アクションからバックアップ先オプションにアクセスします

ダッシュボードには多くの推奨事項が表示されます。 1 つの推奨事項としては、バックアップの保存先を構成することが挙げられます。

手順

1. ランサムウェア耐性ダッシュボードで、[推奨されるアクション] ペインを確認します。



ページ"]

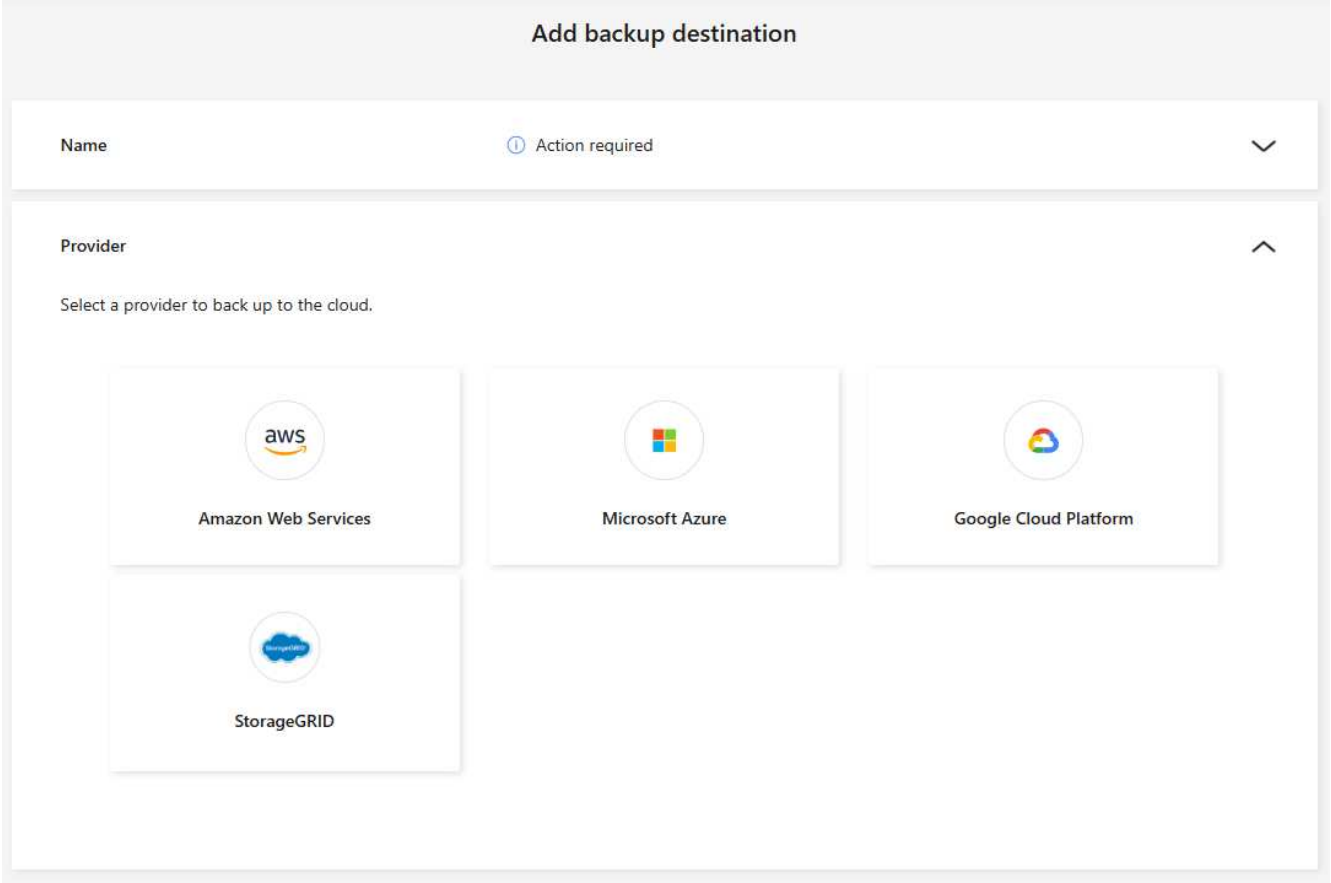
2. ダッシュボードから、「<バックアップ プロバイダー> をバックアップ先として準備する」という推奨事項の [確認して修正] を選択します。
3. バックアップ プロバイダーに応じて手順に従って続行します。

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

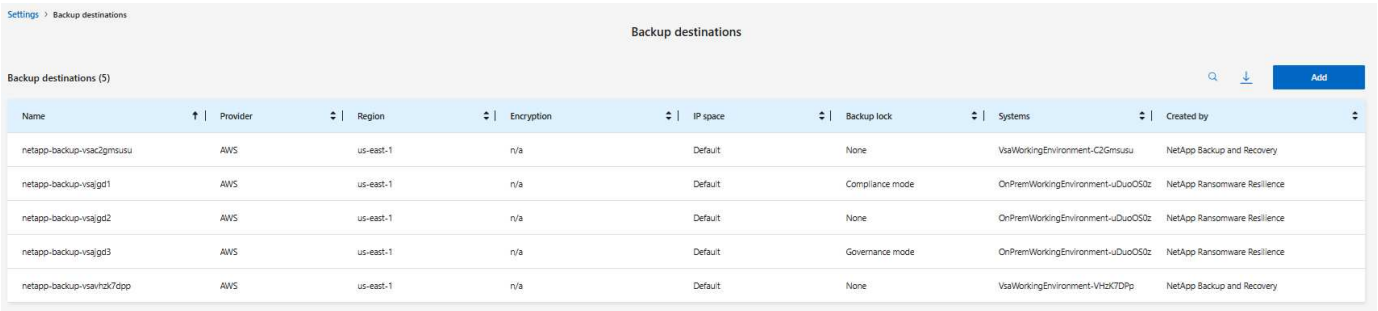
1. 設定 > バックアップ先 ページで、追加 を選択します。
2. バックアップ先の名前を入力します。



3. * StorageGRID*を選択します。
4. 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、バックアップを保存する独自のバケットを用意してください。
     - StorageGRIDゲートウェイ ノードの完全修飾ドメイン名、ポート、 StorageGRIDアクセス キーおよび秘密キーの資格情報。
   - 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。
5. *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。



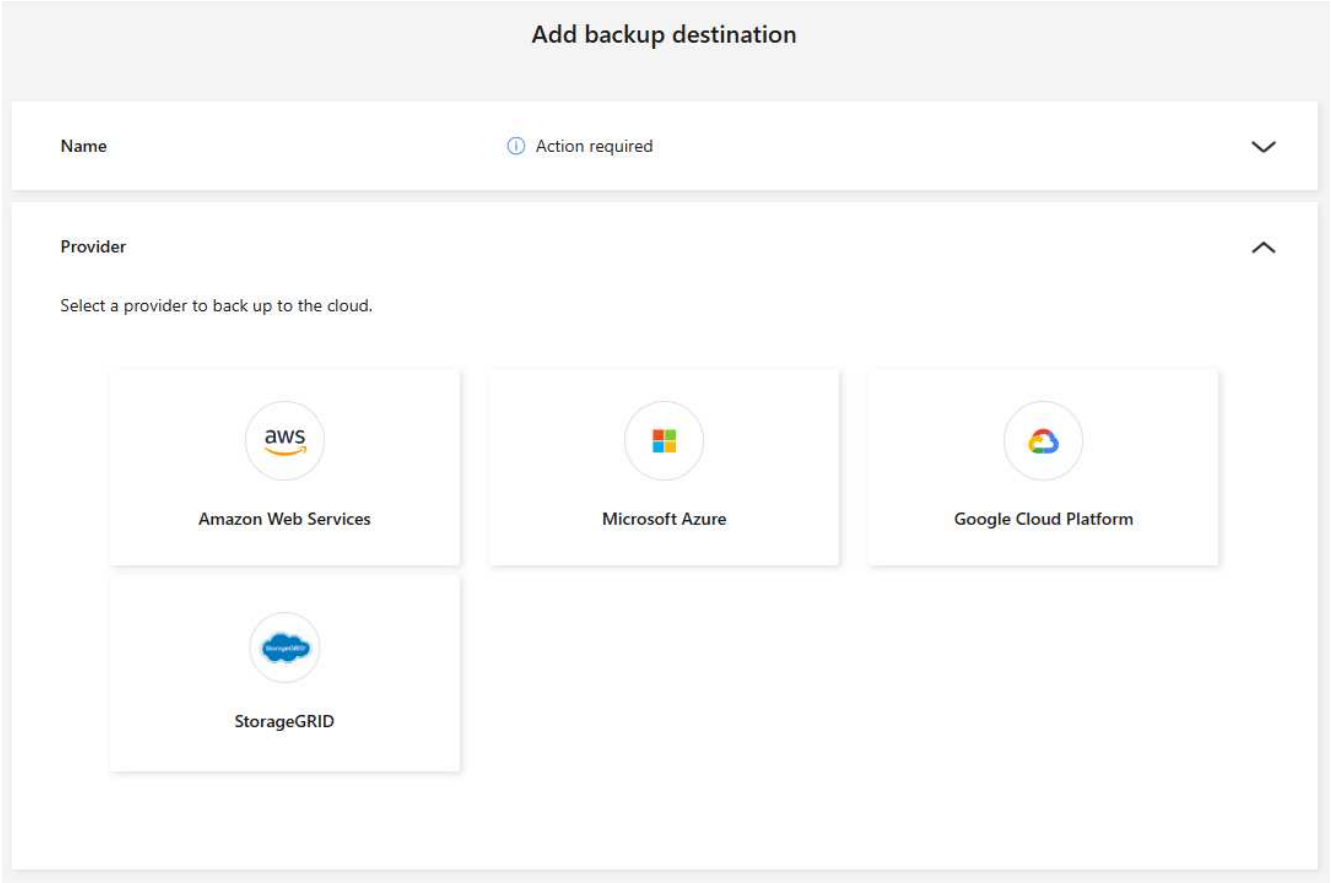
Amazon Web Servicesをバックアップ先として追加する

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、以下を参照してください。 "Amazon S3バケットを管理する" 。

手順

1. 設定 **>** バックアップ先 ページで、追加 を選択します。
2. バックアップ先の名前を入力します。



3. *Amazon Web Services*を選択します。
4. 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。

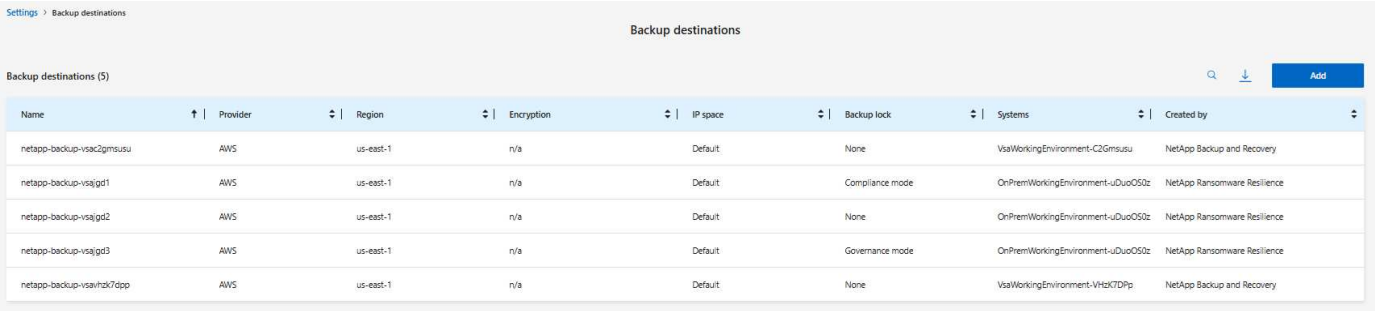
  ここでバックアップ ロック設定を構成すると、バックアップ先の構成後に設定を変更することはできません。

  - 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。

5. *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。



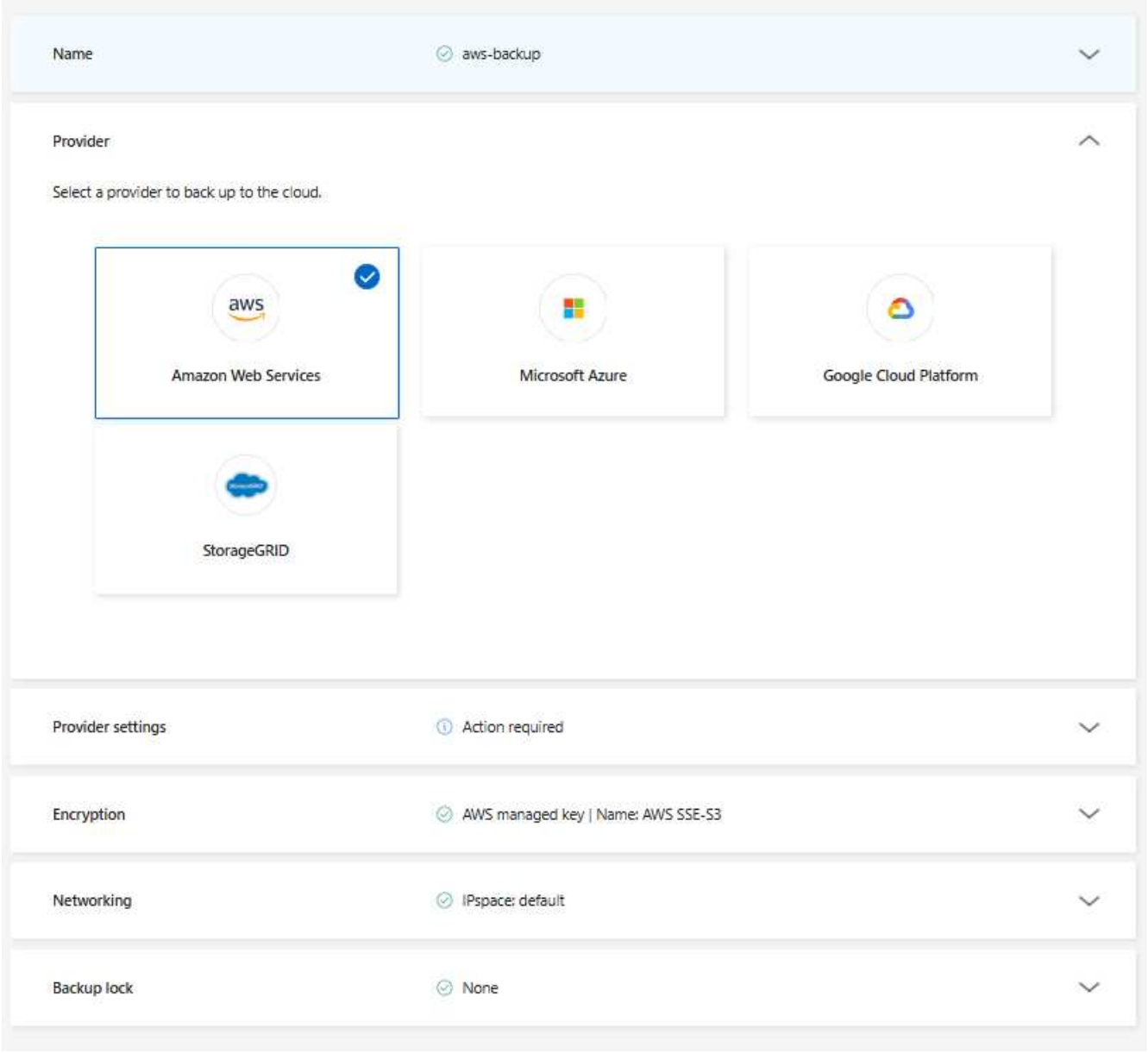
Google Cloud Platform をバックアップ先として追加する

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、以下を参照してください。 "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" 。

手順

1. 設定 > バックアップ先 ページで、追加 を選択します。
2. バックアップ先の名前を入力します。



3. **Google Cloud Platform** を選択します。
4. 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します。アクセスキーとシークレットキーを入力します。
     - Google Cloud Platform プロジェクトとリージョンを入力または選択します。
   - 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 が管理するキーは引き続きご利用いただけます。
   - 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 GCP 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。

5. *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。

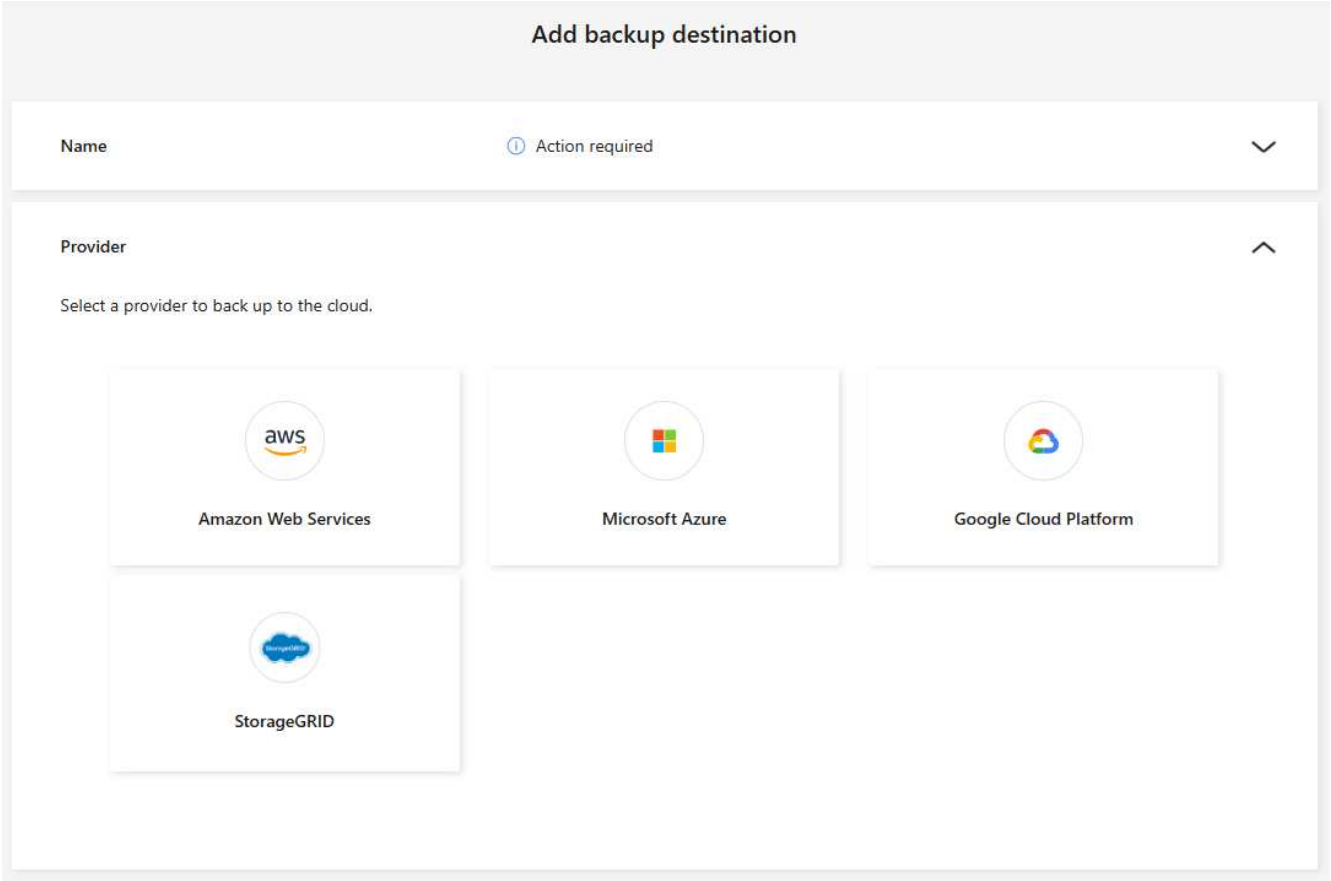
バックアップ先として **Microsoft Azure** を追加する

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. 設定 **>** バックアップ先 ページで、追加 を選択します。
2. バックアップ先の名前を入力します。



3. **Azure** を選択します。
4. 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。

- Azure 資格情報の Azure サブスクリプション、リージョン、リソース グループ

  "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: 新しいストレージ アカウン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。既存のアカウントを選択した場合は、暗号化情報がすでに利用可能です。

  アカウント内のデータは、既定では Microsoft 管理キーで暗号化されます。 Microsoft が管理する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。

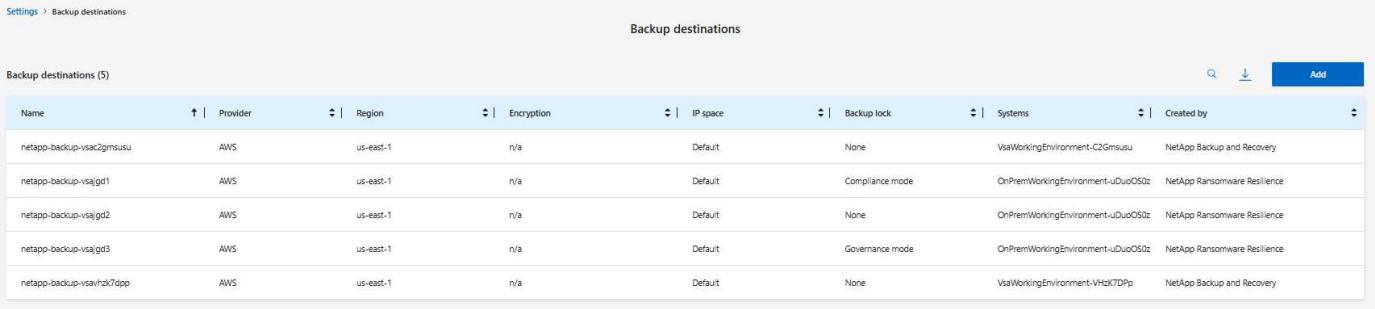
- ネットワーク: IPspace を選択し、プライベート エンドポイントを使用するかどうかを選択します。
  - IPspace は、バックアップするボリュームが存在するクラスターです。この IPspace のクラスタ間 LIF には、アウトバウンド インターネット アクセスが必要です。
  - 必要に応じて、以前に構成した Azure プライベート エンドポイントを使用するかどうかを選択します。

    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" 。

5. *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。



脅威の分析と検出のためにセキュリティおよびイベント管理システム (SIEM) に接続する

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) に自動的に送信できます。 SIEM として、AWS Security Hub、Microsoft Sentinel、または Splunk Cloud を選択できます。

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について

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こと 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. *認証*をクリックします。

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。

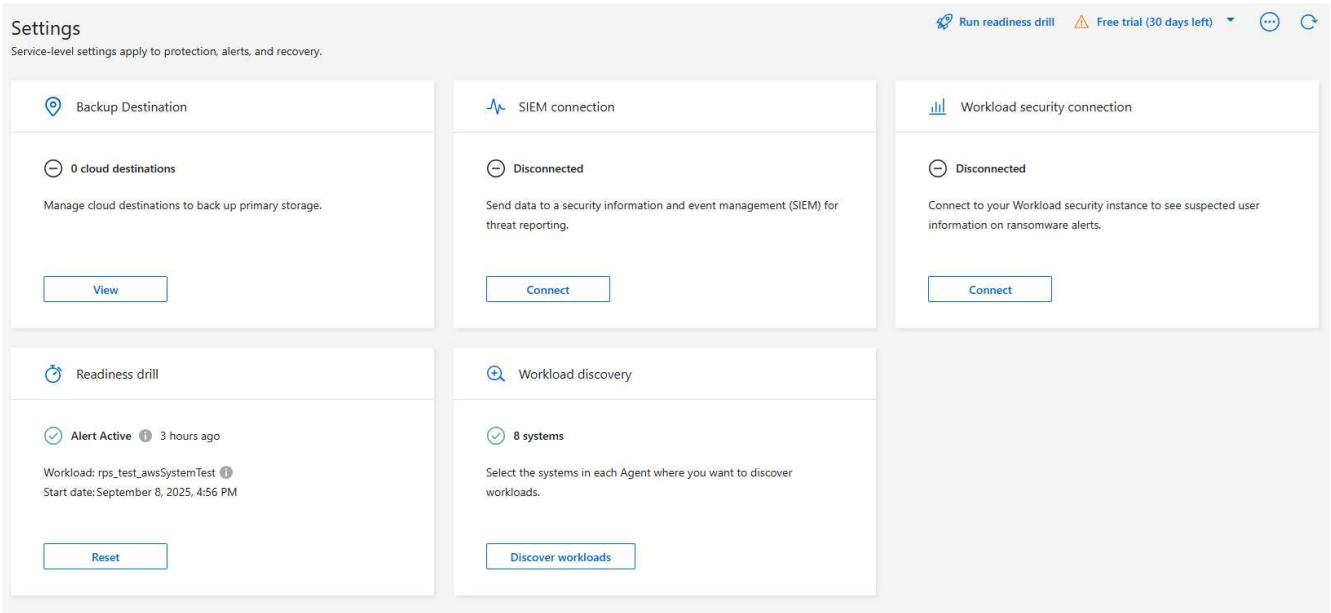
ランサムウェア耐性における**SIEM**の接続

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。

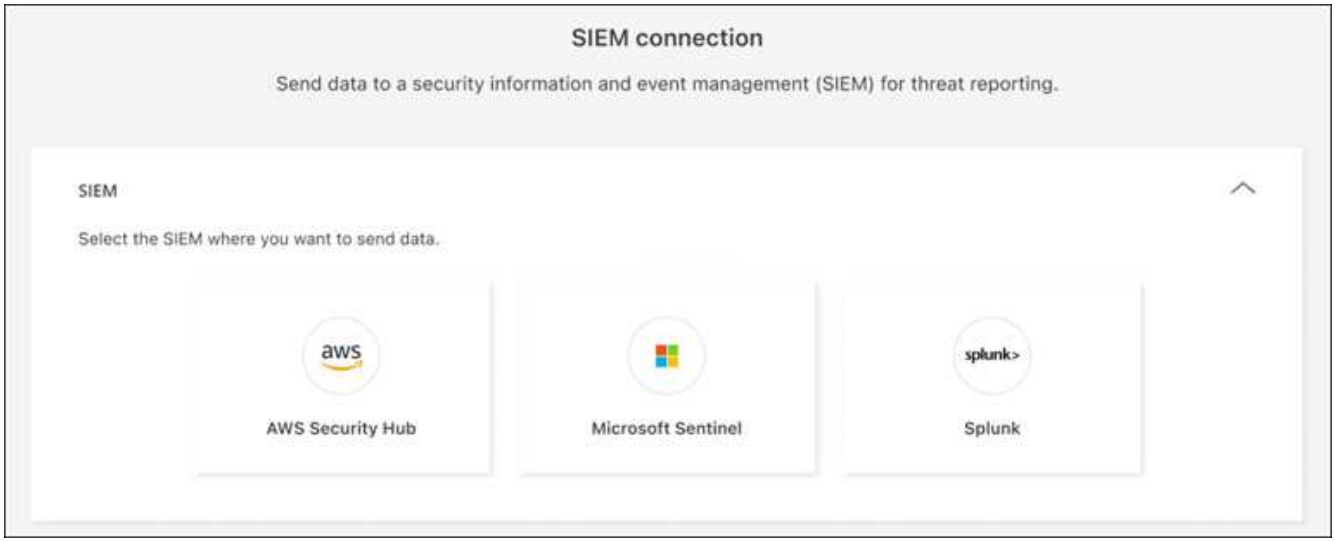
手順

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。

ランサムウェア耐性を活用する

NetAppのランサムウェア耐性を活用する

NetApp Ransomware Resilience を使用すると、ワークロードの健全性を確認し、ワークロードを保護できます。

- "ランサムウェア耐性におけるワークロードの検出" 。
- "ダッシュボードから保護とワークロードの健全性を表示する" 。
  - ランサムウェア保護の推奨事項を確認し、それに従って行動します。
- "ワークロードを保護する" ：
  - ランサムウェア保護戦略をワークロードに割り当てます。
  - 将来のランサムウェア攻撃を防ぐために、アプリケーションの保護を強化します。
  - 保護戦略を作成、変更、または削除します。
- "潜在的なランサムウェア攻撃の検出に対応する" 。
- "攻撃からの回復" （事件が解決した後）。
- "保護設定を構成する" 。

NetAPp ランサムウェア耐性ダッシュボードを使用してワークロードの健全性を監視する

NetAppランサムウェア耐性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。

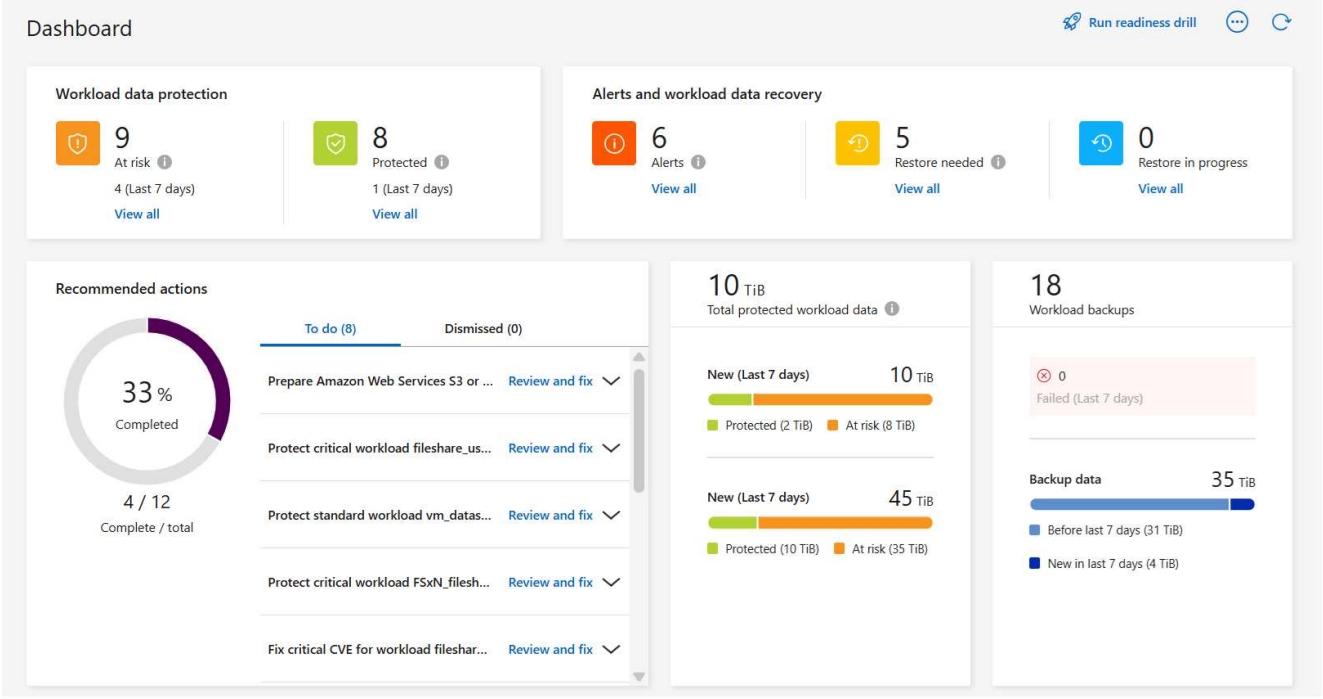
ダッシュボードを使用して、保護の提案を確認したり、設定を変更したり、レポートをダウンロードしたり、ドキュメントを表示したりできます。

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。 "すべてのサービスに対するBlueXPのアクセス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。

見る"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" 。

ランサムウェア耐性では、ダッシュボードに最後にアクセスしてから 24 時間以内に発生した新しい推奨事項が「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それに応じて対処すると、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。アクションを拒否すると、推奨事項は拒否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。。 "保護設定を構成する" 。
アプリケーションまたは VMware のワークロード一貫性保護を有効にします。	これらのワークロードは、SnapCenterソフトウェアまたはSnapCenter Plug-in for VMware vSphereによって管理されません。	これらをSnapCenterで管理するには、ワークロード一貫性保護を有効にします。。 "ランサムウェア攻撃からワークロードを保護する" 。
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"。

推奨事項	説明	解決方法
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。。 "保護設定を構成する" 。
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" 。
VMware vSphere (SCV) 用の利用可能なSnapCenterプラグインをコンソールに登録します。	VM ワークロードは保護されていません。	VMware vSphere 用のSnapCenterプラグインを有効にして、VM ワークロードに VM 整合性保護を割り当てます。。 "ランサムウェア攻撃からワークロードを保護する" 。
利用可能なSnapCenter Serverをコンソールに登録する	アプリケーションは保護されていません。	SnapCenter Server を有効にして、アプリケーション一貫性のある保護をワークロードに割り当てます。。 "ランサムウェア攻撃からワークロードを保護する" 。
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。

ワークロードを保護する

NetAppランサムウェア耐性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。"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" 。

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、検出ポリシーと保護ポリシーの両方が含まれます。

- 検出ポリシー はランサムウェアの脅威を検出し、オプションで疑わしいファイル拡張子をブロックします。
- 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。

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バックアップおよびリカバリ
- VMデータストア用のSnapCenter for VMware
- Oracle および MySQL 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 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。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 の FSx for ONTAPで設定します。バックアップ ポリシーは Ransomware Resilience に表示され、AWS から変更されません。

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

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

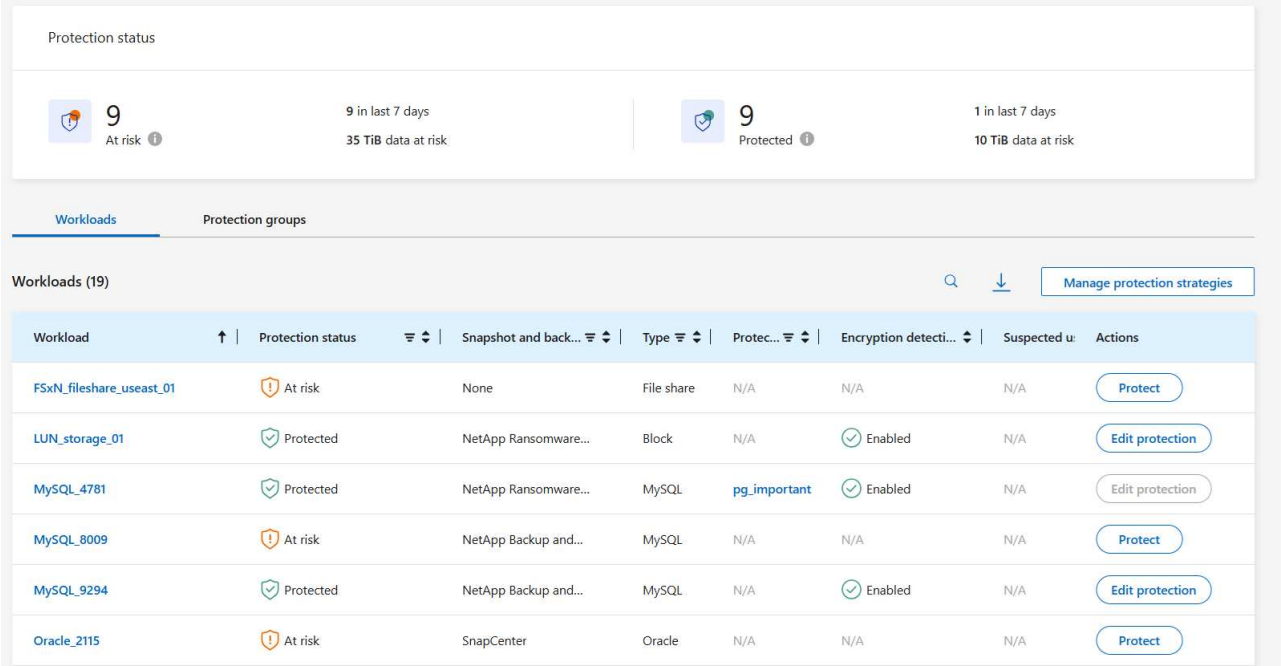
ワークロードのランサムウェア保護を表示する

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

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

手順

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



3. このページから、ワークロードの保護の詳細を表示および変更できます。

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

保護ページを理解する

「保護」ページには、ワークロード保護に関する次の情報が表示されます。

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

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

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

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

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

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。

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: スナップショット コピーが 1 時間あたり 1 回以上作成される (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 コピーは 1 時間あたり 1 回未満ですが、1 日あたり 1 回以上作成されます
- 標準: 1日あたり1回以上のスナップショットコピーの取得

定義済み検出ポリシー

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。

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合計最大数
重要なワークロードポリシー	15分ごと	15分ごと	3	288	309
	日次	1日ごと	14	14	309
	週次	1週間ごと	35	5	309
	毎月	30日ごと	60	2	309
重要なワークロードポリシー	15分ごと	30分ごと	3	144	165
	日次	1日ごと	14	14	165
	週次	1週間ごと	35	5	165
	毎月	30日ごと	60	2	165
標準作業負荷ポリシー	15分ごと	30分ごと	3	72	93
	日次	1日ごと	14	14	93
	週次	1週間ごと	35	5	93
	毎月	30日ごと	60	2	93

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

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

このプロセスは、バックアップとリカバリを使用して、アプリケーション用のSnapCenterソフトウェア サー

バまたは VM 用の SnapCenter Plug-in for VMware vSphereの登録を開始します。

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

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

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

手順

1. ランサムウェア耐性メニューから、*ダッシュボード*を選択します。
2. [推奨事項] ペインで、次のいずれかの推奨事項を見つけて、[確認して修正] を選択します。
   - 利用可能なSnapCenter ServerをNetAppコンソールに登録する
   - 利用可能なSnapCenter Plug-in for VMware vSphere (SCV) をNetAppコンソールに登録します。
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"。

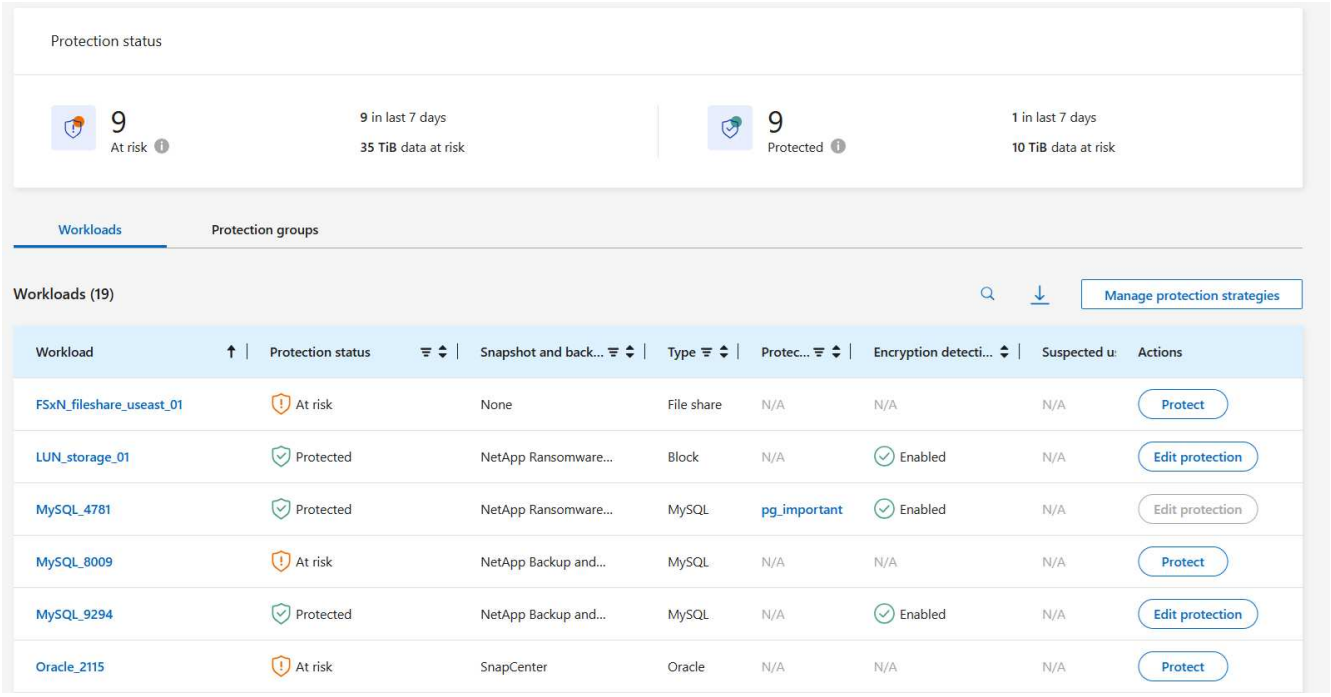
ランサムウェア対策戦略を作成する（スナップショットやバックアップポリシーがない場合）

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。

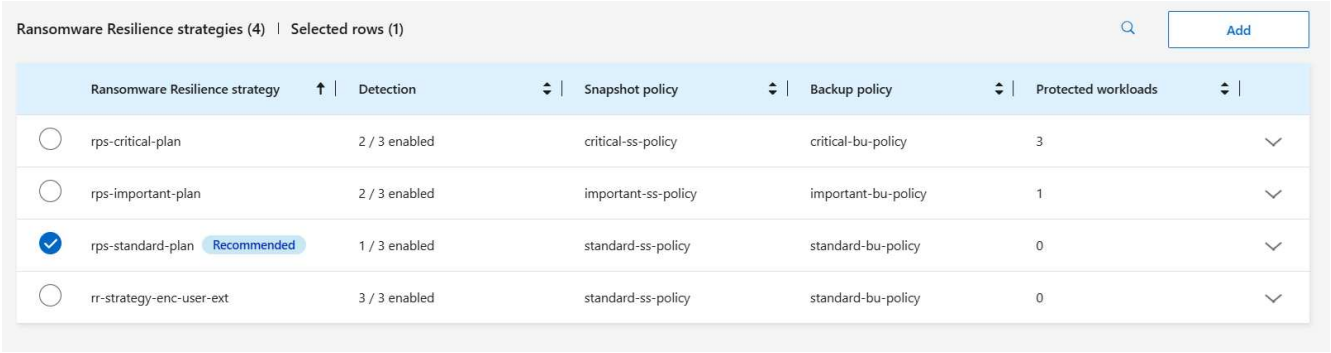
- スナップショットポリシー
- バックアップ ポリシー
- ランサムウェア検出ポリシー

ランサムウェア対策戦略を作成する手順

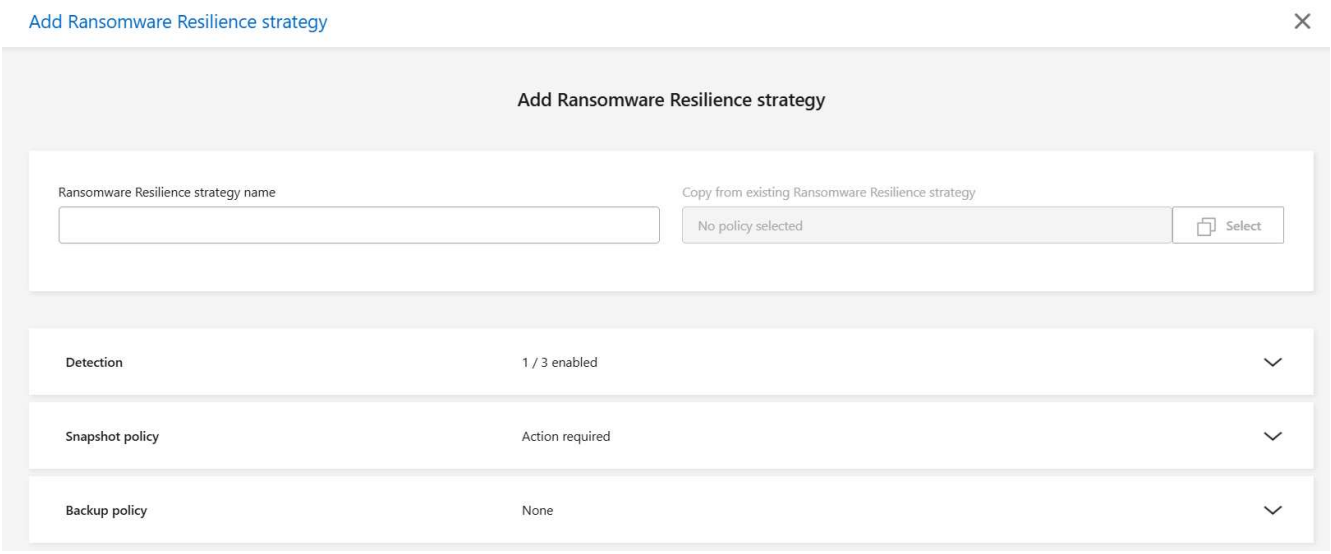
1. ランサムウェア耐性メニューから、*保護*を選択します。



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。
     - プライマリ検出: ランサムウェア検出を有効にして、ランサムウェア耐性により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: これを有効にすると、Ransomware Resilience によって既知の疑わしいファイル拡張子がブロックされます。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。
- バックアップポリシー:
  - バックアップ ポリシーのベース名: 新しい名前を入力するか、既存の名前を選択します。
  - バックアップ スケジュール: セカンダリ ストレージのスケジュール オプションを選択し、スケジュールを有効にします。

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

6. *追加*を選択します。

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

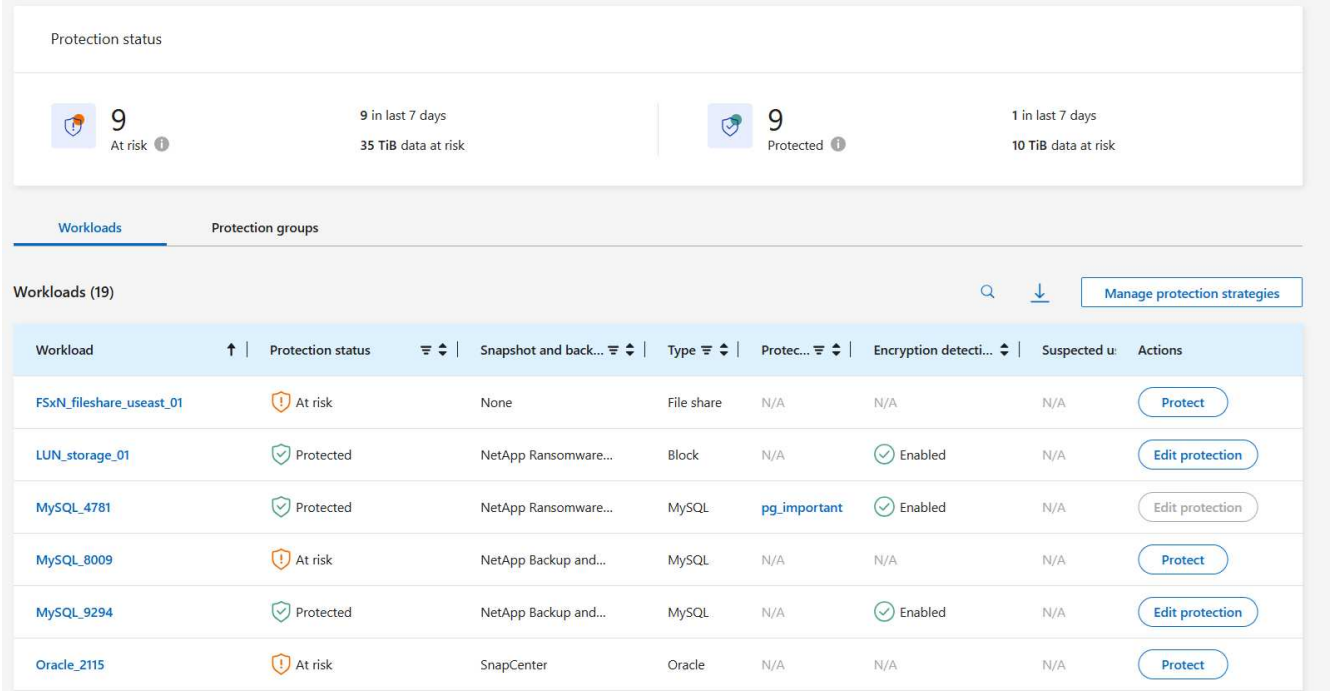
ランサムウェア耐性により、他のNetApp製品またはサービスで管理されている既存のスナップショットおよびバックアップ保護を使用して、ワークロードに検出ポリシーまたは保護ポリシーのいずれかを割り当てることができます。 Backup and Recovery やSnapCenterなどの他のサービスでは、スナップショット、セカンダリ ストレージへのレプリケーション、またはオブジェクト ストレージへのバックアップを管理するポリシーを使用します。

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

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

手順

1. ランサムウェア耐性メニューから、*保護*を選択します。



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

   検出ポリシーを選択し、[保護] を選択します。

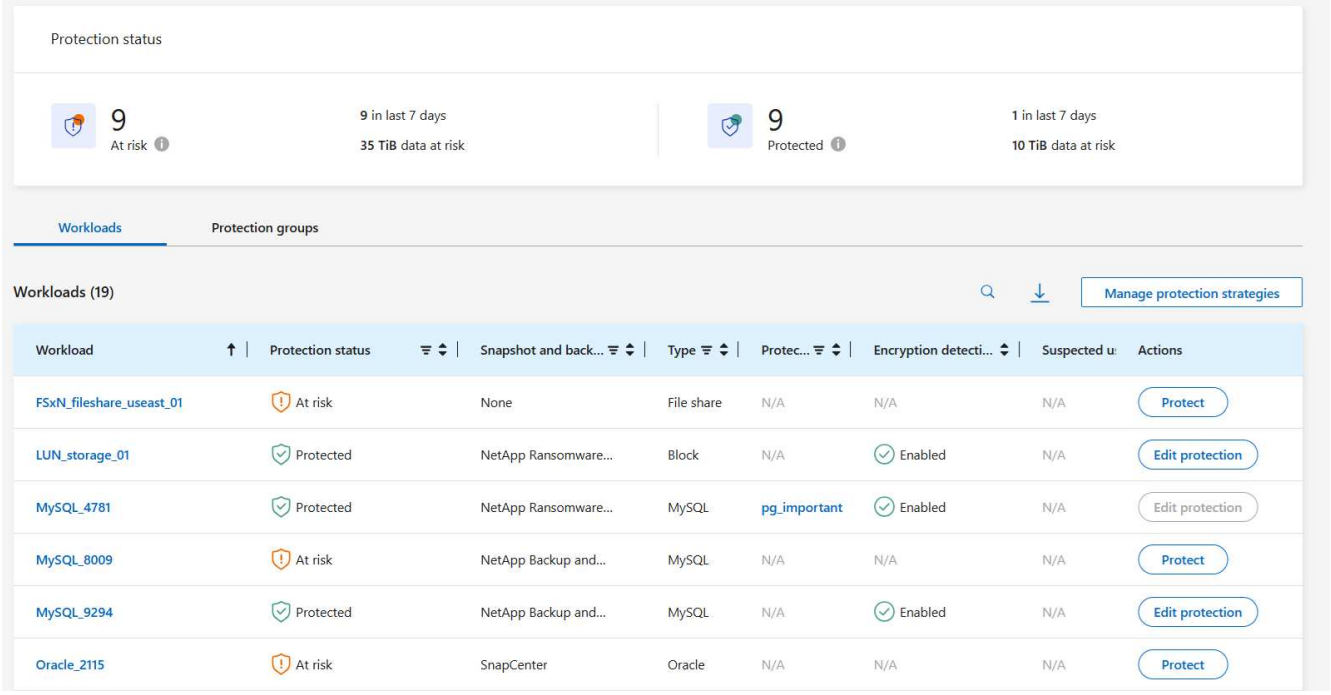
6. [保護] ページで、検出ステータス を確認して、検出がアクティブであることを確認します。

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

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

手順

1. ランサムウェア耐性メニューから、*保護*を選択します。



2. [保護] ページでワークロードを選択し、[保護] を選択します。
3. Ransomware Resilience は、アクティブなバックアップとリカバリ、またはSnapCenterポリシーが既に存在するかどうかを検出します。既存のバックアップとリカバリまたはSnapCenterポリシーを置き換えるには、[既存のポリシーを置き換える] ボックスを選択します。ボックスを選択すると、Ransomware Resilience によって検出ポリシーのリストが検出ポリシーに置き換えられます。
4. 保護ポリシーを選択します。保護ポリシーが存在しない場合は、[追加] を選択して新しいポリシーを作成します。ポリシーの作成方法については、以下を参照してください。保護ポリシーを作成する 。 次へを選択します。
5. 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。
6. 新しい保護戦略を確認し、[保護] を選択して適用します。
7. [保護] ページで、検出ステータス を確認して、検出がアクティブであることを確認します。

別のポリシーを割り当てる

既存のポリシーを別のポリシーに置き換えることができます。

手順

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

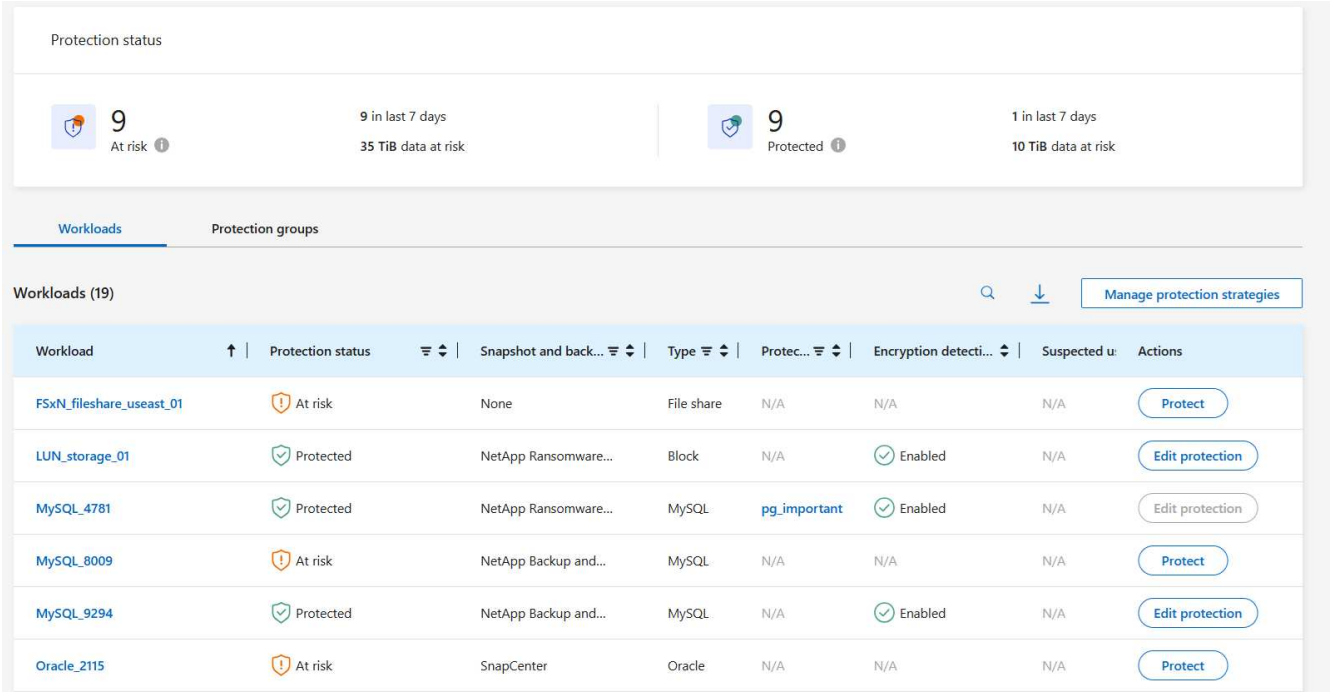
ファイル共有をグループ化して保護を容易にする

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

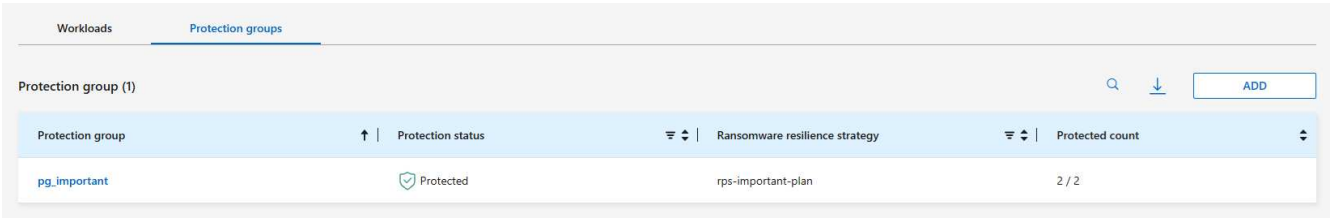
保護ステータスに関係なく (つまり、保護されていないグループと保護されているグループ)、グループを作成できます。保護グループに保護ポリシーを追加すると、 SnapCenterおよびNetApp Backup and Recovery によって管理されるポリシーを含む既存のポリシーが新しい保護ポリシーに置き換えられます。

手順

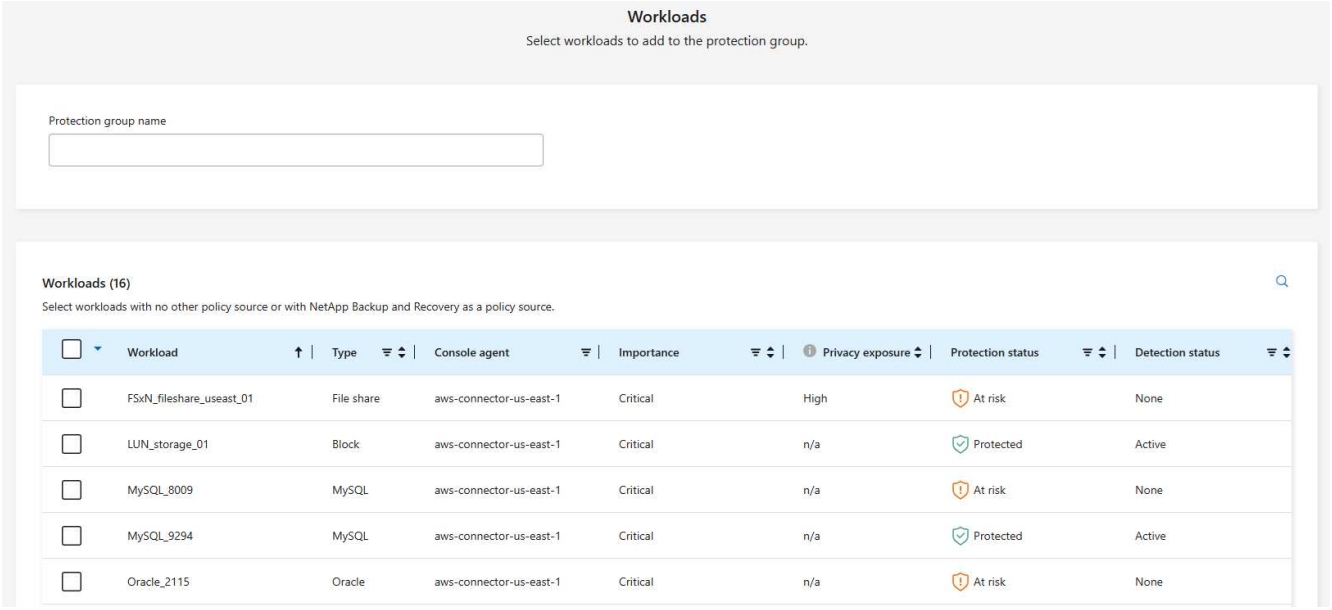
1. ランサムウェア耐性メニューから、*保護*を選択します。



2. [保護] ページで、[保護グループ] タブを選択します。



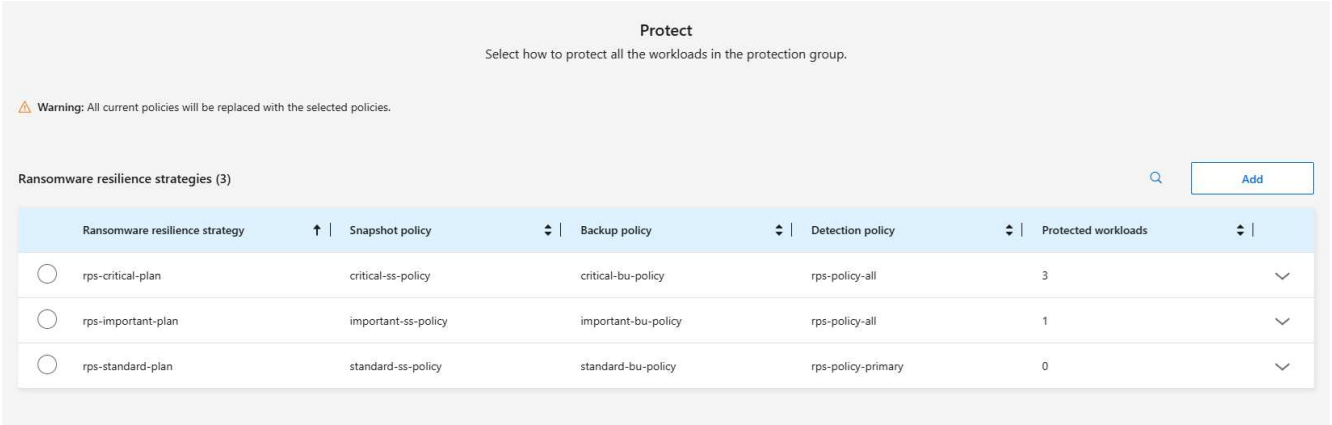
3. *追加*を選択します。



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

   ワークロードの詳細を表示するには、右にスクロールします。

6. *次へ*を選択します。



7. このグループの保護を管理するポリシーを選択します。
8. *次へ*を選択します。
9. 保護グループの選択内容を確認します。
10. *追加*を選択します。

グループ保護を編集

既存のグループの検出ポリシーを変更できます。

手順

1. ランサムウェア耐性メニューから、*保護*を選択します。

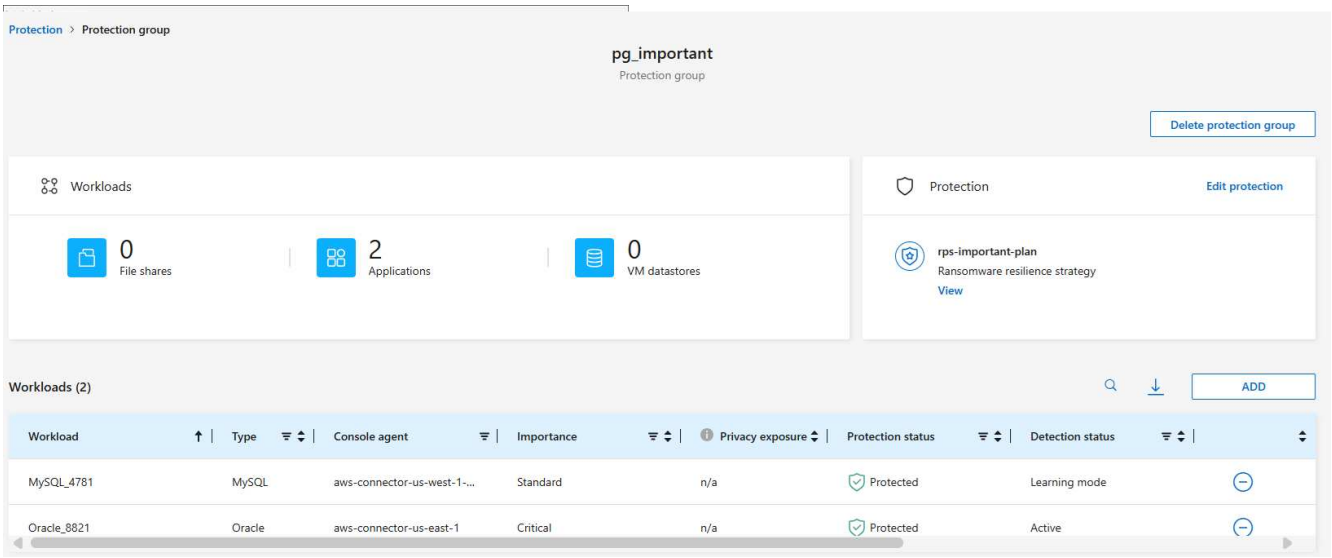
2. [保護] ページで [保護グループ] タブを選択し、ポリシーを変更するグループを選択します。
3. 保護グループの概要ページで、*保護の編集*を選択します。
4. 適用する既存の保護ポリシーを選択するか、[追加] を選択して新しい保護ポリシーを作成します。保護ポリシーの追加の詳細については、以下を参照してください。保護ポリシーを作成する 。次に、[保存] を選択します。
5. バックアップ先の概要で、既存のバックアップ先を選択するか、新しいバックアップ先を追加します。
6. 変更内容を確認するには、[次へ] を選択します。

グループからワークロードを削除する

後で既存のグループからワークロードを削除する必要がある場合があります。

手順

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



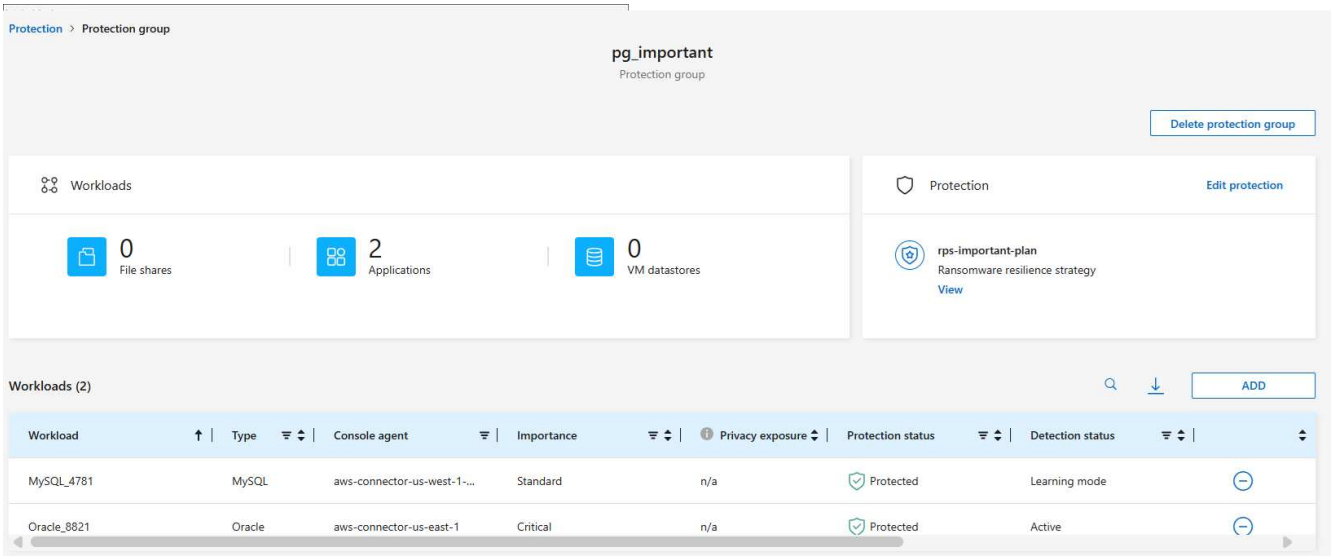
4. 選択した保護グループのページで、グループから削除するワークロードを選択し、*アクション*を選択します。 •••オプション。
5. [アクション] メニューから、[ワークロードの削除] を選択します。
6. ワークロードを削除することを確認し、[削除] を選択します。

保護グループを削除する

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

手順

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



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

ランサムウェア対策戦略の管理

ランサムウェア戦略を削除することができます。

ランサムウェア保護戦略によって保護されているワークロードを表示する

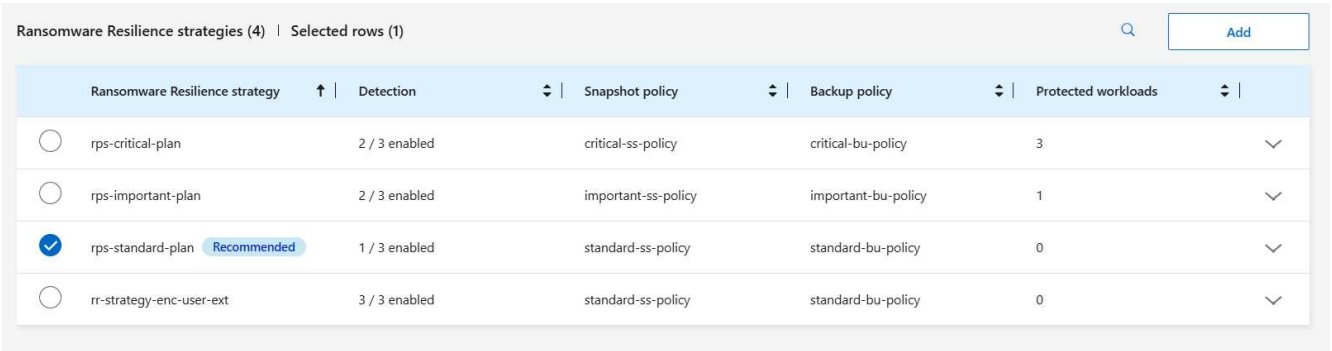
ランサムウェア保護戦略を削除する前に、その戦略によって保護されているワークロードを確認することをお勧めします。

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

戦略リストを表示する手順

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

   ランサムウェア保護戦略ページには、戦略のリストが表示されます。



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

ランサムウェア対策戦略を削除する

現在どのワークロードにも関連付けられていない保護戦略を削除できます。

手順

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

ランサムウェア耐性における**NetApp**データ分類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。データ分類はコンソールのコア 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。

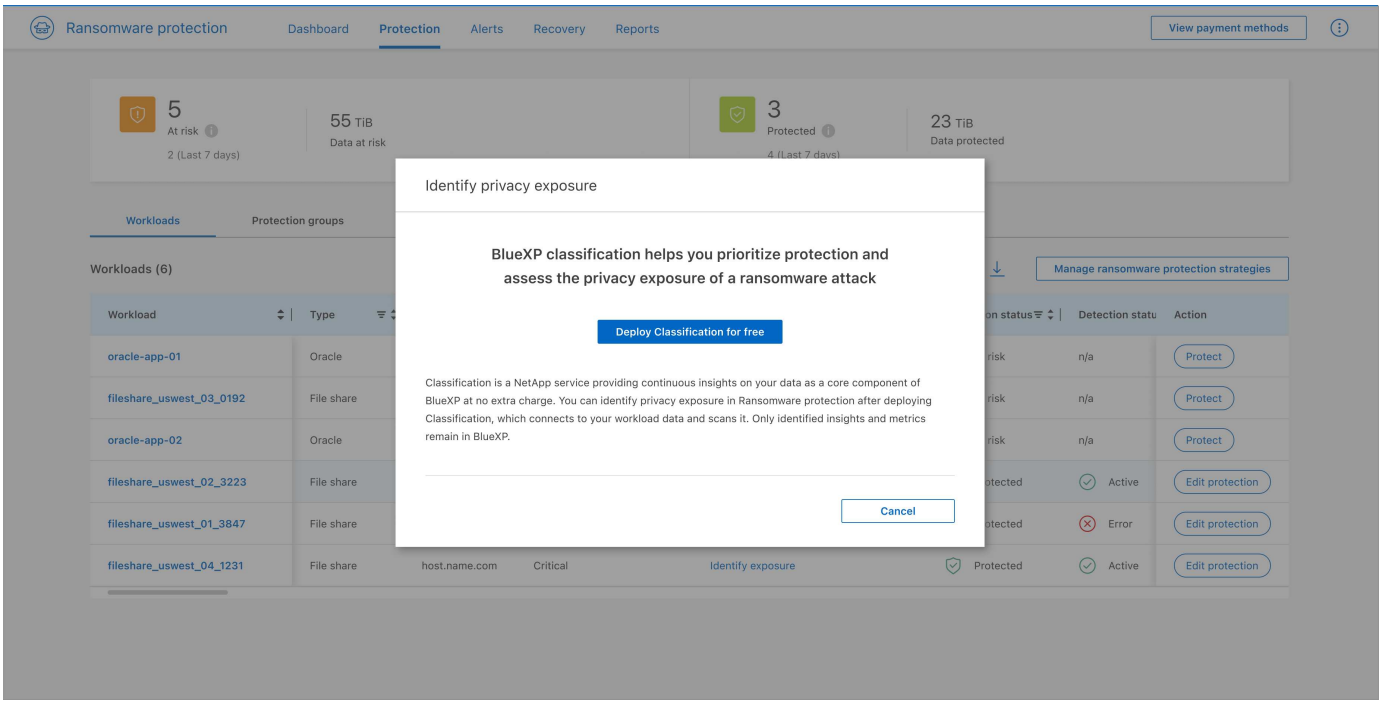
このプロセスはワークロードの重要性に影響を与え、適切な保護が確保されるようにするのに役立ちます。

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。"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" 。

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。

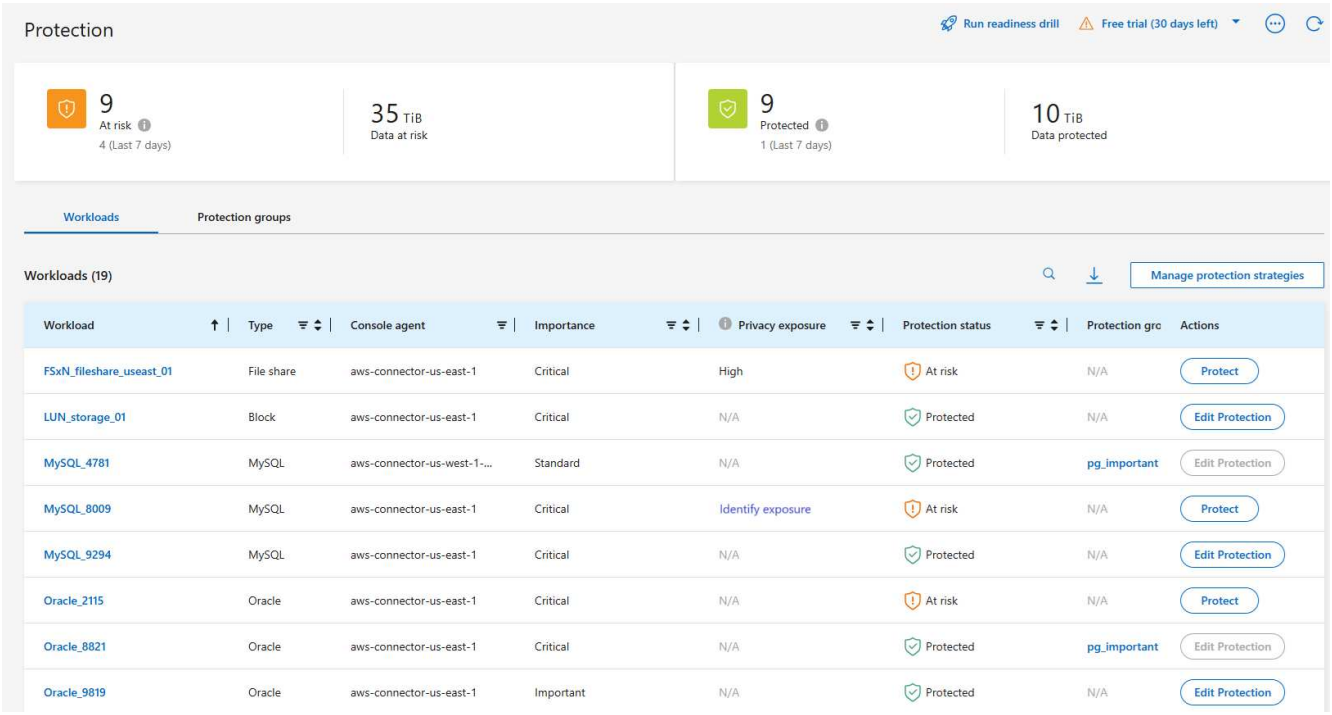
- "データ分類について学ぶ"
- "個人データのカテゴリ"
- "組織内に保存されているデータを調査する"

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

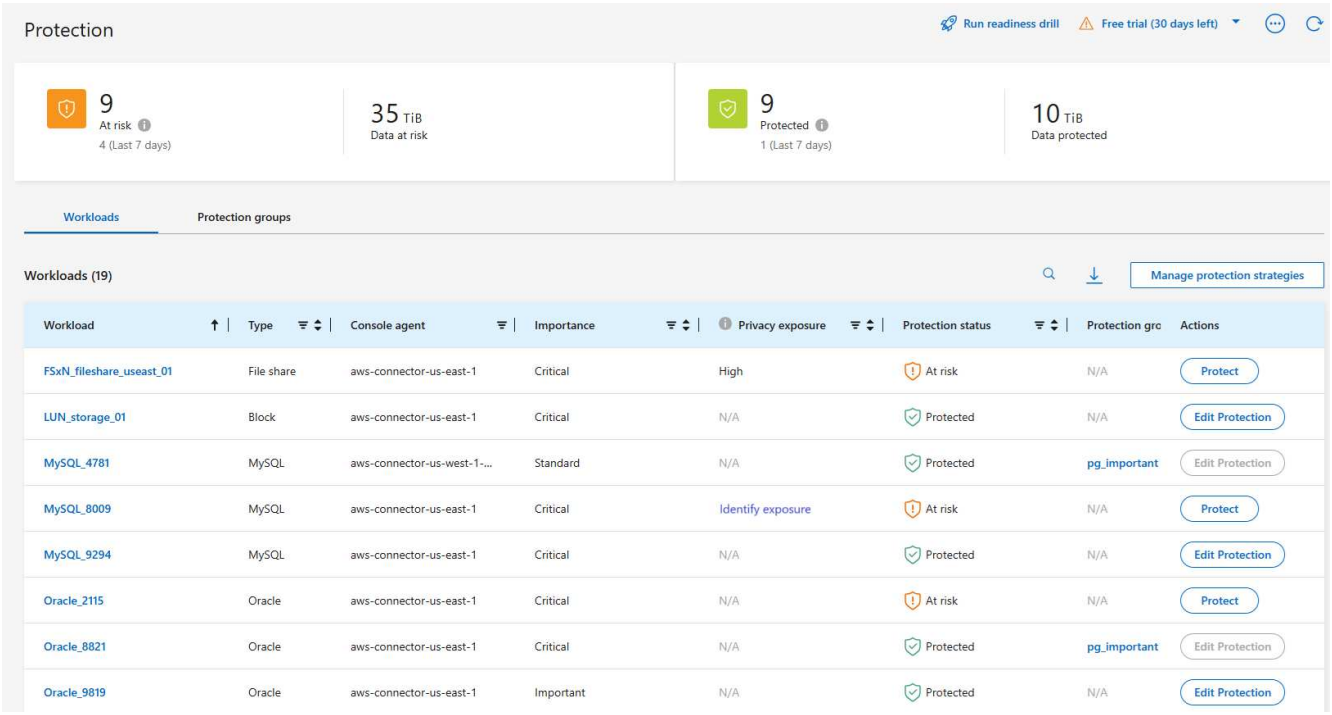
データ分類で PII をスキャンした後、リスクを評価します。

PII データは、次の 3 つの指定のいずれかに分類されます。

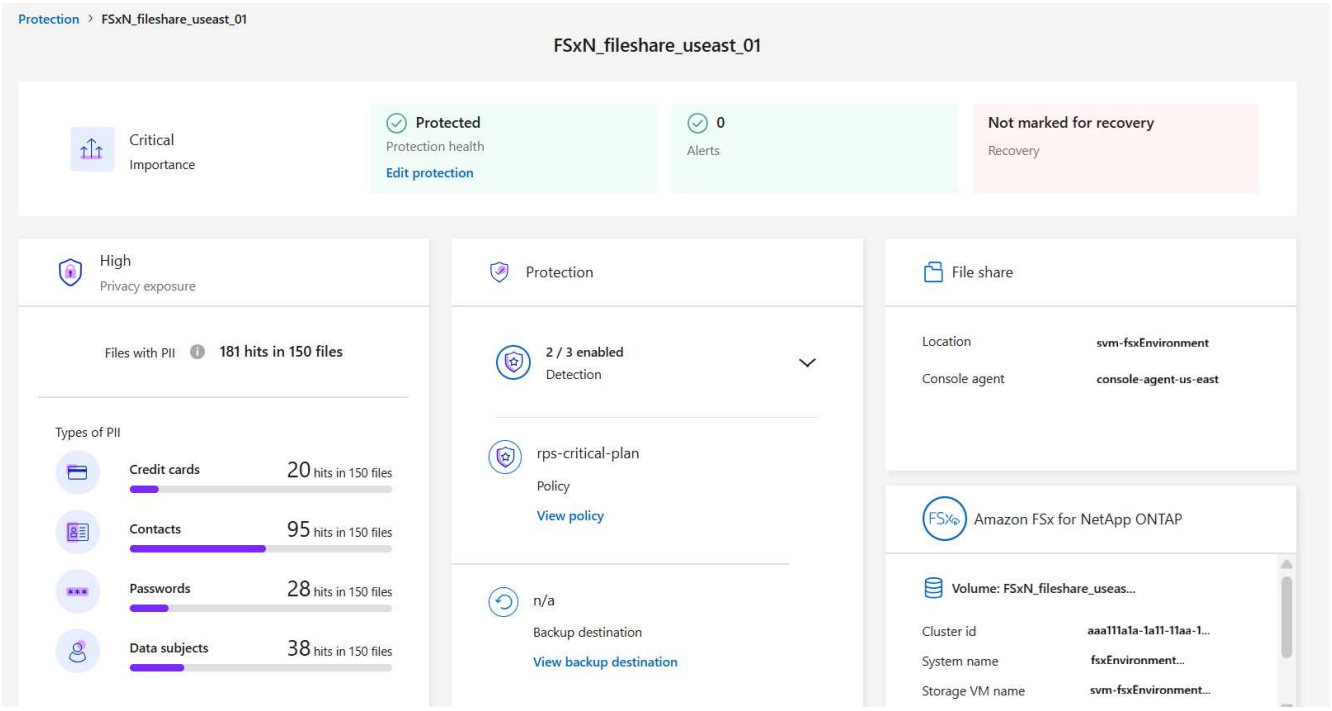
- 高: ファイルの 70% 以上に PII が含まれています
- 中: ファイルの 30% 以上 70% 未満に PII が含まれています
- 低: ファイルの 0% 以上 30% 未満に PII が含まれています

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"

NetApp Ransomware Resilience で検出されたランサムウェアアラートを処理する

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領域にアラートを表示します。 Ransomware Resilience は直ちにスナップショットを作成します。ランサムウェア耐性の アラート タブで潜在的なリスクを確認します。

Ransomware Resilience が攻撃の可能性を検出すると、コンソールの通知設定に通知が表示され、設定されたアドレスに電子メールが送信されます。電子メールには、重大度、影響を受けるワークロード、および Ransomware Resilience の アラート タブのアラートへのリンクに関する情報が含まれます。

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。

Ransomware Resilience は、アラートが発行された原因に関する次のような証拠と呼ばれる情報を提供します。

- 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
- 暗号化レベルが高く、ファイル拡張子を変更しない場合

アラートは次のいずれかに分類されます。

- 潜在的な攻撃: Autonomous Ransomware Protection が新しい拡張機能を検出し、その発生が過去 24 時間以内に 20 回以上繰り返された場合にアラートが発生します (デフォルトの動作)。
- 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に基づいてのみ行われます。

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" 。

アラートのステータスは次のいずれかになります。

- 新しい
- 非アクティブ

アラート インシデントの状態は次のいずれかになります。

- 新規: 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。
- 無視: 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「無視」に変更できます。

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。

- 却下中: インシデントは却下中です。
- 解決済み: インシデントは修正されました。
- 自動解決: 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。

設定ページで Ransomware Resilience にセキュリティおよびイベント管理システム (SIEM) を構成した場合、Ransomware Resilience はアラートの詳細を SIEM システムに送信します。

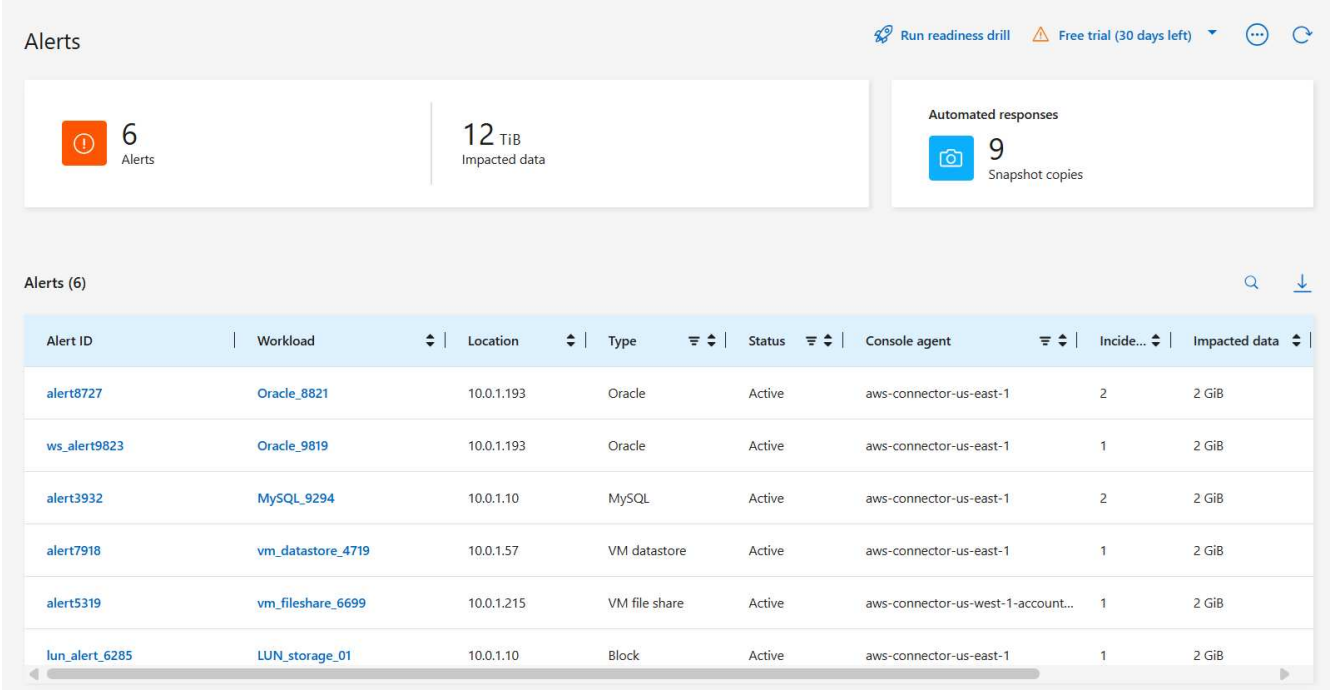
アラートを表示

アラートには、ランサムウェア耐性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。 "すべてのサービスに対するBlueXPのアクセスロールについて学ぶ" 。

手順

1. ランサムウェア耐性ダッシュボードで、[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、サブスクリプションの通知設定に基づいて、登録したユーザーに電子メール通知を送信します。電子メールには、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含まれています。

ランサムウェア耐性アラートの電子メール通知を受信できます。この機能を使用すると、アラート、その重大度、影響を受けるリソースに関する情報を常に把握できます。

メール通知を購読するには、 "メール通知設定を設定する" 。

1. Ransomware Resilience で、[設定] ページに移動します。
2. *通知*の下で、電子メール通知設定を見つけます。
3. アラートを受信するメールアドレスを入力します。
4. 変更を保存します。

新しいアラートが生成されると、電子メール通知が届くようになります。

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。"すべてのサービスに対するBlueXPのアクセス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」をクリックします。
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があるかどうかを確認できます。

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。"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" 。

*どのような詳細が表示されますか?*表示される詳細は、アラートがどのようにトリガーされたかによって異なります。

- ONTAPの Autonomous Ransomware Protection 機能によってトリガーされます。これは、ボリューム内のファイルの動作に基づいて悪意のあるアクティビティを検出します。
- Data Infrastructure Insightsワークロード セキュリティによってトリガーされます。これには、Data Infrastructure Insights Workload security のライセンスが必要であり、Ransomware Resilience でそれを有効にする必要があります。この機能は、ストレージ ワークロード内での異常なユーザー行動を検出し、そのユーザーによる今後のアクセスをブロックできるようにします。

  Ransomware Resilience でワークロード セキュリティを有効にするには、[設定] ページに移動し、[ワークロード セキュリティ接続] オプションを選択します。

  Data Infrastructure Insightsワークロードセキュリティの概要については、 "ワークロードセキュリティについて" 。

Data Infrastructure Workload Security のライセンスを所有しておらず、Ransomware Resilience で有効にしていない場合、異常なユーザー動作の情報は表示されません。

悪意のあるアクティビティが発生すると、アラートが生成され、自動スナップショットが取得されます。

Autonomous Ransomware Protection からの悪意のあるアクティビティのみを表示します

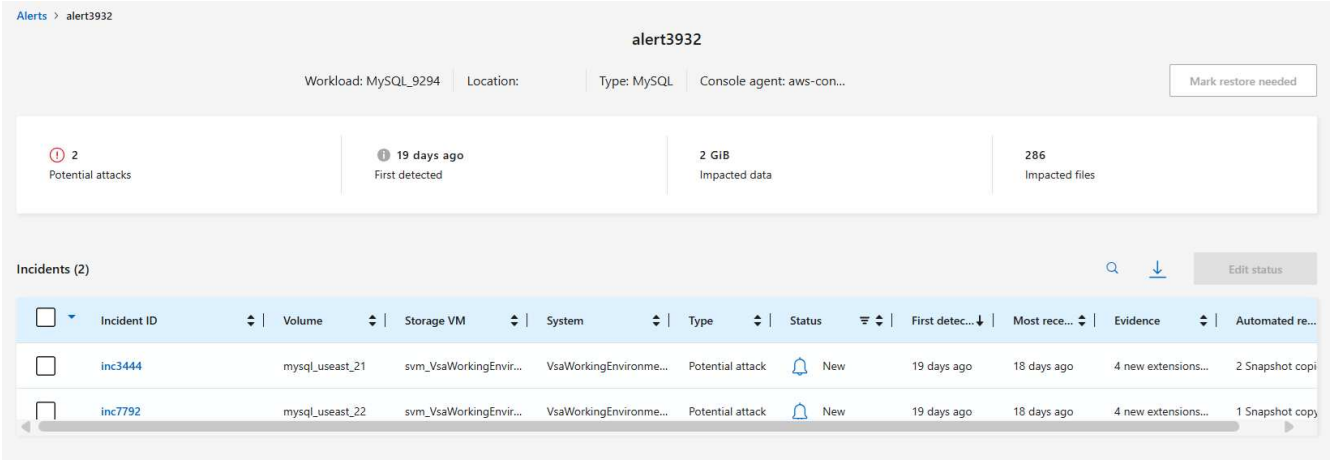
Autonomous Ransomware Protection が Ransomware Resilience でアラートをトリガーすると、次の詳細を表示できます。

- 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
- 影響を受けるファイルとディレクトリ

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。

Data Infrastructure Insightsワークロード セキュリティで異常なユーザー行動を表示する

Data Infrastructure Insights Workload security が Ransomware Resilience でアラートをトリガーした場合、疑わしいユーザーを表示し、ユーザーをブロックし、 Data Infrastructure Insights Workload security で直接ユーザー アクティビティを調査できます。

これらの機能は、Autonomous Ransomware Protection からのみ利用できる詳細情報に追加されるものです。

開始する前に

このオプションには、 Data Infrastructure Insights Workload security のライセンスが必要であり、Ransomware Resilience でそれを有効にする必要があります。

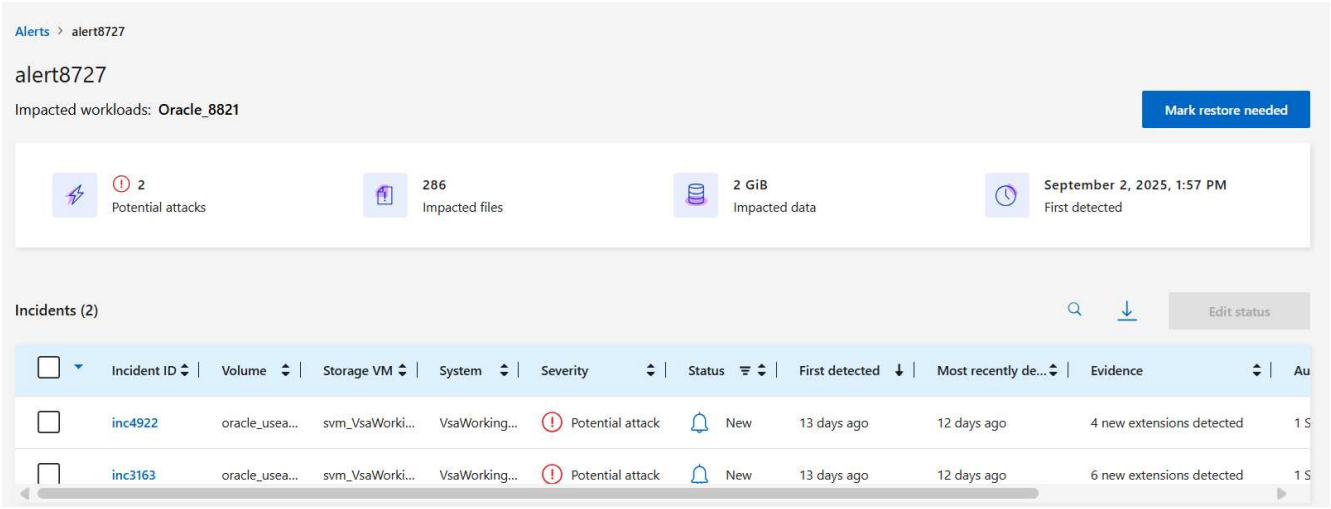
Ransomware Resilience でワークロード セキュリティを有効にするには、次の手順を実行します。

1. *設定*ページに移動します。
2. **Workload Security** 接続 オプションを選択します。

   詳細については、 "ランサムウェア耐性設定を構成する" 。

手順

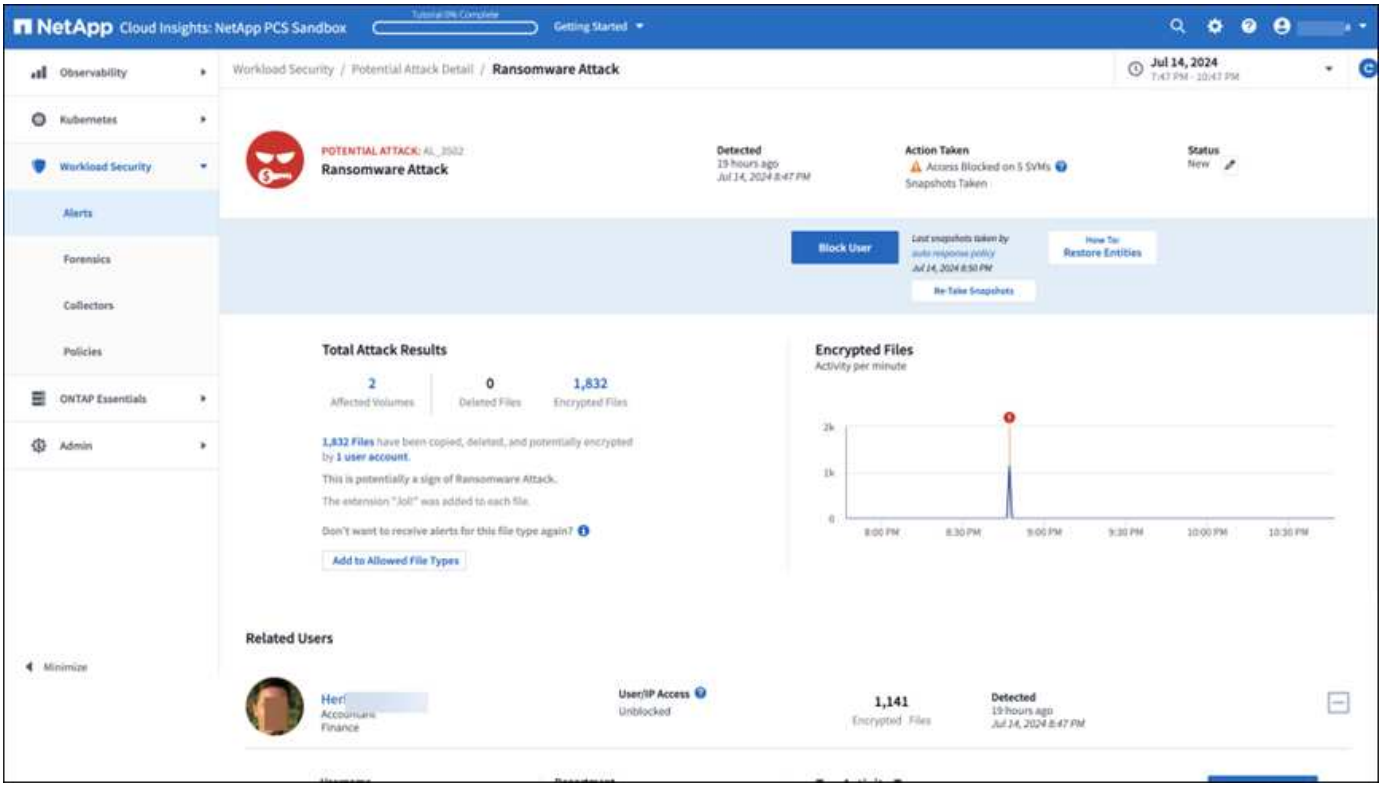
1. ランサムウェア耐性メニューから、*アラート*を選択します。
2. アラートを選択します。
3. アラート内のインシデントを確認します。



4. コンソールによって監視されている環境内で、疑わしいユーザーによるさらなるアクセスをブロックするには、[ユーザーをブロック] リンクを選択します。
5. アラートまたはアラート内のインシデントを調査します。
   a. Data Infrastructure Insights のワークロード セキュリティでアラートをさらに調査するには、ワークロード セキュリティで調査 リンクを選択します。
   b. 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。

Data Infrastructure Insights Workload Security が新しいタブで開きます。

+



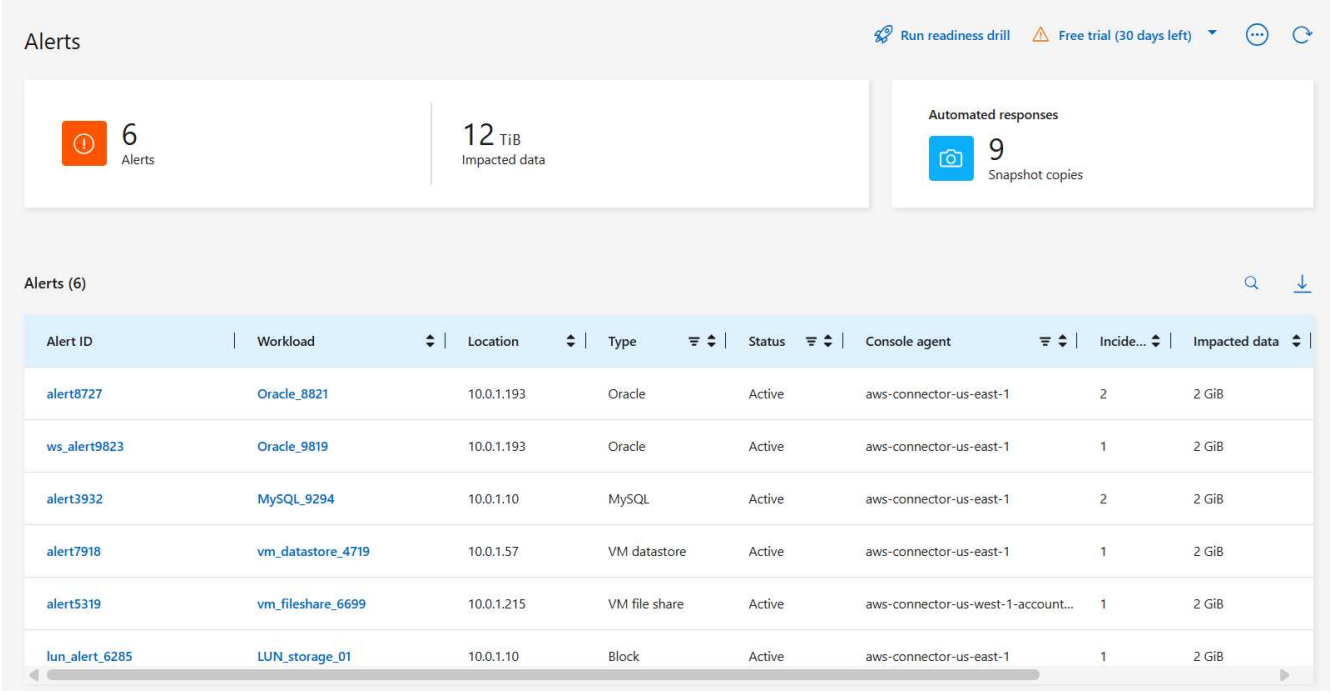
ランサムウェア インシデントを復旧準備完了としてマークする (インシデントが中和された後)

攻撃を阻止した後、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。

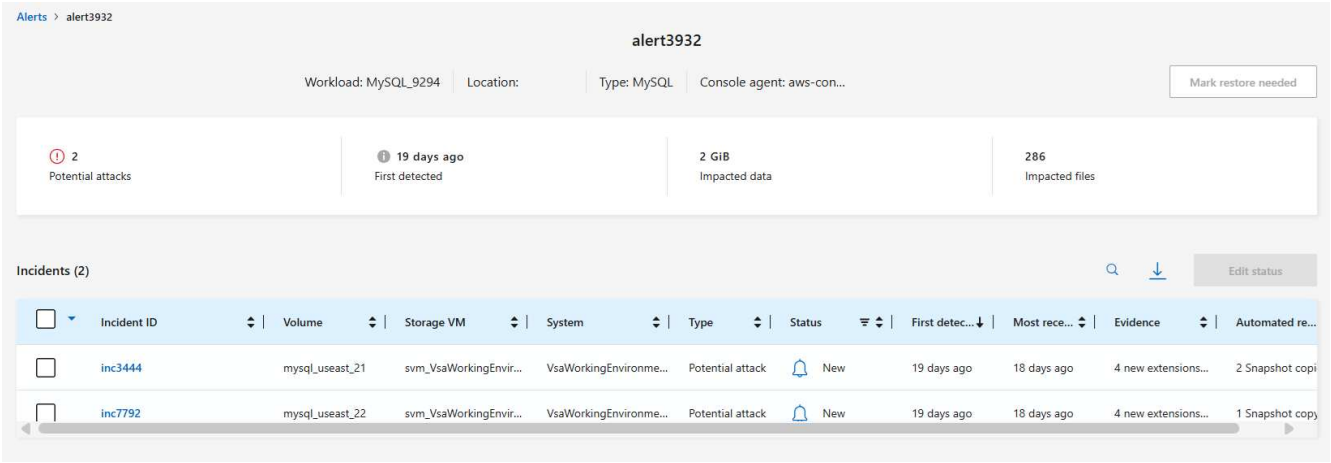
必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"すべてのサービスのコンソールアクセスロールについて学習します" 。

手順

1. 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。前述の条件が満たされない場合は、却下される可能性があります。

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。

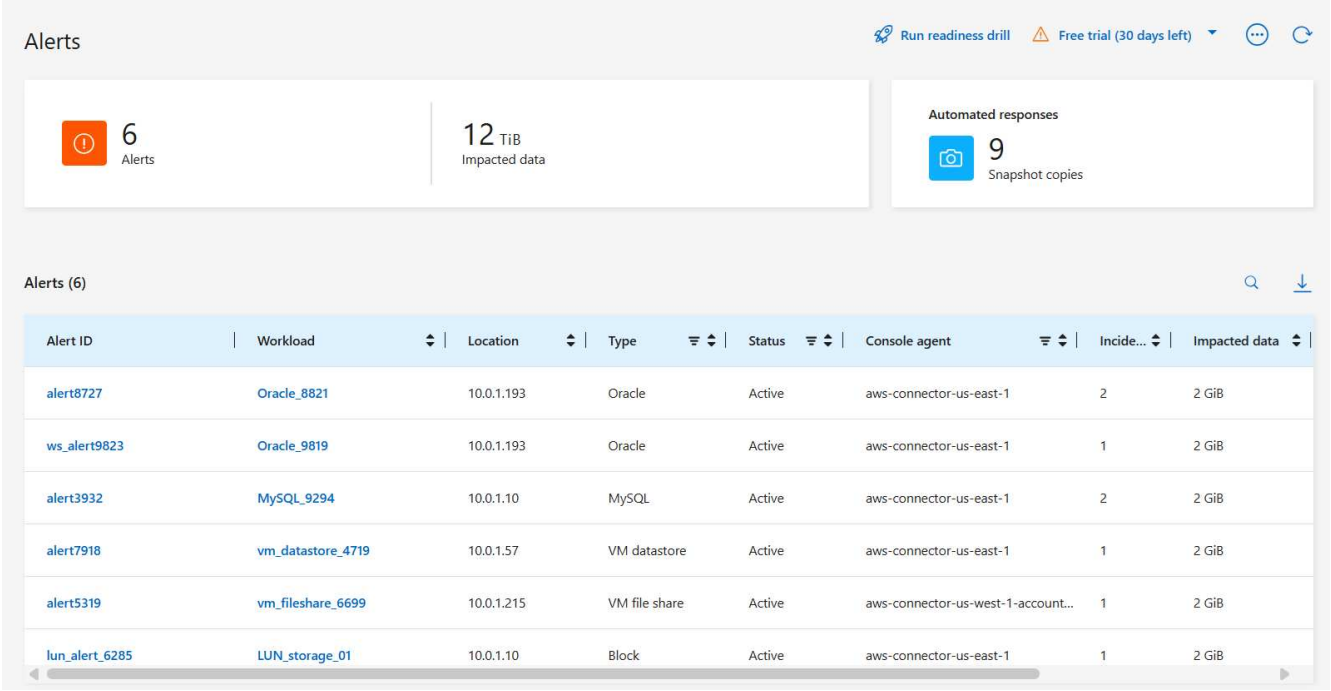
ワークロードを閉じると、潜在的なランサムウェア攻撃に応じて自動的に作成されたすべてのスナップショット コピーが完全に削除されます。

> アラートを無視した場合、そのステータスを他のステータスに戻すことはできず、この変更を元に戻すこともできません。

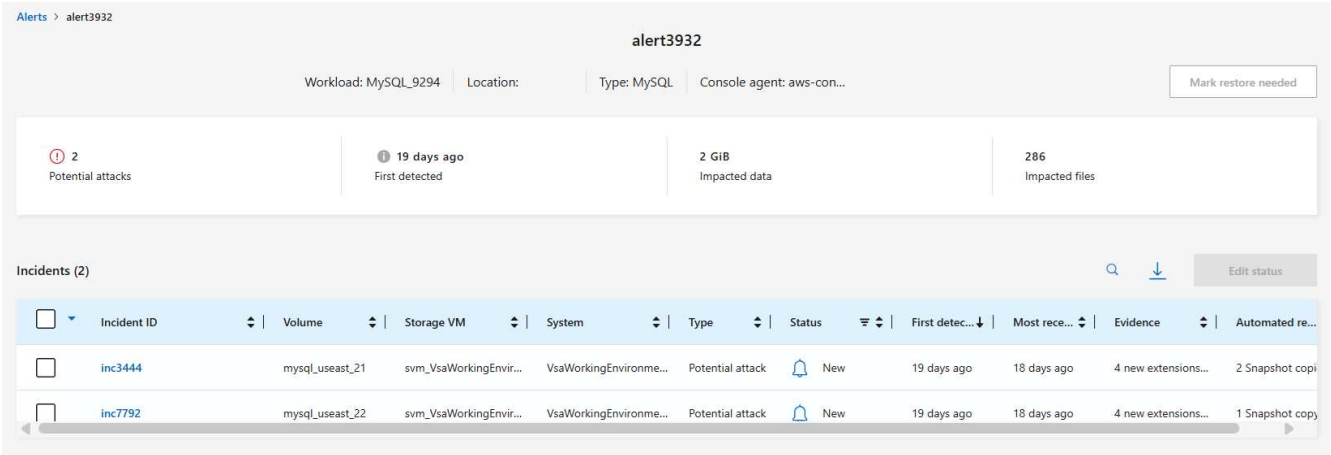
必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"すべてのサービスのコンソールアクセスロールについて学習します" 。

手順

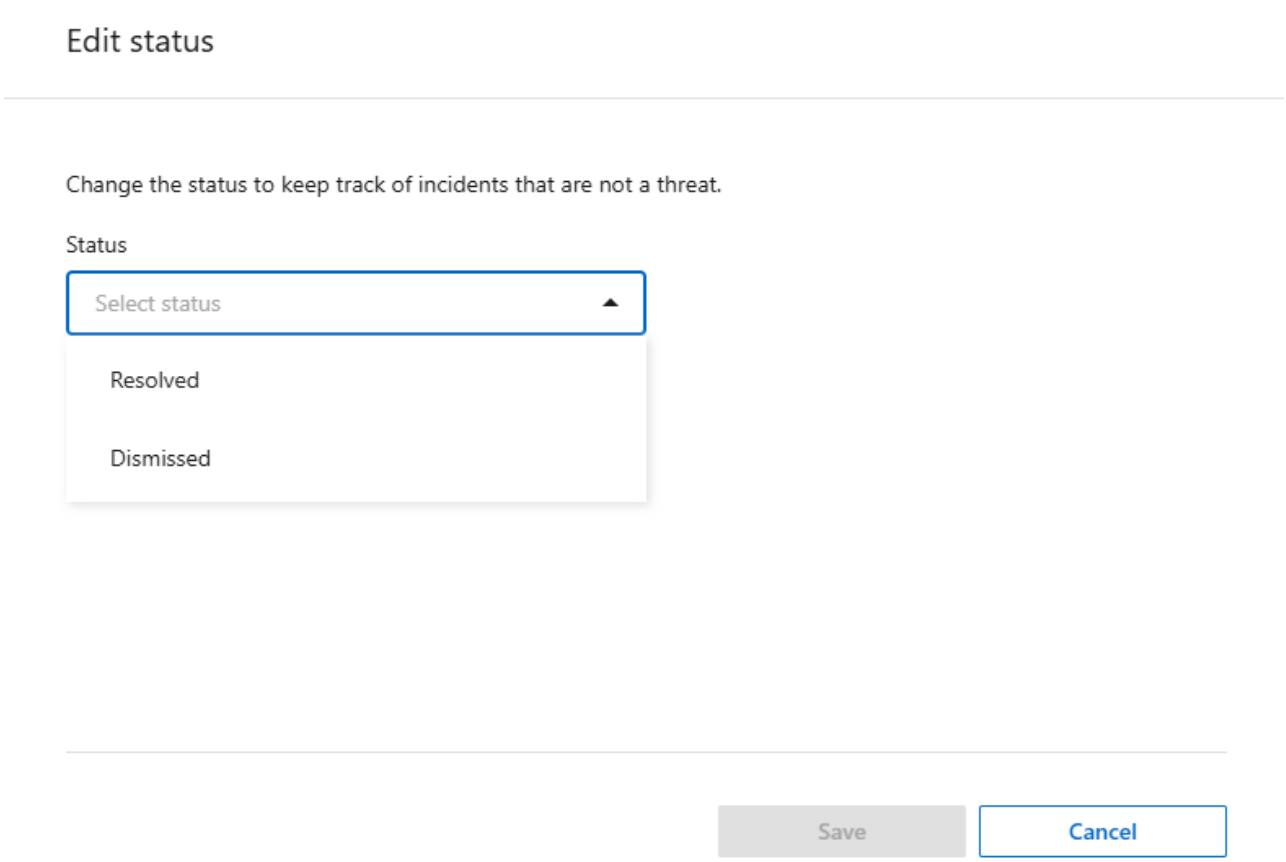
1. ランサムウェア耐性メニューから、*アラート*を選択します。



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。

   ワークロードに関する追加情報とスナップショット コピーが削除されたことが表示されます。

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。

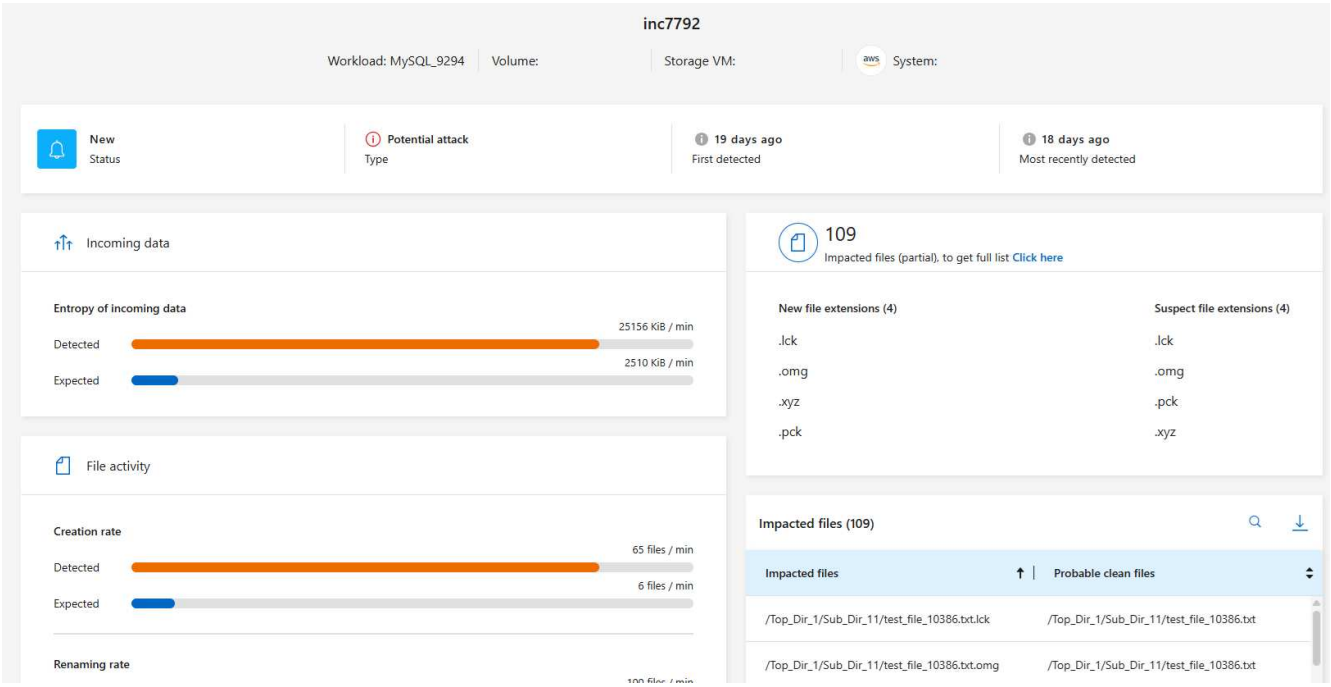
必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"すべてのサービスのコンソールアクセスロールについて学習します" 。

手順

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、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。

- アプリケーションまたは VM がSnapCenterによって管理されている場合、Ransomware Resilience は、アプリケーション整合性または VM 整合性プロセスを使用して、アプリケーションまたは VM を以前の状態と最後のトランザクションに復元します。アプリケーションまたは VM の整合性のある復元では、キャッシュまたは I/O 操作内のデータなど、ストレージに格納されなかったデータがボリューム内のデータに追加されます。

- アプリケーションまたは VM がSnapCenterによって管理されておらず、 NetApp Backup and Recovery または Ransomware Resilience によって管理されている場合、Ransomware Resilience はクラッシュ整合性復元を実行します。つまり、たとえばシステムがクラッシュした場合、同じ時点でボリューム内にあったすべてのデータが復元されます。

  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。

   [回復ページ]

SnapCenterによって管理される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。

復元が必要な場合、アプリケーションの状態は変更されます。バックアップに制御ファイルが含まれている場合、アプリケーションは制御ファイルから以前の状態に復元されます。復元が完了すると、アプリケーションは読み取り/書き込みモードで開きます。

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。"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. ランサムウェア耐性から*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: アプリケーション整合性 (または VM 用SnapCenterの場合、復元範囲は「VM ごと」)
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。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. 元の場所または代替の場所を選択します。
   b. システムを選択します。
   c. ストレージ VM を選択します。
8. 元の宛先にワークロードを復元するのに十分なスペースがない場合は、「一時ストレージ」行が表示されます。ワークロード データを復元するための一時ストレージを選択できます。復元されたデータは一時ストレージから元の場所にコピーされます。一時ストレージ行の*下矢印*をクリックし、宛先クラスター、ストレージ VM、およびローカル層を設定します。
9. *保存*を選択します。
10. *次へ*を選択します。
11. 選択内容を確認します。
12. *復元*を選択します。
13. 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。

SnapCenterで管理されていない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。"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" 。

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

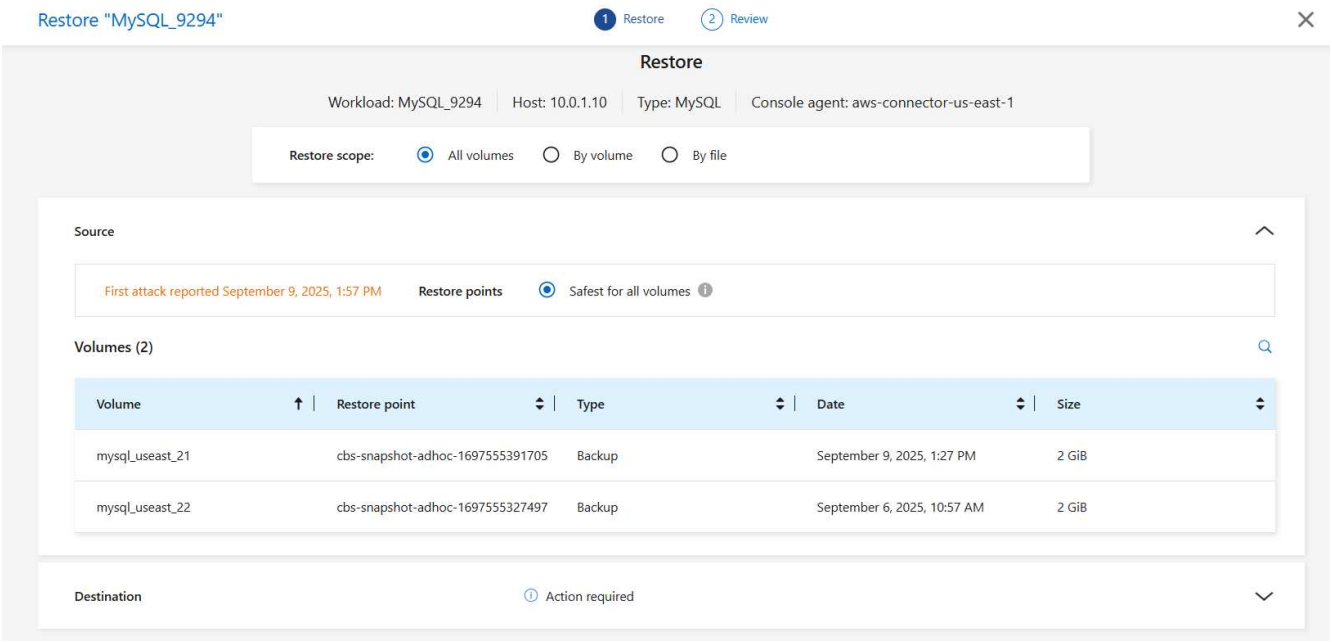
1. ランサムウェア耐性メニューから、「回復」を選択します。
2. 回復 ページでワークロード情報を確認します。
3. 「復元が必要」状態にあるワークロードを選択します。
4. 復元するには、[復元] を選択します。
5. 復元範囲: 実行する復元の種類を選択します。
   - 全巻
   - 量別
   - ファイル別: 復元するフォルダーまたは単一のファイルを指定できます。

   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。

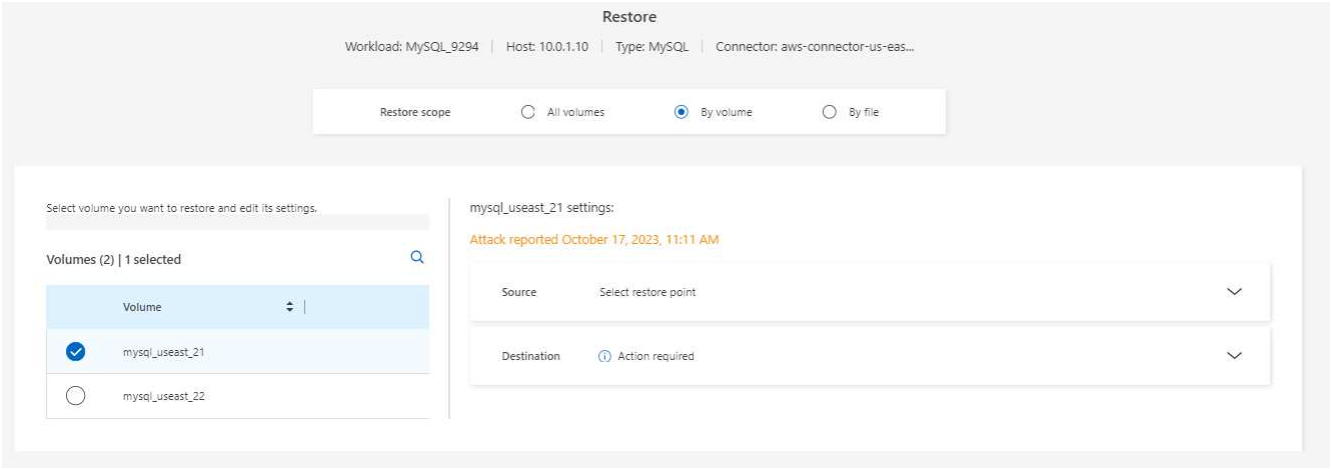
6. 目的地: 詳細を表示するには、目的地の横にある下矢印を選択します。
   a. システムを選択します。
   b. ストレージ VM を選択します。
   c. 集計を選択します。
   d. すべての新しいボリューム プレフィックスを変更します。

> 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。

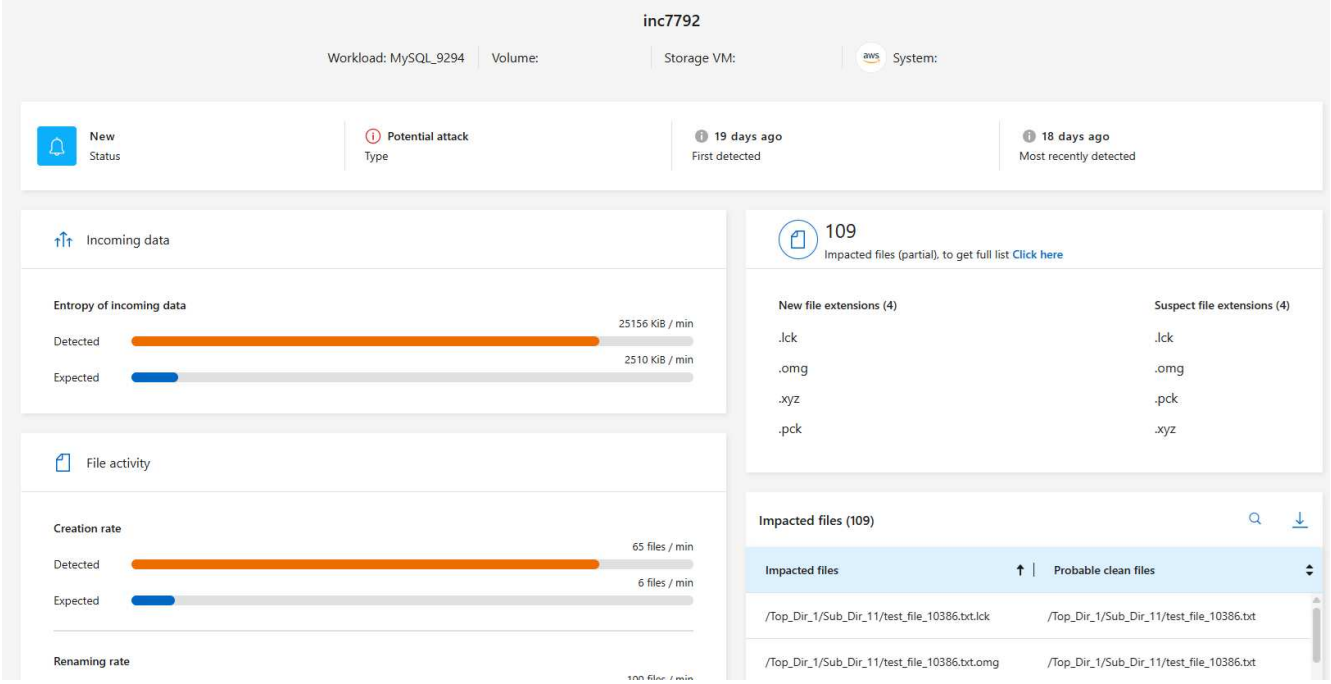
アプリケーション ワークロードをファイル レベルで同じシステムまたは別のシステムに復元できます。

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。



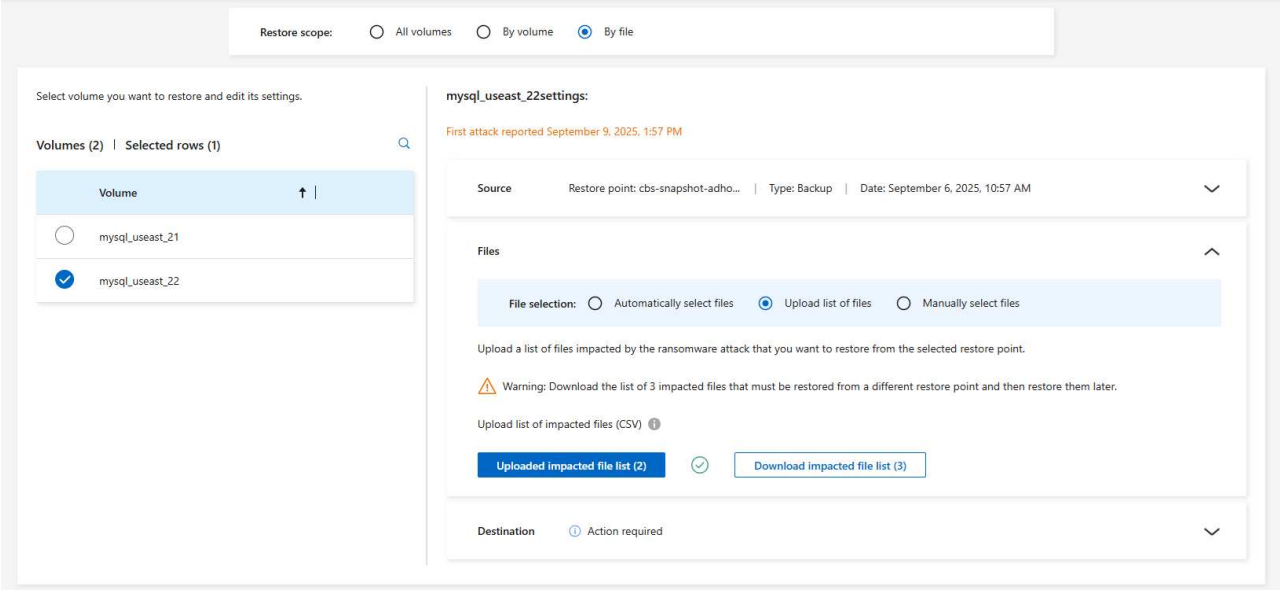
5. ファイルの完全なリストを表示するには、[影響を受けるファイル] ペインの上部にある [ここをクリック] を選択します。
6. そのインシデントについては、ダウンロード アイコンを選択し、影響を受けるファイルのリストを CSV 形式でダウンロードします。

これらのファイルを復元する手順

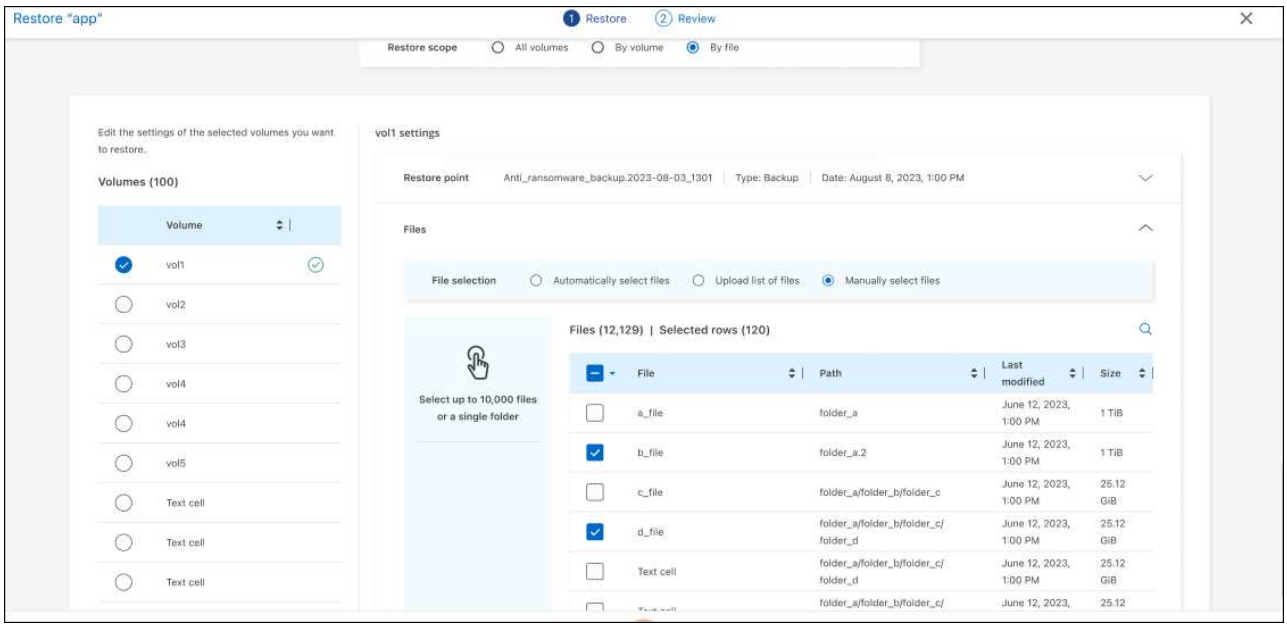
1. ランサムウェア耐性メニューから、「回復」を選択します。
2. 「復元が必要」状態にあるアプリケーション ワークロードを選択します。
3. 復元するには、[復元] を選択します。
4. [復元] ページの [復元範囲] で、[ファイル別] を選択します。
5. ボリュームのリストで、復元するファイルが含まれているボリュームを選択します。
6. 復元ポイント: 詳細を表示するには、*復元ポイント*の横にある下矢印を選択します。データを復元するために使用する復元ポイントを選択します。

> [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。

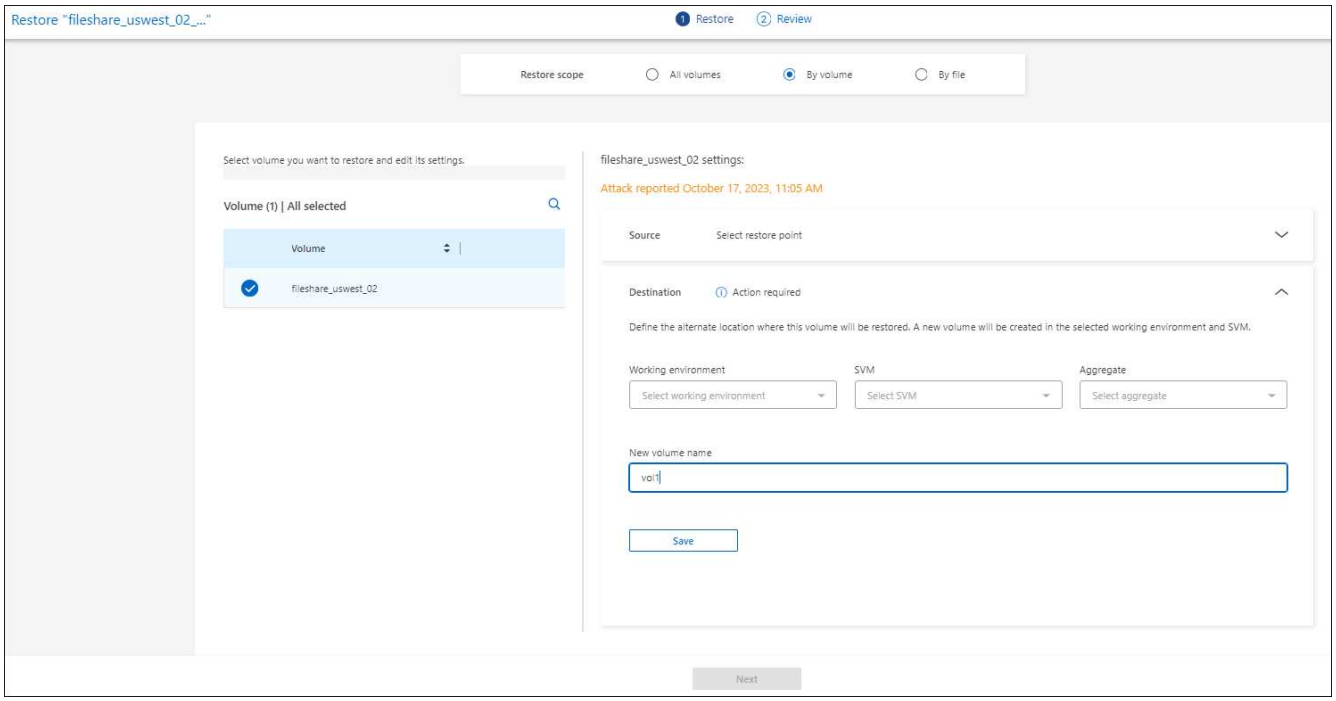
> 復元のパスを指定しない場合は、ファイルは最上位ディレクトリの新しいボリュームに復元されます。

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。

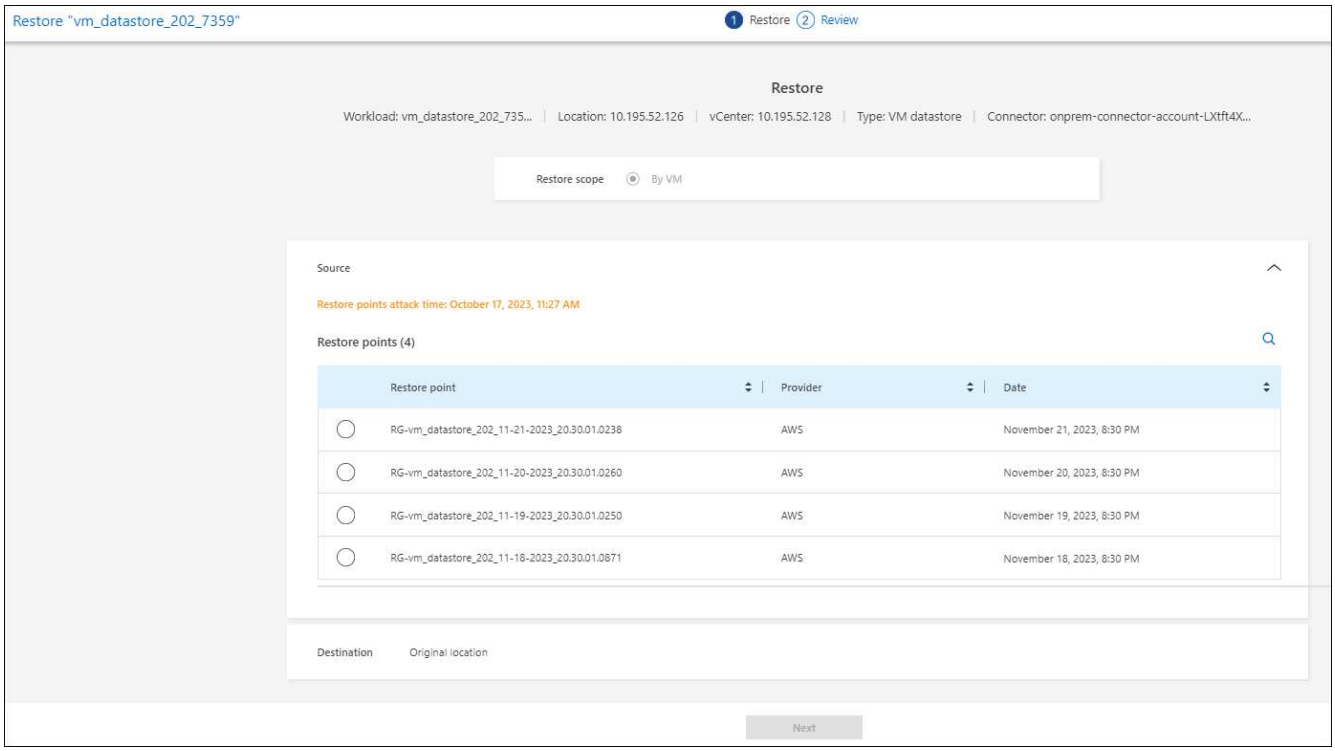
復元のパスを指定しない場合は、ファイルは最上位ディレクトリの新しいボリュームに復元されます。

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 のレポートをダウンロード

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

ファイルをダウンロードする前に、データを更新する必要があります。これにより、ファイルに表示されるデータも更新されます。

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。"すべてのサービスに対するBlueXPのアクセスロールについて学ぶ" 。

*ダウンロードできるデータは何ですか?*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。

- 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。

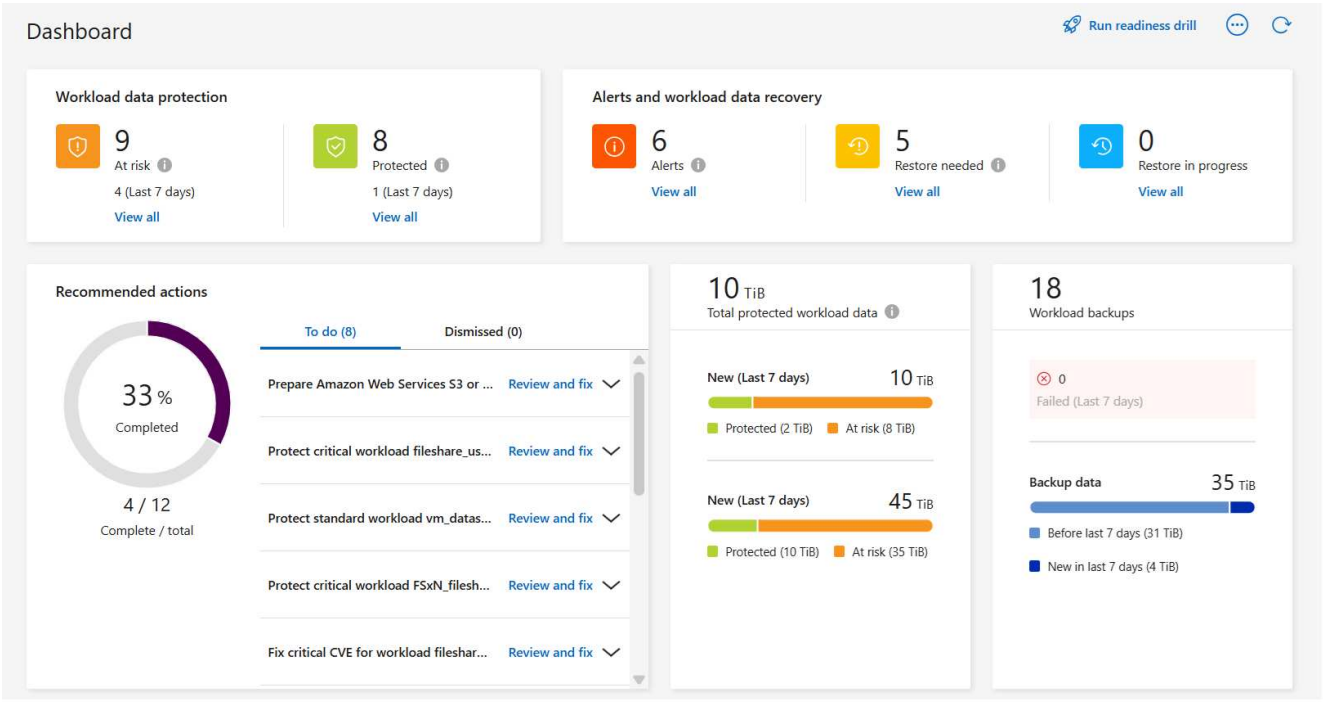
  準備ドリルレポートは、レポート ページからのみダウンロードできます。

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。

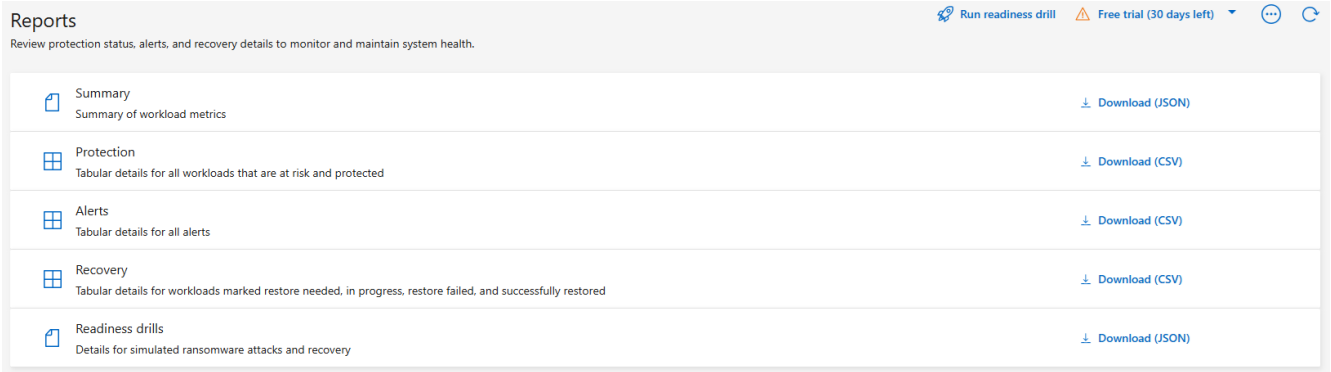
手順

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*更新*を選択します。 右上の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。



知識とサポート

サポートに登録する

BlueXPおよびそのストレージ ソリューションとサービスに固有のテクニカル サポートを受けるには、サポート登録が必要です。Cloud Volumes ONTAPシステムの主要なワークフローを有効にするには、サポート登録も必要です。

サポートに登録しても、クラウド プロバイダー ファイル サービスに対するNetAppサポートは有効になりません。クラウド プロバイダーのファイル サービス、そのインフラストラクチャ、またはサービスを使用するソリューションに関連するテクニカル サポートについては、その製品のBlueXPドキュメントの「ヘルプの取得」を参照してください。

- "Amazon FSx for ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

サポート登録の概要

サポート資格を有効にするには、次の 2 つの登録形式があります。

- BlueXPアカウントのシリアル番号を登録します (BlueXPのサポート リソース ページにある 20 桁の 960xxxxxxxxx シリアル番号)。

  これは、BlueXP内のすべてのサービスに対する単一のサポート サブスクリプション ID として機能します。各BlueXPアカウント レベルのサポート サブスクリプションを登録する必要があります。

- クラウド プロバイダーのマーケットプレイスで、サブスクリプションに関連付けられたCloud Volumes ONTAPシリアル番号を登録します (これらは 20 桁の 909201xxxxxxxx シリアル番号です)。

  これらのシリアル番号は一般に *PAYGO* シリアル番号 と呼ばれ、 Cloud Volumes ONTAP の展開時にBlueXPによって生成されます。

両方のタイプのシリアル番号を登録すると、サポート チケットの開設やケースの自動生成などの機能が有効になります。登録は、以下の説明に従ってNetAppサポート サイト (NSS) アカウントをBlueXPに追加することで完了します。

NetAppサポートのために**BlueXP**を登録する

サポートに登録し、サポート資格を有効にするには、 BlueXP組織 (またはアカウント) 内の 1 人のユーザーがNetAppサポート サイト アカウントをBlueXPログインに関連付ける必要があります。NetAppサポートに登録する方法は、 NetAppサポート サイト (NSS) アカウントをすでにお持ちかどうかによって異なります。

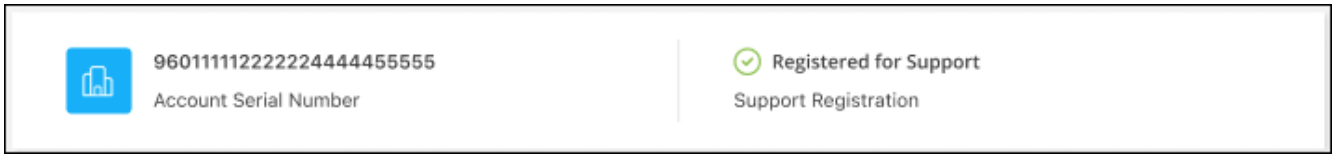
NSSアカウントをお持ちの既存顧客

NSS アカウントをお持ちのNetApp のお客様の場合は、 BlueXPを通じてサポートに登録するだけです。

手順

1. BlueXPコンソールの右上にある設定アイコンを選択し、*資格情報*を選択します。
2. *ユーザー資格情報*を選択します。
3. **NSS** 資格情報の追加 を選択し、 NetAppサポート サイト (NSS) の認証プロンプトに従います。
4. 登録プロセスが成功したことを確認するには、[ヘルプ] アイコンを選択し、[サポート] を選択します。

   リソース ページには、 BlueXP組織がサポートに登録されていることが表示されます。



   他のBlueXPユーザーは、 NetAppサポート サイト アカウントをBlueXPログインに関連付けていない場合、同じサポート登録ステータスを表示しないことに注意してください。ただし、これはBlueXP組織がサポートに登録されていないことを意味するものではありません。組織内の 1 人のユーザーがこれらの手順を実行すれば、組織は登録されます。

既存の顧客だが**NSS**アカウントがない

既存のNetApp顧客であり、既存のライセンスとシリアル番号を持っているものの、NSS アカウントを持っていない場合は、NSS アカウントを作成し、それをBlueXPログインに関連付ける必要があります。

手順

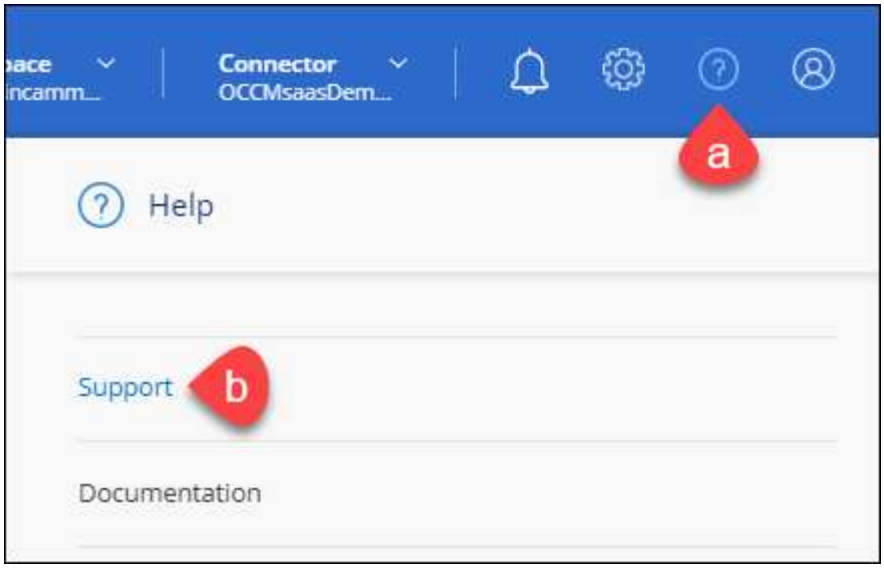
1. NetAppサポートサイトのアカウントを作成するには、 "NetAppサポートサイト ユーザー登録フォーム"
   a. 適切なユーザー レベル (通常は * NetApp顧客/エンド ユーザー*) を選択してください。
   b. 上記で使用したBlueXPアカウントのシリアル番号 (960xxxx) を必ずシリアル番号フィールドにコピーしてください。これにより、アカウント処理が高速化されます。
2. 以下の手順を完了して、新しいNSSアカウントをBlueXPログインに関連付けます。NSSアカウントをお持ちの既存顧客 。

NetAppの新着情報

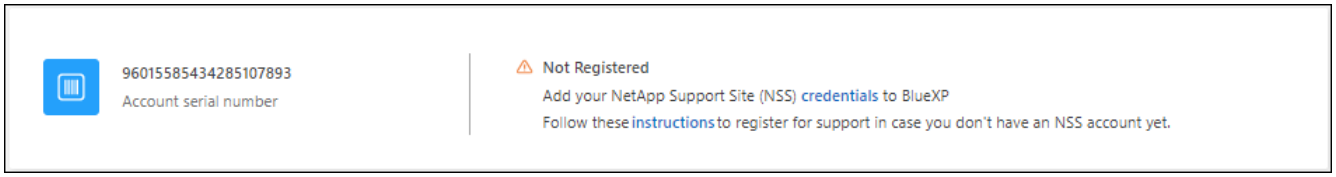
NetAppを初めて使用し、NSS アカウントをお持ちでない場合は、以下の手順に従ってください。

手順

1. BlueXPコンソールの右上にあるヘルプ アイコンを選択し、サポート を選択します。



2. サポート登録ページからアカウント ID シリアル番号を見つけます。



3. 移動先 "NetAppのサポート登録サイト"私は登録済みの**NetApp**顧客ではありません を選択します。
4. 必須フィールド（赤いアスタリスクが付いているフィールド）に入力します。
5. 製品ライン フィールドで、**Cloud Manager** を選択し、該当する請求プロバイダーを選択します。
6. 上記の手順 2 からアカウントのシリアル番号をコピーし、セキュリティ チェックを完了して、NetApp のグローバル データ プライバシー ポリシーを読んだことを確認します。

   この安全な取引を完了するために、指定されたメールボックスに電子メールが直ちに送信されます。検証メールが数分以内に届かない場合は、必ずスパム フォルダーを確認してください。

7. メール内からアクションを確認します。

   確認すると、リクエストがNetAppに送信され、 NetAppサポート サイトのアカウントを作成することが推奨されます。

8. NetAppサポートサイトのアカウントを作成するには、 "NetAppサポートサイト ユーザー登録フォーム"
   a. 適切なユーザー レベル (通常は * NetApp顧客/エンド ユーザー*) を選択してください。
   b. 上記で使用したアカウントのシリアル番号 (960xxxx) を必ずシリアル番号フィールドにコピーしてください。これにより処理速度が向上します。

終了後の操作

このプロセス中に、 NetAppから連絡が来るはずです。これは、新規ユーザー向けの 1 回限りのオンボーディング演習です。

NetAppサポートサイトのアカウントを取得したら、以下の手順を実行してアカウントをBlueXPログインに関連付けます。NSSアカウントをお持ちの既存顧客 。

Cloud Volumes ONTAPサポートに NSS 認証情報を関連付ける

Cloud Volumes ONTAPの次の主要なワークフローを有効にするには、 NetAppサポート サイトの認証情報をBlueXP組織に関連付ける必要があります。

- 従量課金制のCloud Volumes ONTAPシステムをサポート対象として登録する

  システムのサポートを有効にし、 NetAppテクニカル サポート リソースにアクセスするには、NSS アカウントを提供する必要があります。

- BYOL（個人ライセンス使用）時にCloud Volumes ONTAP を導入する

  BlueXP がライセンス キーをアップロードし、購入した期間のサブスクリプションを有効にするには、NSS アカウントを提供する必要があります。これには、期間更新の自動更新が含まれます。

- Cloud Volumes ONTAPソフトウェアを最新リリースにアップグレードする

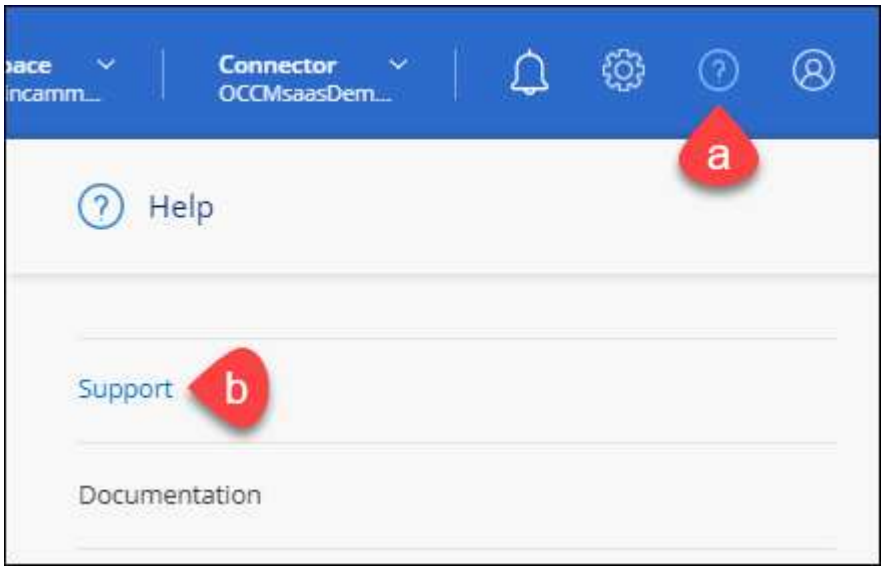
NSS 資格情報をBlueXP組織に関連付けることは、 BlueXPユーザー ログインに関連付けられている NSS アカウントとは異なります。

これらの NSS 資格情報は、特定のBlueXP組織 ID に関連付けられています。BlueXP組織に属するユーザーは、サポート **> NSS** 管理 からこれらの資格情報にアクセスできます。

- 顧客レベルのアカウントをお持ちの場合は、1 つ以上の NSS アカウントを追加できます。
- パートナー アカウントまたは再販業者アカウントをお持ちの場合は、1 つ以上の NSS アカウントを追加できますが、顧客レベルのアカウントと一緒に追加することはできません。

手順

1. BlueXPコンソールの右上にあるヘルプ アイコンを選択し、サポート を選択します。



2. *NSS管理 > NSSアカウントの追加*を選択します。
3. プロンプトが表示されたら、[続行] を選択して、Microsoft ログイン ページにリダイレクトします。

   NetApp は、サポートとライセンスに固有の認証サービスの ID プロバイダーとして Microsoft Entra ID を使用します。

4. ログイン ページで、 NetAppサポート サイトに登録した電子メール アドレスとパスワードを入力して、認証プロセスを実行します。

   これらのアクションにより、 BlueXP はライセンスのダウンロード、ソフトウェア アップグレードの検証、将来のサポート登録などに NSS アカウントを使用できるようになります。

   次の点に注意してください。

   - NSS アカウントは顧客レベルのアカウントである必要があります (ゲスト アカウントや一時アカウントではありません)。顧客レベルの NSS アカウントを複数持つことができます。
   - パートナー レベルのアカウントの場合、NSS アカウントは 1 つだけ存在できます。顧客レベルの NSS アカウントを追加しようとしたときにパートナー レベルのアカウントが存在する場合は、次のエラー メッセージが表示されます。

     「異なるタイプの NSS ユーザーがすでに存在するため、このアカウントでは NSS 顧客タイプは許可されません。」

   既存の顧客レベルの NSS アカウントがあり、パートナー レベルのアカウントを追加しようとする場合も同様です。

   - ログインが成功すると、 NetApp はNSS ユーザー名を保存します。

     これは、メールにマッピングされるシステム生成の ID です。*NSS管理*ページでは、 ••• メニュー。

   - ログイン認証トークンを更新する必要がある場合は、 ••• メニュー。

     このオプションを使用すると、再度ログインするよう求められます。これらのアカウントのトークンは 90 日後に期限切れになることに注意してください。これを知らせる通知が投稿されます。

ヘルプを受ける

NetAppは、 BlueXPとそのクラウドサービスに対して、様々なサポートを提供しています。ナレッジベース（KB）記事やコミュニティフォーラムなど、充実した無料のセルフサポートオプションを24時間365日ご利用いただけます。サポート登録には、Webチケットによるリモートテクニカルサポートも含まれます。

クラウドプロバイダーのファイルサービスのサポートを受ける

クラウド プロバイダーのファイル サービス、そのインフラストラクチャ、またはサービスを使用するソリューションに関連するテクニカル サポートについては、その製品のBlueXPドキュメントの「ヘルプの取得」を参照してください。

- "Amazon FSx for ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

BlueXPとそのストレージ ソリューションおよびサービスに固有のテクニカル サポートを受けるには、以下に説明するサポート オプションを使用してください。

セルフサポートオプションを使用する

以下のオプションは、24 時間 365 日無料でご利用いただけます。

- ドキュメント

  現在表示しているBlueXPドキュメント。

- "ナレッジベース"

  BlueXPナレッジベースを検索して、問題のトラブルシューティングに役立つ記事を見つけます。

- "コミュニティ"

  BlueXPコミュニティに参加して、進行中のディスカッションをフォローしたり、新しいディスカッションを作成したりしてください。

NetAppサポートでケースを作成する

上記のセルフ サポート オプションに加えて、サポートを有効にした後は、 NetAppサポート スペシャリストと協力して問題を解決することもできます。

始める前に

- *ケースの作成*機能を使用するには、まずNetAppサポート サイトの資格情報をBlueXPログインに関連付ける必要があります。 "BlueXPログインに関連付けられた資格情報を管理する方法を学びます" 。
- シリアル番号を持つONTAPシステムのケースを開く場合は、NSS アカウントがそのシステムのシリアル番号に関連付けられている必要があります。

手順

1. BlueXPで、*ヘルプ > サポート*を選択します。
2. *リソース*ページで、テクニカル サポートの下にある利用可能なオプションのいずれかを選択します。

   a. 電話で誰かと話したい場合は、「電話する」を選択してください。電話をかけることができる電話番号をリストした netapp.com のページに移動します。

   b. NetAppサポート スペシャリストとのチケットを開くには、[ケースを作成] を選択します。

      - サービス: 問題が関連付けられているサービスを選択します。たとえば、サービス内のワークフローまたは機能に関するテクニカル サポートの問題に固有の場合はBlueXP。
      - 作業環境: ストレージに該当する場合は、* Cloud Volumes ONTAP* または * On-Prem* を選択し、関連する作業環境を選択します。

        作業環境のリストは、サービスのトップバナーで選択したBlueXP組織 (またはアカウント)、プロジェクト (またはワークスペース)、およびコネクタの範囲内にあります。

      - ケースの優先度: ケースの優先度 (低、中、高、重大) を選択します。

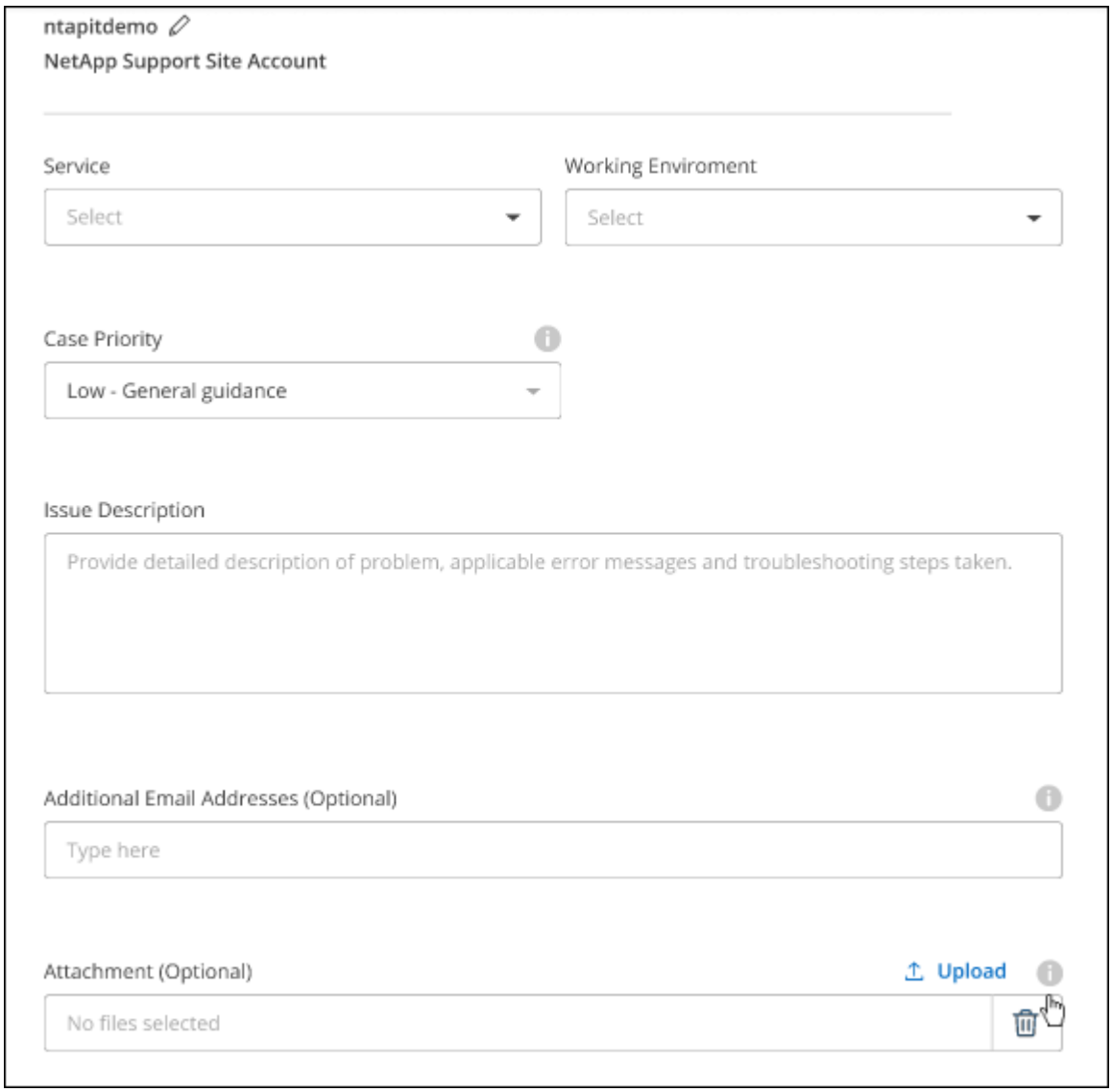
        これらの優先順位の詳細を確認するには、フィールド名の横にある情報アイコンの上にマウスを置きます。

      - 問題の説明: 該当するエラー メッセージや実行したトラブルシューティング手順など、問題の詳細

な説明を入力します。

- 追加のメールアドレス:この問題を他の人に知らせたい場合は、追加のメールアドレスを入力してください。
- 添付ファイル (オプション): 一度に 1 つずつ、最大 5 つの添付ファイルをアップロードします。

  添付ファイルはファイルごとに 25 MB までに制限されます。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、csv です。



終了後の操作

サポート ケース番号を示すポップアップが表示されます。NetAppサポート スペシャリストがお客様のケースを確認し、すぐにご連絡いたします。

サポート ケースの履歴については、設定 > タイムライン を選択し、「サポート ケースの作成」というアクションを探します。右端のボタンを使用すると、アクションを展開して詳細を表示できます。

ケースを作成しようとすると、次のエラー メッセージが表示される場合があります。

「選択したサービスに対してケースを作成する権限がありません」

このエラーは、NSS アカウントとそれに関連付けられているレコード会社が、 BlueXPアカウントのシリアル番号のレコード会社と同じではないことを意味している可能性があります (つまり、960xxxx) または作業環境のシリアル番号。次のいずれかのオプションを使用してサポートを求めることができます。

- 製品内チャットを使用する
- 非技術的なケースを提出する https://mysupport.netapp.com/site/help

サポートケースを管理する（プレビュー）

アクティブおよび解決済みのサポート ケースをBlueXPから直接表示および管理できます。NSS アカウントおよび会社に関連付けられたケースを管理できます。

ケース管理はプレビューとして利用できます。今後のリリースでは、このエクスペリエンスを改良し、機能強化を追加する予定です。製品内チャットを使用してフィードバックをお送りください。

次の点に注意してください。

- ページ上部のケース管理ダッシュボードには、次の 2 つのビューがあります。
  - 左側のビューには、指定したユーザー NSS アカウントによって過去 3 か月間に開かれたケースの合計が表示されます。
  - 右側のビューには、ユーザーの NSS アカウントに基づいて、会社レベルで過去 3 か月間に開かれたケースの合計が表示されます。

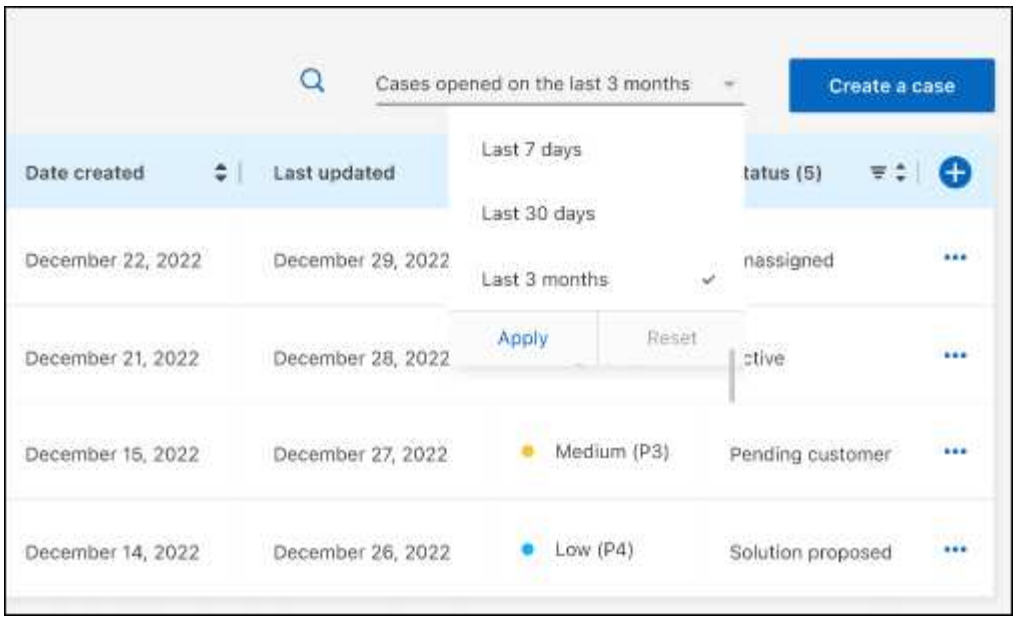
  表の結果には、選択したビューに関連するケースが反映されます。
- 関心のある列を追加または削除したり、優先度やステータスなどの列の内容をフィルタリングしたりできます。その他の列は並べ替え機能のみを提供します。

  詳細については、以下の手順をご覧ください。
- ケースごとに、ケースメモを更新したり、まだ「クローズ」または「クローズ保留中」ステータスになっていないケースをクローズしたりする機能を提供します。

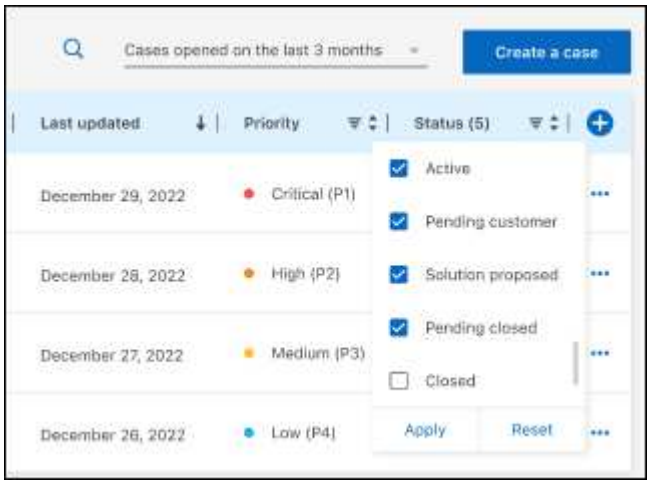
手順

1. BlueXPで、*ヘルプ > サポート*を選択します。
2. *ケース管理*を選択し、プロンプトが表示されたら、NSS アカウントをBlueXPに追加します。

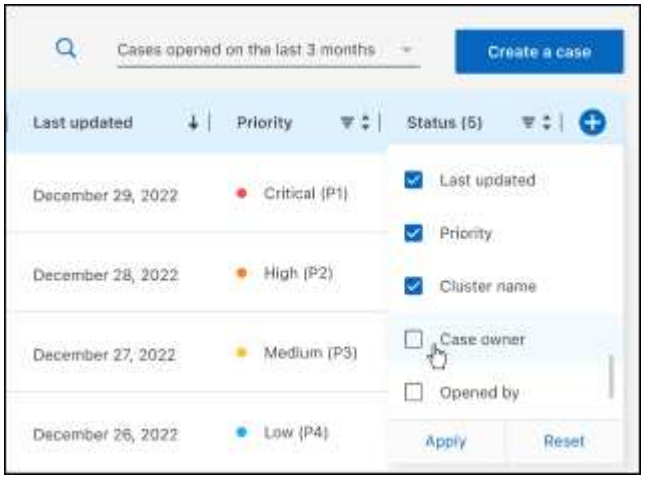
   ケース管理 ページには、 BlueXPユーザー アカウントに関連付けられている NSS アカウントに関連するオープン ケースが表示されます。これは、**NSS** 管理 ページの上部に表示される NSS アカウントと同じです。
3. 必要に応じて、テーブルに表示される情報を変更します。
   - *組織のケース*の下で*表示*を選択すると、会社に関連付けられているすべてのケースが表示されます。
   - 正確な日付範囲を選択するか、別の期間を選択して日付範囲を変更します。



◦ 列の内容をフィルタリングします。



◦ 表に表示される列を変更するには、＋次に、表示する列を選択します。

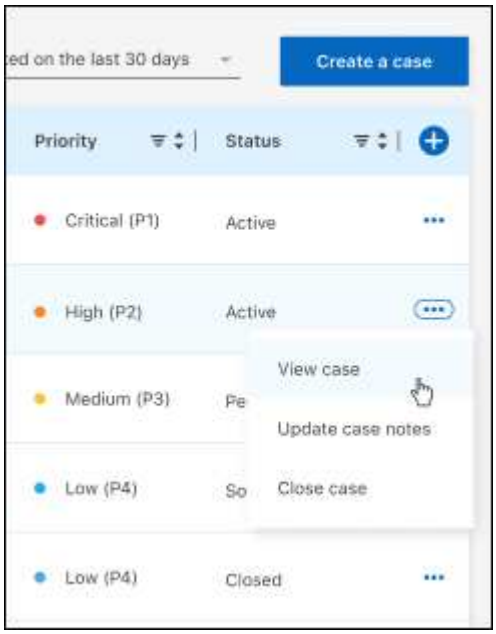


4. 既存のケースを管理するには、•••利用可能なオプションのいずれかを選択します。

- ケースを表示: 特定のケースに関する詳細をすべて表示します。
- ケースノートを更新: 問題に関する追加の詳細を入力するか、*ファイルのアップロード*を選択して最大 5 つのファイルを添付します。

  添付ファイルはファイルごとに 25 MB までに制限されます。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、csv です。

- ケースを閉じる: ケースを閉じる理由の詳細を入力し、[ケースを閉じる] を選択します。



NetAppランサムウェア耐性に関するよくある質問

この FAQ は、 NetApp Ransomware Resilience に関する質問への簡単な回答を探している場合に役立ちます。

導入

Ransomware Resilience を使用するにはライセンスが必要ですか**?**

次のライセンス タイプを使用できます。

- 30 日間の無料トライアルにサインアップしてください。
- Amazon Web Services (AWS) Marketplace、Google Cloud Marketplace、Microsoft Azure Marketplace で、 NetApp Intelligent Services および Ransomware Resilience の従量課金制 (PAYGO) サブスクリプションを購入します。
- BYOL (Bring Your Own License) は、 NetApp の営業担当者から取得したNetAppライセンス ファイル (NLF) です。ライセンス シリアル番号を使用して、コンソールのライセンスとサブスクリプション セクションで BYOL をアクティブ化できます。

*ランサムウェア耐性を有効にするにはどうすればいいですか?*ランサムウェア耐性には有効化は必要ありません。 NetAppコンソールから Ransomware Resilience にアクセスできます。

開始するには、サインアップするか、 NetApp の営業担当者に連絡してこのサービスを試す必要があります。その後、コンソール エージェントを使用すると、ランサムウェア耐性のための適切な機能が含まれるようになります。

Ransomware Resilience を開始するには、最初のランディング ページから [ワークロードの検出を開始する] を選択します。

*Ransomware Resilience は、標準モード、制限モード、プライベートモードで利用できますか?*現時点では、ランサムウェア耐性は標準モードでのみ利用可能です。今後もご期待ください。

NetAppデータサービス全体にわたるこれらのモードの説明については、 "NetAppコンソールの展開モード" 。

アクセス

*ランサムウェア耐性 URL とは何ですか?*ブラウザで次のように入力します "https://console.netapp.com/ransomware-resilience"コンソールにアクセスします。

*アクセス権限はどのように処理されますか?*https://docs.netapp.com/us-en/bluexp-setup-admin/reference-iam-predefined-roles.html["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"^] 。

*どのデバイスの解像度が最適ですか?*Ransomware Resilience に推奨されるデバイス解像度は 1920x1080 以上です。

*どのブラウザを使用すればよいですか?*任意の最新ブラウザ。

他のサービスとのやり取り

*Ransomware Resilience はNetApp ONTAPで行われた保護設定を認識しますか?*はい、Ransomware Resilience はONTAPで設定されたスナップショット スケジュールを検出します。

*Ransomware Resilience を使用してポリシーを設定した場合、今後の変更はこのサービスでのみ行う必要がありますか?*ランサムウェア耐性からポリシーの変更を行うことをお勧めします。

Ransomware Resilience は、 **NetApp Backup and Recovery** および**SnapCenter**とどのように連携しますか**?**

Ransomware Resilience では、次の製品とサービスを使用します。

- ファイル共有ワークロードのスナップショットとバックアップ ポリシーを検出して設定するためのバックアップとリカバリ
- SnapCenterまたはSnapCenter for VMware を使用して、アプリケーションおよび VM ワークロードのスナップショットおよびバックアップ ポリシーを検出し、設定します。

さらに、Ransomware Resilience は、バックアップとリカバリ、およびSnapCenter / SnapCenter for VMware を使用して、ファイルとワークロードの整合性のあるリカバリを実行します。

ワークロード

*作業負荷を構成するものは何ですか?*ワークロードは、アプリケーション、VM、またはファイル共有です。ワークロードには、単一のアプリケーション インスタンスによって使用されるすべてのボリュームが含まれます。たとえば、ora3.host.com にデプロイされた Oracle DB インスタンスには、データとログ用にそれぞれ vol1 と vol2 を設定できます。これらのボリュームが組み合わさって、Oracle DB インスタンスの特定のインスタンスのワークロードを構成します。

*ランサムウェア耐性はワークロードデータをどのように優先順位付けしますか?*データの優先順位は、作成されたスナップショットのコピーとスケジュールされたバックアップによって決まります。

ワークロードの優先度 (クリティカル、標準、重要) は、ワークロードに関連付けられた各ボリュームにすでに適用されているスナップショット頻度によって決まります。

"作業負荷の優先度や重要性について知る" 。

Ransomware Resilience はどのようなワークロードをサポートしますか**?**

Ransomware Resilience は、Oracle、MySQL、ファイル共有、ブロック ストレージ、VM、VM データストアなどのワークロードを識別できます。

さらに、 SnapCenterまたはSnapCenter for VMware を使用している場合は、これらの製品でサポートされているすべてのワークロードも Ransomware Resilience で識別され、Ransomware Resilience はワークロードの一貫性を保ちながらこれらを保護および回復できます。

データとワークロードをどのように関連付けますか**?**

ランサムウェア耐性は、次の方法でデータをワークロードに関連付けます。

- Ransomware Resilience はボリュームとファイル拡張子を検出し、適切なワークロードに関連付けます。

- さらに、 SnapCenterまたはSnapCenter for VMware があり、バックアップとリカバリでワークロードを構成している場合、Ransomware Resilience は、 SnapCenterおよびSnapCenter for VMware によって管理されているワークロードとそれらに関連付けられたボリュームを検出します。

*「保護された」ワークロードとは何ですか?*ランサムウェア耐性では、プライマリ検出ポリシーが有効になっている場合、ワークロードは「保護」ステータスを表示します。現時点では、これはワークロードに関連するすべてのボリュームで ARP が有効になっていることを意味します。

*「リスクのある」ワークロードとは何ですか?*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、バックアップおよびスナップショット 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。

新しいボリュームが追加されましたが、まだ表示されません 環境に新しいボリュームを追加した場合は、検出を再度開始し、保護ポリシーを適用してその新しいボリュームを保護します。

保護ポリシー

*Ransomware Resilience ランサムウェア ポリシーは、他の種類のワークロード ポリシーと共存しますか?*現在、バックアップとリカバリ (クラウド バックアップ) では、ボリュームごとに 1 つのバックアップ ポリシーがサポートされています。したがって、バックアップとリカバリとランサムウェア耐性はバックアップ ポリシーを共有します。

スナップショット コピーには制限がなく、各サービスから個別に追加できます。

ランサムウェア保護戦略にはどのようなポリシーが必要ですか**?**

ランサムウェア保護戦略には次のポリシーが必要です。

- ランサムウェア検出ポリシー
- スナップショットポリシー

ランサムウェア耐性戦略では、バックアップ ポリシーは必要ありません。

Ransomware Resilience は**NetApp ONTAP**で行われた保護設定を認識しますか**?**

はい、Ransomware Resilience は、 ONTAPで設定されたスナップショット スケジュールと、検出されたワークロード内のすべてのボリュームで ARP と FPolicy が有効になっているかどうかを検出します。ダッシュボードに最初に表示される情報は、他のNetAppソリューションおよび製品から集約されたものです。

ランサムウェア耐性は、バックアップとリカバリおよび**SnapCenter**ですでに作成されているポリシーを認識しますか**?**

はい、Backup and Recovery またはSnapCenterで管理されているワークロードがある場合、それらの製品によって管理されているポリシーは Ransomware Resilience に取り込まれます。

- NetApp Backup and Recovery やSnapCenterから引き継がれたポリシーを変更できますか?*

いいえ、Ransomware Resilience から Backup and Recovery またはSnapCenterによって管理されるポリシーを変更することはできません。これらのポリシーに対する変更は、Backup and Recovery またはSnapCenterで管理します。

- ONTAPからのポリシーが存在する場合 (ARP、FPolicy、スナップショットなど、System Manager ですで

に有効になっている)、それらは Ransomware Resilience で変更されますか? *

いいえ。Ransomware Resilience は、 ONTAPの既存の検出ポリシー (ARP、FPolicy 設定) を変更しません。

Ransomware Resilience にサインアップした後、**Backup and Recovery** または**SnapCenter**に新しいポリシーを追加するとどうなりますか**?**

Ransomware Resilience は、Backup and Recovery またはSnapCenterで作成された新しいポリシーを認識します。

- ONTAPからポリシーを変更できますか?*

はい、Ransomware Resilience のONTAPからポリシーを変更できます。 Ransomware Resilience で新しいポリシーを作成し、ワークロードに適用することもできます。このアクションにより、既存のONTAPポリシーが Ransomware Resilience で作成されたポリシーに置き換えられます。

ポリシーを無効にできますか**?**

System Manager UI、API、または CLI を使用して、検出ポリシーで ARP を無効にすることができます。

FPolicy およびバックアップ ポリシーを無効にするには、それらを含まない別のポリシーを適用します。