はじめに

BlueXP ransomware protection

NetApp
March 22, 2024

目次

はじめに

BlueXPランサムウェア対策プレビューの詳細

ランサムウェア攻撃は、システムやデータへのアクセスをブロックし、データのリリースや復号と引き換えに身代金を要求する可能性があります。IDCによると、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。攻撃によって、1日から数週間の間、データへのアクセスが中断される可能性があります。

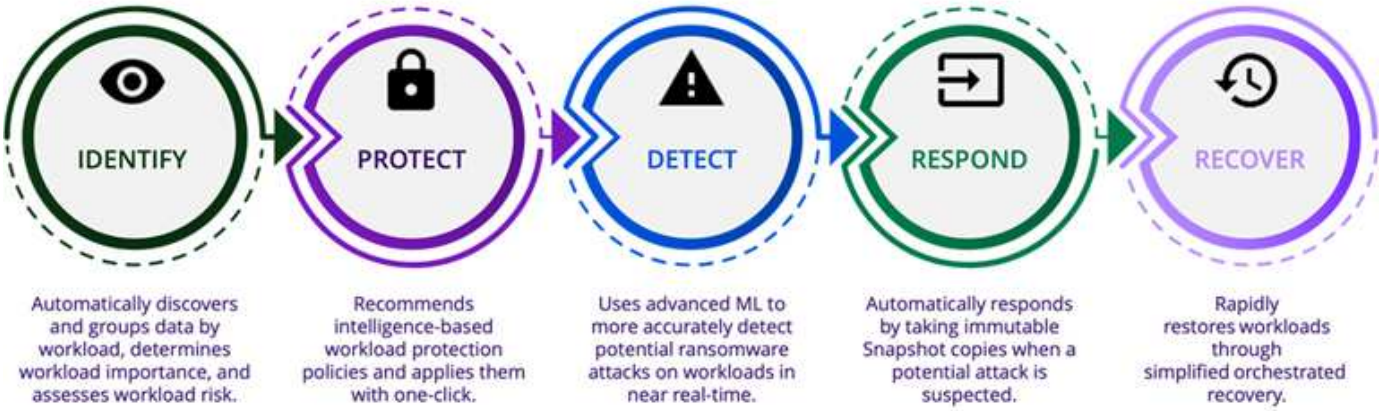
BlueXPランサムウェア対策は、ランサムウェアの保護、検出、リカバリのためのオーケストレーションサービスです。プレビュー版では、Oracle、MySQL、VMデータストアのアプリケーションベースのワークロードを保護し、 また、オンプレミスのNASストレージでのファイル共有や、Amazon Web ServicesのCloud Volumes ONTAP（NFSプロトコルを使用）をBlueXPアカウント間で共有し、Amazon Web Servicesのクラウドストレージまたは NetApp StorageGRIDにデータをバックアップできます。

> このドキュメントはテクノロジプレビュー版です。 このプレビューサービスでは、NetAppは、一般提供前にサービスの詳細、内容、スケジュールを変更する権利を留保します。

BlueXPのランサムウェア対策でできること

BlueXPのランサムウェア対策サービスは、複数のNetAppテクノロジをフル活用して、ストレージ管理者、データセキュリティ管理者、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。

- * BlueXPのアカウント、ワークスペース、BlueXPコネクタにわたって、オンプレミスのNetApp NASとNFSの作業環境にある、アプリケーションベース、ファイル共有、VMwareが管理するワークロードをすべて特定*します。次に、データの優先順位を分類し、ランサムウェア対策の強化に関する推奨事項を提供します。
- *データ上のバックアップやSnapshotコピーを有効にして、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。
- * NetApp ONTAP Snapshotコピーを自動的に開始して、ランサムウェア攻撃の可能性に対応*します。
- *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、ワークロードのアップタイムを促進するワークロードをリカバリ*します。ボリューム、フォルダ、または特定のファイルのリカバリを選択できます。このサービスは、最適なオプションに関する推奨事項を提供します。



BlueXPのランサムウェア対策を使用するメリット

BlueXPのランサムウェア対策には、次のようなメリットがあります。

- ワークロードとデータセットを検出し、使用状況の指標に基づいて優先度を分析し、相対的な重要度をランク付けします。
- ランサムウェアからの保護態勢を評価し、わかりやすいダッシュボードに表示します。
- 検出と保護のポスチャ分析に基づいて、次のステップに関する推奨事項を提示します。
- AI / MLベースのデータ保護に関する推奨事項をワンクリックで適用
- MySQL、Oracle、VMwareデータストア、ファイル共有など、最上位のアプリケーションベースワークロードのデータを保護します。
- AIテクノロジを活用して、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。
- Snapshot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、検出された潜在的な攻撃に対応して自動化されたアクションを開始します。
- RPOポリシーを満たすために、厳選されたリカバリを適用します。BlueXPのランサムウェア対策は、BlueXPのバックアップとリカバリ（旧称Cloud Backup）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オーケストレーションします。

コスト

プレビュー版のBlueXPランサムウェア対策を使用した場合、NetAppから料金が請求されることはありません。

ライセンス

BlueXPランサムウェア対策プレビュー自体に特別なライセンスは必要ありません。 すべてのプレビューライセンスは評価ライセンスです。

プレビュー版では、NetAppを使用して評価版と必要なライセンスを設定できます。

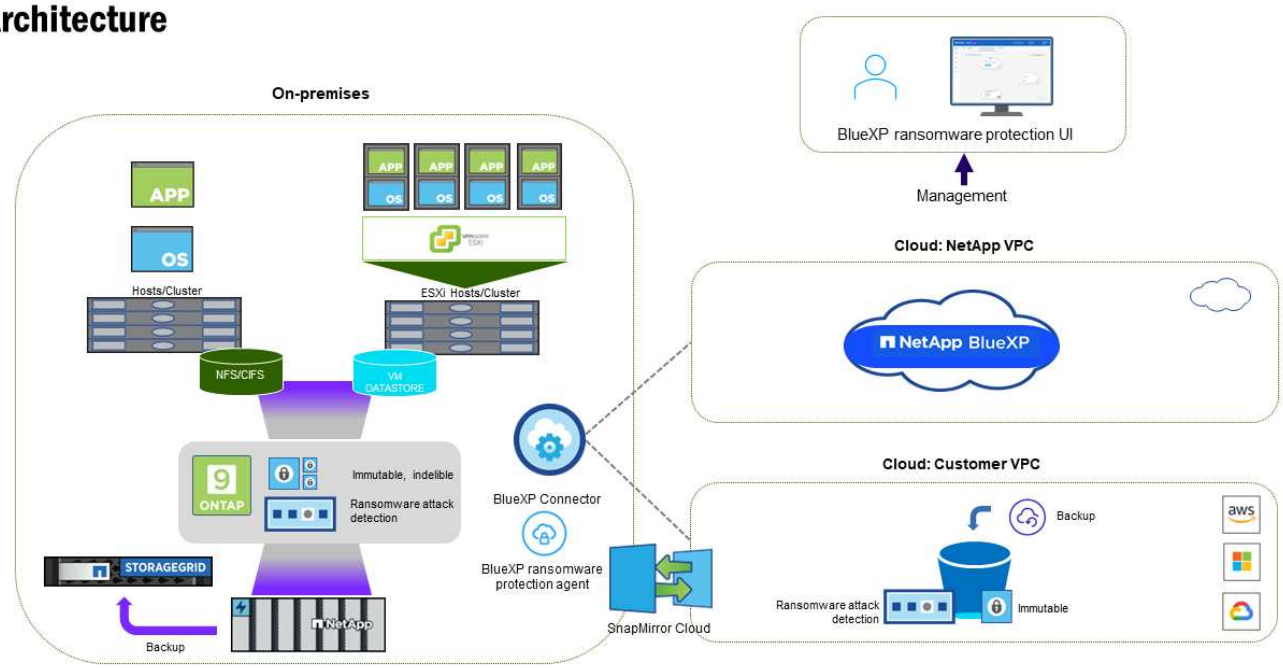
BlueXPランサムウェア対策プレビューには、次のライセンスが必要です。

- ONTAP
- NetApp自律型ランサムウェア対策テクノロジ：を参照してください "Autonomous Ransomware Protection Overview" を参照してください。
- BlueXPバックアップ/リカバリサービス

BlueXPのランサムウェア対策の仕組み

BlueXPのランサムウェア対策は、大まかに言ってこのように機能します。

Architecture



フィーチャー（ **Feature** ）	説明
識別	• BlueXPに接続されているオンプレミスのNAS（NFSマウント）データをすべて検出 • ONTAPサービスAPIから顧客データを特定し、ワークロードに関連付けます。の詳細を確認してください "ONTAP" および "SnapCenter ソフトウェア"。 • 各ボリュームのNetApp Snapshotコピーとバックアップポリシーの現在の保護レベル、および組み込みの検出機能を検出します。その後、サービスは、BlueXPのバックアップとリカバリ、BlueXPデジタルアドバイザ、ONTAPサービスと、Autonomous Ransomware Protection、FPolicy、バックアップポリシー、Snapshotポリシーなどの NetAppテクノロジを使用して、この保護体制をワークロードに関連付けます。 の詳細を確認してください "自律的なランサムウェア防御" および "BlueXPのバックアップとリカバリ"、 "BlueXP Digital Advisor"および "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に保護ポリシーを推奨します。 • ランサムウェア対策は、ポリシーの関連付けを学習し、類似するワークロードに対してカスタムポリシーを推奨します。
保護	• 特定された各ワークロードにポリシーを適用することで、ワークロードをアクティブに監視し、BlueXPのバックアップとリカバリとONTAP APIの使用をオーケストレーションします。

フィーチャー（ **Feature** ）	説明
検出	• 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におけるランサムウェア攻撃の可能性を検出し、自動化されたSnapshotコピーを追加で作成して最も近いデータリストア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ことから始まる、デュアルレイヤの検出機能を提供します。このサービスは、プライマリ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、潜在的な攻撃をより詳細に特定する機能を提供します。 • ONTAP、自律型ランサムウェア対策、FPolicyの各テクノロジを使用して、特定の疑わしいファイルを特定し、その攻撃を関連するワークロードにマッピングします。
応答	• ファイルアクティビティ、ユーザアクティビティ、エントロピーなどの関連データが表示され、攻撃に関するフォレンジックレビューを完了できます。 • は、ONTAP、Autonomous Ransomware Protection、FPolicyなどのNetAppテクノロジや製品を使用して、Snapshotコピーを迅速に作成します。
リカバリ	• BlueXPのバックアップとリカバリ、ONTAP、自律型ランサムウェア対策、FPolicyのテクノロジとサービスを使用して、最適なSnapshotまたはバックアップを特定し、実際のリカバリポイント（RPA）を推奨します。 • アプリケーションと整合性のある状態で、VM、ファイル共有、データベースなどのワークロードのリカバリをオーケストレーションします。

サポートされるバックアップターゲット、作業環境、データソース

BlueXPランサムウェア対策のプレビューでは、次のタイプのバックアップターゲット、作業環境、データソースに対するサイバー攻撃に対するデータの耐障害性を確認できます。

サポートされるバックアップターゲット

- Amazon Web Services（AWS）S3
- NetApp StorageGRID

サポートされる作業環境

- オンプレミスのONTAP NAS（NFSプロトコルを使用）
- ONTAP Select の場合
- AWSのCloud Volumes ONTAP（NFSプロトコルを使用）

データソース

プレビュー版では、次のアプリケーションベースのワークロードが保護されます。

- NetAppファイル共有
- VMware データストア

- データベース（プレビューバージョンのOracleとMySQL用）

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用語を理解しておくと便利です。

- 保護：BlueXPのランサムウェア対策の保護とは、保護ポリシーを使用して、Snapshotと変更不可のバックアップを別のセキュリティドメインに定期的に実行することを意味します。
- ワークロード：BlueXPランサムウェア対策プレビューのワークロードには、MySQL、Oracleデータベース、VMwareデータストア、ファイル共有を含めることができます。

BlueXPのランサムウェア対策の前提条件

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、BlueXPランサムウェア対策を始めましょう。

BlueXPランサムウェア対策プレビューバージョンを使用するには、次の前提条件が必要です。

- バックアップターゲットとアクセス権限が設定されたNetApp StorageGRIDまたはAWS S3のアカウント

  を参照してください "AWS権限リスト" を参照してください。

- ONTAP 9.11.1以降
  - クラスタカンリシヤONTAPノケンケン
  - オンプレミスのONTAPインスタンスで有効にする、BlueXPランサムウェア対策で使用するNetApp自律型ランサムウェア対策のライセンス。使用しているONTAPのバージョンに応じて異なります。を参照してください "Autonomous Ransomware Protection Overview"。

    ライセンスの詳細については、を参照してください。 "BlueXPランサムウェア対策の詳細をご確認ください"。

- BlueXPの場合：
  - BlueXPでは、各Virtual Private Cloud（VPC）またはオンプレミスのリージョンごとにBlueXPコネクタを設定する必要があります。を参照してください "コネクタを設定するためのBlueXPドキュメント"。

    > BlueXPコネクタが複数ある場合は、BlueXP UIに現在表示されているコネクタ以外のすべてのコネクタのデータがスキャンされます。

  - 作業環境でバックアップを有効にしたBlueXPのバックアップとリカバリサービス
  - オンプレミスストレージのNetApp NASを使用したBlueXPの作業環境
  - オンプレミスのONTAPクラスタに接続するアクティブなコネクタが少なくとも1つあるBlueXPアカウント。すべてのソース環境と作業環境が同じBlueXPアカウントに属している必要があります。
  - リソースを検出するためのアカウント管理者権限を持つBlueXPユーザアカウント
  - "BlueXPの標準の要件"

BlueXPランサムウェア対策のクイックスタート

ここでは、BlueXPのランサムウェア対策を開始するために必要な手順の概要を示します。各ステップ内のリンクから、詳細が記載されたページに移動できます。

1 前提条件を確認する

"環境がこれらの要件を満たしていることを確認します"。

2 ランサムウェア対策サービスをセットアップする

- "バックアップ先としてのNetApp StorageGRIDまたはAmazon Web Servicesの準備"。
- "BlueXPでのコネクタの設定"。
- "バックアップデスティネーションの設定"。
- "BlueXPでワークロードを検出"。

3 次の手順

サービスを設定した後、次に行うべき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常性を確認する"。
- "ワークロードを保護"。
- "ランサムウェア攻撃の可能性の検出に対応"。
- "攻撃からの復旧（インシデントが無力化された後）"。

BlueXPランサムウェア対策のセットアップ

BlueXPランサムウェア対策を使用するには、いくつかの手順を実行してセットアップします。

作業を開始する前に、 "前提条件" 環境の準備が整っていることを確認します。

バックアップ先の準備

次のいずれかのバックアップ先を準備します。

- NetApp StorageGRID
- Amazon Web Services の

バックアップ先自体でオプションを設定したら、あとでBlueXPランサムウェア対策サービスでバックアップ先として設定します。

StorageGRIDをバックアップ先にするための準備

StorageGRIDをバックアップ先として使用する場合は、を参照してください。 "StorageGRID のドキュメント" を参照してくださいStorageGRID。

バックアップ先としての**AWS**の準備

- AWSでアカウントをセットアップします。
- 設定 "AWS権限" 実現します。

BlueXPでのAWSストレージの管理の詳細については、 "Amazon S3バケットを管理します"。

BlueXPをセットアップします

次のステップでは、BlueXPとBlueXPランサムウェア対策サービスをセットアップします。

レビュー "BlueXPの標準の要件"。

BlueXPでコネクタを作成します

このサービスをお試しいただくには、NetApp営業担当者にお問い合わせください。その後、BlueXPコネクタを使用すると、ランサムウェア対策サービスに適した機能が含まれます。

サービスを使用する前にBlueXPでコネクタを作成する方法については、該当するBlueXPのドキュメントを参照してください "BlueXPコネクタの作成方法"。

> BlueXPコネクタが複数ある場合は、BlueXP UIに現在表示されているコネクタ以外のすべてのコネクタのデータがスキャンされます。このサービスは、このアカウントに関連付けられているすべてのワークスペースとすべてのコネクタを検出します。

BlueXPのランサムウェア対策にアクセス

NetApp BlueXPを使用して、BlueXPランサムウェア対策サービスにログインします。BlueXPの左側のナビゲーションで、**[**保護**]**>*[Ransomware protection]*を選択します。

詳細については、を参照してください "BlueXPのランサムウェア対策にアクセス"。

BlueXPランサムウェア対策でのバックアップ先の設定

BlueXPランサムウェア対策のバックアップ先オプションを使用して、バックアップ先を設定します。詳細については、を参照してください "設定オプションの設定"。

BlueXPのランサムウェア対策にアクセス

NetApp BlueXPを使用して、BlueXPランサムウェア対策サービスにログインします。

BlueXPにログインするには、NetApp Support Site のクレデンシャルを使用するか、Eメールとパスワードを使用してネットアップクラウドへのログインにサインアップします。 "ログインの詳細については、こちらをご覧ください"。

手順

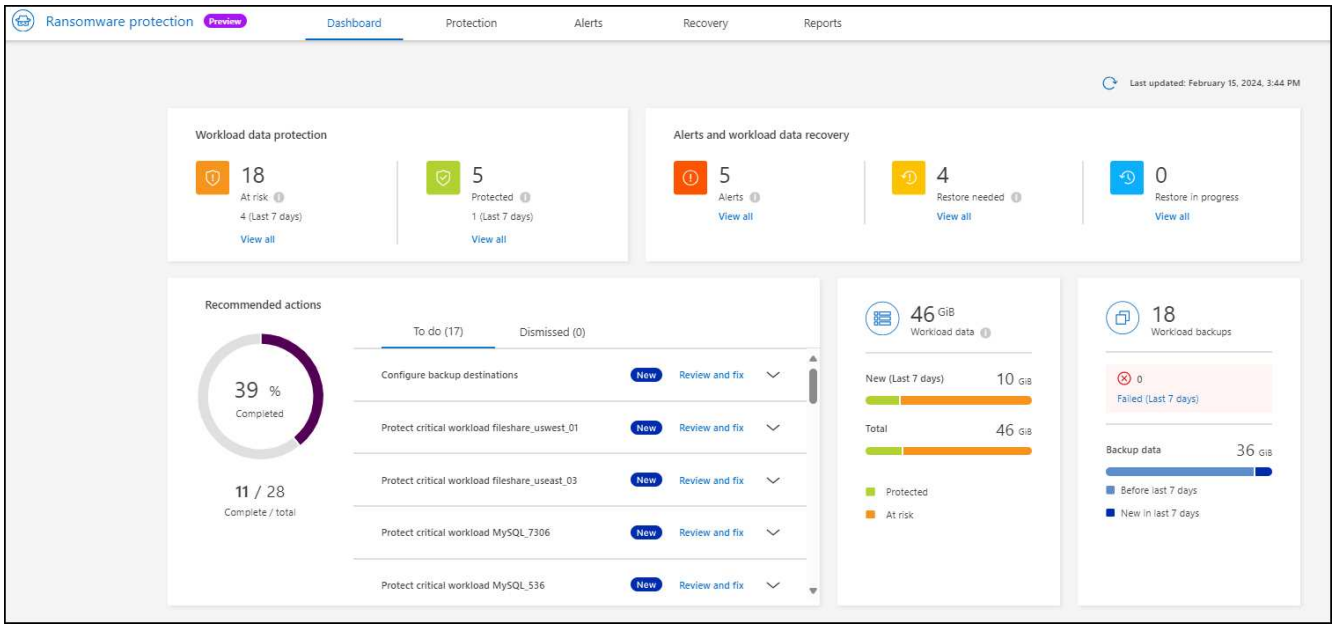
1. Webブラウザを開き、にアクセスします "BlueXPコンソール"。

   NetApp BlueXPのログインページが表示されます。

2. BlueXPにログインします。
3. BlueXPの左側のナビゲーションで、**[保護]**>*[Ransomware protection]*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。

   それ以外の場合は、BlueXPランサムウェア対策ダッシュボードが表示されます。



4. サービスの使用を開始します。
   - BlueXPコネクタがない場合や、このプレビュー用のコネクタではない場合は、NetAppサポートに連絡するか、メッセージに従ってこのプレビューにサインアップする必要があります。
   - BlueXPを初めて使用し、コネクタを使用したことがない場合は、「ランサムウェア対策」を選択すると、サインアップに関するメッセージが表示されます。フォームを送信してください。評価リクエストについては、NetAppからご連絡させていただきます。
   - 既存のコネクタを使用しているBlueXPユーザの場合は、「ランサムウェア対策」を選択すると、サインアップに関するメッセージが表示されます。
   - すでにプレビューに参加している場合は、「ランサムウェア対策」を選択すると、サービスを続行できます。まだ実行していない場合は、*[ワークロードを検出]*オプションを選択します。

BlueXPのランサムウェア対策でワークロードを検出

BlueXPのランサムウェア対策を使用するには、まずデータを検出する必要があります。BlueXPのランサムウェア対策は、調査の際に、アカウント内のすべてのBlueXPコネクタとワークスペースにわたって、作業環境内のすべてのボリュームとファイルを分析します。

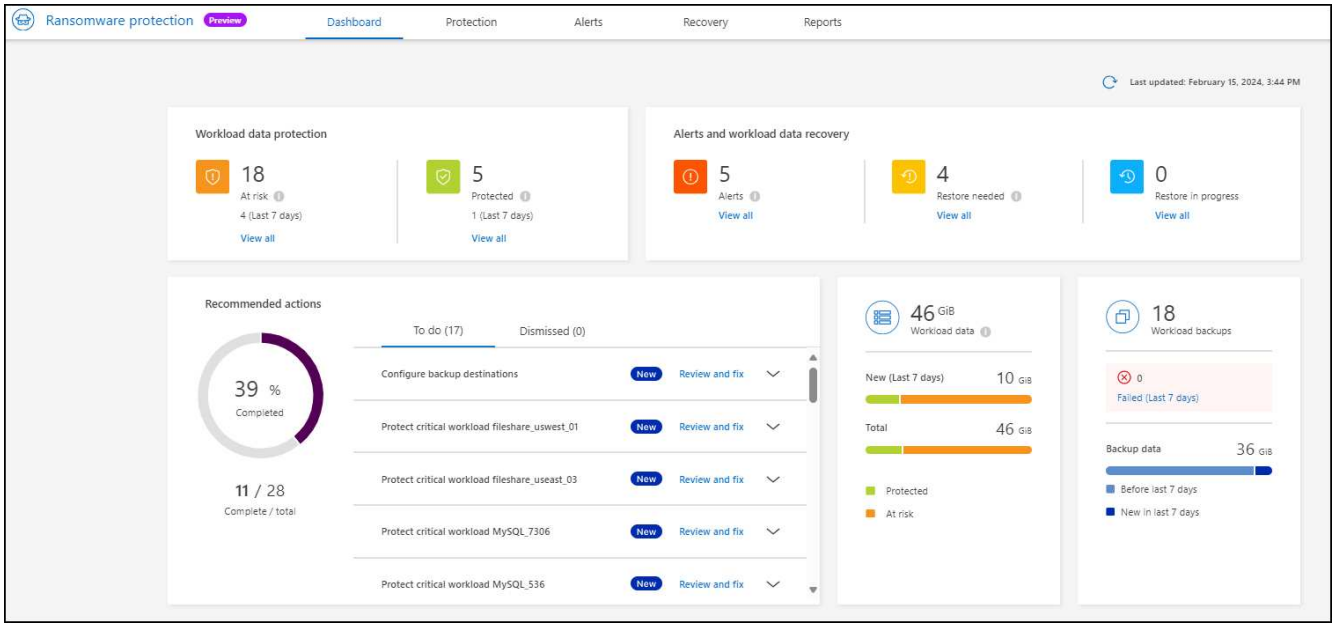
プレビュー版では、BlueXPのランサムウェア対策でMySQLアプリケーション、Oracleアプリケーション、VMwareデータストア、ファイル共有を評価します。

このサービスは、現在のバックアップ保護、Snapshotコピー、NetApp Autonomous Ransomware Protectionのオプションなど、既存の保護レベルを評価します。評価に基づいて、サービスはランサムウェア対策を改善する方法を提案します。

手順

1. BlueXPの左側のナビゲーションで、**[保護]**>*[Ransomware protection]*を選択します。
2. 最初のランディングページで*[Discover workloads]*を選択します。

   サービスによってワークロードデータが検出され、ダッシュボードにデータ保護の健常性が表示されます。



BlueXPのランサムウェア対策の設定

ダッシュボードで推奨事項を確認して、バックアップ先を設定できます。

バックアップ先の追加

BlueXPのランサムウェア対策なら、バックアップがまだないワークロードだけでなく、バックアップ先がまだ割り当てられていないワークロードも特定できます。

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。

- NetApp StorageGRID
- Amazon Web Services （AWS）

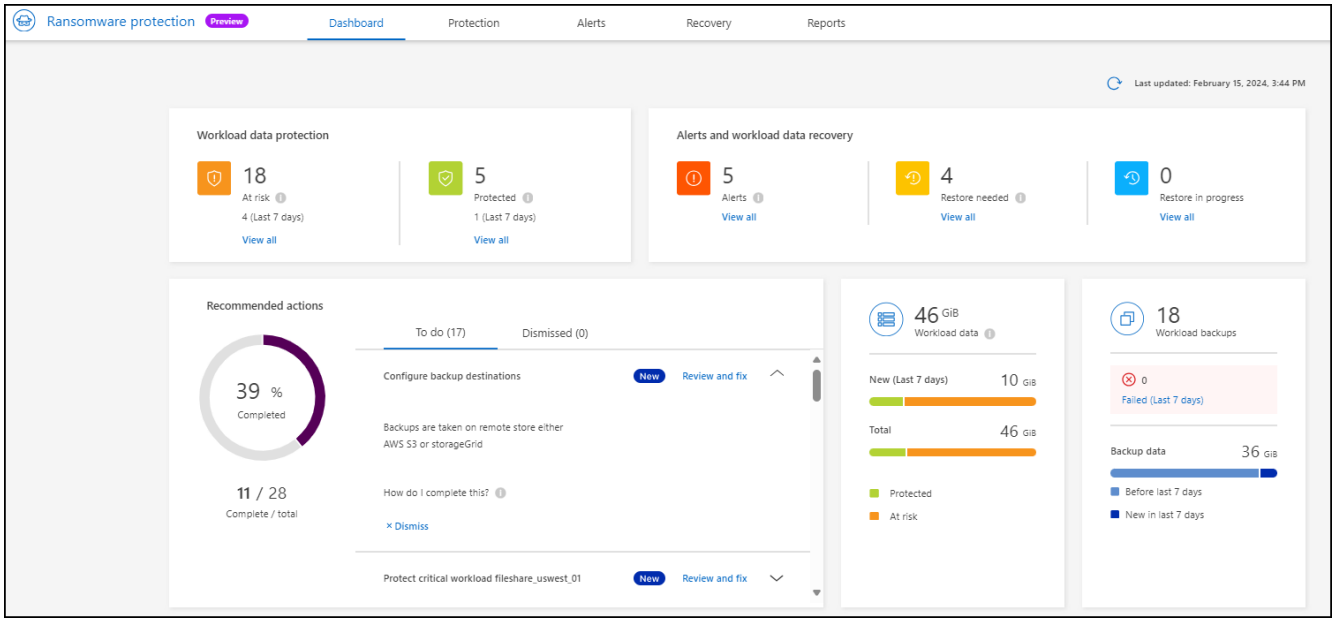
ダッシュボードで推奨される対処方法に基づいてバックアップ先を追加できます。

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する

ダッシュボードにはさまざまな推奨事項が表示されます。バックアップ先を設定することも推奨されます。

手順

1. BlueXPの左側のナビゲーションで、[保護]>*[Ransomware protection]*を選択します。
2. ダッシュボードの推奨される操作ウィンドウを確認します。

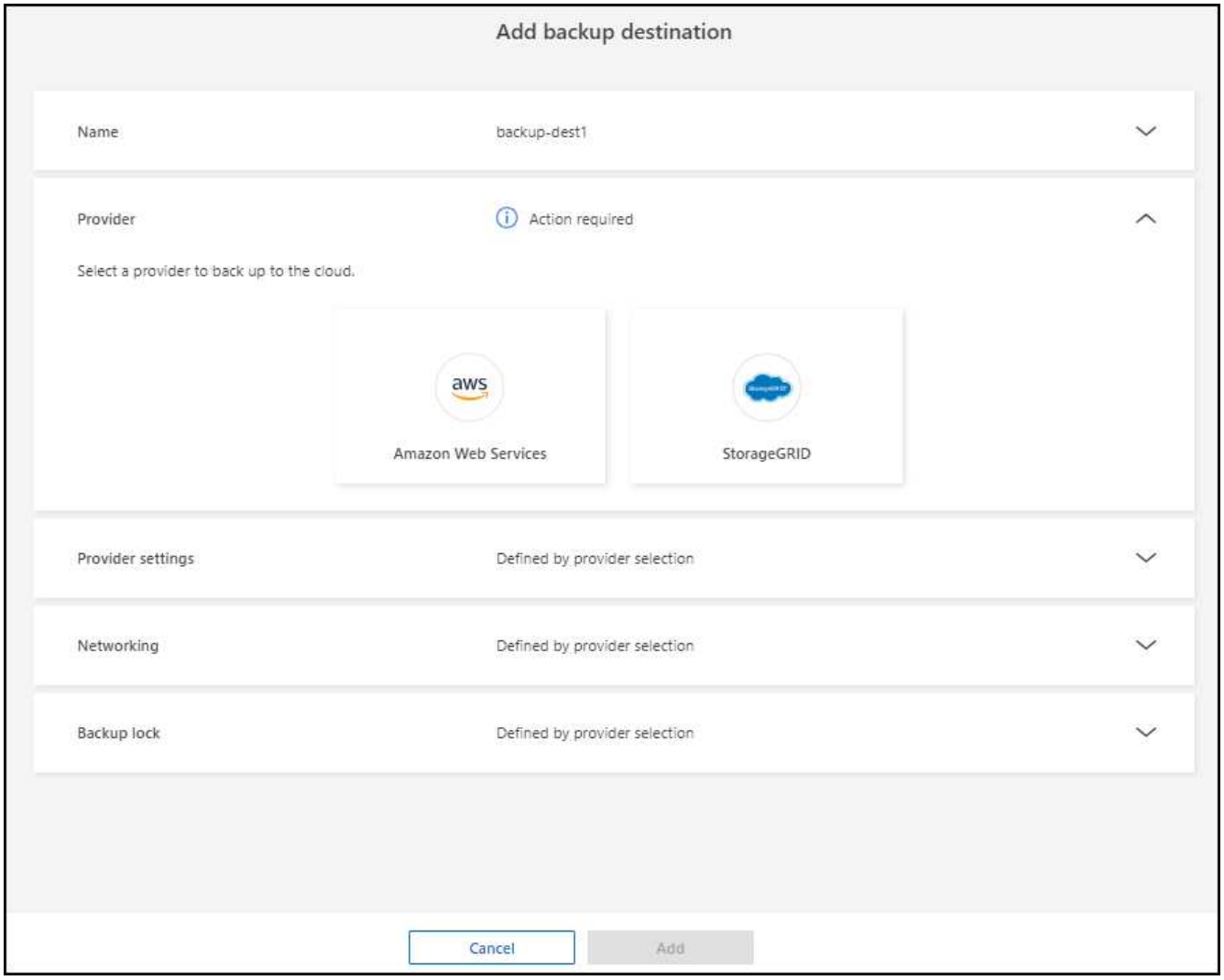


3. ダッシュボードで、[バックアップ先の設定]の推奨事項について*[確認と修正]*を選択します。
4. バックアッププロバイダに応じて手順を続行します。

バックアップ先としての**StorageGRID**の追加

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。

1. [設定]>[バックアップデスティネーション]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。



ページ"]

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使用します。
     - 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、シークレットキーのクレデンシャル。
   - 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配置されているクラスタです。この IPspace のクラスタ間 LIF には、アウトバウンドのインターネットアクセスが必要です。
   - バックアップロック：バックアップが変更または削除されないようにサービスで保護するかどうかを選択します。このオプションは、NetApp DataLockテクノロジを使用します。各バックアップは、保持期間中（最低30日間）、および最大14日間のバッファ期間中にロックされます。

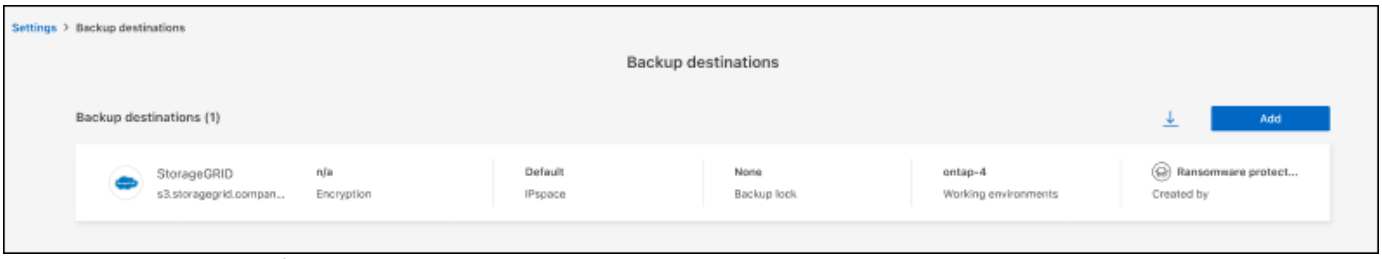
> ここでバックアップロックの設定を行う場合は、バックアップ先の設定後に設定を変更することはできません。

- 準拠モード：保持期間中は、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。



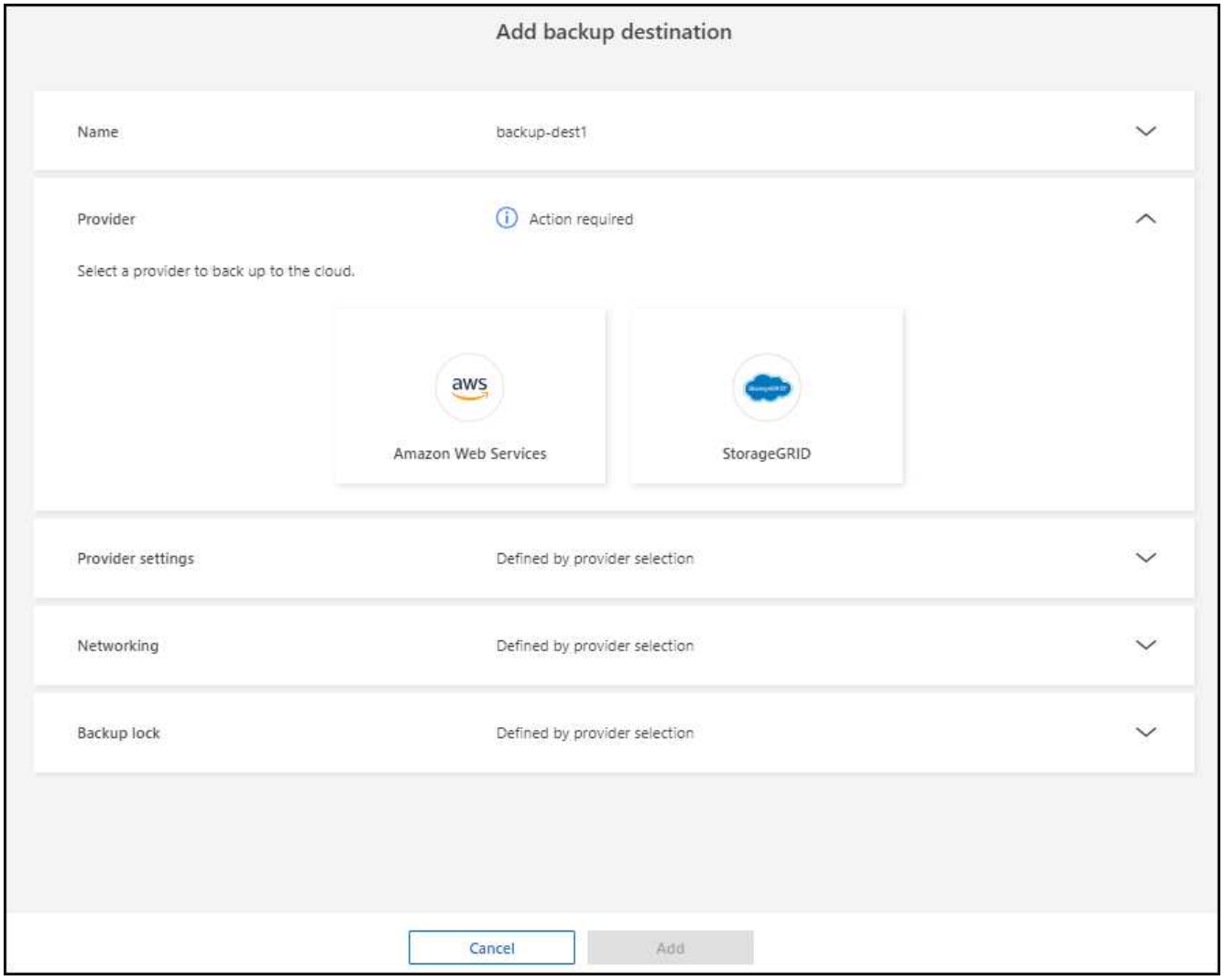
ページの[Settings]オプション"]

バックアップ先として**Amazon Web Services**を追加

バックアップ先としてAWSを設定するには、次の情報を入力します。

BlueXPでのAWSストレージの管理の詳細については、 "Amazon S3バケットを管理します"。

1. [設定]>[バックアップデスティネーション]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。



ページ"]

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。
   - プロバイダ設定：
     - 新しいバケットを作成し、BlueXPに既存のバケットがある場合は既存のバケットを選択するか、バックアップを格納する独自のバケットを使用します。
     - AWSクレデンシャル用の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表示されています。

     バケット内のデータは、デフォルトでAWSが管理するキーを使用して暗号化されます。AWSで管理され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と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配置されているクラスタです。この IPspace のクラス

タ間 LIF には、アウトバウンドの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、を参照してください。 "Amazon S3用のAWS PrivateLink"。

- バックアップロック：バックアップが変更または削除されないようにサービスで保護するかどうかを選択します。このオプションは、NetApp DataLockテクノロジを使用します。各バックアップは、保持期間中（最低30日間）、および最大14日間のバッファ期間中にロックされます。

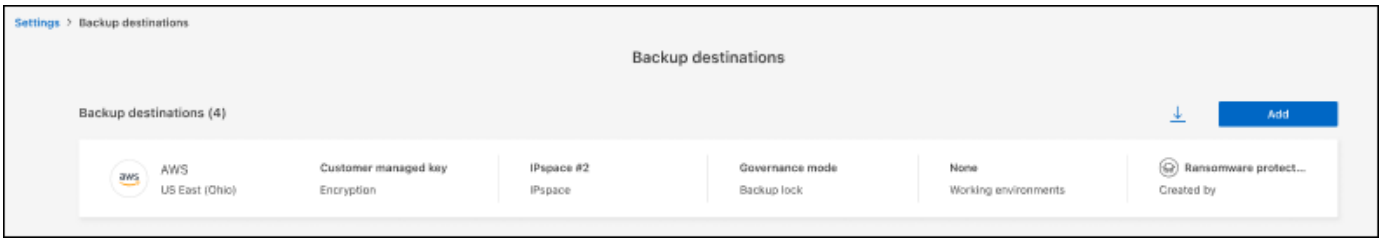
  ここでバックアップロックの設定を行う場合は、バックアップ先の設定後に設定を変更することはできません。

  - ガバナンスモード：特定のユーザ（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。
  - 準拠モード：保持期間中は、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。



ページの[Settings]オプション"]

BlueXPのランサムウェア対策に関するFAQ

この FAQ は、質問に対する簡単な回答を探している場合に役立ちます。

にアクセスします

- BlueXPランサムウェア対策URLとは？*
  URLの場合は、ブラウザで次のように入力します。 "https://console.bluexp.netapp.com/" をクリックしてBlueXPコンソールにアクセスします。
- BlueXPランサムウェア対策を使用するにはライセンスが必要ですか？*
  ネットアップライセンスファイル（NLF）は必要ありません。BlueXPランサムウェア対策プレビュー自体に特別なライセンスは必要ありません。 すべてのプレビューライセンスは評価ライセンスです。

このサービスのプレビュー版には、BlueXPバックアップ/リカバリサービスのライセンスが必要です。

プレビュー版では、NetAppを使用して評価版と必要なライセンスを設定できます。

- BlueXPのランサムウェア対策を有効にするには、どうすればよいですか？*
  BlueXPのランサムウェア対策を有効にする必要はありません。ランサムウェア対策オプションは、BlueXPの左側のナビゲーションで自動的に有効になります。

プレビュー版の場合は、サインアップするか、NetApp営業担当者に連絡してこのサービスを試用する必要があります。BlueXP Connectorを使用すると、サービスに適した機能が含まれます。

- BlueXPのランサムウェア対策は、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、BlueXPのランサムウェア対策は標準モードでのみ利用できます。今後もご期待ください。

すべてのBlueXPサービスにおけるこれらのモードの詳細については、を参照してください。 "BlueXPの導入モード"。

アクセス権限はどのように処理されますか**?**
サービスを開始してワークロードを検出できるのはアカウント管理者だけです（リソースの使用をコミットする必要があるため）。その後の対話は、任意の役割で行うことができます。

どのデバイス解像度が最適ですか**?**
BlueXPのランサムウェア対策で推奨されるデバイス解決方法は、1920 x 1080以上です。

どのブラウザを使用すればよいですか**?**
最新のブラウザは機能します。

他のサービスとのやり取り

- BlueXPのランサムウェア対策はNetApp ONTAPで行われた保護設定を認識していますか？*
  はい。BlueXPのランサムウェア対策では、ONTAPで設定されたSnapshotスケジュールが検出されます。
- BlueXPランサムウェア対策を使用してポリシーを設定した場合、今後このサービスのみを変更する必要がありますか？*
  BlueXPランサムウェア対策サービスからポリシーを変更することをお勧めします。

ワークロード

ワークロードの構成要素
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で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に導入されたOracle DBインスタンスのデータとログには、それぞれvol1とvol2を含めることができます。これらのボリュームを合わせて、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。

- BlueXPのランサムウェア対策では、ワークロードデータの優先順位をどのように設定しますか？*
  プレビューバージョンのデータ優先度は、作成されたSnapshot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順位は、次のSnapshotの頻度によって決まります。

- 重要：Snapshotコピーが1時間に1回未満（非常に積極的な保護スケジュール）
- 重要：Snapshotコピーは1日に1回未満、1時間に1回以上作成されます。
- 標準：1日に1つ以上のSnapshotコピーを作成

新しいボリュームが追加されましたが、まだ表示されていません
新しいボリュームを環境に追加した場合は、もう一度検出を開始し、保護ポリシーを適用して新しいボリュー

ムを保護します。

ダッシュボードにすべてのワークロードが表示されない。何が間違っている可能性がありますか。
現時点では、NFSボリュームのみがサポートされています。iSCSIボリューム、CIFSボリューム、およびサポートされないその他の構成は除外され、ダッシュボードには表示されません。

保護ポリシー

- BlueXP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ていますか？*
  現時点では、BlueXPのバックアップとリカバリ（Cloud Backup）でサポートされるバックアップポリシーはボリュームごとに1つです。そのため、BlueXPのバックアップとリカバリとBlueXPのランサムウェア対策は、バックアップポリシーを共有しています。

Snapshotコピーに制限はなく、各サービスとは別に追加できます。