

## ワークロードを保護 BlueXP ransomware protection

NetApp October 07, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/bluexp-ransomware-protection/rp-use-protect.html on October 07, 2024. Always check docs.netapp.com for the latest.

# 目次

ワークロードを保護・・・・・・・・・・・・・・・・・・・・・・・・・	
ランサムウェア戦略でワークロードを保護	

## ワークロードを保護

## ランサムウェア戦略でワークロードを保護

BlueXPのランサムウェア対策を使用して次の操作を実行することで、ランサムウェア攻撃からワークロードを保護できます。

- SnapCenterソフトウェアまたはSnapCenter Plug-in for VMware vSphereと連携して、ワークロードと整合性のある保護を実現します。
- ランサムウェア対策戦略を作成または管理します。この戦略には、Snapshot、バックアップ、ランサムウェア対策用に作成するポリシー(detection policies)が含まれます。
- ストラテジーをインポートして調整します。
- •ファイル共有をグループ化すると、ワークロードを個別に保護するのではなく、簡単に保護できます。
- ・ ランサムウェア対策戦略を削除

\*保護にはどのサービスが使用されていますか?\*保護ポリシーの管理には次のサービスを使用できます。これ らのサービスからの保護情報は、BlueXP ransomware protectionに表示されます。

- ・ファイル共有、VMファイル共有のBlueXP バックアップとリカバリ
- ・VMデータストア用のVMware SnapCenter
- OracleおよびMySQL向けSnapCenter

保護ポリシー

変更可能な保護ポリシーに関する情報や保護戦略に含まれるポリシーのタイプを確認すると役立つことがあり ます。

どの保護ポリシーを変更できますか?

現在のワークロード保護に基づいて保護ポリシーを変更できます。

- \* NetAppアプリケーションで保護されていないワークロード\*:これらのワークロードは、SnapCenter 、SnapCenter Plug-in for VMware vSphere、BlueXPのバックアップとリカバリでは管理されません。このようなワークロードでは、ONTAPやその他の製品の一部としてSnapshotが作成される場合があります。ONTAPのFPolicy保護が設定されている場合は、ONTAPを使用してFPolicyの保護を変更できます。
- \* NetAppアプリケーションによる既存の保護が適用されるワークロード\*:これらのワークロードには、SnapCenter、SnapCenter for VMware vSphere、またはBlueXP バックアップ/リカバリで管理されるバックアップポリシーまたはSnapshotポリシーが適用されます。
  - SnapCenter、SnapCenter for VMware、またはBlueXPのバックアップとリカバリでSnapshotポリシーやバックアップポリシーを管理している場合は、それらのアプリケーションで引き続き管理されます。BlueXP ランサムウェア対策を使用すると、これらのワークロードにランサムウェア検出ポリシーを適用することもできます。
  - <sup>。</sup>ランサムウェア検出ポリシーがAutonomous Ransomware Protection(ARP)およびONTAPのFPolicy で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およびFPolicyで管理されま す。

ランサムウェア対策戦略で必要なポリシーはどれですか?

ランサムウェア対策戦略では、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

BlueXP ランサムウェア対策戦略ではバックアップポリシーは必要ありません。

ワークロードに対するランサムウェア対策を表示する

ワークロードを保護するための最初の手順の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。次のタイプのワークロードが表示されます。

- アプリケーションワークロード
- ・VMワークロード
- ファイル共有のワークロード
- 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. 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]ペインで、\*[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。

0 16 At Hilk (0) 4 (Let 7 1)	) Mays()		32 Gi8 Data at risk			7 Protecter 1 (Last 7	deys	14 Gits Data protecter	ŧ ()		
Workfoada	6	Protection grou	pi								
forkloads (24)									٩	4 Manage protection	on stratege
Workload = 1	type = a	Connector \$	Importance # 2	0 Marys. :	Protection T \$	Protection # \$	Detection _ T 2	Detection T \$	Snapshot _ T \$	Backup desti 🗧	
Vm,datastrone.useau	VM Ne share	ave-connector-us	onical	49	Protected	10	Attive	rps-policy-ait	Buot lanomia.	netapo-backup-vs.	is boyeta
Vm_datastrine_unvery	VM file share	ais-connector-us	ontical	0.9	Protected	e'u	Learning mode	rpr-policy-all	Buot? tanomika	netapp-backup-vs.	lit proheimi
vire, distantione, unwer	VM file share	ava convector-us	Mandard	n/8	🕕 Atrisk	n.*	None	None	None	netapp-backup-st	Profect
Viri, datastore Juwen	VM Ne share	avs connector-us	Mahdard	e/a	🕕 "±trisk	0.14	None	None	None	netapo-backat-vi	Psonect
Vm_datamore_useas	VM file share	ave-connector-us	Standard	n/a	T Atrick	n/a	None	None	Nore	netapp-backup-vs	Protect
Vm datastow 201.3	VVI file share	onprem-connecto	Standard	103	() Atrok	na	None	None	None	netapp-badup-vs.	Protect

3. このページでは、ワークロードの保護の詳細を表示および変更できます。

**()** 

SnapCenterまたはBlueXPのバックアップおよびリカバリサービスですでに保護ポリシーが設定されているワークロードについては、保護を編集することはできません。これらのワークロードに対して、BlueXPランサムウェアは自律型ランサムウェア対策やFPolicy保護(他のサービスですでにアクティブ化されている場合)を有効にします。、およびの詳細については、を参照して "自律的なランサムウェア防御" "BlueXPのバックアップとリカバリ" "ONTAP FPolicy"ください。

#### [Protection]ページでの保護の詳細

[Protection]ページには、ワークロードの保護に関する次の情報が表示されます。

保護ステータス:ワークロードには、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 スが表示されます。

- •保護:ポリシーが適用されます。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。
- ・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 場合は、Snapshotポリシーとバックアップポリシーが有効になっていても「リスク」になります。
- ・進行中:ポリシーが適用されていますが、まだ完了していません。
- ・失敗:ポリシーは適用されていますが、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を持つことができます。

- ・学習中:最近、ランサムウェア検出ポリシーがワークロードに割り当てられ、サービスがワークロードを スキャンしています。
- \* Active \*: 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。
- ・ 設定なし: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、サービスでエラーが発生しました。



BlueXP ランサムウェア対策で保護を有効にすると、ランサムウェア検出ポリシーのステー タスがラーニングモードからアクティブモードに変わった後にアラート検出とレポートが 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の名前が割り当てられている場合は、そ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。

- Snapshotポリシーと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Snapshotポリ シーとバックアップポリシー、および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が管理
- SnapCenter Plug-in for VMware vSphereで管理
- BlueXPのバックアップとリカバリで管理
- Snapshotとバックアップを管理するランサムウェア対策ポリシーの名前
- なし

ワークロードの重要性

BlueXPのランサムウェア対策では、各ワークロードの分析に基づいて、検出時に各ワークロードの重要度や 優先度を割り当てます。ワークロードの重要度は、次のSnapshot作成頻度によって決まります。

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

事前定義された検出ポリシー

次のいずれかのBlueXP ランサムウェア対策事前定義ポリシーを選択でき、ワークロードの重要性に応じて調整できます。

ポリシー レベル	スナップショッ ト	頻度	保持(日数)	<b>Snapshot</b> コピー の数	<b>Snapshot</b> コピー の最大総数
重要なワ ークロー	四半期毎時間	15分ごと	3.	288	309
ドポリシ ー	毎日	1日ごと	14	14	309
	毎週	1週間ごと	35	5.	309
	毎月	30日ごと	60ドルだ	2.	309
重要なワ ークロー	四半期毎時間	30分ごと	3.	144です	165
ドポリシ ー	毎日	1日ごと	14	14	165
	毎週	1週間ごと	35	5.	165
	毎月	30日ごと	60ドルだ	2.	165
標準ワー クロード	四半期毎時間	30分ごと	3.	72です	93
ポリシー	毎日	1日ごと	14	14	93
	毎週	1週間ごと	35	5.	93
	毎月	30日ごと	60ドルだ	2.	93

## SnapCenterでアプリケーションまたはVMと整合性のある保護を実現

アプリケーションまたはVMと整合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ワークロードを 一貫した方法で保護し、休止状態と整合性のある状態を実現して、リカバリが必要になった場合のデータ損失 を回避できます。

このプロセスでは、BlueXPの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SnapCenter Plug-in for VMware vSphere for VMの登録が開始されます。

ワークロードと整合性のある保護を有効にしたら、BlueXPのランサムウェア対策で保護戦略を管理できま す。保護戦略には、他の場所で管理されるSnapshotポリシーとバックアップポリシー、およびBlueXP ランサ ムウェア対策で管理されるランサムウェア検出ポリシーが含まれます。 BlueXPの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サーバソフトウェアの登録"
- ・"SnapCenter Plug-in for VMware vSphereの登録"

#### 手順

- 1. BlueXPのランサムウェア対策メニューから、\*[ダッシュボード]\*を選択します。
- 2. [Recommendations]ペインで、次のいずれかの推奨事項を探し、\*[Review and fix]\*を選択します。
  - 。利用可能なSnapCenterサーバをBlueXPに登録
  - 。使用可能なSnapCenter Plug-in for VMware vSphere(SCV)をBlueXPに登録
- 3. 表示された情報に従って、BlueXPの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ホストを登録します。
- 4. BlueXPランサムウェア対策に戻ります。
- 5. BlueXPのランサムウェア対策から、ダッシュボードに移動して検出プロセスを再度開始します。
- 6. BlueXPのランサムウェア対策で、\* Protection \*を選択してProtectionページを表示します。
- 7. [Protection]ページの[snapshot policies]列で詳細を確認して、別の場所でポリシーが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

ワークロードにランサムウェア対策戦略を追加できます。この方法は、Snapshotポリシーとバックアップポリシーがすでに存在するかどうかによって異なります。

- スナップショットポリシーやバックアップポリシーがない場合は、ランサムウェア対策戦略を作成。ワークロードにSnapshotポリシーやバックアップポリシーがない場合は、ランサムウェア対策戦略を作成できます。この戦略には、BlueXP ランサムウェア対策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
  - <sup>。</sup>バックアップポリシー
  - 。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とバックアップポリシー\*がすでに設定されているワークロードに対して検出 ポリシーを作成します。これらのポリシーは、他のNetApp製品またはサービスで管理されています。検出 ポリシーでは、他の製品で管理されているポリシーは変更されません。

ランサムウェア対策戦略を作成する(Snapshotポリシーやバックアップポリシーがない場合)

ワークロードにSnapshotポリシーやバックアップポリシーがない場合は、ランサムウェア対策戦略を作成で きます。この戦略には、BlueXP ランサムウェア対策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の策定手順

1. BlueXPのランサムウェア対策メニューから、\* Protection \*を選択します。

0 10 Atink 0 404971	tays)		32 die Data at risk				Protecter 1 (Last 7)	f () deys	14 Giß Dets protecter			
Workfoada		Protection grou	н									
orkfoads (24)										٩	4 Manage p	objection strateg
workload =	type v a	Connector 0	Importance # \$	O muscy s_ +	Protectio	01	Protection T 2	Detection _ T \$	Detection _ T \$	Snapshot _ T 2	Backup desti 🎗	
Vm_datactore_useau	VM Ne share	ave-connector-us	princel	<b>na</b>	() Pr	otected	n,a	Adhe	rps-policy-ad	Build lanomika	netapp-backup-vs	(For poten
Vm_datactive_convey	VM file share	avis-connector-us	Ortical	n'a	() P	otected	n'a	Learning mode	rps-polcy-all	Buco taruomka.,	netapp-backup-vs.,	(Let provers
Vm, datastore, uswer	vM file share	ave convector us.	therdard	n/8	0 4	trisk	0.8	None	Note	None	netapp-backup-st	Protect
Vin datastore uswer	vM file share	avs connector-us	that-stand	n/a	① #	risk	n/a	None	None	None	netapp-backup-vs	Protect
Vm_datactore_useas	VM file share	ave-connector-us	Standard	n/a	() A	visk	n/a	None	None	Nore	netapp-backup-us	Protect
Vendatatione 201_3	VV file share	onprem-connecto	Standard	na	1 A	visk	n/a	None	hore	None	netapp-backsp-v6	Putert

2. [保護]ページで、\*[保護戦略の管理]\*を選択します。

	Ransomware protectio	on strategies				
(1)			d.	±	A05	
<ul> <li>Parabinot bondy</li> </ul>	<ul> <li>Backup policy</li> </ul>	<ul> <li>Detection policy</li> </ul>	<ul> <li>Protected workloads</li> </ul>		• 1 1	
initial-is-policy	oritical-bu-policy	rpt-policy-all	3		$\sim$	
important-is-policy	important-bu-policy	rps-policy-all	<b>x</b>		$\sim$	1.000
standard-si-policy	standard bu policy	ipu-policy-all	Ø.)		$\sim$	
	c0) 2   Snapshot policy antical-si-policy important-si-policy stanilard-si-policy	Ransomware protection (0) 2   Snapshor policy 2   Backup policy ortical-bu-policy important-su-policy important-su-policy istandard-bu-policy istandard-bu-policy	C0       2       Backup pekty       2       Detection pokty         2       5       Supphot pokty       2       Backup pekty       2       Detection pokty         2       1       Supphot pokty       2       Backup pekty       2       Detection pokty         2       1       Supphot pokty       2       Backup pekty       2       Detection pokty         1       Interfair-supplicy       0       Official-bu-pokty       1       Detection pokty         1       Interfair-supplicy       0       Important-supplicy       1       Detection pokty         1       Interfair-supplicy       1       Important-supplicy       1       Important-supplicy       1         1       Interfair-supplicy       1       Interfair-supplicy       1       1       1         1       Interfair-supplicy       1       Interfair-supplicy       1 <td< td=""><td>C0)       Q         21       Supphot policy       21       Backup policy       21       Description policy       21       Protected workloads         antical-supplicy       antical-supplicy       antical-supplicy       app-policy-all       3         importune-supplicy       importane-supplicy       app-policy-all       1       1         standard-surpolicy       spi-policy-all       1       0</td><td>Ransomware protection strategies       Q ±         (0)       Q ±         2   supphot policy       2   succes policy       2   protected workbads         antical-sinpolicy       antical-sinpolicy       4   protected workbads         important-sinpolicy       antical-sinpolicy       9   protected workbads         important-sinpolicy       antical-sinpolicy       9   protected workbads         important-sinpolicy       antical-sinpolicy       9   protected workbads         important-sinpolicy       important-bulpolicy       9   protected workbads</td><td>Ransomware protection strategies          Add       Q ± Add         1 Supplied policy       2   Backup policy       2   Detection policy       2   Protected workboalds       2   I         attical-singolicy       official-bu-policy       (the policy-all       3       &lt;</td>         important-singolicy       important-bu-policy       (the policy-all       1       &lt;</td<>	C0)       Q         21       Supphot policy       21       Backup policy       21       Description policy       21       Protected workloads         antical-supplicy       antical-supplicy       antical-supplicy       app-policy-all       3         importune-supplicy       importane-supplicy       app-policy-all       1       1         standard-surpolicy       spi-policy-all       1       0	Ransomware protection strategies       Q ±         (0)       Q ±         2   supphot policy       2   succes policy       2   protected workbads         antical-sinpolicy       antical-sinpolicy       4   protected workbads         important-sinpolicy       antical-sinpolicy       9   protected workbads         important-sinpolicy       antical-sinpolicy       9   protected workbads         important-sinpolicy       antical-sinpolicy       9   protected workbads         important-sinpolicy       important-bulpolicy       9   protected workbads	Ransomware protection strategies          Add       Q ± Add         1 Supplied policy       2   Backup policy       2   Detection policy       2   Protected workboalds       2   I         attical-singolicy       official-bu-policy       (the policy-all       3       <

3. [Ransomware protection strategory]ページで、\*[Add]\*を選択します。

Protection > Manage protection strategies > Add ransomware p	protection strategy				
			Add ransomware	protection strategy	
	Ransomware protection strategy name			Copy from existing ransomware protecti	on strategy
	RPS strategy 1			No policy selected	G Select
	Detection policy	rps-policy-primary			$\sim$
	Process and all				
	Snapshot poincy	important-ss-policy			*
	Backup policy	None			~
			(		
			Cancel	Add	

セクションを示す[Add strategy]ページ"]

新しいストラテジー名を入力するか、既存の名前を入力してコピーします。既存の名前を入力した場合は、コピーする名前を選択して\*コピー\*を選択します。



既存のストラテジーをコピーして変更する場合は、元の名前に「\_copy」が追加されます。 一意にするには、名前と少なくとも1つの設定を変更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いずれかを選択します。
- 一次検出:ランサムウェアの検出を有効にして、ランサムウェア攻撃の可能性を検出します。
- ファイル拡張子をブロック:これを有効にすると、既知の疑わしいファイル拡張子がサービスブロックされます。プライマリ検出が有効になっている場合、このサービスは自動スナップショットコピーを作成します。

ブロックされるファイル拡張子を変更する場合は、System Managerで編集します。

<sup>°</sup> \* Snapshotポリシー\*:

- \* Snapshotポリシーのベース名\*:ポリシーを選択するか\*[作成]\*を選択してSnapshotポリシーの名 前を入力します。
- \* Snapshotロック\*:このオプションを有効にすると、プライマリストレージ上のSnapshotコピー がロックされ、ランサムウェア攻撃を受けてバックアップ先にたどり着いた場合でも、一定期間 変更や削除ができないようになります。これは\_不変ストレージ\_とも呼ばれます。これにより、 リストア時間が短縮されます。

Snapshotがロックされると、ボリュームの有効期限はSnapshotコピーの有効期限に設定されます。

Snapshot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、 "ONTAPのSnapLock"。

 \* Snapshotスケジュール\*:スケジュールオプションと保持するSnapshotコピーの数を選択し、ス ケジュールを有効にする場合に選択します。

<sup>•</sup> 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 してバックアップ先を設定します。詳細については、を参照してください "セツテイノセツ テイ"。

6. 「\*追加」を選択します。

Snapshotポリシーとバックアップポリシーがすでに設定されているワークロードに検出ポリシーを追加する

BlueXP ランサムウェア対策では、Snapshotポリシーとバックアップポリシーがすでに設定されているワーク ロードにランサムウェア検出ポリシーを割り当てることができます。これらのポリシーは、他のNetApp製品 やサービスで管理されます。検出ポリシーでは、他の製品で管理されているポリシーは変更されません。

BlueXPのバックアップとリカバリやSnapCenterなどの他のサービスでは、次のタイプのポリシーを使用して ワークロードを管理しています。

- スナップショットを管理するポリシー
- セカンダリストレージへのレプリケーションを管理するポリシー
- オブジェクトストレージへのバックアップに関するポリシー

手順

1. BlueXPのランサムウェア対策メニューから、\* Protection \*を選択します。

0 16 Atria 0 40.897.0	(a)(4)		32 die Data at risk			Distance Freedom Freed	d D	14 Gið Deta protada	e::		
Workfords		Protection grou	н (								
kloade (24)									٩	🛓 🛛 Manage pr	dection strateg
t a heating	type == =	Connector 2	Importance # \$	O mucys. :	Protection # \$	Protection # \$	Detection T 2	Detection T \$	Snapshot _ T 2	Backup desti 🗧	
im datamene unear	VM file share	aws-connector-us	pricel	na.	Protected	69	Adhe	rps-policy-all	Buell? (anomica	netapp-backup-vs	(Fot polein
m_datactive_conver	VM file share	ain-connector-us	Ortical	0.9	Protected	e'n	Learning mode	rpr-policy-all	Buell? carsonisa	netapp-backup-vs.,	(1.62 protects
m, datastre uswer	VM file share	ave convector us.	Mandard	n/8	🕕 4t risk	n/W	None	None	None	netapp-backup-st-	Product
in datastee usees	vM Ne share	ans connector-us	that-shared	n/a	🛈 "Atrisk	n/a	None	Nore	None	netapp-backgrv4	Protect
m_datactore_useas	VM file share	ave-connector-us	Standard	0/3	🛈 Atrisk	0/3	tione	None	Nore	netapp-backup-us	Protect
m datastore 201.3	vivi file share	onprem-convecto	Standard	0.9	() Atrick	103	None	None	None	netapp-backup-v6	Putert

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。

[保護]ページには、SnapCenterソフトウェア、SnapCenter for VMware vSphere、およびBlueXPのバック アップとリカバリで管理されるポリシーが表示されます。

次の例は、SnapCenterで管理されるポリシーを示しています。

					Protect			
				Sele	ct a detection policy to apply to	the workload	Oracle_9819.	
Detec	ction policies (2)	)   1 sele	ected			Q	Policies managed by SnapCenter	
	Name	÷	Primary detection	\$	Block suspicious file extensions	÷	These policies managed by SnapCenter will not be modified by	
0	rps-policy-1		Yes		Yes		applying a detection policy to this workload.	_
0	rps-policy-2		Yes		No		ss-policy-daily1 Snapshot policy	~
							ss-policy-weekly1 Snapshot policy	~
							ss-policy-weekly2 Snapshot policy	~
							ss-policy-monthly1 Snapshot policy	~

ページ"]

## 次の例は、BlueXPのバックアップとリカバリで管理されるポリシーを示しています。

Dete	ction policies (2	:)   1 selec	ted			Q	😰 Poli	icies managed by BlueXP backup and	l recovery
	Name	<b>‡</b>	Primary detection	<b>\$</b>	Block suspicious file extensions	÷	These po	licies managed by BlueXP backup and rec	overy will not be
2	rps-policy-1		Yes		Yes			by appying a detection party to the nor	KIOODI .
)	rps-policy-2		Yes		No		۲	standart-snapshot-policy Snapshot policy	
							(1)	standart-backup-policy Backup policy	`

- 3. 他の場所で管理されているポリシーの詳細を表示するには、\*下矢印\*をクリックします。
- 他の場所で管理されているスナップショットポリシーとバックアップポリシーに加えて検出ポリシーを適用するには、検出ポリシーを選択します。
- 5. [保護]\*を選択します。
- [Protection]ページで、[Detection policy]列を確認して、割り当てられた検出ポリシーを確認します。また、スナップショットポリシーとバックアップポリシーの列には、ポリシーを管理している製品またはサービスの名前が表示されます。

別のポリシーを割り当てる

現在の保護ポリシーを置き換える別の保護ポリシーを割り当てることができます。

手順

- 1. BlueXPのランサムウェア対策メニューから、\* Protection \*を選択します。
- 2. [保護]ページのワークロードの行で、\*[保護の編集]\*を選択します。
- 3. [Policies]ページで、割り当てるポリシーの下矢印をクリックして詳細を確認します。
- 4. 割り当てるポリシーを選択します。
- 5. [保護]\*を選択して変更を終了します。

#### グループファイル共有による保護の強化

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。このサービスでは、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。

手順

1. BlueXPのランサムウェア対策メニューから、\* Protection \*を選択します。

0 10 Atriak (0 4 Card 7 st	(ay4)		32 die Data at risk				Distant 7	f D days	14 Gið Deta protecter			
Workfords		Protection grou	н (									
kloads (24)										٩	4 Manage p	obection strateg
Noritical a	τype τ ≎	Connector 0	Importance # \$	0 macys. :	Protec	tion # \$	Protection T \$	Detection _ T \$	Detection _ T \$	Snapshot _ T 2	Backup desti 🗘	
im datastone uneau	VM file share	ave-connector-us	pricel	na.	0	Protected	69	Adhe	rps-policy-all	Buel? (anomica	netapp-backup-vs	(Fox poles
m_datactive_uneer	VM file share	avis-connector-us	Ontical	19	0	Protected	e/a	Learning mode	rpe-policy-all	Buot/ taruomika	netapp-backup-vs.,	
m, datastine juswei	VM file share	ave consector us.	Mandard	n/8	0	4t risk	n/#	None	None	None	netapp-backup-vt	Protect
Wro, datastore, uswes	vM Ne share	ans connector-us	Mahdard	ey/a	•	±† risk	n/a	None	None	None	netapp-backup-vs	Putter
Vm_datamore_useas	VM file share	ave-connector-us	Standard	n/a	0	Ad visik	n/a	None	None	Nore	netapp-backup-us	Protect
Vm datatione 201 8	vivi file share	onprem-connecto	Standard	03	O.	At risk	na	None	None	None	netapp-backsp-v6	Puted

2. [保護]ページで、\*[保護グループ]\*タブを選択します。

0 16 At this 0 4 (Last 7 Caluti)	32 G/6 Cette at mile	Protected (0) 1 (Last 7 days)	14 Gits Deta protected	
Workloads	Protection groups			
stection groups (1)				Q 🛓 🔐
d proups to manage protection across multi	ple workloads which share similar characteristics.			
d proups to manage protection across multi Protection group 2   Detection	ple workloads which share similar characteristics. policy == 2   Snapshot and backup policies	T 2   Protection status	v 1   O Protected count	π \$   Nackup distinution τ \$



3. 「\*追加」を選択します。

		Workle Select workloads to add to	oads o the protection group.		
Protection group name protect-group-syst			Select the type of workloads Workloads with unapshot ar SnapCenter or Backup (	to add to the protection group. Ind backup policies managed by and recovery O Ramamware protect	001
Workloads (4)   2 selected					
Workload	t i Tome	T 2 Connector	2   Importance	T 2 0 Rian entrum	2 Bustection status
Workload	\$   Type Oracle	▼ 2   Connector	t i Importance	τ Σ	Protection status     Protected
Workload  Oucle,9815  Oracle,2115	Type     Oracle     Oracle	T Connector	Importance     Importance     Important     Important     Critical	v I   ⊕ Privacy exposure r/s	2   Protection statu
Workload  Oracle,9819  Oracle,2115  NySQL,9294	Type     Oracle     Oracle     Oracle     MySQL		Importance onull-sate1 onull-sate1 Ontical onull-sate1 Ontical		<ul> <li>Protection statu</li> <li>Protected</li> <li>At mik</li> <li>Protected</li> </ul>

- 4. 保護グループの名前を入力します。
- 5. 次のいずれかの手順を実行します。
  - a. 保護ポリシーがすでに設定されている場合は、次のいずれかでワークロードが管理されているかどう かに基づいてワークロードをグループ化するかどうかを選択します。
    - BlueXPのランサムウェア対策
    - SnapCenterまたはBlueXP のバックアップとリカバリ
  - b. 保護ポリシーがまだ設定されていない場合は、設定済みのランサムウェア対策戦略がページに表示されます。
    - i. 1つを選択してグループを保護し、\*次へ\*を選択します。
    - ii. 選択したワークロードに複数の作業環境にボリュームが含まれている場合は、複数の作業環境の バックアップ先を選択してクラウドにバックアップできるようにします。
- 6. グループに追加するワークロードを選択します。



7. 「\*次へ\*」を選択します。

0	Add protection gro	oup		⊙ Wor	kloeds 🤇	Protection (3) Revie	w		×
				Select a detection	n policy to ap	Protect ply to all the workloads in th	e protection gro	ugi.	
	Detection p	alicy (2)   Selected rows (1	ij				à	SnapCenter and BlueXP backup and recovery	
	Select	Detection policy	\$1	Primary detection	\$1	© Block suspicious file extensions	= 1	Existing snepshot and hackup policies manaped by SnepCenter and BueCP backup and recovery will not be modified by applying	
	0	rps-detection-1		Xee		Yes		e detection policy to the salected workloads.	
	0	rps-diffection-7		Yes		No			
					Previo	a			

-[Policy]ページ"]

8. このグループの保護を制御するポリシーを選択します。

- 9. 「\*次へ\*」を選択します。
- 10. 保護グループの選択内容を確認します。
- 11. 「\*追加」を選択します。

グループにワークロードを追加する

あとで既存のグループにワークロードを追加しなければならない場合があります。

BlueXP ランサムウェア対策のみで管理されるワークロードがグループに含まれている場合(SnapCenter やBlueXP のバックアップとリカバリでは管理されない)、BlueXP ランサムウェア対策のみで管理されるワ ークロードには別 々 のグループを使用し、他のサービスで管理されるワークロードには別 々 のグループを 使用する

手順

- 1. BlueXPのランサムウェア対策メニューから、\* Protection \*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。

0 16 At topic 0 4 (Last 7 clays)	32 G-B Curte et mik	Protected @ 1 (Last T days)	14 Gutt Deta protected	
Workloads	Protection groups			
offection groups (1) of groups to manage protection across multi	ple workloads which share similar characteristics.			Q <u>1</u> AN
Protection group 2 Detection	policy T 2 Snapshot and backup policies	T 2 Protection status	v 1   @ Protected count	T 2 Backup destination T 2

ページ"]

3. ワークロードを追加するグループを選択します。

		bo	<b>xp-dev-apps-group</b> Protection group				
						Delete pro	staction group
88 Workloads				0 /	rotection		It protection
Pile shares	0 Acote	ations	2 vvir datastores	۲	rps-policy-all Protection group		
Workloads (4)					٩	±	AM
Workload \$	Туре та	Connector +	Importance T C	Privacy exposure	Protection status	Detection st	ah.
vm_datastore_202_7359	VM datastore	onprem-connector-accou	Standard	n/a	Protected	Active	Θ
vm_datastore_202_7359 vm_datastore_203_2676	VM datastore VM datastore	onprem-connector accou	Standard Important	nja nja	<ul> <li>Protected</li> <li>At risk</li> </ul>	Active None	Θ

ページ"]

4. [選択した保護グループ]ページで、\*[追加]\*を選択します。

BlueXP ランサムウェア対策では、グループに含まれていないワークロードのうち、Snapshotポリシーと バックアップポリシーがグループと同じであるワークロードだけが表示されます。



ページの上部には、スナップショット、バックアップ、および検出のポリシーを保持して いるサービスが表示されます。

5. グループに追加するワークロードを選択します。

6. [保存(Save)]を選択します。

グループ保護の編集

既存のグループの検出ポリシーを変更できます。検出ポリシーがこのグループにまだ追加されていない場合 は、ここで追加できます。

手順

1. BlueXPのランサムウェア対策メニューから、\* Protection \*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。

on > finance-appe									
			fin P	nance-apps 🖉					
22 Workloads						O Protec	tion	Edit de stack	iou hard
1 File stures		2 Applications		0 VW datastoo		() rps- Ran	detection-1 someare detection policy		
Workloads (3)							٩	<u>1</u> Add	
Worktood	0  Type	♥\$  importance ₹\$	Privacy exposure      T	Protection == = = = = = = = = = = = = = = = = =	Detection w :   status	Detection policy $\Psi$ \$ [	Snapshot and backup policies # :	Backup destination = :	F
oracle-app-01	Dracie	Critical	riva	Protected	<ul> <li>Active</li> </ul>	rps-detection-1	ShapCentor	AWS US East 10%ct	(
fileshare_submest_03_0192	Fie share.	Critical	identify exposure	Protected	Error	rps-detection-1	SnapCentar	AWS US East (ONc)	(
practe-anst-02	Dade	imoortaili	104	Protected	Active	tps-detection-1	ShapCenter	AWS US East IONel	0

- 3. [保護]ペインで、\*[保護の編集]\*を選択します。
- 4. このグループに検出ポリシーを選択または追加します。

グループからワークロードを削除する

あとで既存のグループからワークロードを削除しなければならない場合があります。

手順

- 1. BlueXPのランサムウェア対策メニューから、\* Protection \*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. ワークロードを削除するグループを選択します。

		b	xp-dev-apps-group Protection group				
						Delete p	rotection group
80 Workloads				O Pr	otection		Left protection
E 2 File stares	B8 0	plications	2 VM datastores	۲	rps-policy-all Protection group		
Workloads (4)					٩	Ŧ	AM
Workloads (4) Workload	C Type T C	Convector =	Importance T C   (	O Privacy exposure 🗧	Q Protection status	± Detection s	ANI NA
Workloads (4) Workload vm_datattore_202_7339	C Type T C	Connector ====================================	tesportance v C     Standard	0: Privacy imposure ÷   n/3	Q Protection status 🗧	± Detection s Active	Add Add
Workloads (4) Workload vm_datastore_202_7384 vm_datastore_203_2676	C Type T C	Connector C onpremi-connector-accou- onpremi-connector-accou-	Emportance TO C   ( Standard)	Privacy exposure 2   n/a n/a	Q Protection status Protected D Protected	± Detection s Active None	Add Add O

ページ"]

4. [選択した保護グループ]ページで、グループから削除するワークロードを選択し、\*[アクション]\*オプションを選択し---ボタン"]ます。

- 5. [操作]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。

保護グループの削除

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. BlueXPのランサムウェア対策メニューから、\* Protection \*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. ワークロードを削除するグループを選択します。

		b	xp-dev-apps-group Protection group				
						Delete p	otection grou
88 Workloads				0	Protection		all polyclor
E 2 File shares	B8 0	fation	2 vvir datastores	0	ps-policy at Protection group		
Workloads (4)					٩	Ŧ	AM
Workloads (4) Workload ÷	Туре та	Connector 2	importance == C	Privacy exposure	Q Protection status	± Detection a	
Workloads (4) Workload C vm_datastore_202_7355	1 Type T 2 VVI datatore	Convector ====================================	importance == C   Standard	<ul> <li>Privacy imposure 2</li> <li>n/a</li> </ul>	Q Protection status Protected	± Detection s Active	
Workloads (4) Workload C vm_datattore_202_7359 vm_datattore_202_7359	Type         T 2           VAII datastore         VAI datastore           VAI datastore         VAI datastore	Connector Connector-accou- onprem-connector-accou-	Importance == C   Standard Important	Privacy exposure      Inda	Q Protection status Protected C Arrok	± Detection s Active None	Latit

ページ"]

4. [選択した保護グループ]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

ランサムウェア対策は削除できます。

ランサムウェア対策戦略で保護されているワークロードを表示する

ランサムウェア対策戦略を削除する前に、その戦略で保護されているワークロードを確認することができま す。

ワークロードは、戦略のリストから表示するか、特定の戦略を編集するときに表示できます。

- ストラテジーのリストを表示する際の手順
- 1. BlueXPのランサムウェア対策メニューから、\* Protection \*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。

[Ransomware protection strategory]ページには、戦略のリストが表示されます。

Protection # Ra	n # Ransomware protection strategies Ransomware protection strategies												
	Ransomware protection strategies (4)								Q	<u>*</u>		Add	
	Rationmware protection strategy	÷	Situpuhot policy		Backup policy		Detection policy	٥	Protected workloads		:	ж	
	sps-stratagy-critical		ortical-si-policy		critical-bu-policy		spe-policy-all		3			~	
	spi-stratag-important		important-us-policy		important-bu-policy		spepoley-all		(a))			~	200
	epi-dratagy-standard		standard-to-policy		standard-bu-policy		rps-policy-all		0			~	
	#25 strategy 4		standard-so-policy-344		standard bu policy-344		rps-policy-all		20 S			~	***
										Delete	icy policy		

3. [Ransomware protection strategory]ページの[Protected workloads]列で、行の最後にある下矢印をクリックします。

ランサムウェア対策戦略を削除

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. BlueXPのランサムウェア対策メニューから、\* Protection \*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. [ストラテジーの管理]ページで、削除するストラテジーの\*[アクション]\*オプションを選択し ・・・ボタン"] ます。
- 4. [操作]メニューから\*[ポリシーの削除]\*を選択します。

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

権利の制限について:政府による使用、複製、開示は、DFARS 252.227-7013(2014年2月)およびFAR 5252.227-19(2007年12月)のRights in Technical Data -Noncommercial Items(技術データ - 非商用品目に関 する諸権利)条項の(b)(3)項、に規定された制限が適用されます。

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

#### 商標に関する情報

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