Commencez

BlueXP ransomware protection

NetApp
March 22, 2024

Sommaire

Commencez

Découvrez la présentation de la protection contre les ransomwares BlueXP

Les attaques par ransomware peuvent bloquer l'accès à vos systèmes et à vos données, et les pirates peuvent demander une rançon en échange de la publication des données ou du décryptage. Selon l'IDC, il n'est pas rare que les victimes d'un ransomware se trouvent plusieurs attaques. L'attaque peut interrompre l'accès à vos données entre un jour et plusieurs semaines.

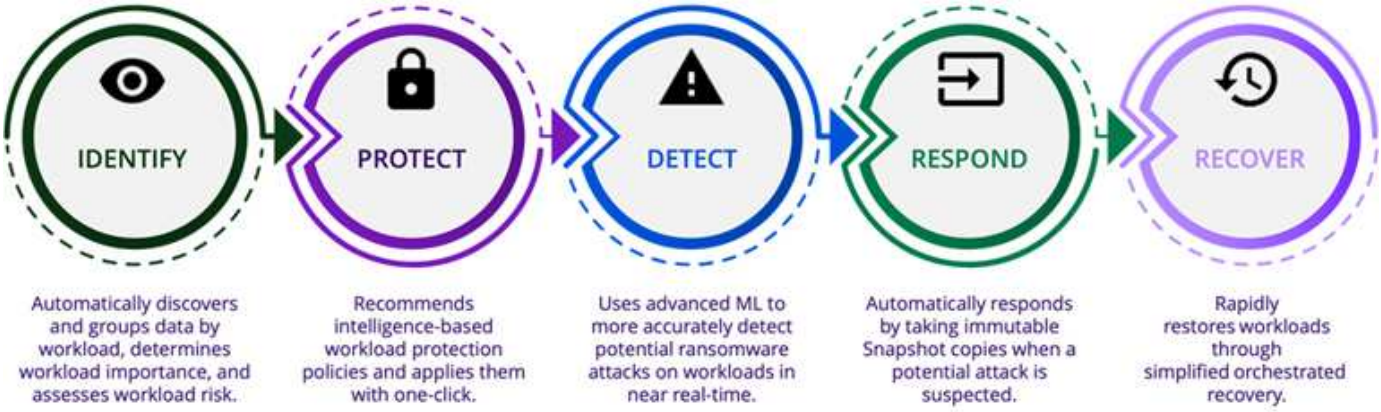
La protection contre les ransomwares BlueXP est un service d'orchestration pour la protection contre les ransomwares, la détection et la restauration. Pour la version de prévisualisation, le service protège les charges de travail basées sur les applications d'Oracle, de MySQL, de datastores de machines virtuelles, et partages de fichiers sur un stockage NAS sur site et sur Cloud Volumes ONTAP dans Amazon Web Services (à l'aide du protocole NFS) dans l'ensemble des comptes BlueXP, et sauvegardes des données dans le stockage cloud Amazon Web Services ou NetApp StorageGRID.

CETTE DOCUMENTATION EST FOURNIE SOUS FORME D'APERÇU TECHNOLOGIQUE. Avec cette offre de présentation, NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de l'offre avant la disponibilité générale.

Les possibilités de la protection BlueXP contre les ransomware

Le service de protection contre les ransomwares BlueXP permet d'exploiter pleinement plusieurs technologies NetApp. Votre administrateur du stockage, votre administrateur de la sécurité des données ou votre ingénieur en opérations de sécurité peuvent ainsi atteindre les objectifs suivants :

- **Identifiez** tous les workloads applicatifs, de partage de fichiers ou gérés par VMware dans NetApp NAS sur site avec les environnements de travail NFS dans BlueXP, entre les comptes BlueXP, les espaces de travail et les connecteurs BlueXP. Il catégorise ensuite la priorité des données et fournit des recommandations d'amélioration de la protection contre les ransomware.
- **Protégez** vos charges de travail en activant les sauvegardes et les copies Snapshot sur vos données.
- **Détectez** anomalies qui pourraient être des attaques par ransomware.
- **Répondre** aux attaques par ransomware potentielles en lançant automatiquement une copie Snapshot NetApp ONTAP.
- **Récupérez** vos charges de travail qui accélèrent la disponibilité des charges de travail grâce à l'orchestration de plusieurs technologies NetApp. Vous pouvez choisir de restaurer des volumes, des dossiers ou des fichiers spécifiques. Le service fournit des recommandations sur les meilleures options.



Avantages de l'utilisation de la protection contre les ransomware BlueXP

La protection contre les ransomwares BlueXP offre les avantages suivants :

- Découvre les workloads et les datasets, analyse la priorité en fonction de l'indice d'utilisation et classe leur importance relative.
- Évaluez votre stratégie de protection contre les ransomwares et affichez-la dans un tableau de bord facile à comprendre.
- Fournit des recommandations sur les étapes suivantes basées sur la découverte et l'analyse des postures de protection.
- Vous pouvez appliquer les recommandations de protection des données basées sur l'IA ou le ML en un clic.
- Protège les données des principaux workloads basés sur les applications, tels que MySQL, Oracle, les datastores VMware et les partages de fichiers.
- Détection des attaques par ransomware visant les données en temps réel sur le stockage primaire à l'aide de la technologie d'IA
- Lancement d'actions automatisées en réponse à des attaques potentielles détectées grâce à la création de copies Snapshot et à l'envoi d'alertes en cas d'activité anormale
- Récupération adaptée pour respecter les politiques de RPO La protection contre les ransomwares BlueXP orchestre la restauration en cas d'incidents de ransomware à l'aide de plusieurs services de restauration NetApp, notamment la sauvegarde et la restauration BlueXP (anciennement Cloud Backup).

Le coût

NetApp ne vous facture pas pour l'utilisation de la version préliminaire de la protection contre les ransomwares BlueXP.

Licences

La préversion de la protection contre les ransomware BlueXP elle-même ne nécessite aucune licence spéciale. Toutes les licences d'aperçu sont des licences d'évaluation.

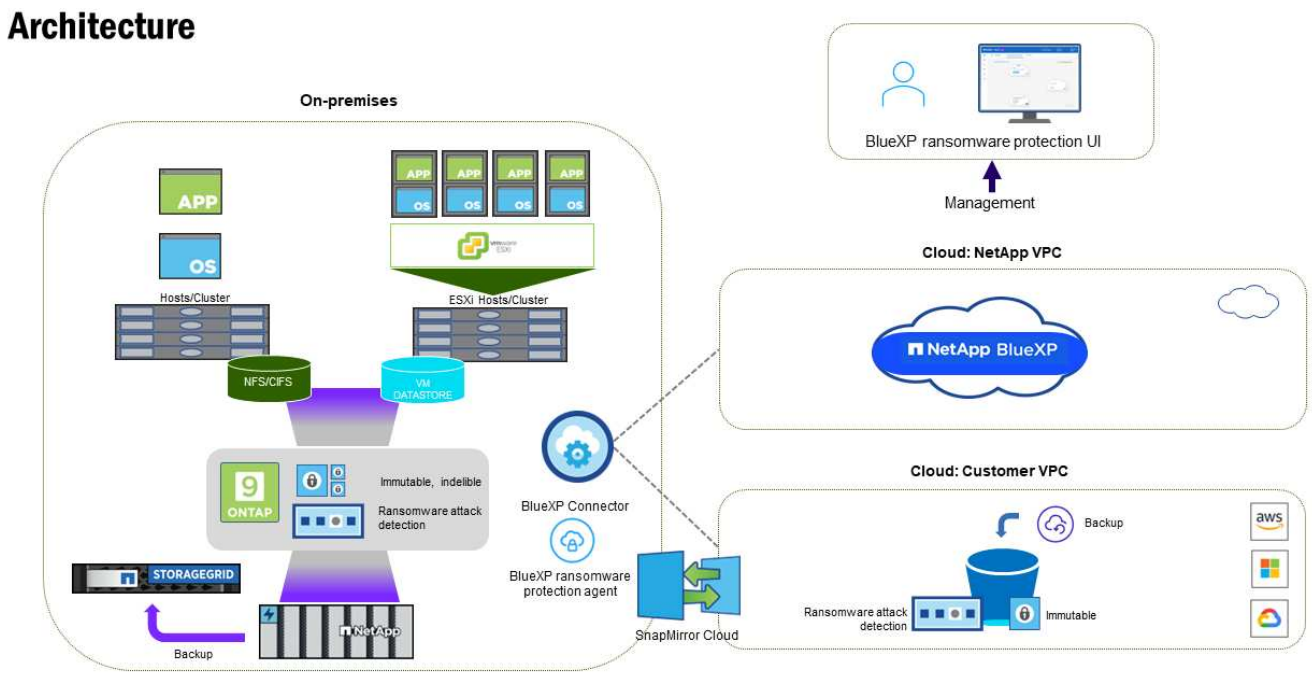
Pour la version de prévisualisation, NetApp vous aide à configurer l'évaluation et les licences requises.

La prévisualisation de la protection contre les ransomware BlueXP nécessite les licences suivantes :

- ONTAP
- Technologie de protection anti-ransomware autonome de NetApp. Reportez-vous à la section "Présentation de la protection autonome contre les ransomwares" pour plus d'informations.
- Service de sauvegarde et de restauration BlueXP

Fonctionnement de la protection BlueXP contre les ransomware

À un niveau élevé, la protection contre les ransomwares BlueXP fonctionne comme ça.



Fonction	Description
IDENTIFIER	• Recherche toutes les données NAS (montages NFS) sur site du client connectées à BlueXP. • Identifie les données des clients à partir des API de service ONTAP et les associe à des workloads. En savoir plus sur "ONTAP" et "Logiciel SnapCenter". • Découvre le niveau de protection actuel de chaque volume des copies Snapshot NetApp, les règles de sauvegarde et les fonctionnalités de détection intégrées. Le service associe ensuite cette stratégie de protection aux workloads à l'aide de la sauvegarde et de la restauration BlueXP, de BlueXP Digital Advisor, des services ONTAP et des technologies NetApp, telles que la protection anti-ransomware autonome, FPolicy, les règles de sauvegarde et les règles Snapshot. En savoir plus sur "Protection autonome contre les ransomwares" et "Sauvegarde et restauration BlueXP", "Conseiller digital BlueXP", et "ONTAP FPolicy". • Attribue une priorité commerciale à chaque charge de travail en fonction des niveaux de protection automatiquement découverts et recommande des règles pour les charges de travail en fonction de leurs priorités. • La protection contre les ransomwares apprend également les associations de règles et recommande vos règles personnalisées pour des charges de travail similaires.
PROTÉGER	• Surveille activement les workloads et orchestre l'utilisation de la sauvegarde et de la restauration BlueXP et des API ONTAP en appliquant des règles à chacun des workloads identifiés.
DÉTECTER	• Détecte les attaques potentielles à l'aide d'un modèle de machine learning intégré qui détecte les activités et le chiffrement potentiellement anormaux. • Cette fonctionnalité propose une détection double couche, qui commence par détecter les attaques par ransomware potentielles dans le stockage primaire et répondre aux activités anormales avec des copies Snapshot automatisées supplémentaires qui créent les points de restauration de données les plus proches. Ce service permet d'approfondir l'identification des attaques potentielles avec plus de précision sans affecter les performances des principaux workloads. • Déterminez les fichiers suspects spécifiques et mappent cette attaque aux workloads associés à l'aide de ONTAP, de la protection anti-ransomware autonome et des technologies FPolicy.
RÉPONDRE	• Affiche les données pertinentes, telles que l'activité des fichiers, l'activité des utilisateurs et l'entropie, pour vous aider à mener à bien les analyses d'attaque. • Initie des copies Snapshot rapides à l'aide des technologies et produits NetApp tels que ONTAP, la protection anti-ransomware autonome et FPolicy.
RÉCUPÉRER	• Détermine le meilleur Snapshot ou sauvegarde et recommande le meilleur point de restauration réel (RPA) à l'aide des technologies de sauvegarde et de restauration BlueXP, de ONTAP, de protection anti-ransomware autonome et des services et technologies FPolicy. • Orchestre la restauration des workloads, y compris les machines virtuelles, les partages de fichiers et les bases de données avec cohérence des applications.

Cibles de sauvegarde, environnements de travail et sources de données pris en charge

Utilisez l'aperçu de la protection contre les ransomwares BlueXP pour découvrir comment vos données sont résilientes face à une cyberattaque sur les types de cibles de sauvegarde, d'environnements de travail et de sources de données suivants :

Cibles de sauvegarde prises en charge

- Amazon Web Services (AWS) S3
- NetApp StorageGRID

Environnements de travail pris en charge

- NAS ONTAP sur site (utilisant le protocole NFS)
- ONTAP Select
- Cloud Volumes ONTAP dans AWS (via le protocole NFS)

Sources de données

Pour la version Preview, le service protège les charges de travail basées sur les applications suivantes :

- Partages de fichiers NetApp
- Les datastores VMware
- Bases de données (pour la version preview, Oracle et MySQL)

Des conditions qui peuvent vous aider à protéger vos données contre les ransomwares

Pour en savoir plus sur la terminologie relative à la protection contre les ransomwares,

- **Protection** : la protection dans BlueXP contre les ransomware signifie que les snapshots et les sauvegardes immuables s'effectuent sur une base régulière vers un domaine de sécurité différent à l'aide de politiques de protection.
- **Charge de travail** : dans la version préliminaire de la protection contre les ransomwares BlueXP, une charge de travail peut inclure des bases de données MySQL ou Oracle, des datastores VMware ou des partages de fichiers.

Protection BlueXP contre les ransomware requise

Commencez à utiliser la protection contre les ransomwares BlueXP en vérifiant le niveau de préparation de votre environnement opérationnel, de votre connexion, de votre accès réseau et de votre navigateur Web.

Pour utiliser la version d'aperçu de la protection contre les ransomwares BlueXP, vous devez disposer des conditions préalables suivantes :

- Un compte dans NetApp StorageGRID ou AWS S3 pour les cibles de sauvegarde et les autorisations d'accès définies

  Reportez-vous à la "Liste d'autorisations AWS" pour plus d'informations.

- ONTAP 9.11.1 et versions ultérieures
  - Autorisations ONTAP de l'administrateur du cluster
  - Une licence pour la protection anti-ransomware autonome de NetApp, utilisée par la protection anti-ransomware BlueXP, activée sur l'instance ONTAP sur site, selon la version de ONTAP que vous utilisez. Reportez-vous à la section "Présentation de la protection autonome contre les ransomwares".

    Pour plus d'informations sur les licences, reportez-vous à la section "Découvrez la protection contre les ransomwares BlueXP".

- Dans BlueXP :
  - Un connecteur BlueXP pour chaque cloud privé virtuel (VPC) ou une région sur site doit être configuré dans BlueXP. Reportez-vous à la section "Documentation BlueXP pour configurer le connecteur".

    > Si vous disposez de plusieurs connecteurs BlueXP, le service analyse les données entre tous les connecteurs au-delà de celui qui s'affiche actuellement dans l'interface utilisateur BlueXP.

  - Service de sauvegarde et de restauration BlueXP avec sauvegarde activée dans l'environnement de travail
  - Un environnement de travail BlueXP avec le stockage sur site NetApp NAS
  - Un compte BlueXP avec au moins un connecteur actif connecté aux clusters ONTAP sur site. Tous les environnements source et de travail doivent se trouver sur le même compte BlueXP.
  - Un compte utilisateur BlueXP avec des privilèges d'administrateur de compte pour la découverte des ressources
  - "Exigences standard de BlueXP"

Démarrage rapide de la protection contre les ransomware BlueXP

Voici les étapes à suivre pour démarrer avec la protection BlueXP contre les ransomwares. Les liens de chaque étape vous mènent à une page qui fournit plus de détails.

1 Passer en revue les prérequis

"Assurez-vous que votre environnement répond à ces exigences".

2 Configurez le service de protection contre les ransomwares

- "Préparez NetApp StorageGRID ou Amazon Web Services en tant que destination de sauvegarde".
- "Configurez un connecteur dans BlueXP".
- "Configurer les destinations de sauvegarde".
- "Découvrez les workloads dans BlueXP".

3 Et la suite ?

Après avoir configuré le service, voici ce que vous pourriez faire ensuite.

- "Consultez l'état de la protection des workloads dans le tableau de bord".
- "Protégez les workloads".
- "Répondez à la détection des attaques par ransomware potentielles".
- "Récupérer après une attaque (après neutralisation des incidents)".

Configurez la protection BlueXP contre les ransomware

Pour configurer la protection contre les ransomwares BlueXP, effectuez quelques étapes.

Avant de commencer, consultez "prérequis" pour vous assurer que votre environnement est prêt.

Préparer la destination de sauvegarde

Préparez l'une des destinations de sauvegarde suivantes :

- NetApp StorageGRID
- Amazon Web Services

Une fois que vous avez configuré les options de la destination de sauvegarde elle-même, vous la configurez ultérieurement en tant que destination de sauvegarde dans le service de protection contre les ransomwares BlueXP.

Préparez StorageGRID à devenir une destination de sauvegarde

Si vous souhaitez utiliser StorageGRID comme destination de sauvegarde, reportez-vous à la section "Documentation StorageGRID" Pour plus d'informations sur StorageGRID.

Préparez AWS à devenir une destination de sauvegarde

- Configuration d'un compte dans AWS.
- Configurer "Autorisations AWS" Dans AWS.

Pour en savoir plus sur la gestion de votre stockage AWS dans BlueXP, consultez la section "Gestion de vos compartiments Amazon S3".

Configurez BlueXP

L'étape suivante consiste à configurer BlueXP et le service de protection contre les ransomwares BlueXP.

Révision "Exigences standard de BlueXP".

Créez un connecteur dans BlueXP

Contactez votre ingénieur commercial NetApp pour essayer ce service. Ensuite, lorsque vous utilisez le connecteur BlueXP, il inclut les fonctionnalités appropriées pour le service de protection contre les ransomware.

Pour créer un connecteur dans BlueXP avant d'utiliser le service, reportez-vous à la documentation BlueXP qui décrit "Comment créer un connecteur BlueXP".

> Si vous disposez de plusieurs connecteurs BlueXP, le service analyse les données entre tous les connecteurs au-delà de celui qui s'affiche actuellement dans l'interface utilisateur BlueXP. Ce service détecte tous les espaces de travail et tous les connecteurs associés à ce compte.

Accédez à la protection BlueXP contre les ransomware

Vous utilisez NetApp BlueXP pour vous connecter au service de protection contre les ransomwares BlueXP. Dans le menu de navigation de gauche de BlueXP, sélectionnez **protection** > **protection contre les ransomware**.

Pour plus de détails, reportez-vous à "Accédez à la protection BlueXP contre les ransomware".

Configurez les destinations de sauvegarde dans la protection contre les ransomwares BlueXP

Utilisez l'option BlueXP ransomware protection backup destinations pour configurer les destinations de sauvegarde. Pour plus de détails, reportez-vous à "Configurer les options de paramètres".

Accédez à la protection BlueXP contre les ransomware

Vous utilisez NetApp BlueXP pour vous connecter au service de protection contre les ransomwares BlueXP.

Pour vous connecter à BlueXP, vous pouvez utiliser vos identifiants du site de support NetApp ou vous inscrire à une connexion au cloud NetApp à l'aide de votre e-mail et de votre mot de passe. "En savoir plus sur la connexion".

Étapes

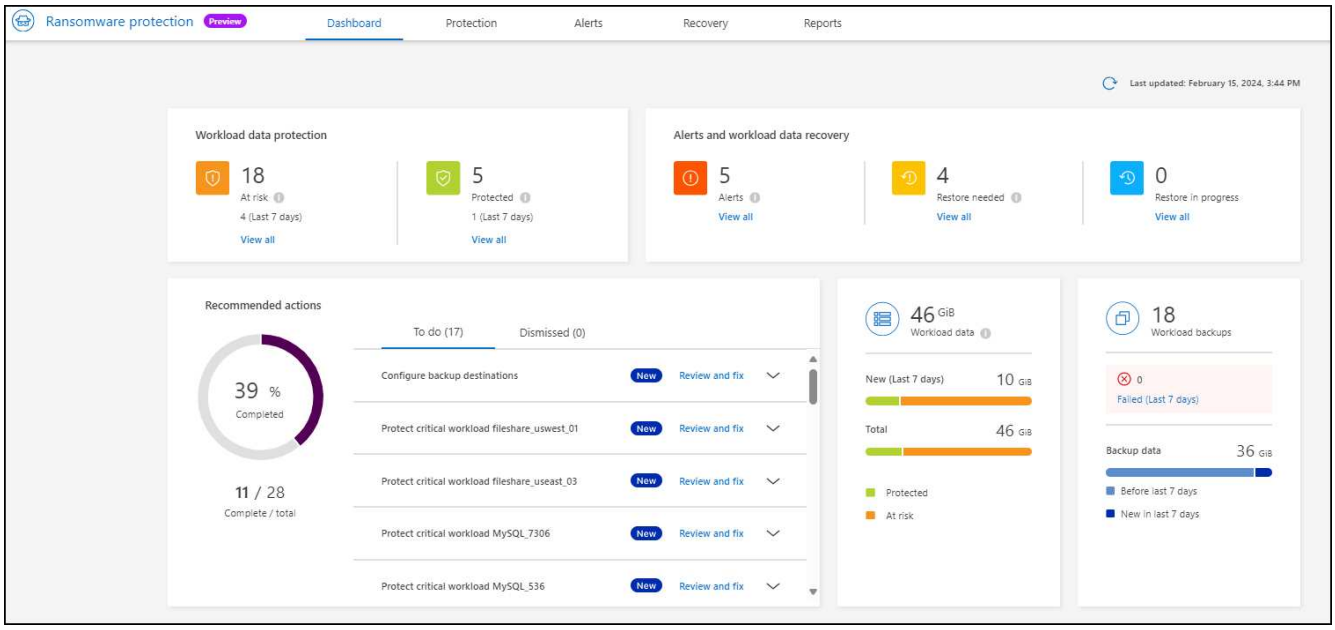
1. Ouvrez un navigateur Web et accédez au "Console BlueXP".

   La page de connexion NetApp BlueXP s'affiche.

2. Connectez-vous à BlueXP.
3. Dans le menu de navigation de gauche de BlueXP, sélectionnez **protection** > **protection contre les ransomware**.

   S'il s'agit de votre première connexion à ce service, la page d'accueil s'affiche.

   Sinon, le tableau de bord de protection BlueXP contre les ransomwares s'affiche.



4. Commencez à utiliser le service.
   - Si vous ne disposez pas d'un connecteur BlueXP ou que ce n'est pas le cas pour cette présentation, vous devrez peut-être contacter le support NetApp ou suivre les messages pour vous inscrire à cette présentation.
   - Si vous découvrez BlueXP et n'avez utilisé aucun connecteur, lorsque vous sélectionnez « * protection contre les ransomware * », un message s'affiche pour vous inscrire. Envoyez le formulaire. NetApp vous contactera au sujet de votre demande d'évaluation.
   - Si vous utilisez BlueXP avec un connecteur existant, lorsque vous sélectionnez "**protection contre les ransomware**", un message s'affiche pour vous inscrire.
   - Si vous participez déjà à l'aperçu, lorsque vous sélectionnez "**protection contre les ransomware**", vous pouvez continuer avec le service. Si vous ne l'avez pas déjà fait, vous devez sélectionner l'option **découvrir les charges de travail**.

Découvrez les workloads dans la solution de protection BlueXP contre les ransomwares

Pour utiliser la protection contre les ransomwares BlueXP, le service doit d'abord détecter les données. Pendant la découverte, la protection contre les ransomwares BlueXP analyse tous les volumes et fichiers des environnements de travail sur tous les connecteurs BlueXP et espaces de travail d'un compte.

Pour la version préliminaire, la protection contre les ransomwares BlueXP évalue les applications MySQL, les applications Oracle, les datastores VMware et les partages de fichiers.

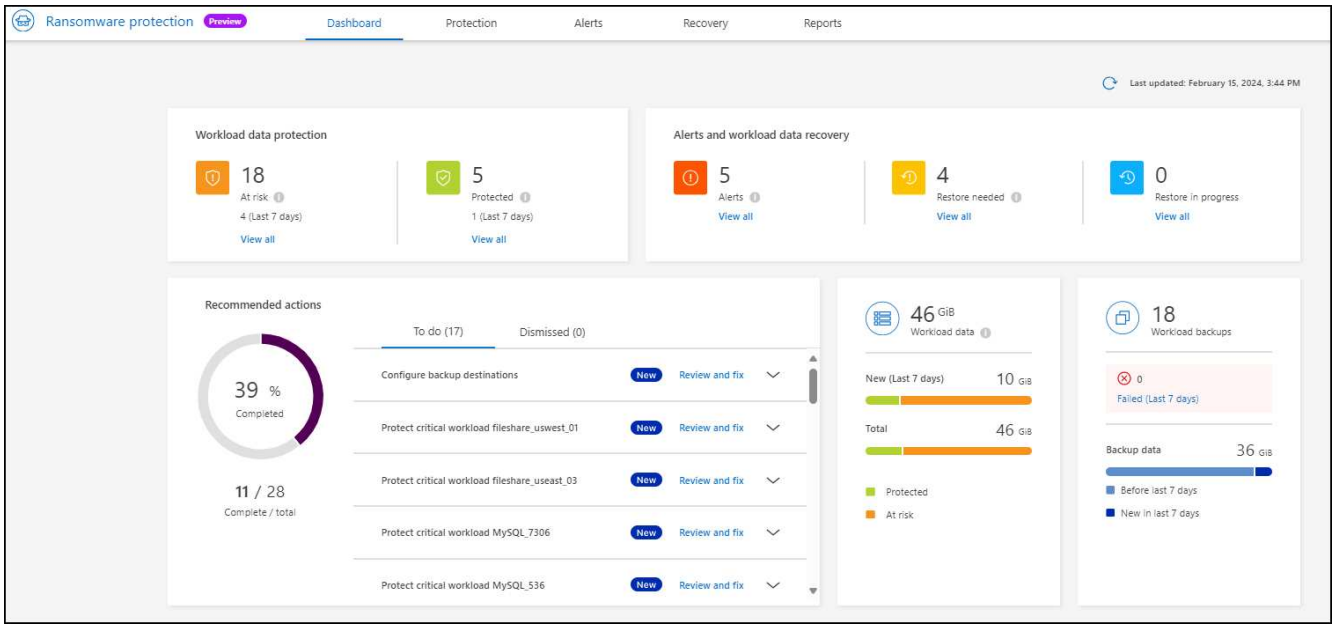
Le service évalue le niveau de protection existant, notamment la protection de sauvegarde actuelle, les copies Snapshot et les options de protection anti-ransomware autonome de NetApp. En fonction de l'évaluation, le service recommande ensuite comment améliorer la protection contre les ransomwares.

Étapes

1. Dans le menu de navigation de gauche de BlueXP, sélectionnez **protection** > **protection contre les ransomware**.

2. Sélectionnez **découvrir les charges de travail** sur la page d'accueil initiale.

   Le service détecte les données du workload et affiche l'état de santé de la protection des données dans le tableau de bord.



Configurez les paramètres de protection contre les ransomwares BlueXP

Vous pouvez configurer une destination de sauvegarde en consultant les recommandations du tableau de bord.

Ajouter une destination de sauvegarde

La protection contre les ransomwares BlueXP permet d'identifier les workloads qui ne disposent pas encore de sauvegardes, ainsi que les workloads pour lesquels aucune destination de sauvegarde n'est attribuée.

Pour protéger ces charges de travail, vous devez ajouter une destination de sauvegarde. Vous pouvez choisir l'une des destinations de sauvegarde suivantes :

- NetApp StorageGRID
- Services Web Amazon (AWS)

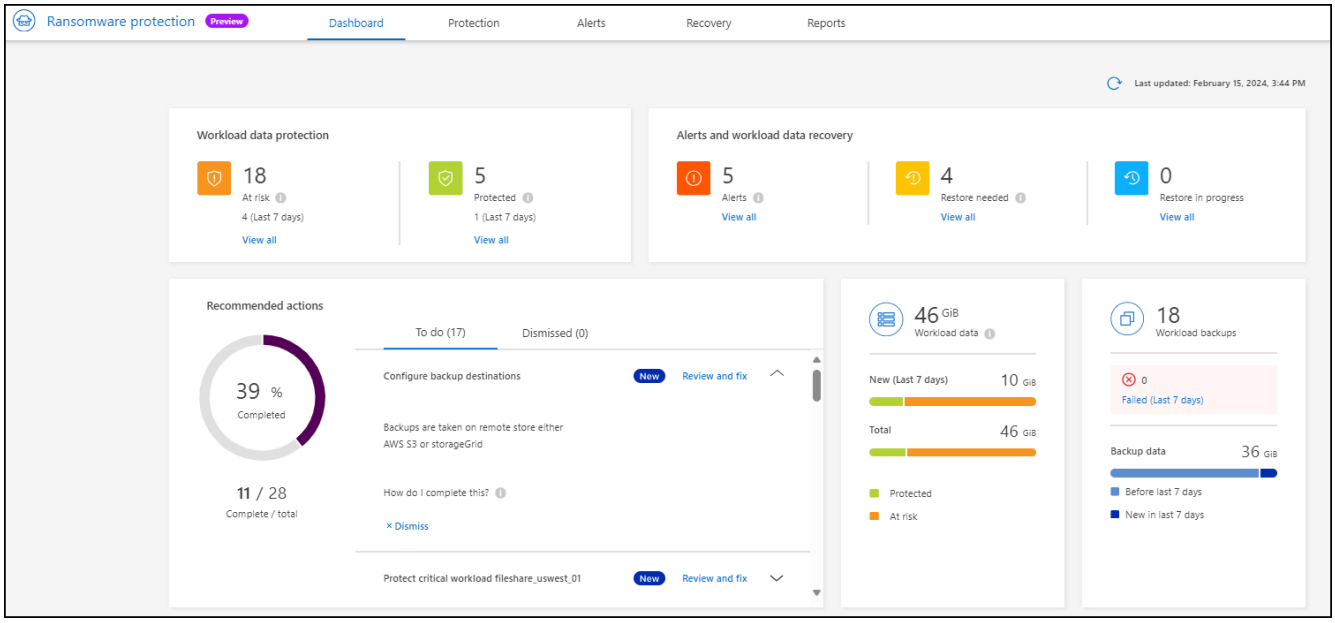
Vous pouvez ajouter une destination de sauvegarde en fonction d'une action recommandée dans le tableau de bord.

Accédez aux options de destination de sauvegarde à partir des actions recommandées du tableau de bord

Le tableau de bord fournit de nombreuses recommandations. Il peut être recommandé de configurer une destination de sauvegarde.

Étapes

1. Dans le menu de navigation de gauche de BlueXP, sélectionnez **protection** > **protection contre les ransomware**.
2. Vérifiez le volet actions recommandées du tableau de bord.

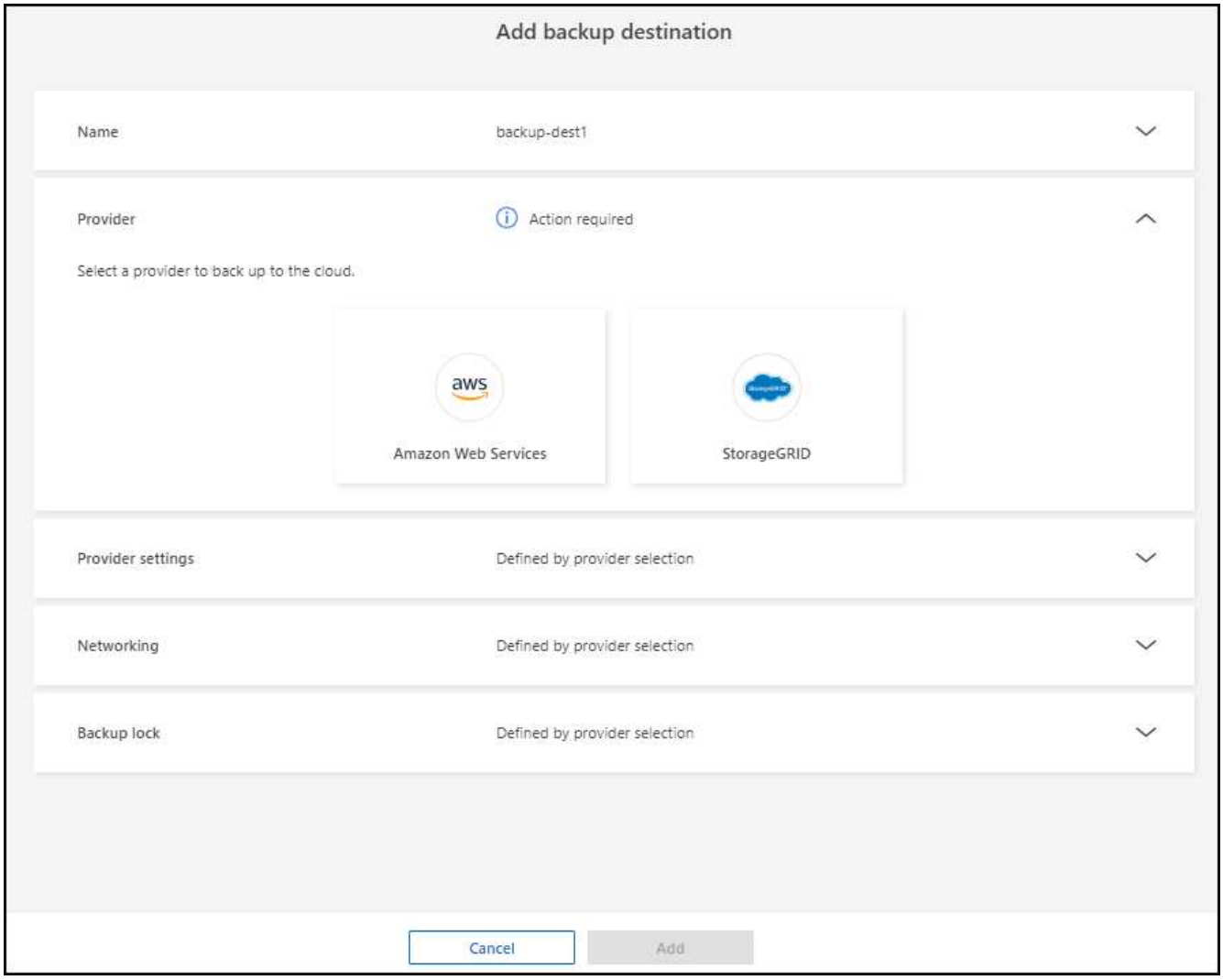


3. Dans le tableau de bord, sélectionnez **revoir et corriger** pour la recommandation de "configurer les destinations de sauvegarde".
4. Suivez les instructions en fonction du fournisseur de sauvegarde.

Ajouter StorageGRID comme destination de sauvegarde

Pour configurer NetApp StorageGRID comme destination de sauvegarde, entrez les informations suivantes.

1. Sur la page **Paramètres > destinations de sauvegarde**, sélectionnez **Ajouter**.
2. Entrez un nom pour la destination de sauvegarde.



3. Sélectionnez **StorageGRID**.
4. Sélectionnez la flèche vers le bas en regard de chaque paramètre et entrez ou sélectionnez des valeurs :
   - **Paramètres du fournisseur** :
     - Créez un nouveau compartiment ou utilisez votre propre compartiment pour stocker les sauvegardes.
     - Nœud de passerelle StorageGRID Nom de domaine complet, port, clé d'accès StorageGRID et informations d'identification de clé secrète.
   - **Mise en réseau** : choisissez l'IPspace.
     - L'IPspace est le cluster où résident les volumes à sauvegarder. Les LIF intercluster pour cet IPspace doivent avoir un accès Internet sortant.
   - **Verrou de sauvegarde** : choisissez si vous souhaitez que le service protège les sauvegardes contre la modification ou la suppression. Cette option utilise la technologie NetApp DataLock. Chaque sauvegarde sera verrouillée pendant la période de conservation, ou pendant un minimum de 30 jours, plus une période tampon de 14 jours maximum.

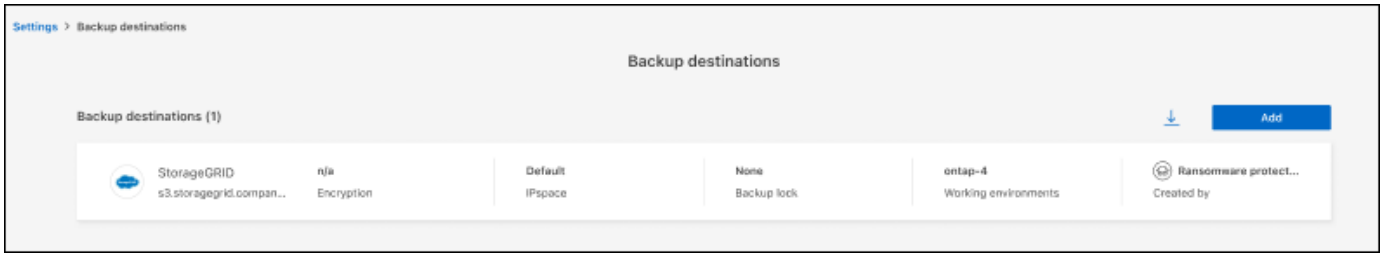
> Si vous configurez le paramètre de verrouillage de sauvegarde maintenant, vous ne pouvez pas le modifier ultérieurement après la configuration de la destination de sauvegarde.

- **Mode de conformité** : les utilisateurs ne peuvent pas écraser ou supprimer les fichiers de sauvegarde protégés pendant la période de conservation.

5. Sélectionnez **Ajouter**.

Résultat

La nouvelle destination de sauvegarde est ajoutée à la liste des destinations de sauvegarde.

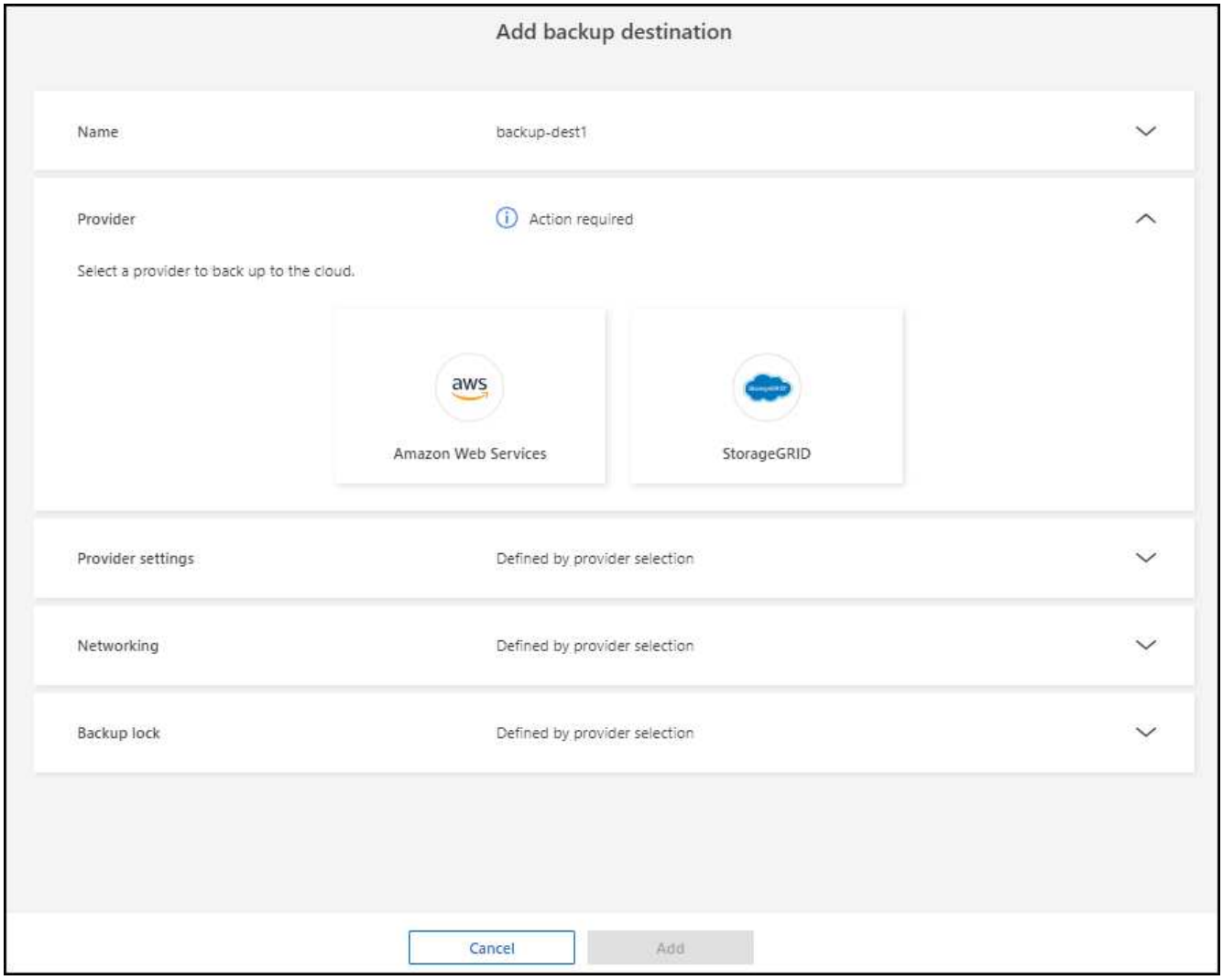


Ajoutez Amazon Web Services comme destination de sauvegarde

Pour configurer AWS en tant que destination de sauvegarde, entrez les informations suivantes.

Pour en savoir plus sur la gestion de votre stockage AWS dans BlueXP, consultez la section "Gestion de vos compartiments Amazon S3".

1. Sur la page **Paramètres > destinations de sauvegarde**, sélectionnez **Ajouter**.
2. Entrez un nom pour la destination de sauvegarde.



3. Sélectionnez **Amazon Web Services**.
4. Sélectionnez la flèche vers le bas en regard de chaque paramètre et entrez ou sélectionnez des valeurs :
   - **Paramètres du fournisseur** :
     - Créez un nouveau compartiment, sélectionnez un compartiment existant s'il en existe déjà dans BlueXP, ou utilisez votre propre compartiment pour stocker les sauvegardes.
     - Compte AWS, région, clé d'accès et clé secrète pour les identifiants AWS

       "Pour ajouter votre propre compartiment, reportez-vous à la section Ajout de compartiments S3".
   - **Encryption** : si vous créez un nouveau compartiment S3, entrez les informations de clé de chiffrement qui vous ont été fournies par le fournisseur. Si vous avez choisi un compartiment existant, les informations de chiffrement sont déjà disponibles.

     Les données qui se trouvent dans le compartiment sont chiffrées avec des clés gérées par AWS par défaut. Vous pouvez continuer à utiliser des clés gérées par AWS ou gérer le chiffrement de vos données à l'aide de vos propres clés.
   - **Mise en réseau** : choisissez l'IPspace et si vous allez utiliser un terminal privé.
     - L'IPspace est le cluster où résident les volumes à sauvegarder. Les LIF intercluster pour cet IPspace doivent avoir un accès Internet sortant.

- Vous pouvez également choisir d'utiliser un terminal privé AWS (PrivateLink) que vous avez configuré précédemment.

  Pour utiliser AWS PrivateLink, reportez-vous à la section "AWS PrivateLink pour Amazon S3".

- **Verrou de sauvegarde** : choisissez si vous souhaitez que le service protège les sauvegardes contre la modification ou la suppression. Cette option utilise la technologie NetApp DataLock. Chaque sauvegarde sera verrouillée pendant la période de conservation, ou pendant un minimum de 30 jours, plus une période tampon de 14 jours maximum.

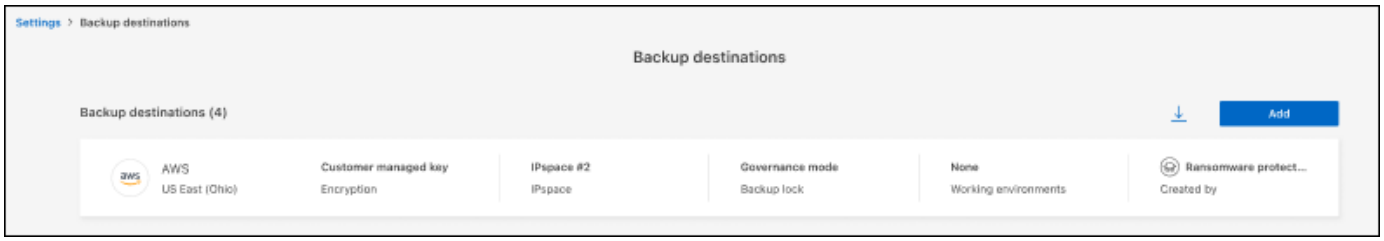
  Si vous configurez le paramètre de verrouillage de sauvegarde maintenant, vous ne pouvez pas le modifier ultérieurement après la configuration de la destination de sauvegarde.

  - **Mode gouvernance** : des utilisateurs spécifiques (avec l'autorisation s3:BypassGovernanceRetention) peuvent écraser ou supprimer des fichiers protégés pendant la période de conservation.
  - **Mode de conformité** : les utilisateurs ne peuvent pas écraser ou supprimer les fichiers de sauvegarde protégés pendant la période de conservation.

5. Sélectionnez **Ajouter**.

Résultat

La nouvelle destination de sauvegarde est ajoutée à la liste des destinations de sauvegarde.



Forum aux questions sur la protection contre les ransomwares BlueXP

Cette FAQ peut vous aider si vous cherchez juste une réponse rapide à une question.

L'accès

Quelle est l'URL de protection contre les ransomware BlueXP ?
Pour l'URL, dans un navigateur, entrez : "https://console.bluexp.netapp.com/" Pour accéder à la console BlueXP.

Avez-vous besoin d'une licence pour utiliser la protection contre les ransomware BlueXP ?
Aucun fichier de licence NetApp n'est requis. La préversion de la protection contre les ransomware BlueXP elle-même ne nécessite aucune licence spéciale. Toutes les licences d'aperçu sont des licences d'évaluation.

La version préliminaire de ce service nécessite une licence du service de sauvegarde et de restauration BlueXP.

Pour la version de prévisualisation, NetApp vous aide à configurer l'évaluation et les licences requises.

Comment activez-vous la protection contre les ransomware BlueXP ?
La protection contre les ransomwares BlueXP ne nécessite aucune activation. L'option de protection contre les ransomware est automatiquement activée dans le menu de navigation gauche de BlueXP.

Pour obtenir la version préliminaire, vous devez vous inscrire ou contacter votre ingénieur commercial NetApp pour essayer ce service. Ensuite, lorsque vous utilisez le connecteur BlueXP, il inclut les fonctionnalités appropriées pour le service.

La protection BlueXP contre les ransomware est-elle disponible en modes standard, restreint et privé ?
Pour l'instant, la protection contre les ransomwares BlueXP n'est disponible qu'en mode standard. Restez à l'affût de tout.

Pour plus d'informations sur ces modes dans tous les services BlueXP, reportez-vous à la section "Modes de déploiement BlueXP".

Comment les autorisations d'accès sont-elles gérées?
Seuls les administrateurs de comptes ont la possibilité de lancer le service et de découvrir les workloads (car cela implique de s'engager à utiliser une ressource). Les interactions suivantes peuvent être effectuées par n'importe quel rôle.

Quelle est la meilleure résolution de périphérique?
La résolution recommandée pour la protection contre les ransomwares BlueXP est de 1920 x 1080 ou supérieure.

Quel navigateur dois-je utiliser?
N'importe quel navigateur moderne fonctionnera.

Interaction avec d'autres services

La protection contre les ransomware BlueXP est-elle consciente des paramètres de protection créés dans NetApp ONTAP ?
Oui, la protection contre les ransomware BlueXP découvre les calendriers Snapshot définis dans ONTAP.

Si vous avez défini une stratégie à l'aide de la protection contre les ransomware BlueXP, devez-vous apporter des modifications futures uniquement dans ce service ?
Nous vous recommandons de modifier les règles à partir du service de protection contre les ransomwares BlueXP.

Charges de travail

Qu'est-ce qui constitue une charge de travail?
Une charge de travail inclut tous les volumes utilisés par une seule instance d'application. Par exemple, une instance de base de données Oracle déployée sur ora3.host.com peut avoir vol1 et vol2 pour ses données et ses journaux, respectivement. Ces volumes constituent ensemble la charge de travail de cette instance spécifique de l'instance Oracle DB.

Comment la protection par ransomware BlueXP hiérarchise-t-elle les données de workload ?
La priorité des données pour la version d'aperçu dépend des copies Snapshot effectuées et des sauvegardes planifiées.

La priorité de la charge de travail est déterminée par les fréquences Snapshot suivantes :

- **Critique** : copies Snapshot prises moins de 1 par heure (planning de protection extrêmement agressif)
- **Important** : copies snapshot prises moins de 1 par jour mais supérieures à 1 par heure
- **Standard**: Copies snapshot prises plus de 1 par jour

Nouveau volume ajouté, mais n'apparaît pas encore
Si vous avez ajouté un volume à votre environnement, lancez de nouveau la découverte et appliquez des règles de protection pour protéger ce nouveau volume.

Le tableau de bord n'affiche pas toutes mes charges de travail. Qu'est-ce qui pourrait se passer?
Actuellement, seuls les volumes NFS sont pris en charge. Les volumes iSCSI, les volumes CIFS et les autres configurations non prises en charge sont filtrés et n'apparaissent pas dans le tableau de bord.

Règles de protection

Les politiques de ransomware de BlueXP coexistent-elles avec les autres types de politiques de workloads ?
À ce stade, la sauvegarde et la restauration BlueXP (Cloud Backup) prennent en charge une règle de sauvegarde par volume. Ainsi, la sauvegarde et la restauration BlueXP ainsi que la protection contre les ransomwares BlueXP partagent les politiques de sauvegarde.

Les copies Snapshot ne sont pas limitées et peuvent être ajoutées séparément pour chaque service.