Notes de version

NetApp Ransomware Resilience

NetApp
January 20, 2026

Sommaire

Notes de version

Nouveautés de NetApp Ransomware Resilience

Découvrez les nouveautés de NetApp Ransomware Resilience.

19 janvier 2026

Volumes non pris en charge

Les rapports de résilience aux ransomwares capturent désormais des informations sur les volumes pris en charge et non pris en charge dans le rapport **Résumé**. Utilisez ces informations pour diagnostiquer pourquoi certains volumes d'un système pourraient ne pas être éligibles à la protection contre les ransomwares.

Pour plus d'informations, voir "Télécharger les rapports dans Ransomware Resilience".

12 janvier 2026

Répliquer les instantanés sur ONTAP

Ransomware Resilience prend désormais en charge l'ajout de la réplication des instantanés vers un site ONTAP secondaire. Avec les groupes de protection qui utilisent une stratégie de réplication, vous pouvez répliquer vers la même destination ou vers des destinations différentes pour chaque charge de travail. Vous pouvez créer une stratégie de protection contre les ransomwares incluant la réplication ou utiliser la stratégie prédéfinie.

Pour plus d'informations, voir "Protéger les charges de travail grâce à la résilience contre les ransomwares".

Exclure les charges de travail de la résilience aux ransomwares

Ransomware Resilience prend désormais en charge l'exclusion de certaines charges de travail d'un système de la protection et du tableau de bord Ransomware Resilience. Vous pouvez exclure les charges de travail après leur découverte, puis les réinclure si vous souhaitez ajouter une protection contre les ransomwares. Les charges de travail exclues ne vous seront pas facturées.

Pour plus d'informations, voir "Exclure les charges de travail".

Les alertes marquées comme étant en cours de révision

Ransomware Resilience vous permet désormais de marquer les alertes comme « En cours d'examen ». Utilisez l'étiquette « En cours d'examen » pour améliorer la clarté au sein de votre équipe lors du tri et de la gestion des menaces de ransomware actives.

Pour plus d'informations, voir "Gérer les alertes dans Ransomware Resilience".

8 décembre 2025

Le blocage des extensions est activé au niveau de la charge de travail.

Lorsque vous activez le blocage des extensions, celui-ci est désormais activé au niveau de la charge de travail et non plus au niveau de la machine virtuelle de stockage.

Modifier l’état d’alerte du comportement de l’utilisateur

Ransomware Resilience vous permet désormais de modifier le statut des alertes comportementales des utilisateurs. Vous pouvez ignorer et résoudre manuellement les alertes.

Pour plus d’informations, voir "Gérer les alertes dans Ransomware Resilience".

Prise en charge de plusieurs agents de console

Ransomware Resilience prend désormais en charge l’utilisation de plusieurs agents Console pour gérer les mêmes systèmes.

Pour plus d’informations sur les agents de console, consultez"Créer un agent de console" .

10 novembre 2025

Cette version comprend des améliorations générales.

06 octobre 2025

La BlueXP ransomware protection est désormais NetApp Ransomware Resilience

Le service de BlueXP ransomware protection a été renommé NetApp Ransomware Resilience.

BlueXP est désormais NetApp Console

La NetApp Console offre une gestion centralisée des services de stockage et de données dans les environnements sur site et dans le cloud à l’échelle de l’entreprise, offrant des informations en temps réel, des flux de travail plus rapides et une administration simplifiée.

Pour plus de détails sur ce qui a changé, consultez le "Notes de version de la NetApp Console" .

Détection de violation de données

Ransomware Resilience inclut un nouveau mécanisme de détection qui peut être activé en quelques étapes pour détecter les lectures anormales des utilisateurs comme indicateur précoce d’une violation de données. La résilience des ransomwares collecte et analyse les événements de lecture des utilisateurs en créant une base de référence historique, qui est un profil du comportement normal attendu à partir des données passées. Lorsque l’activité d’un nouvel utilisateur s’écarte considérablement de cette norme établie (comme une augmentation inattendue des lectures associée à des modèles de lecture suspects), une alerte est générée. Ransomware Resilience inclut un modèle d’IA pour détecter les modèles de lecture suspects.

Contrairement à la détection de chiffrement par ARP au niveau de la couche de stockage, la détection de l’anomalie de comportement de l’utilisateur est effectuée dans le service SaaS Ransomware Resilience en collectant les événements FPolicy.

> Vous devez utiliser le nouveau"Administrateur du comportement utilisateur de Ransomware Resilience et visualiseur du comportement utilisateur de Ransomware Resilience" rôles pour accéder aux paramètres de détection des comportements suspects des utilisateurs.

Pour plus d’informations, voir"Activer la détection des activités suspectes des utilisateurs" et"Afficher le comportement anormal des utilisateurs" .

Détections supplémentaires d'activités suspectes d'utilisateurs

En plus de la détection des violations de données, Ransomware Resilience détecte également les types d'alertes suivants en fonction de l'activité suspecte observée des utilisateurs :

- **Destruction de données - attaque potentielle** - Une alerte avec la gravité d'une attaque potentielle est créée lorsque le nombre de suppressions de fichiers dépasse la norme historique.
- **Comportement suspect de l'utilisateur - attaque potentielle** - Une alerte avec la gravité d'une attaque potentielle est créée lorsque des opérations de lecture, de renommage et de suppression dans une séquence similaire à une attaque de ransomware sont observées
- **Comportement suspect de l'utilisateur - Avertissement** - Une alerte avec la gravité d'un avertissement est créée lorsque le nombre total d'activités de fichiers (lecture, suppression, renommage, etc.) dépasse la norme historique

Nouveaux rôles d'utilisateur pour la détection des violations de données

Pour gérer les alertes d'activité utilisateur suspecte, Ransomware Resilience a introduit deux nouveaux rôles pour les administrateurs de l'organisation de la console afin d'accorder l'accès à la détection d'activité utilisateur suspecte : administrateur du comportement utilisateur Ransomware Resilience et visualiseur du comportement utilisateur Ransomware Resilience.

Vous devez être un administrateur du comportement utilisateur pour configurer les paramètres de comportement utilisateur suspect. Le rôle d'administrateur Ransomware Resilience n'est pas pris en charge pour la configuration des paramètres de comportement utilisateur suspect.

Pour plus d'informations, consultez la section "Accès basé sur les rôles NetApp Ransomware Resilience" .

12 août 2025

Cette version comprend des améliorations générales.

15 juillet 2025

Prise en charge de la charge de travail SAN

Cette version inclut la prise en charge des charges de travail SAN dans la BlueXP ransomware protection. Vous pouvez désormais protéger les charges de travail SAN en plus des charges de travail NFS et CIFS.

Pour plus d'informations, reportez-vous à "Conditions préalables à la BlueXP ransomware protection" .

Protection améliorée de la charge de travail

Cette version améliore le processus de configuration des charges de travail avec des stratégies de snapshot et de sauvegarde provenant d'autres outils NetApp tels que SnapCenter ou BlueXP backup and recovery. Dans les versions précédentes, la BlueXP ransomware protection détectait les politiques d'autres outils, vous permettant uniquement de modifier la politique de détection. Avec cette version, vous pouvez désormais remplacer les politiques de snapshot et de sauvegarde par les politiques de BlueXP ransomware protection ou continuer à utiliser les politiques d'autres outils.

Pour plus de détails, reportez-vous à"Protéger les charges de travail" .

Notifications par e-mail

Si la BlueXP ransomware protection détecte une attaque possible, une notification apparaît dans les notifications BlueXP et un e-mail est envoyé à l'adresse e-mail que vous avez configurée.

L'e-mail contient des informations sur la gravité, la charge de travail impactée et un lien vers l'alerte dans l'onglet **Alertes** de BlueXP ransomware protection .

Si vous avez configuré un système de gestion de la sécurité et des événements (SIEM) dans la BlueXP ransomware protection, le service envoie les détails des alertes à votre système SIEM.

Pour plus de détails, reportez-vous à"Gérer les alertes de ransomware détectées" .

9 juin 2025

Mises à jour de la page de destination

Cette version inclut des mises à jour de la page de destination pour la BlueXP ransomware protection qui facilitent le démarrage de l'essai gratuit et la découverte.

Mises à jour sur les exercices de préparation

Auparavant, vous pouviez exécuter un exercice de préparation aux ransomwares en simulant une attaque sur un nouvel exemple de charge de travail. Grâce à cette fonctionnalité, vous pouvez enquêter sur l'attaque simulée et récupérer la charge de travail. Utilisez cette fonctionnalité pour tester les notifications d'alerte, la réponse et la récupération. Exécutez et planifiez ces exercices aussi souvent que nécessaire.

Avec cette version, vous pouvez utiliser un nouveau bouton sur le tableau de bord de BlueXP ransomware protection pour exécuter un exercice de préparation aux ransomwares sur une charge de travail de test, ce qui vous permet de simuler plus facilement des attaques de ransomwares, d'étudier leur impact et de récupérer efficacement les charges de travail, le tout dans un environnement contrôlé.

Vous pouvez désormais exécuter des exercices de préparation sur les charges de travail CIFS (SMB) en plus des charges de travail NFS.

Pour plus de détails, reportez-vous à "Effectuer un exercice de préparation aux attaques de ransomware" .

Activer les mises à jour de BlueXP classification

Avant d'utiliser la BlueXP classification dans le service de BlueXP ransomware protection , vous devez activer la BlueXP classification pour analyser vos données. La classification des données vous aide à trouver des informations personnelles identifiables (PII), ce qui peut augmenter les risques de sécurité.

Vous pouvez déployer la BlueXP classification sur une charge de travail de partage de fichiers à partir de la BlueXP ransomware protection. Dans la colonne **Exposition à la confidentialité**, sélectionnez l'option **Identifier l'exposition**. Si vous avez activé le service de classification, cette action identifie l'exposition. Sinon, avec cette version, une boîte de dialogue présente la possibilité de déployer la BlueXP classification. Sélectionnez **Déployer** pour accéder à la page de destination du service de BlueXP classification , où vous pouvez déployer ce service. W

Pour plus de détails, reportez-vous à "Déployer la BlueXP classification dans le cloud" et pour utiliser le service dans la BlueXP ransomware protection, reportez-vous à "Rechercher des informations personnelles identifiables avec la BlueXP classification" .

13 mai 2025

Signalement d'environnements de travail non pris en charge dans la BlueXP ransomware protection

Pendant le flux de travail de découverte, la BlueXP ransomware protection signale plus de détails lorsque vous passez la souris sur les charges de travail prises en charge ou non prises en charge. Cela vous aidera à comprendre pourquoi certaines de vos charges de travail ne sont pas détectées par le service de BlueXP ransomware protection .

Il existe de nombreuses raisons pour lesquelles le service ne prend pas en charge un environnement de travail. Par exemple, la version ONTAP de votre environnement de travail peut être inférieure à la version requise. Lorsque vous survolez un environnement de travail non pris en charge, une info-bulle affiche la raison.

Vous pouvez afficher les environnements de travail non pris en charge lors de la découverte initiale, où vous pouvez également télécharger les résultats. Vous pouvez également afficher les résultats de la découverte à partir de l'option **Découverte de charge de travail** dans la page Paramètres.

Pour plus de détails, reportez-vous à "Découvrez les charges de travail dans la BlueXP ransomware protection" .

29 avril 2025

Prise en charge d' Amazon FSx for NetApp ONTAP

Cette version prend en charge Amazon FSx for NetApp ONTAP. Cette fonctionnalité vous aide à protéger vos charges de travail FSx for ONTAP avec la BlueXP ransomware protection.

FSx for ONTAP est un service entièrement géré qui fournit la puissance du stockage NetApp ONTAP dans le cloud. Il offre les mêmes fonctionnalités, performances et capacités administratives que celles que vous utilisez sur site avec l'agilité et l'évolutivité d'un service AWS natif.

Les modifications suivantes ont été apportées au flux de travail de BlueXP ransomware protection :

- Discovery inclut les charges de travail dans les environnements de travail FSx pour ONTAP 9.15.
- L'onglet Protection affiche les charges de travail dans les environnements FSx for ONTAP . Dans cet environnement, vous devez effectuer des opérations de sauvegarde à l'aide du service de sauvegarde FSx for ONTAP . Vous pouvez restaurer ces charges de travail à l'aide des instantanés de BlueXP ransomware protection .

  Les politiques de sauvegarde pour une charge de travail exécutée sur FSx pour ONTAP ne peuvent pas être définies dans BlueXP. Toutes les politiques de sauvegarde existantes définies dans Amazon FSx for NetApp ONTAP restent inchangées.

- Les incidents d'alerte montrent le nouvel environnement de travail FSx pour ONTAP .

Pour plus de détails, reportez-vous à "En savoir plus sur la BlueXP ransomware protection" .

Pour plus d'informations sur les options prises en charge, reportez-vous à la "Limitations de la BlueXP ransomware protection" .

Rôle d'accès BlueXP requis

Vous avez désormais besoin de l'un des rôles d'accès suivants pour afficher, découvrir ou gérer la BlueXP ransomware protection: administrateur de l'organisation, administrateur de dossier ou de projet, administrateur

de la protection contre les ransomwares ou visualiseur de protection contre les ransomwares.

"En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

14 avril 2025

Rapports d'exercices de préparation

Avec cette version, vous pouvez consulter les rapports d'exercices de préparation aux attaques de ransomware. Un exercice de préparation vous permet de simuler une attaque de ransomware sur un échantillon de charge de travail nouvellement créé. Ensuite, examinez l'attaque simulée et récupérez l'exemple de charge de travail. Cette fonctionnalité vous aide à savoir que vous êtes préparé en cas d'attaque réelle de ransomware en testant les processus de notification d'alerte, de réponse et de récupération.

Pour plus de détails, reportez-vous à "Effectuer un exercice de préparation aux attaques de ransomware" .

Nouveaux rôles et autorisations de contrôle d'accès basés sur les rôles

Auparavant, vous pouviez attribuer des rôles et des autorisations aux utilisateurs en fonction de leurs responsabilités, ce qui vous aide à gérer l'accès des utilisateurs à la BlueXP ransomware protection. Avec cette version, il existe deux nouveaux rôles spécifiques à la BlueXP ransomware protection avec des autorisations mises à jour. Les nouveaux rôles sont :

- Administrateur de la protection contre les ransomwares
- Visionneuse de protection contre les ransomwares

Pour plus de détails sur les autorisations, reportez-vous à "Accès aux fonctionnalités basé sur les rôles de BlueXP ransomware protection" .

Améliorations des paiements

Cette version inclut plusieurs améliorations au processus de paiement.

Pour plus de détails, reportez-vous à "Configurer les options de licence et de paiement" .

10 mars 2025

Simulez une attaque et répondez

Avec cette version, simulez une attaque de ransomware pour tester votre réponse à une alerte de ransomware. Cette fonctionnalité vous aide à savoir que vous êtes préparé en cas d'attaque réelle de ransomware en testant les processus de notification d'alerte, de réponse et de récupération.

Pour plus de détails, reportez-vous à "Effectuer un exercice de préparation aux attaques de ransomware" .

Améliorations du processus de découverte

Cette version inclut des améliorations aux processus de découverte et de redécouverte sélectives :

- Avec cette version, vous pouvez découvrir les charges de travail nouvellement créées qui ont été ajoutées aux environnements de travail précédemment sélectionnés.
- Vous pouvez également sélectionner de *nouveaux* environnements de travail dans cette version. Cette fonctionnalité vous aide à protéger les nouvelles charges de travail ajoutées à votre environnement.

- Vous pouvez effectuer ces processus de découverte au cours du processus de découverte initial ou dans l'option Paramètres.

Pour plus de détails, reportez-vous à "Découvrez les charges de travail nouvellement créées pour les environnements de travail précédemment sélectionnés" et "Configurer les fonctionnalités avec l'option Paramètres" .

Alertes déclenchées lorsqu'un cryptage élevé est détecté

Avec cette version, vous pouvez afficher des alertes lorsqu'un cryptage élevé est détecté sur vos charges de travail, même sans modifications d'extension de fichier élevées. Cette fonctionnalité, qui utilise l'IA ONTAP Autonomous Ransomware Protection (ARP), vous aide à identifier les charges de travail exposées au risque d'attaques de ransomware. Utilisez cette fonctionnalité et téléchargez la liste complète des fichiers impactés avec ou sans modifications d'extension.

Pour plus de détails, reportez-vous à "Répondre à une alerte de ransomware détectée" .

16 décembre 2024

Détectez les comportements anormaux des utilisateurs à l'aide de Data Infrastructure Insights Storage Workload Security

Avec cette version, vous pouvez utiliser Data Infrastructure Insights Storage Workload Security pour détecter les comportements anormaux des utilisateurs dans vos charges de travail de stockage. Cette fonctionnalité vous aide à identifier les menaces de sécurité potentielles et à bloquer les utilisateurs potentiellement malveillants pour protéger vos données.

Pour plus de détails, reportez-vous à "Répondre à une alerte de ransomware détectée" .

Avant d'utiliser Data Infrastructure Insights Storage Workload Security pour détecter un comportement utilisateur anormal, vous devez configurer l'option à l'aide de l'option **Paramètres** de BlueXP ransomware protection .

Se référer à "Configurer les paramètres de BlueXP ransomware protection" .

Sélectionnez les charges de travail à découvrir et à protéger

Avec cette version, vous pouvez désormais effectuer les opérations suivantes :

- Dans chaque connecteur, sélectionnez les environnements de travail dans lesquels vous souhaitez découvrir les charges de travail. Vous pourriez bénéficier de cette fonctionnalité si vous souhaitez protéger des charges de travail spécifiques dans votre environnement et pas d'autres.
- Lors de la découverte de charges de travail, vous pouvez activer la découverte automatique des charges de travail par connecteur. Cette fonctionnalité vous permet de sélectionner les charges de travail que vous souhaitez protéger.
- Découvrez les charges de travail nouvellement créées pour les environnements de travail précédemment sélectionnés.

Se référer à "Découvrir les charges de travail" .

7 novembre 2024

Activer la classification des données et rechercher des informations personnelles identifiables (PII)

Avec cette version, vous pouvez activer la BlueXP classification, un composant essentiel de la famille BlueXP , pour analyser et classer les données dans vos charges de travail de partage de fichiers. La classification des données vous aide à identifier si vos données contiennent des informations personnelles ou privées, ce qui peut augmenter les risques de sécurité. Ce processus a également un impact sur l'importance de la charge de travail et vous aide à garantir que vous protégez les charges de travail avec le niveau de protection approprié.

L'analyse des données PII dans la BlueXP ransomware protection est généralement disponible pour les clients qui ont déployé la BlueXP classification. La BlueXP classification est disponible dans le cadre de la plateforme BlueXP sans frais supplémentaires et peut être déployée sur site ou dans le cloud client.

Se référer à "Configurer les paramètres de BlueXP ransomware protection" .

Pour lancer l'analyse, sur la page Protection, cliquez sur **Identifier l'exposition** dans la colonne Exposition à la confidentialité.

"Recherchez des données sensibles personnellement identifiables avec la BlueXP classification" .

Intégration SIEM avec Microsoft Sentinel

Vous pouvez désormais envoyer des données à votre système de gestion de la sécurité et des événements (SIEM) pour l'analyse et la détection des menaces à l'aide de Microsoft Sentinel. Auparavant, vous pouviez sélectionner AWS Security Hub ou Splunk Cloud comme SIEM.

"En savoir plus sur la configuration des paramètres de BlueXP ransomware protection" .

Essai gratuit maintenant 30 jours

Avec cette version, les nouveaux déploiements de la BlueXP ransomware protection bénéficient désormais d'un essai gratuit de 30 jours. Auparavant, la BlueXP ransomware protection offrait 90 jours d'essai gratuit. Si vous bénéficiez déjà de l'essai gratuit de 90 jours, cette offre se poursuit pendant 90 jours.

Restaurer la charge de travail de l'application au niveau du fichier pour Podman

Avant de restaurer une charge de travail d'application au niveau du fichier, vous pouvez désormais afficher une liste des fichiers susceptibles d'avoir été affectés par une attaque et identifier ceux que vous souhaitez restaurer. Auparavant, si les connecteurs BlueXP d'une organisation (auparavant un compte) utilisaient Podman, cette fonctionnalité était désactivée. Il est désormais activé pour Podman. Vous pouvez laisser la BlueXP ransomware protection choisir les fichiers à restaurer, vous pouvez télécharger un fichier CSV qui répertorie tous les fichiers impactés par une alerte, ou vous pouvez identifier manuellement les fichiers que vous souhaitez restaurer.

"En savoir plus sur la récupération après une attaque de ransomware" .

30 septembre 2024

Regroupement personnalisé des charges de travail de partage de fichiers

Avec cette version, vous pouvez désormais regrouper les partages de fichiers en groupes pour faciliter la protection de votre parc de données. Le service peut protéger tous les volumes d'un groupe en même temps. Auparavant, vous deviez protéger chaque volume séparément.

"En savoir plus sur le regroupement des charges de travail de partage de fichiers dans les stratégies de protection contre les ransomwares" .

2 septembre 2024

Évaluation des risques de sécurité par Digital Advisor

La BlueXP ransomware protection collecte désormais des informations sur les risques de sécurité élevés et critiques liés à un cluster à partir de NetApp Digital Advisor. Si un risque est détecté, la BlueXP ransomware protection fournit une recommandation dans le volet **Actions recommandées** du tableau de bord : « Corriger une vulnérabilité de sécurité connue sur le cluster <nom>. » À partir de la recommandation sur le tableau de bord, cliquer sur **Examiner et corriger** suggère de consulter Digital Advisor et un article sur les vulnérabilités et expositions courantes (CVE) pour résoudre le risque de sécurité. S'il existe plusieurs risques de sécurité, consultez les informations dans Digital Advisor.

Se référer à "Documentation du Digital Advisor" .

Sauvegarde sur Google Cloud Platform

Avec cette version, vous pouvez définir une destination de sauvegarde sur un bucket Google Cloud Platform. Auparavant, vous pouviez ajouter des destinations de sauvegarde uniquement à NetApp StorageGRID, Amazon Web Services et Microsoft Azure.

"En savoir plus sur la configuration des paramètres de BlueXP ransomware protection" .

Prise en charge de Google Cloud Platform

Le service prend désormais en charge Cloud Volumes ONTAP pour Google Cloud Platform pour la protection du stockage. Auparavant, le service prenait uniquement en charge Cloud Volumes ONTAP pour Amazon Web Services et Microsoft Azure ainsi que le NAS sur site.

"En savoir plus sur la BlueXP ransomware protection et les sources de données prises en charge, les destinations de sauvegarde et les environnements de travail" .

Contrôle d'accès basé sur les rôles

Vous pouvez désormais limiter l'accès à des activités spécifiques grâce au contrôle d'accès basé sur les rôles (RBAC). La BlueXP ransomware protection utilise deux rôles de BlueXP: administrateur de compte BlueXP et administrateur non-compte (spectateur).

Pour plus de détails sur les actions que chaque rôle peut effectuer, voir "Privilèges de contrôle d'accès basés sur les rôles" .

5 août 2024

Détection des menaces avec Splunk Cloud

Vous pouvez envoyer automatiquement des données à votre système de gestion de la sécurité et des événements (SIEM) pour l'analyse et la détection des menaces. Avec les versions précédentes, vous pouviez sélectionner uniquement AWS Security Hub comme SIEM. Avec cette version, vous pouvez sélectionner AWS Security Hub ou Splunk Cloud comme SIEM.

"En savoir plus sur la configuration des paramètres de BlueXP ransomware protection" .

1er juillet 2024

Apportez votre propre permis de conduire (BYOL)

Avec cette version, vous pouvez utiliser une licence BYOL, qui est un fichier de licence NetApp (NLF) que vous obtenez auprès de votre représentant commercial NetApp .

"En savoir plus sur la configuration des licences" .

Restaurer la charge de travail de l'application au niveau du fichier

Avant de restaurer une charge de travail d'application au niveau du fichier, vous pouvez désormais afficher une liste des fichiers susceptibles d'avoir été affectés par une attaque et identifier ceux que vous souhaitez restaurer. Vous pouvez laisser la BlueXP ransomware protection choisir les fichiers à restaurer, vous pouvez télécharger un fichier CSV qui répertorie tous les fichiers impactés par une alerte, ou vous pouvez identifier manuellement les fichiers que vous souhaitez restaurer.

Avec cette version, si tous les connecteurs BlueXP d'un compte n'utilisent pas Podman, la fonction de restauration de fichier unique est activée. Sinon, il est désactivé pour ce compte.

"En savoir plus sur la récupération après une attaque de ransomware" .

Télécharger une liste des fichiers impactés

Avant de restaurer une charge de travail d'application au niveau du fichier, vous pouvez désormais accéder à la page Alertes pour télécharger une liste des fichiers impactés dans un fichier CSV, puis utiliser la page Récupération pour télécharger le fichier CSV.

"En savoir plus sur le téléchargement des fichiers concernés avant de restaurer une application" .

Supprimer le plan de protection

Avec cette version, vous pouvez désormais supprimer une stratégie de protection contre les ransomwares.

"En savoir plus sur la protection des charges de travail et la gestion des stratégies de protection contre les ransomwares" .

10 juin 2024

Verrouillage de copie instantanée sur le stockage principal

Activez cette option pour verrouiller les copies instantanées sur le stockage principal afin qu'elles ne puissent pas être modifiées ou supprimées pendant une certaine période, même si une attaque de ransomware parvient à atteindre la destination de stockage de sauvegarde.

"En savoir plus sur la protection des charges de travail et l'activation du verrouillage des sauvegardes dans une stratégie de protection contre les ransomwares" .

Prise en charge de Cloud Volumes ONTAP pour Microsoft Azure

Cette version prend en charge Cloud Volumes ONTAP pour Microsoft Azure en tant que système en plus de Cloud Volumes ONTAP pour AWS et du NAS ONTAP sur site.

"Démarrage rapide de Cloud Volumes ONTAP dans Azure"

"En savoir plus sur la BlueXP ransomware protection" .

Microsoft Azure ajouté comme destination de sauvegarde

Vous pouvez désormais ajouter Microsoft Azure comme destination de sauvegarde avec AWS et NetApp StorageGRID.

"En savoir plus sur la configuration des paramètres de protection" .

14 mai 2024

Mises à jour des licences

Vous pouvez vous inscrire pour un essai gratuit de 90 jours. Bientôt, vous pourrez acheter un abonnement à la carte auprès d'Amazon Web Services Marketplace ou apporter votre propre licence NetApp .

"En savoir plus sur la configuration des licences" .

Protocole CIFS

Le service prend désormais en charge ONTAP sur site et Cloud Volumes ONTAP dans les systèmes AWS utilisant les protocoles NFS et CIFS. La version précédente ne prenait en charge que le protocole NFS.

Détails de la charge de travail

Cette version fournit désormais plus de détails sur les informations de charge de travail à partir des pages Protection et autres pour une meilleure évaluation de la protection de la charge de travail. À partir des détails de la charge de travail, vous pouvez consulter la politique actuellement attribuée et examiner les destinations de sauvegarde configurées.

"En savoir plus sur l'affichage des détails de la charge de travail dans les pages de protection" .

Protection et récupération cohérentes avec les applications et les machines virtuelles

Vous pouvez désormais effectuer une protection cohérente au niveau des applications avec le logiciel NetApp SnapCenter et une protection cohérente au niveau des machines virtuelles avec le SnapCenter Plug-in for VMware vSphere, en obtenant un état de repos et cohérent pour éviter toute perte de données potentielle ultérieure si une récupération est nécessaire. Si une récupération est nécessaire, vous pouvez restaurer l'application ou la machine virtuelle à l'un des états précédemment disponibles.

"En savoir plus sur la protection des charges de travail" .

Stratégies de protection contre les ransomwares

Si les stratégies de capture instantanée ou de sauvegarde n'existent pas sur la charge de travail, vous pouvez créer une stratégie de protection contre les ransomwares, qui peut inclure les stratégies suivantes que vous créez dans ce service :

- Politique d'instantané
- Politique de sauvegarde
- Politique de détection

"En savoir plus sur la protection des charges de travail" .

Détection des menaces

L'activation de la détection des menaces est désormais disponible à l'aide d'un système tiers de gestion de la sécurité et des événements (SIEM). Le tableau de bord affiche désormais une nouvelle recommandation « Activer la détection des menaces » qui peut être configurée sur la page Paramètres.

"En savoir plus sur la configuration des options de paramètres" .

Ignorer les alertes de faux positifs

Depuis l'onglet Alertes, vous pouvez désormais ignorer les faux positifs ou décider de récupérer vos données immédiatement.

"En savoir plus sur la réponse à une alerte de ransomware" .

État de détection

De nouveaux statuts de détection apparaissent sur la page Protection, indiquant le statut de la détection de ransomware appliquée à la charge de travail.

"En savoir plus sur la protection des charges de travail et l'affichage des états de protection" .

Télécharger les fichiers CSV

Vous pouvez télécharger des fichiers CSV* à partir des pages Protection, Alertes et Récupération.

"En savoir plus sur le téléchargement de fichiers CSV à partir du tableau de bord et d'autres pages" .

Lien vers la documentation

Le lien vers la documentation est désormais inclus dans l'interface utilisateur. Vous pouvez accéder à cette documentation à partir du tableau de bord vertical **Actions***  **option. Sélectionnez *Quoi de neuf** pour afficher les détails dans les notes de publication ou **Documentation** pour afficher la page d'accueil de la documentation sur la BlueXP ransomware protection .

BlueXP backup and recovery

Le service de BlueXP backup and recovery n'a plus besoin d'être déjà activé sur le système. Voir "prérequis" . Le service de BlueXP ransomware protection permet de configurer une destination de sauvegarde via l'option Paramètres. Voir "Configurer les paramètres" .

Option Paramètres

Vous pouvez désormais configurer des destinations de sauvegarde dans les paramètres de BlueXP ransomware protection .

"En savoir plus sur la configuration des options de paramètres" .

5 mars 2024

Gestion des politiques de protection

En plus d'utiliser des politiques prédéfinies, vous pouvez désormais créer des politiques. "En savoir plus sur la

gestion des politiques" .

Immuabilité sur le stockage secondaire (DataLock)

Vous pouvez désormais rendre la sauvegarde immuable dans le stockage secondaire à l'aide de la technologie NetApp DataLock dans le magasin d'objets. "En savoir plus sur la création de politiques de protection" .

Sauvegarde automatique sur NetApp StorageGRID

En plus d'utiliser AWS, vous pouvez désormais choisir StorageGRID comme destination de sauvegarde. "En savoir plus sur la configuration des destinations de sauvegarde" .

Fonctionnalités supplémentaires pour enquêter sur les attaques potentielles

Vous pouvez désormais afficher davantage de détails médico-légaux pour enquêter sur l'attaque potentielle détectée. "En savoir plus sur la réponse à une alerte de ransomware détectée" .

Processus de récupération

Le processus de récupération a été amélioré. Vous pouvez désormais récupérer volume par volume ou tous les volumes d'une charge de travail. "En savoir plus sur la récupération après une attaque de ransomware (après la neutralisation des incidents)" .

"En savoir plus sur la BlueXP ransomware protection" .

6 octobre 2023

Le service de BlueXP ransomware protection est une solution SaaS permettant de protéger les données, de détecter les attaques potentielles et de récupérer les données après une attaque de ransomware.

Pour la version préliminaire, le service protège les charges de travail applicatives d'Oracle, les banques de données de machines virtuelles et les partages de fichiers sur le stockage NAS sur site ainsi que sur Cloud Volumes ONTAP sur AWS (en utilisant le protocole NFS) au sein des organisations BlueXP individuellement et sauvegarde les données sur le stockage cloud Amazon Web Services.

Le service de BlueXP ransomware protection offre une utilisation complète de plusieurs technologies NetApp afin que votre administrateur de sécurité des données ou votre ingénieur des opérations de sécurité puisse atteindre les objectifs suivants :

- Affichez en un coup d'œil la protection contre les ransomwares sur toutes vos charges de travail.
- Obtenez un aperçu des recommandations de protection contre les ransomwares
- Améliorez votre posture de protection en fonction des recommandations de BlueXP ransomware protection .
- Attribuez des politiques de protection contre les ransomwares pour protéger vos principales charges de travail et vos données à haut risque contre les attaques de ransomwares.
- Surveillez la santé de vos charges de travail contre les attaques de ransomware à la recherche d'anomalies de données.
- Évaluez rapidement l'impact des incidents de ransomware sur votre charge de travail.
- Récupérez intelligemment des incidents de ransomware en restaurant les données et en garantissant qu'aucune réinfection à partir des données stockées ne se produise.

"En savoir plus sur la BlueXP ransomware protection" .

Limitations connues de NetApp Ransomware Resilience

Les limitations connues identifient les plates-formes, les appareils ou les fonctions qui ne sont pas pris en charge par cette version du produit ou qui n'interagissent pas correctement avec elle. Examinez attentivement ces limitations.

Problème d'option de réinitialisation de l'exercice de préparation

Si vous sélectionnez un volume ONTAP 9.11.1 pour l'exercice de préparation aux attaques de ransomware, Ransomware Resilience envoie une alerte. Si vous récupérez les données à l'aide de l'option « cloner sur volume » et réinitialisez la perceuse, l'opération de réinitialisation échoue.

Limitations Amazon FSx for NetApp ONTAP

Le système Amazon FSx for NetApp ONTAP est pris en charge dans Ransomware Resilience. Les limitations suivantes s'appliquent à Amazon FSx pour ONTAP:

- Les stratégies de sauvegarde ne sont pas prises en charge pour Amazon FSx for ONTAP. Dans cet environnement, vous devez effectuer des opérations de sauvegarde à l'aide d' Amazon FSx pour les sauvegardes. Vous pouvez restaurer ces charges de travail à l'aide de Ransomware Resilience.
- Les opérations de restauration sont effectuées uniquement à partir de snapshots.