Notes de mise à jour

BlueXP ransomware protection

NetApp
December 20, 2024

Sommaire

Notes de mise à jour

Nouveautés de la solution de protection BlueXP contre les ransomwares

Découvrez les nouveautés de la protection contre les ransomwares BlueXP.

16 décembre 2024

Détectez les comportements anormaux des utilisateurs avec 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 workloads 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 "Répondez à la détection d'une alerte par ransomware" .

Avant d'utiliser Data Infrastructure Insights Storage Workload Security pour détecter les comportements anormaux d'utilisateurs, vous devez configurer l'option en utilisant l'option BlueXP ransomware protection **Settings**.

Reportez-vous à la "Configurez les paramètres de protection contre les ransomwares BlueXP".

Sélectionnez les workloads à découvrir et à protéger

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

- Dans chaque connecteur, sélectionnez les environnements de travail dans lesquels vous souhaitez découvrir les workloads. Vous pouvez bénéficier de cette fonctionnalité si vous souhaitez protéger des charges de travail spécifiques dans votre environnement et non d'autres.
- Lors de la détection des workloads, vous pouvez activer la détection automatique des workloads par connecteur. Cette fonction vous permet de sélectionner les charges de travail à protéger.
- Découvrez les nouveaux workloads créés pour les environnements de travail précédemment sélectionnés.

Reportez-vous à la "Découvrir les workloads".

7 novembre 2024

Permettre la classification et l'analyse des données pour identifier les informations personnelles

Avec cette version, vous pouvez activer la classification BlueXP , un composant clé de la gamme BlueXP , pour analyser et classer les données dans les workloads de partage de fichiers. La classification des données vous aide à déterminer si vos données incluent des informations personnelles ou privées, ce qui peut augmenter les risques de sécurité. Ce processus a également un impact sur l'importance des workloads et vous aide à vous assurer que vous protégez ces mêmes workloads avec le niveau de protection approprié.

L'analyse des données de RP dans la protection contre les ransomwares BlueXP est généralement disponible pour les clients qui ont déployé la classification BlueXP . La classification BlueXP est disponible gratuitement en tant que composant de la plateforme BlueXP et peut être déployée sur site ou dans le cloud du client.

Reportez-vous à la "Configurez les paramètres de protection contre les ransomwares BlueXP".

Pour lancer la numérisation, sur la page protection, cliquez sur **identifier l'exposition** dans la colonne exposition privée.

"Analysez les données sensibles à caractère personnel pour les classer BlueXP ".

Intégration de SIEM à 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 en tant que système SIEM.

"En savoir plus sur la configuration des paramètres de protection contre les ransomwares de BlueXP ".

Essai gratuit de 30 jours

Avec cette version, les nouveaux déploiements de la protection contre les ransomware BlueXP disposent désormais de 30 jours pour un essai gratuit. Auparavant, la protection contre les ransomwares de BlueXP nous a permis de bénéficier de 90 jours d'essai gratuit. Si vous êtes déjà dans l'essai gratuit de 90 jours, cette offre se poursuit pendant les 90 jours.

Restaurez la charge de travail applicative au niveau des fichiers pour Podman

Avant de restaurer une charge applicative au niveau des fichiers, vous pouvez afficher la 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 fonction était désactivée. Il est maintenant activé pour Podman. Vous pouvez laisser la protection contre les ransomwares BlueXP 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 à restaurer.

"En savoir plus sur la restauration suite à une attaque par ransomware".

30 septembre 2024

Regroupement personnalisé des workloads de partage de fichiers

Avec cette version, vous pouvez désormais regrouper les partages de fichiers en groupes afin de protéger plus facilement l'intégrité de vos données. Le service peut protéger simultanément tous les volumes d'un groupe. Auparavant, chaque volume devait être protégé séparément.

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

2 septembre 2024

Évaluation des risques de sécurité par Digital Advisor

La protection contre les ransomwares de BlueXP recueille désormais des informations sur les risques de sécurité élevés et stratégiques liés à un cluster par le conseiller digital NetApp. Si un risque est détecté, la protection contre les ransomware BlueXP fournit une recommandation dans le volet **actions recommandées** du tableau de bord : « corriger une vulnérabilité de sécurité connue sur le cluster <name> ». Dans la recommandation du tableau de bord, cliquez sur **Review and fix** suggère de consulter Digital Advisor et un article CVE (Common Vulnerability & Exposure) pour résoudre le risque de sécurité. S'il existe plusieurs

risques de sécurité, consultez les informations dans Digital Advisor.

Reportez-vous à la "Documentation de Digital Advisor".

Sauvegarde dans Google Cloud Platform

Avec cette version, vous pouvez définir une destination de sauvegarde dans un compartiment 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 protection contre les ransomwares de BlueXP ".

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 ne prenaient en charge que Cloud Volumes ONTAP pour Amazon Web Services, Microsoft Azure et le NAS sur site.

"Découvrez la protection contre les ransomwares BlueXP , les sources de données prises en charge, les destinations de sauvegarde et les environnements de travail".

Contrôle d'accès basé sur des rôles

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

Pour plus de détails sur les actions que chaque rôle peut exécuter, reportez-vous à la section "Contrôle d'accès basé sur des rôles Privileges".

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) à des fins d'analyse et de détection des menaces. Avec les versions précédentes, vous pouviez uniquement sélectionner AWS Security Hub comme système SIEM. Avec cette version, vous pouvez sélectionner AWS Security Hub ou Splunk Cloud en tant que système SIEM.

"En savoir plus sur la configuration des paramètres de protection contre les ransomwares de BlueXP ".

1er juillet 2024

Modèle BYOL (Bring Your Own License)

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

"En savoir plus sur la configuration des licences".

Restaurez la charge de travail applicative au niveau des fichiers

Avant de restaurer une charge applicative au niveau des fichiers, vous pouvez afficher la liste des fichiers susceptibles d'avoir été affectés par une attaque et identifier ceux que vous souhaitez restaurer. Vous pouvez

laisser la protection contre les ransomwares BlueXP 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 à restaurer.

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

"En savoir plus sur la restauration suite à une attaque par ransomware".

Téléchargez une liste des fichiers impactés

Avant de restaurer une charge applicative au niveau du fichier, vous pouvez maintenant accéder à la page alertes pour télécharger une liste des fichiers affectés dans un fichier CSV, puis utiliser la page récupération pour télécharger le fichier CSV.

"En savoir plus sur le téléchargement des fichiers impactés avant la restauration d'une application".

Supprimer le plan de protection

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

"Découvrez comment protéger vos workloads et gérer vos stratégies de protection contre les ransomwares".

10 juin 2024

Verrouillage des copies Snapshot sur le stockage primaire

Activez cette fonctionnalité pour verrouiller les copies Snapshot sur le stockage primaire afin qu'elles ne puissent pas être modifiées ou supprimées pendant un certain temps, même si une attaque par ransomware parvient à atteindre la destination du stockage de sauvegarde.

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

Prise en charge de Cloud Volumes ONTAP pour Microsoft Azure

Cette version prend en charge Cloud Volumes ONTAP pour Microsoft Azure en tant qu'environnement de travail en plus d'Cloud Volumes ONTAP pour AWS et NAS ONTAP sur site.

"Démarrage rapide de Cloud Volumes ONTAP dans Azure"

"Découvrez la protection contre les ransomwares BlueXP".

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

Inscrivez-vous pour bénéficier d'un essai gratuit de 90 jours. Vous pourrez bientôt souscrire un abonnement avec paiement à l'utilisation sur Amazon Web Services Marketplace ou utiliser votre propre licence NetApp.

"En savoir plus sur la configuration des licences".

Protocole CIFS

Le service prend désormais en charge ONTAP et Cloud Volumes ONTAP sur site dans les environnements de travail AWS avec les protocoles NFS et CIFS. La version précédente ne prenaient en charge que le protocole NFS.

Détails de la charge de travail

Cette version fournit désormais plus de détails dans les informations sur la charge de travail des pages protection et autres pour une meilleure évaluation de la protection des charges de travail. Dans les détails de la charge de travail, vous pouvez consulter la stratégie actuellement affectée et les destinations de sauvegarde configurées.

"Pour en savoir plus sur l'affichage des détails des charges de travail, consultez les pages protection".

Protection et restauration cohérentes au niveau des applications et des machines virtuelles

Vous pouvez désormais assurer une protection cohérente au niveau des applications avec le logiciel NetApp SnapCenter et une protection cohérente avec les machines virtuelles grâce au plug-in SnapCenter pour VMware vSphere, en obtenant un état de repos et cohérent afin d'éviter toute perte potentielle de données ultérieurement si une restauration est nécessaire. Si une restauration 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 ransomware

Si des règles Snapshot ou de sauvegarde n'existent pas sur le workload, vous pouvez créer une stratégie de protection contre les ransomware, qui peut inclure les règles suivantes que vous créez dans ce service :

- Règle Snapshot
- Politique de sauvegarde
- Règle 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 via un système tiers de gestion de la sécurité et des événements (SIEM). Le tableau de bord affiche désormais une nouvelle recommandation d'activation de la détection des menaces, qui peut être configurée sur la page Paramètres.

"En savoir plus sur la configuration des options Paramètres".

Ignorer les fausses alertes positives

Dans l'onglet alertes, vous pouvez désormais ignorer les faux positifs ou décider de restaurer vos données immédiatement.

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

État de détection

Les nouveaux statuts de détection s'affichent sur la page protection et indiquent le statut de la détection des ransomware appliquée au workload.

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

Télécharger des 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 Afficher la documentation est désormais inclus dans l'interface utilisateur. Vous pouvez accéder à cette documentation à partir de l'option **actions** verticale du tableau de bord  . Sélectionnez **Nouveautés** pour afficher les détails dans les notes de version ou dans la **Documentation** pour afficher la page d'accueil de la documentation sur la protection contre les ransomwares BlueXP.

Sauvegarde et restauration BlueXP

Le service de sauvegarde et de restauration BlueXP n'a plus besoin d'être déjà activé dans l'environnement de travail. Voir "prérequis". Le service de protection contre les ransomwares BlueXP 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 protection contre les ransomwares BlueXP .

"En savoir plus sur la configuration des options Paramètres".

5 mars 2024

Gestion des règles de protection

Outre l'utilisation de règles prédéfinies, vous pouvez désormais créer des règles. "En savoir plus sur la gestion des règles".

Immuabilité sur le stockage secondaire (DataLock)

Vous pouvez désormais rendre la sauvegarde immuable dans le stockage secondaire en utilisant la technologie NetApp DataLock dans le magasin d'objets. "En savoir plus sur la création de règles de protection".

Sauvegarde automatique vers NetApp StorageGRID

Outre AWS, vous pouvez 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 d'analyse pour étudier l'attaque potentielle détectée. "En savoir plus sur la réponse à une alerte de ransomware détectée".

Processus de restauration

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

"Découvrez la protection contre les ransomwares BlueXP".

6 octobre 2023

Le service de protection contre les ransomwares BlueXP est une solution SaaS qui protège vos données, détecte les attaques et vous permet de restaurer vos données suite à une attaque par ransomware.

Pour la version préliminaire, le service protège les workloads applicatifs d'Oracle, de MySQL, de datastores de machines virtuelles et de partages de fichiers sur un stockage NAS sur site ainsi que Cloud Volumes ONTAP sur AWS (à l'aide du protocole NFS) pour toutes les entreprises BlueXP et sauvegarde individuellement les données dans un stockage cloud Amazon Web Services.

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

- Consultez rapidement la protection contre les ransomwares sur tous vos workloads.
- Obtenez des recommandations sur la protection contre les ransomwares
- Améliorez votre protection en vous appuyant sur les recommandations de BlueXP pour la protection contre les ransomwares.
- Appliquez des règles de protection contre les ransomwares pour protéger vos principaux workloads et les données à haut risque contre les attaques par ransomware.
- Surveillez l'état de vos workloads contre les attaques par ransomware à la recherche d'anomalies des données.
- Évaluez rapidement l'impact des incidents de ransomware sur votre workload.
- Restaurez intelligemment les données après des incidents de ransomware en vous assurant qu'elles ne sont pas réinfectées par les données stockées.

"Découvrez la protection contre les ransomwares BlueXP".

Informations sur le copyright

Informations sur les marques commerciales