



Commencez

Ransomware Protection

NetApp
January 09, 2023

This PDF was generated from <https://docs.netapp.com/fr-fr/cloud-manager-ransomware/concept-ransomware-protection.html> on January 09, 2023. Always check docs.netapp.com for the latest.

Table des matières

- Commencez 1
 - Découvrez la protection contre les ransomwares 1
 - Surveillance de l'état des alertes par ransomware 3

Commencez

Découvrez la protection contre les ransomwares

Les attaques par ransomware peuvent coûter du temps, des ressources et de la réputation à l'entreprise. Le service BlueXP (anciennement Cloud Manager) protection contre les attaques par ransomware vous permet de consulter des informations pertinentes sur la cybersécurité et d'évaluer la résilience de votre entreprise face à une cyberattaque. Il fournit également une liste d'alertes et de résolutions de problèmes afin de sécuriser vos données.

["Découvrez les utilisations de la protection contre les ransomwares"](#).



Le service de protection contre les ransomwares est actuellement une offre bêta.

Caractéristiques

La protection contre les ransomwares offre un point unique de visibilité et de contrôle pour gérer et affiner la sécurité des données dans divers environnements de travail et couches d'infrastructure afin de mieux répondre aux menaces à mesure qu'elles se produisent. Il fournit actuellement plusieurs fonctions qui vous aideront dans vos efforts de protection du cyberstockage. Les fonctions actuelles identifient les cas suivants :

- Les volumes de vos environnements de travail ne sont pas protégés par des copies Snapshot périodiques.
- Les volumes de vos environnements de travail ne sont pas protégés en créant des sauvegardes sur le cloud à l'aide de ["La sauvegarde dans le cloud"](#).
- Les volumes de vos environnements de travail sont protégés contre les modifications et les suppressions sur le stockage WORM grâce à la technologie ONTAP SnapLock. ["En savoir plus sur SnapLock"](#).
- Les données de vos environnements de travail et les sources de données ne sont pas en cours d'analyse à l'aide de ["Sens des données cloud"](#) afin d'identifier les problèmes de conformité et de confidentialité, et de trouver des opportunités d'optimisation.

Cette fonctionnalité est également essentielle du point de vue de la protection par ransomware, car elle vous permet de mieux comprendre où se trouvent vos données importantes (sensibles et stratégiques) afin de vous assurer que vous concentrez sur votre protection.

- Au cas où vous souhaiteriez pouvoir récupérer vos données suite à une attaque par ransomware, vos catégories les plus importantes de données ne sont pas sauvegardées.
- Une augmentation anormale du pourcentage de fichiers chiffrés dans un environnement de travail ou une source de données s'est produite.

Cela peut être un indicateur qu'une attaque par ransomware a commencé sur votre réseau.

- Les données sensibles se trouvent dans les fichiers d'un environnement de travail ou d'une source de données et le niveau d'autorisation d'accès est trop élevé.
- Des utilisateurs ont été ajoutés à vos groupes d'administrateurs de domaine Active Directory.
- La version du logiciel ONTAP de vos clusters est ancienne et doit être mise à jour pour offrir les meilleures fonctionnalités de protection et de sécurité, ainsi que les toutes nouvelles fonctionnalités.
- L'audit du système de fichiers NAS n'est pas activé sur vos systèmes ONTAP.

L'activation de l'audit CIFS génère des événements d'audit pour vos administrateurs système qui permettent de suivre les informations telles que les changements d'autorisation de dossier, les tentatives échouées de lecture ou d'écriture de fichiers, ainsi que la création, la modification ou la suppression de fichiers.

- Les fonctionnalités anti-ransomwares intégrées ne sont pas activées sur vos systèmes ONTAP.

Les fonctionnalités anti-ransomwares de ONTAP détectent et avertissent lorsque la condition d'activité anormale est susceptible d'indiquer une attaque par ransomware.

- Lorsque les logiciels anti-ransomwares de ONTAP sont activés sur vos systèmes, le nombre d'incidents liés à des attaques par ransomware apparaît sous la forme d'alertes.
- Nombre de vulnérabilités de sécurité élevées, moyennes et faibles détectées par l'outil Active IQ Digital Advisor sur vos clusters ONTAP.

Vous pouvez afficher la vulnérabilité, puis suivre l'action recommandée pour résoudre le problème.

["Découvrez comment visualiser ces problèmes potentiels dans le tableau de bord protection contre les ransomwares."](#)

Avec les systèmes Cloud Volumes ONTAP, vous pouvez déployer directement depuis l'environnement de travail certaines protections par ransomware supplémentaires. ["Découvrez comment renforcer la protection contre les attaques par ransomware"](#).

Environnements de travail et sources de données pris en charge

["Sens des données cloud"](#) Est une condition préalable à l'utilisation du service de protection contre les ransomwares. Une fois Data SENSE installé et activé, vous pouvez utiliser protection par ransomware pour déterminer la résilience de vos données face à une cyberattaque sur les types d'environnements de travail et de sources de données suivants :

Environnements de travail:

- Cloud Volumes ONTAP (déployé dans AWS, Azure ou GCP)
- Clusters ONTAP sur site
- Azure NetApp Files
- Amazon FSX pour ONTAP
- Amazon S3

Sources de données:

- Partages de fichiers non NetApp
- Stockage objet (qui utilise le protocole S3)
- Bases de données (Amazon RDS, MongoDB, MySQL, Oracle, PostgreSQL, SAP HANA ET SQL SERVER)
- Comptes OneDrive
- SharePoint Online et des comptes sur site
- Comptes Google Drive

Par ailleurs, la protection contre les ransomwares surveille votre configuration Active Directory globale, si vous

l'avez ["Configuré dans le sens des données du cloud"](#).

Fonctionnement de la protection contre les ransomwares

À un niveau élevé, la protection contre les ransomwares fonctionne comme suit :


1. La protection contre les ransomwares collecte d'informations de vos systèmes de stockage, Cloud Data Sense, Cloud Backup, et d'autres ressources BlueXP et NetApp, pour alimenter le tableau de bord de protection contre les ransomwares.
2. Vous utilisez le tableau de bord protection contre les attaques par ransomware pour obtenir un aperçu de la protection de vos systèmes.
3. Vous utilisez les outils de reporting fournis pour vous aider dans vos opérations de protection du cyberstockage.

Le coût

Il n'existe aucun coût distinct pour le service de protection contre les attaques par ransomware lors de la version bêta.

Surveillance de l'état des alertes par ransomware

Vous pouvez afficher le statut des alertes par ransomware dans le Centre de notification BlueXP. Vous pouvez également configurer les notifications à envoyer par e-mail afin de vous informer de l'activité importante du système, même lorsque vous n'êtes pas connecté au système.

Le centre de notification surveille la progression des incidents par ransomware afin que vous puissiez vérifier s'ils ont été résolus ou non. Vous pouvez afficher les notifications en cliquant sur le bouton  Dans la barre de menus BlueXP. Vous pouvez également configurer BlueXP pour envoyer des notifications par e-mail en tant qu'alertes.

À ce stade, un seul événement déclenche des alertes par e-mail :

- Attaques par ransomware potentielles détectées sur votre système

Par défaut, les administrateurs de compte BlueXP recevront des e-mails pour toutes les alertes « critiques » et « recommandations ». Par défaut, tous les autres utilisateurs et destinataires sont configurés pour ne pas recevoir d'e-mails de notification. Des e-mails peuvent être envoyés à tout utilisateur BlueXP qui fait partie de votre compte Cloud NetApp, ou à tout autre destinataire ayant besoin de connaître des incidents liés à la protection par ransomware.

Vous devez sélectionner le type de notification « critique » pour recevoir les alertes par e-mail de protection contre les ransomwares.

["En savoir plus sur le Centre de notification"](#) et comment envoyer des e-mails d'alerte en cas d'incident de protection par ransomware.

Informations sur le copyright

Copyright © 2023 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.