FICHE SOLUTION

Assurez-vous de bloquer les ransomwares avec InfiniGuard® CyberRecovery

LE DEFI

Un ransomware est un programme malveillant qui prend les données en otage en les chiffrant.

En règle générale, les entreprises disposant d'un processus de sauvegarde approprié peuvent restaurer leurs données sur les systèmes de production impactés. Mais le code des ransomwares ne cesse de gagner en sophistication et les attaques visent désormais également les sauvegardes. Sachant que les entreprises sont visées par une attaque de ransomware toutes les 11 secondes1, il ne suffit plus de compter sur les seules sauvegardes pour restaurer les données.

Les victimes sont confrontées à plusieurs options : certaines choisissent de payer la rançon et obtiennent une clé de déchiffrement en échange. Beaucoup payent mais n'obtiennent rien en échange. D'autres vont souscrire des services onéreux d'annulation du chiffrement et d'autres encore vont rapatrier les sauvegardes conservées sur bande sur un site distant et organiser un processus de restauration long et laborieux.

A quel prix ? IDC estime que les ransomwares coûtent aux entreprises 20 milliards de dollars par an. Et ce chiffre augmente encore si l'on ajoute aux victimes les petites et moyennes entreprises.

Les ransomwares aujourd'hui

Au cours des premiers mois de 2021, le spécialiste de la cybersécurité BlackFog2 a signalé plusieurs cyberattaques particulièrement importantes : le district scolaire Victor Central à New York a été visé par une attaque qui s'est traduite par le chiffrement de ses données et systèmes ainsi que le verrouillage des accès des utilisateurs. Toutes les écoles du district ont dû fermer. En mars, le constructeur informatique Acer s'est vu demander une rançon de 50 millions de dollars pour que les hackers ne divulguent pas des données sensibles exfiltrées.

Plus récemment, Colonial Pipeline, le fournisseur de 45% du carburant sur la côte est des Etats-Unis, a été visé par une attaque de ransomware, perpétrée par des hackers russes. L'exploitant a dû fermer rapidement ses systèmes pour contenir l'attaque. Malgré cela, les stations-service d'une grande partie du pays ont peiné à s'approvisionner en carburant.

De plus petites organisations sont aussi visées. La société de sécurité Infrascale estime que 46% des petites entreprises ont subi une attaque de ransomware et 73% ont confirmé avoir versé une rançon. Les montants de ces rançons ne sont généralement pas de l'ordre de 50 millions de dollars mais elles demeurent importantes sans garantie que les hackers tiendront parole.

Les sauvegardes à la rescousse ?

Si vos sauvegardes survivent à l'attaque, vous avez de la chance. Mais même dans ce cas, il faut savoir que la restauration de gros volumes de sauvegardes sur des systèmes principaux coûte cher en temps et en ressources mobilisées.

Les équipes IT cherchent à accélérer les vitesses de sauvegarde en optant pour des sauvegardes complètes synthétiques avec stockage dédupliqué. Mais les opérations de restauration à grande échelle suite à une cyberattaque supposent d'assembler les données de plusieurs générations de sauvegardes, ce qui induit des IO de lecture hautement aléatoires de lecture du système de stockage en backend et donc des délais de restauration prolongés avec un impact négatif potentiellement sérieux pour l'activité de l'entreprise.

Avantages et caractéristiques d'InfiniGuard CyberRecovery :

- Restaurations rapides de plusieurs pétaoctets
- Protection des sauvegardes au moyen de snapshots immuables impossibles à supprimer, chiffrer ou modifier
- Conformité réglementaire au moyen de sauvegardes consolidées et snapshots immuables
- Plusieurs opérations simultanées de sauvegarde et restauration sans ralentir les performances
- Validation de l'environnement de restauration
- Moteurs de déduplication redondants en configuration active/active/passive pour la protection des données et des échecs de sauvegarde et restauration
- Réduction des coûts énergétiques et des frais d'administration par la consolidation des sauvegardes à hauteur de 50 Po
- Très grande évolutivité et support des protocoles VTL, NFS, CIFS, OST, RMAN et DB/2
- Préservation des recettes et de la réputation par la restauration fiable et quasi instantanée des données
- Restauration des données avec une parfaite intégrité garantie, quelle que soit la cause : cyberattaque, panne technique, catastrophe naturelle ou erreur humaine

[1] Cybersecurity Ventures https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021
[2] BlackFog https://www.blackfog.com/the-state-of-ransomware-in-2021

INFINIDAT

LA SOLUTION : InfiniGuard avec CyberRecovery

La technologie CyberRecovery est incluse dans la solution InfiniGuard d'Infinidat pour la protection et la restauration des données. CyberRecovery repose sur l'architecture de protection des données InfiniGuard, qui permet une restauration rapide pour bien moins cher que les appliances de sauvegardes dédiées concurrentes (PBBA). InfiniGuard utilise en back-end les systèmes InfiniBox d'une capacité de plusieurs Po auxquels est ajoutée une couche logicielle innovante pour optimiser l'agencement des données afin de pouvoir les restaurer rapidement, sans nuire à la rapidité de sauvegarde.

La technologie innovante InfiniGuard utilise une large couche DRAM (dynamic random- access memory) comme cache principal, couplée à une couche encore plus importante de disques SSD (solid-state drives) comme cache secondaire. Un algorithme TRIE propriétaire (un arbre de nœuds plutôt qu'une arborescence binaire ou un algorithme de hachage) prédit les tendances d'IO et pré-fetch les données pour accélérer les délais de sauvegarde et de restauration.

Au lieu de vouloir restaurer les données à partir de plusieurs appliances de sauvegarde, différents types de supports et sites de stockage, InfiniGuard consolide plusieurs sauvegardes en une appliance facile à administrer capable d'atteindre 2 Po de capacité utilisable et jusqu'à 50 Po de capacité effective. Les restaurations en parallèle au travers de tous les axes dans la baie aident à réduire les délais.

Regardons CyberRecovery de plus près

Les fonctionnalités natives CyberRecovery d'InfiniGuard améliorent encore les conditions de protection et de restauration. Pour vous protéger des attaques de ransomware, CyberRecovery prend des snapshots immuables de vos sauvegardes, impossibles à supprimer, à chiffrer ou à modifier. Vous validez l'environnement à restaurer et pouvez entamer le processus de restauration quasi snaphotment. La restauration est rapide avec intégrité garantie des données.

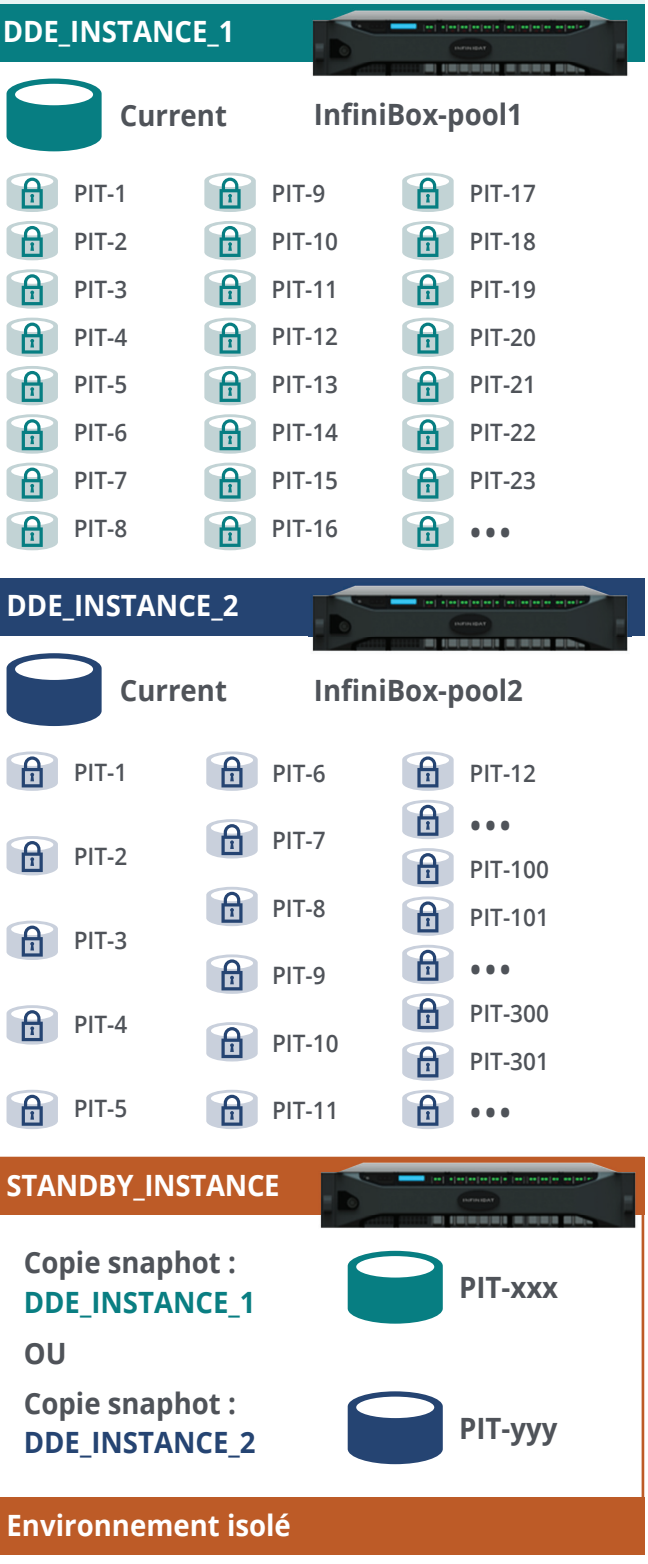
Le mécanisme de création des snapshots immuables est inclus et piloté au travers d'un moteur de règles de planification, d'ordonnancement et d'expiration, permettant de créer et gérer plusieurs copies ponctuelles et sécurisées de l'environnement de sauvegarde.

Les snapshots immuables de CyberRecovery et l'architecture de restauration rapide d'InfiniGuard contribuent à une solution de sauvegarde d'entreprise avec une disponibilité de cinq 9 (99,999%) en cas de cyberattaque. Et comme CyberRecovery est une fonctionnalité native de l'appliance InfiniGuard, elle est comprise dans le prix.

Des snapshots immuables

CyberRecovery crée des snapshots WORM (write once, read many) de tout un environnement et permet des restaurations ponctuelles selon des règles définies.

InfiniGuard avec CyberRecovery protège vos sauvegardes au moyen des snapshots immuables Infinidat. Chaque moteur de déduplication (DDE) peut être restauré séparément à la date voulue. Il est aussi possible d'activer CyberRecovery ou des tests de découverte en environnement autonome.



[3] Etude Infrascale 2020 https://www.infrascale.com/press-release/infrascale-survey-reveals-close-to-half-of-smbs-have-been-ransomware-attack-targets/

Ces snapshots immuables ne peuvent en aucun cas être corrompus par une attaque de ransomware. Même si un ransomware demeure indétecté sur un réseau, un fichier sauvegardé ne peut pas modifier les snapshots existants. Et avec la restauration ponctuelle, les services IT peuvent restaurer le dernier snapshot valide en quelques minutes.

Les services IT peuvent créer différents types de snapshots :

1. Snapshots système. Les snapshots système sont immuables et ne peuvent être ni supprimés, ni modifiés. Les experts du support Infinidat vous aident à configurer vos snapshots système au plus près de vos besoins de cybersécurité, y compris les paramètres de rétention et les snapshots programmés. Aucun individu malveillant, ni personnel IT inexpérimenté ne peut modifier les paramètres de vos snapshots immuables, ni supprimer un snaphots immuable.
2. Snaphots utilisateur. Les snapshots utilisateur protègent les données des télétravailleurs. Mais ces snapshots individuels ne sont pas immuables et les services IT peuvent les configurer. Ils s'utilisent comme les snapshots système pour n'importe quelle opération de restauration.
3. Snaphots manuel. Les services IT peuvent créer des snapshots supplémentaires de l'environnement de sauvegarde à tout moment.
4. Snaphost pré-restauration. Les règles système prévoient la création automatique de snapshots de l'environnement de sauvegarde avant toute opération de restauration. Il est possible d'utiliser ce snaphots pour revenir en arrière et restaurer les données dans leur état, juste avant une restauration précédente.

Les opérations de restauration deviennent systématiques, rapides et vérifiables et il est possible de procéder à des restaurations quasi instantanées sur tout point de l'historique des données. Un environnement de test isolé et très simple à utiliser permet aux entreprises de vérifier les données avant de les restaurer dans l'environnement opérationnel, et de procéder à des validations de routine de sauvegardes sécurisées sans perturber les opérations de sauvegarde quotidiennes.

SYNTHESE

S'il est inutile de craindre une attaque improbable, il ne faut pas non plus sous-estimer le risque et les conséquences désastreuses d'une cyberattaque.

Ne présumez pas non plus de l'incompétence des hackers. Mieux vaut considérer qu'il sera suffisamment malin pour tenter de viser vos sauvegardes et vos systèmes principaux.

Soyez plus intelligent. En déployant InfiniGuard avec CyberRecovery, vous vous protégerez de quantité de menaces : cyberattaques, pannes techniques, catastrophes naturelles jusqu'aux simples erreurs humaines. InfiniGuard avec CyberRecovery vous garantit que vous pourrez restaurer vos données rapidement pour poursuivre vos activités avec le moins de perturbations possible.