PRÉSENTATION DE LA SOLUTION

Défense des données InfiniBox® : quelle que soit la menace – ransomware, catastrophe naturelle, défaillance des systèmes, erreur humaine – InfiniBox vous protège.

LE DÉFI

De nos jours, les données évoluent dans un monde plus dangereux que jamais. Les catastrophes naturelles se multiplient, et une simple erreur humaine peut rendre totalement inutiles des volumes entiers de vos précieuses données. Ajoutez à cela la cybercriminalité, à l'image des ransomware et des logiciels malveillants, qui se trouve en haut de la liste des inquiétudes des directeurs généraux, des directeurs des systèmes d'information et des responsables de la sécurité.

Si tout cela semble dramatique et dangereux, c'est parce que ça l'est, ou peut le devenir, si vous n'y faites pas attention. Pour préserver leurs données face à ces menaces., la plupart des dirigeants adoptent une stratégie de protection des données classique (basée sur des sauvegardes). Nombre d'entre eux pratiquent également la planification de la continuité des activités, qui permet de maintenir la fiabilité et la disponibilité de leurs données malgré les interruptions et les attaques. L'augmentation des ransomware et des logiciels malveillants complique encore plus cette planification.

Même les entreprises sophistiquées ne sont pas toujours certaines d'avoir suffisamment protégé leurs données. Afin d'assurer une protection moderne des données, y compris la cyber-résilience, l'InfiniBox et l'InfiniBox SSA d'Infinidat proposent l'architecture de référence InfiniSafe®. L'architecture de référence InfiniSafe® vous permet d'établir les bons process avec les bons outils et les bonnes technologies pour vous aider à garder vos données en sécurité, disponibles et fiables.

Dans cette Présentation de la solution, nous allons examiner l'une des menaces les plus courantes et sérieuses qui pèsent sur les données : la cybercriminalité et les ransomware.

> *« ... la cybercriminalité est devenue si grave que des enquêtes récentes auprès des directeurs généraux de Fortune en mai 2021 et de KPMG en mars 2021 citaient les risques de cybersécurité comme étant la menace numéro un pour leurs entreprises. »*

La cybercriminalité connaît une croissance exponentielle

- Il ne s'agit pas de savoir SI, mais QUAND vous allez subir une attaque, et à quelle fréquence cela est susceptible de se produire. Cette menace est aujourd'hui inévitable, et toutes les entreprises doivent s'y préparer.
- La cybercriminalité ne se limite pas à un seul type d'attaque. Parmi les attaques les plus courantes figurent les tentatives de hameçonnage, les atteintes à la propriété intellectuelle en ligne et la fraude sur Internet (l'omniprésent secrétaire général des Nations Unis offrant des dizaines de millions de dollars à l'heureux destinataire).
- Les attaques de logiciels malveillants sophistiqués telles que les « Advanced Persistent Threats » (APT) sont plus difficiles à orchestrer, mais les gains sont considérables. Les pirates adeptes des APT ciblent les réseaux riches en données, avec des données précieuses, des poches profondes et la possibilité d'un embarras public maximal en cas d'attaque réussie.[1]
- Finalement, la cybercriminalité est devenue si grave que des enquêtes récentes auprès des directeurs généraux de Fortune en mai 2021[2] et de KPMG en mars 2021[3] citaient les risques de cybersécurité comme étant la menace numéro un pour leurs entreprises.
- Il est avéré que les cyberattaques sont exécutées après plusieurs mois de planification. Le temps d'arrêt moyen se situe au-delà de 9 mois après que les intrus ont infiltré l'environnement d'une entreprise.

Ransomware

Un ransomware est une forme de logiciel malveillant. Cependant, contrairement aux attaques APT ultra risquées qui rapportent beaucoup

[1] « Qu'est-ce qu'une menace persistante avancée ? » Kaspersky
[2] « Fortune 500 CEO survey »
[3] « Enquête KPMG 2021 CEO Outlook Pulse »
[4] Révélée : Les supermarchés qui vous vendront des logiciels malveillants pour 50 $ » Forbes

d'argent, les pirates peuvent acheter des ransomware sur le dark web. Un grand nombre d'entre eux sont bon marché, et certains vendeurs entreprenants louent même des ransomware, ce qui a créé la cybercriminalité en tant que service (CaaS).[4]

Les attaques par ransomware introduisent un logiciel qui chiffre automatiquement l'ensemble des fichiers et volumes auxquels il peut accéder. Si le ransomware attaque un ordinateur en réseau, le processus de chiffrement se répand sur le réseau, affectant l'ensemble du stockage primaire et secondaire, y compris les sauvegardes et les archives. La plupart du temps, les espaces de stockage secondaires sont en réalité ciblés en premier, ce qui restreint votre capacité à récupérer vos données et qui renforce la position de l'intrus. Les pirates demandent ensuite aux victimes de les payer pour obtenir la clé de décryptage.

> *« J'ai été très impressionné par les performances, la rentabilité et la gestion du système d'OFFSITE...Sa fonctionnalité de prise de snapshots immuables [Infinidat] offre une excellente valeur ajoutée pour protéger les données contre les ransomware . »*
>
> — **Directeur de la technologie**, OFFSITE

Pourquoi ne pas payer ?

De nombreuses victimes préfèrent payer la rançon et espérer recevoir la clé en retour plutôt que de purement et simplement perdre leurs données.

Elles y perdent à coup sûr. Le rapport de Sophos intitulé **« State of Ransomware 2021 »** (Où en sont les ransomware en 2021) révèle les résultats de ses recherches sur les incidents de ransomware : 92 % des entreprises qui ont payé une rançon au cours des 12 derniers mois n'ont pas récupéré la totalité de leurs données. En moyenne, seuls 65 % des données de l'ensemble des participants à l'enquête ont été récupérés, ce qui signifie que certains les ont récupérés partiellement, d'autres entièrement et d'autres encore n'ont rien récupéré du tout. Toujours selon ce rapport de Sophos, le coût de récupération (recovery) moyen au cours du premier semestre 2021 a déjà doublé par rapport à celui de 2020. Au final, il peut s'agir de millions de dollars.

PEn outre, les gouvernements du monde entier établissent des règles, des règlements et des lois concernant le paiement des rançons et le signalement des incidents. Il est important que les entreprises se tiennent informées des exigences de leurs régions en particulier.

LA SOLUTION

InfiniBox, le système de stockage performant d'Infinidat, fournit une solution axée sur l'intelligence artificielle de type « configurez et n'y pensez plus » avec une disponibilité à 100 % sans précédent, des performances sans pareil et un coût total de possession considérablement réduit. Un management, et une gestion des données distincte créent une puissante protection des données au sein de l'architecture système.

Les fonctionnalités de défense et protection d'InfiniBox vous permettent de mieux protéger les données grâce à des snapshots immuables et des commandes de réplication, le chiffrement et les contrôles d'accès ; détectez plus rapidement les menaces grâce à des alertes de seuil de capacité de pool de stockage et rétablissez rapidement vos systèmes grâce à des snapshots locaux et répliqués.

InfiniSafe : l'architecture de référence de la famille InfiniBox

Il est plus important que jamais de comprendre comment créer un environnement cyber-résilient pour votre espace de stockage principal. Les entreprises ont besoin d'une stratégie à plusieurs niveaux pour protéger davantage leurs données les plus critiques. L'architecture de référence InfiniSafe définit des méthodologies pouvant être facilement mises en œuvre pour aider à renforcer la cyber-résilience. Son approche repose sur quatre piliers :

- **Snapshots immuables**
- **Air Gap logique distant**
- **Environnement d'investigation en boucle fermée**
- **Recovery quasi instantanée**

La création de copies verrouillées et immuables de vos données est d'une importance capitale. On peut considérer qu'il s'agit d'un air-gapped logique en soi, mais il est important de l'étendre à une deuxième copie immuable par le biais d'une meilleure pratique de réplication, tout comme pour le DR. Vous devez ensuite tester et/ou valider vos données dans cette copie. Un environnement clôturé (parfois appelé "confiance zéro") vous sépare de la production et n'est actif que pendant le temps nécessaire pour valider ce dont vous voulez vous assurer qu'il est propre. Vous êtes en mesure d'utiliser les outils et applications les plus à même de vous aider à valider et/ou à tester les données. Enfin, une fois ces éléments validés dans le temps, vous avez la possibilité de restaurer ces données de quelques secondes à quelques minutes. L'exploitation de nos capacités au sein de la famille InfiniBox vous permet de bénéficier de tous ces avantages sans avoir besoin d'être propriétaire ou d'être lié à un fournisseur ou à un ensemble d'outils particulier.

Snapshots : Colonne vertébrale de la protection des données et de la continuité des activités

InfiniSnap®, le mécanisme de prise de snapshots d'Infinidat, étend les fonctionnalités de protection des données critiques sans impacter la scalabilité ni les performances. InfiniSnap utilise un mécanisme de redirection sur écriture, non verrouillé, qui crée des snapshots et des snapshots immuables, et permet une restauration rapide à la demande.

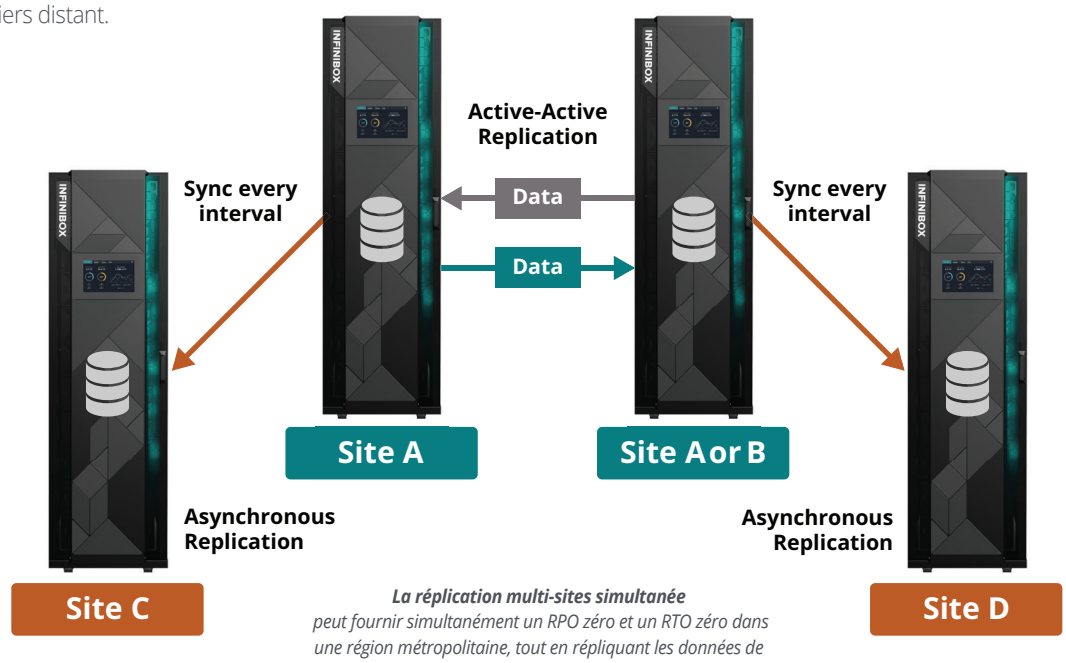
Les snapshots peuvent être en lecture seule ou accessibles en écriture, et chaque jeu de données peut stocker jusqu'à 1 000 snapshots. InfiniSnap permet de prendre des snapshots immuables de volumes, de systèmes de fichiers et de groupes de cohérence. Le(s) répertoire(s) de snapshots permettent aux utilisateurs finaux de parcourir, de sélectionner et de récupérer facilement des fichiers qui ont été involontairement supprimés ou modifiés.

- **Snapshots immuables :** les snapshots immuables ne peuvent pas être modifiés ni supprimés pendant une période de rétention définie. Même si les administrateurs peuvent reporter la date d'expiration du verrouillage, ils ne peuvent pas l'avancer. La fonctionnalité de snapshot immuable permet également d'activer les snapshots masqués sous forme d'images de sauvegarde, renforçant ainsi encore davantage la protection des snapshots contre les attaques.
- **Détection des menaces :** le chiffrement des ransomware augmente la taille des données, ce qui, à son tour, augmente la taille des snapshots des données. Les administrateurs peuvent définir des seuils de consommation de capacité pour être alertés si le volume de snapshots dépasse brusquement les paramètres moyens. S'ils détectent une attaque, les administrateurs peuvent rapidement accéder aux données et les tester et les restaurer rapidement à partir du dernier bon snapshot.

Réplication : renforcez la continuité des activités

La réplication étend le pouvoir des snapshots pour protéger et récupérer les données menacées. InfiniBox permet différents types de réplication en fonction des besoins environnementaux changeants.

- **Réplication asynchrone :** permet d'atteindre un objectif de point de récupération (Recovery Point Objective ou RPO) de 4 secondes. Via une infrastructure IP, réduit les coûts et la complexité.
- **Réplication synchrone :** permet d'atteindre un RPO de zéro seconde avec une latence inférieure à 400 microsecondes pour les applications essentielles. En cas de lenteur ou de défaillance du WAN, la réplication synchrone InfiniBox bascule en mode asynchrone. Lorsque le WAN est rétabli, le moteur réplique automatiquement toutes les données manquantes et reprend la synchronisation sans perturber les IO.
- **Réplication actif-actif :** les systèmes InfiniBox permettent la lecture et l'écriture simultanées de groupes de cohérence sur des régions métro. Les volumes sont des images externes qui apparaissent au travers de plusieurs chemins (multipath) sur le même volume. La réplication synchrone préserve toujours la cohérence des volumes. Il n'existe pas de relation maître-esclave ni d'allers-retours supplémentaires pour effectuer des mises à jour en écriture de volumes. Si nécessaire, un witness (client léger externe) peut être placé sur un nœud autonome ou une VM basée dans le cloud.
- **Réplication multi-sites simultanée :** InfiniBox peut simultanément répliquer des groupes de cohérence depuis des sites de réplication principaux vers un autre site d'une région métropolitaine. Ensuite, les utilisateurs peuvent effectuer une réplication asynchrone vers un emplacement tiers distant.



***La réplication multi-sites simultanée** peut fournir simultanément un RPO zéro et un RTO zéro dans une région métropolitaine, tout en répliquant les données de manière asynchrone sur un troisième ou un quatrième site situé à distance avec un RPO proche de zéro.*

INFINIDAT

Chiffrement : protection des données chiffrées

Les ransomware peuvent rechiffrer les fichiers chiffrés. C'est pourquoi les snapshots et la réplication constituent la première ligne de défense. Mais, plus le chiffrement est fort, plus il est difficile pour les pirates de les rechiffrer.

- **Validé par les Federal Information Processing Standards (FIPS) 140-2 :** le National Institute of Standards and Technology (NIST) a remis la validation FIPS 140-2 au module de chiffrement d'Infinidat. La norme certifie qu'InfiniBox est conforme à une utilisation dans un ensemble défini de projets IT du gouvernement américain et de certaines industries régulées.
- **Disques à auto-chiffrement (SED) standard avec chiffrement AES-256 :** InfiniBox utilise des disques à auto-chiffrement (Self Encrypting Drives ou SED) standard avec le chiffrement AES-256 conforme aux FIPS 140-2, à savoir, les clés d'authentification les plus puissantes prises en charge par les disques.
- **Fonctions de dérivation de clé (KDF) :** Infinidat utilise la technologie KDF approuvée par le gouvernement fédéral américain, qui génère des clés uniques au monde par disque. Notre gestionnaire de clés pluggable facilite la gestion des clés externes via le protocole KMIP (Key Management Interoperability Protocol).
- **Intégration aux tiers :** assure une intégration forte avec n'importe quel produit de chiffrement tel que Thales, VMware, Oracle TDE ou Microsoft TDE sans programmation spécialisée ni coûts élevés.

Gestion de l'accès : aucune intrusion

Les cybercriminels peuvent emprunter plusieurs routes pour accéder à un réseau. La plus prisée est celle des informations d'identification de l'administrateur. InfiniBox est déjà configuré pour empêcher les cybercriminels de parvenir à ce point : tous les accès sont effectués via l'API, qui empêche toute modification des snapshots, même avec des informations d'identification d'administrateur.

En outre, de toute façon, grâce à la gestion de l'accès InfiniBox, les attaquants n'iront pas bien loin.

- **Contrôle d'accès basés sur les rôles (RBAC) :** RBAC (Role-Based Access Control) s'exécute dans le plan de contrôle du système pour protéger les comptes locaux et les groupes de domaines/LDAP. Les rôles attribués aux groupes permettent aux utilisateurs d'avoir un contrôle total, un contrôle sur un pool de capacité limité ou des autorisations en lecture seule. Les utilisateurs peuvent désactiver ou bloquer des comptes locaux afin qu'ils ne puissent être utilisés que lorsque les techniciens Infinidat effectuent des opérations de maintenance. L'authentification de session protège encore davantage l'accès à la gestion.
- **Authentification des hôtes :** iSCSI utilise CHAP pour authentifier les hôtes sur le plan des données. CHAP nécessite l'authentification multi-facteurs des hôtes pour empêcher un hôte d'accéder aux données d'un autre hôte.
- **Intégration de la gestion des accès tiers :** Infinidat intègre des solutions de gestion des accès externes privilégiés de niveau d'entreprise telles que CyberArk.
- **Accès au poste de gestion et audits :** la gestion de l'accès inclut également un accès au poste de gestion via une liaison sécurisée, tandis que des pistes d'audit consignent l'ensemble des opérations qui modifient la configuration/l'état d'un ordinateur ou des composants. Le système d'audit enregistre également l'administrateur qui modifie la configuration.

CONCLUSION

La protection de vos données est essentielle à la réussite de votre entreprise. L'ensemble de fonctions d'entreprise d'InfiniBox vous permet de renforcer au maximum les données et la cyber-résilience, intégrant le stockage dans votre stratégie de cybersécurité d'entreprise tout entière.

LLorsque vous investissez dans InfiniBox, vous bénéficiez non seulement de performances supérieures, d'une disponibilité à 100%, d'une facilité d'utilisation de type "set-it-and-forget-it" et d'un coût total de possession considérablement réduit à l'échelle, mais vous frustrez également les attaquants potentiels de ransomware. Les cybercriminels s'enrichissent sur le dos des victimes non préparées. Ils ne s'attendent pas à trouver de puissantes barrières de protection des données.

Repoussez ces attaques avec les snapshots immuables d'InfiniBox, une réplication puissante, un chiffrement sophistiqué et une gestion d'accès forte ; et ce, avec un modèle tout compris adapté à votre budget de stockage, votre personnel et à vos objectifs commerciaux.