VERITAS

Améliorez la récupération des données grâce à l'isolement physique

Conservez des copies sécurisées de vos données pour neutraliser l'impact des cyberattaques.

Livre Blanc | Mai 2023

Pourquoi créer un centre de sauvegarde de données ?

La cybersécurité est au centre des préoccupations des chefs d'entreprise. Les cybermenaces sont de plus en plus sophistiquées et leurs auteurs affinent constamment leurs techniques pour causer un maximum de dégâts. Selon Gartner, d'ici 2025, 40 % des conseils d'administration disposeront d'un comité dédié à la cybersécurité, responsable de créer des rapports et des stratégies supplémentaires en matière de politiques de cybersécurité, d'exécution et de récupération[1]. La croissance exponentielle de la cybercriminalité coûte des millions de dollars et d'heures que les entreprises s'efforcent de réduire et de récupérer. En 2022, une cyberattaque est survenue toutes les 15 secondes[2]. Il s'agit donc d'une course contre la montre pour assurer une bonne préparation, avec une stratégie qui réduit les risques, élimine les incertitudes et maintient le contrôle de l'environnement.

Pour qu'un plan de résilience et de récupération soit fiable, il faut mettre en œuvre un cadre de cybersécurité fiable, avec la technologie et les processus appropriés. Disposez-vous d'un plan de réponse aux incidents de cybersécurité que vous pourriez communiquer en toute confiance à votre responsable et à la direction ? Selon Gartner[3], d'ici 2025, 70 % des PDG exigeront une culture de résilience organisationnelle face à la cybercriminalité. Il est temps de comprendre les tendances en matière de cybersécurité et les éléments essentiels d'un plan de récupération efficace. Vous serez ainsi en mesure d'arrêter net une attaque de ransomware et de démontrer à votre conseil d'administration que vous avez mis en œuvre les bons outils pour reprendre le contrôle de votre entreprise.

Qu'est-ce qu'un isolement et pourquoi est-ce important ?

Les cyberattaques devenant de plus en plus sophistiquées, les pirates informatiques s'attaquent non seulement à votre stockage de données principal, mais aussi à votre stockage de données de sauvegarde. Il est indispensable d'en tenir compte dans votre stratégie de reprise après incident. Dans la plupart des cas, les pirates restent inactifs dans votre système jusqu'à ce qu'ils puissent accéder à vos données principales et à vos données de sauvegarde et les compromettre. S'ils parviennent à y accéder, ils peuvent tout perturber.

Selon le National Institute of Standards and Technology (NIST), un isolement est une interface entre deux systèmes (a) qui ne sont pas connectés physiquement et (b) dont la connexion logique n'est pas automatisée (c'est-à-dire que les données sont transférées à travers l'interface uniquement manuellement, sous contrôle humain)[4]. Dans le passé, l'isolement était la norme pour protéger les technologies opérationnelles telles que les thermostats ou les appareils électroménagers. Maintenant que presque tout est connecté via un réseau sans fil ou câblé, il est essentiel de mettre en place un processus d'isolement rigoureux pour conserver une bonne copie des données pour la récupération.

Dans les environnements en réseau, les pirates peuvent exploiter presque tous les points d'entrée, même via un système dont tous les signaux sans fil et câblés sont désactivés. Dans les systèmes les plus fermés pour les données hautement sécurisées, certains services informatiques désactivent tous les ports USB et utilisent une cage de Faraday pour bloquer toute transmission sans fil et empêcher les fuites électromagnétiques.

La technologie Auto Image Replication (AIR) vous permet de répliquer les données de sauvegarde entre les domaines de sauvegarde, qui peuvent se trouver sur le même site ou sur des sites différents, y compris dans les clouds publics. Elle permet également d'effectuer des copies hors ligne et isolées de vos sauvegardes, afin de réduire encore davantage les risques d'accès aux données par des sources non intentionnelles. Au fur et à mesure que les données se multiplient dans vos propres datacenters et dans les clouds publics, il est important de disposer d'une solution de sauvegarde et de récupération qui mette en œuvre une structure isolée pour maintenir une bonne copie des données en dernier recours.

Données cloud et isolement

La mentalité « cloud-first » se développe : 85 % des entreprises déclarent qu'elles seront « cloud-first » d'ici 2025, 94 % d'entre elles mettant en œuvre une stratégie multicloud[5]. Nous avons constaté une forte accélération des stratégies cloud. Cela pourrait entraîner une disparité au niveau des outils et des autorités de décision. Tout comme vous diversifiez et optimisez votre référentiel de données primaires avec différentes options de cloud public, il est important d'optimiser votre approche de récupération des données avec les meilleures solutions construites pour vous remettre sur pied.

Nous recommandons la fonctionnalité d'un environnement de récupération isolé (IRE). Il s'agit de la meilleure option possible. Les solutions d'isolement proposées dans un IRE créent une copie sécurisée de vos données, afin de fournir aux administrateurs un ensemble de fichiers propres à la demande, pour neutraliser l'impact d'une attaque de ransomware dans un environnement multicloud.

Environnements de récupération isolés

Les solutions traditionnelles d'isolement des réseaux interrompent physiquement ou logiquement la connectivité entre les sites sécurisés, rendant toute communication entrante ou sortante impossible. Cela limite le transfert de données vers l'environnement isolé et met en péril les objectifs de délai de reprise (RTO) et de point de reprise (RPO) lorsque la copie tertiaire est nécessaire. Le domaine source traite et soumet de manière indépendante un travail de réplication à un domaine cible, ce que l'on appelle communément pousser des données de réplication de la source vers la cible. Cette approche traditionnelle limite le temps disponible pour répliquer les données critiques dans un environnement sécurisé lorsque la connexion est interrompue ou bloquée.

En revanche, le modèle de réplication Pull initie la demande de réplication à partir de la cible. Veritas propose la solution IRE de NetBackup, qui optimise le mouvement des données en offrant un modèle de réplication Pull dans lequel la demande d'envoi de données provient du pool de déduplication du serveur de médias (MSDP) de l'IRE, et la connexion inverse offre un meilleur contrôle du flux de données pour sécuriser davantage l'environnement logiquement et physiquement. Les réplications vers l'IRE peuvent désormais être entièrement contrôlées à partir de l'IRE, y compris la prise en charge d'une fenêtre spécifique telle que définie dans le calendrier de l'isolement de l'IRE.

L'IRE de NetBackup est impénétrable pendant le transfert des données grâce à plusieurs couches de sécurité, incluant des mécanismes de prévention des intrusions et un chiffrement des données, en transit et au repos. Les données sont sécurisées tout au long de leur parcours, le stockage n'est pas compromis et il n'y a aucun risque que des utilisateurs malveillants ou non autorisés lisent ou modifient les données. Veritas propose des options d'isolement des données sur site et dans le cloud avec NetBackup Recovery Vault. Il s'agit d'un service de stockage cloud transparent, doté d'un isolement pour protéger contre les ransomwares. Il est optimisé pour évoluer et garantit la portabilité des données à des coûts prévisibles.

Veritas propose un workflow simple qui vous permet de transformer n'importe quel NetBackup (sur site ou dans le cloud) en une structure IRE, offrant une résilience contre les ransomwares axée sur trois principes clés :

- **Protection** : incorporez facilement une fonctionnalité de récupération isolée avec la prise en charge de l'authentification multifactorielle (MFA) et du contrôle d'accès basé sur les rôles (RBAC), qui s'aligne sur la stratégie de sécurité zéro confiance de Veritas.
- **Détection** : NetBackup IT Analytics offre une détection des anomalies qui permet de détecter les ransomwares en temps réel. La fonctionnalité intégrée d'analyse des malwares de NetBackup permet d'analyser les malwares avant la restauration et peut être exécutée en priorité en fonction des scores d'anomalie.
- **Récupération** : orchestrez la récupération d'un ensemble de données dans un environnement isolé, dans le cloud ou sur site, avec la capacité de gérer une grande variété d'exigences de RPO et de RTO.

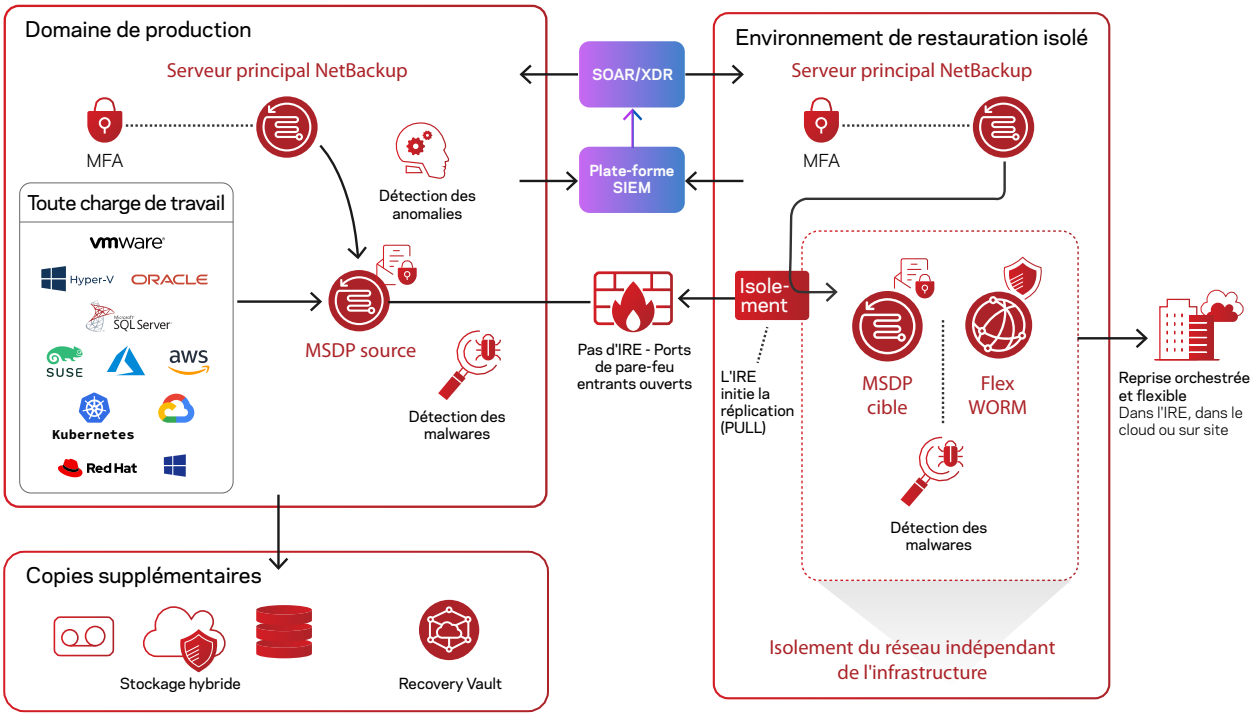

Figure 1 : Environnement de récupération isolé (IRE) NetBackup

Un environnement isolé apporte une couche de résilience supplémentaire pour lutter contre les ransomwares et les malwares.

Renforcer la protection en adoptant une stratégie zéro confiance

Une politique zéro confiance offre une protection supérieure. Il a été prouvé que l'adoption d'un état d'esprit zéro confiance à l'échelle de l'entreprise réduisait le risque d'une attaque dévastatrice.

L'IRE de Veritas s'appuie sur le stockage WORM (Write Once Ready Many) multi-locataire basé sur des conteneurs des appliances Flex, avec un système d'exploitation renforcé et une architecture zéro confiance. En renforçant votre gestion des identités et des accès (IAM) par la MFA et le RBAC pour les utilisateurs, les outils et les machines, vous limitez l'accès aux données hautement sensibles et aux sauvegardes. Seuls les utilisateurs qui ont besoin d'accéder aux données doivent être autorisés. En matière de mots de passe, l'hygiène constitue également une priorité absolue.

Vous pouvez empêcher l'accès à ces zones en mettant en place de solides contrôles IAM, des contrôles de privilèges, un renforcement et un matériel sécurisé, en vous appuyant sur le principe zéro confiance. En cas de violation, cela permet de réduire la surface de l'attaque ou ses effets du fait de la multiplicité des couches de sécurité qui minimisent l'impact. Une fois dans vos systèmes, les cybercriminels se déplacent souvent dans votre environnement à la recherche de données critiques, d'informations confidentielles et de systèmes de sauvegarde.

Détection d'anomalies et analyse de détection des malwares

Avec une visibilité complète, une détection intelligente des anomalies et une analyse des malwares, vous pouvez savoir en toute confiance où se trouvent toutes vos données, tout en réduisant la complexité opérationnelle et en optimisant la gestion des coûts. La détection des anomalies alimentée par l'IA de Veritas reconnaît les données inhabituelles et l'activité des utilisateurs dans l'ensemble de votre environnement, et vous alerte en temps quasi réel en cas d'activité suspecte. Cette fonction garantit que vos données sont toujours récupérables et vous permet de prendre des mesures immédiates en cas de ransomware, en isolant les sauvegardes qui contiennent des malwares et en limitant leur impact sur vos données de sauvegarde. Vous pouvez restaurer des images complètes qui ont été analysées et dont la sécurité a été validée, ou vous pouvez restaurer des fichiers individuels. Si un fichier marqué pour la restauration est infecté, vous pouvez le restaurer à partir d'une sauvegarde non infectée. Vous disposez ainsi d'un moyen sûr et efficace de récupérer les données sans risquer de réinfecter la machine cible.

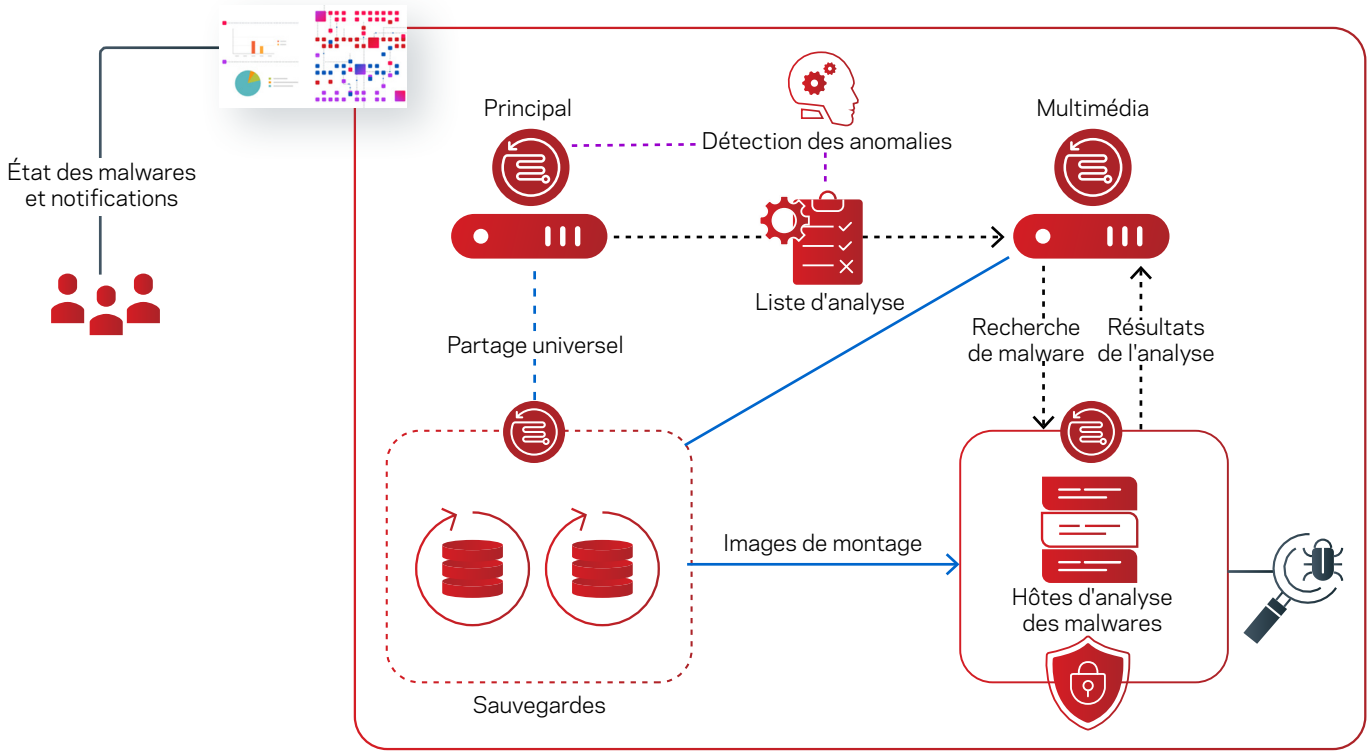

Figure 2 : Analyse des malwares intégrée à NetBackup

Récupérer à l'aide d'un stockage immuable et indélébile

Le stockage immuable et indélébile garantit que les données ne peuvent pas être modifiées, chiffrées ou supprimées pendant une durée déterminée (ou pas du tout). Il empêche également la falsification des données et les accès non autorisés. Dans le cadre de votre stratégie IRE, NetBackup Recovery Vault fournit une solution de stockage immuable et indélébile basée sur le cloud, que vous pouvez adapter en fonction de vos besoins.

Récupérer en toute confiance avec un IRE

Réduisez les risques, éliminez les incertitudes et gardez le contrôle avec l'environnement de récupération isolé (IRE) de NetBackup. Rendez-vous sur Veritas.com ou contactez notre équipe pour en savoir plus sur la façon dont notre solution peut assurer votre résilience contre les ransomwares dans votre environnement multicloud.

Comblez les failles de votre stratégie en matière de cyber-résilience.
En savoir plus >

1. www.gartner.com/en/newsroom/press-releases/2021-01-28
2. www.sonicwall.com/resources/white-papers/2023-sonicwall-cyber-threat-report/
3. www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022
4. csrc.nist.gov/glossary/term/air_gap
5. www.gartner.com/en/newsroom/press-releases/2021-11-10

À propos de Veritas

Veritas Technologies est un leader dans la gestion des données multicloud. Plus de 80 000 entreprises, dont 95 % des entreprises du classement Fortune 100, font confiance à Veritas pour les aider à assurer la protection, la récupération et la conformité de leurs données. Veritas est réputée pour sa fiabilité à grande échelle, qui offre la résilience dont les clients ont besoin contre les interruptions qui pourraient survenir en cas de cyberattaque, par exemple de ransomware. Aucun autre fournisseur n'est en mesure d'égaler la capacité d'exécution de Veritas, avec la prise en charge de plus de 800 sources de données, de plus de 100 systèmes d'exploitation, de plus de 1 400 cibles de stockage et de plus de 60 plates-formes cloud, via une seule approche unifiée. Avec la technologie Cloud Scale, Veritas propose aujourd'hui sa stratégie de gestion autonome des données, qui réduit les coûts opérationnels tout en offrant une plus grande valeur ajoutée. En savoir plus sur www.veritas.com/fr/fr/. Suivez-nous sur Twitter : @veritastechllc.

VERITAS

veritas.com/fr/fr/

Pour obtenir les coordonnées pour le monde entier, consultez la page : veritas.com/fr/fr/company/contact

V1626 05/23