IBM Resiliency Orchestration with Cyber Incident Recovery

Protégez vos données et les fichiers de configuration de votre plateforme avec un outil dédié, pour une reprise rapide, fiable et évolutive après une cyber-attaque

Points clés

- Stockage non modifiable physiquement isolé pour les données et les fichiers de configuration de plateforme.
- Détection rapide des anomalies de configuration des systèmes Windows et Linux, portant sur le registre Windows et la configuration des applications et des périphériques.
- La restauration rapide et orchestrée des données et des fichiers de configuration de la plateforme contribue à réduire l'impact de la perturbation causée par une cyber-attaque ou toute autre panne.
- La fonctionnalité de test et de vérification automatisée permet d'effectuer des tests fréquents sans affecter les systèmes de l'entreprise.
- La visibilité sur le processus et la production de rapports aident à respecter la réglementation.

Les entreprises, quelle que soit leur taille, continuent d'être la cible de cyber-attaques. Alors que les équipes de sécurité informatique améliorent progressivement leur capacité à empêcher ces attaques, le problème demeure de savoir non pas « si » mais « quand » une attaque se produira (si elle n'a pas déjà eu lieu). Si une cyber-attaque endommage les données cruciales et les fichiers de configuration des systèmes d'une entreprise, la perturbation opérationnelle qui en découle peut être aussi préjudiciable à la santé financière et à la réputation de cette entreprise qu'un vol de données ou une panne totale de son outil informatique.

Cela est d'autant plus vrai lorsque la cyber-attaque chiffre les données ou installe un logiciel malveillant qui cible spécifiquement les sauvegardes de données. L'existence d'une connexion réseau permanente avec les sites de sauvegarde et de reprise après incident peut permettre à un logiciel malveillant d'endommager ou de chiffrer aussi ces données, ce qui rend les données principales et les données de sauvegarde inutilisables et retarde de façon importante le retour à un fonctionnement normal.

Ce problème est souvent dû au fait que les solutions de reprise après incident existantes ne sont pas conçues pour récupérer après une cyber-attaque ou souffrent d'insuffisances fonctionnelles usuelles dans ce domaine : trop grand nombre de processus manuels, dossiers d'exploitation périmés et tests inadéquats. Par conséquent, la reprise dure trop longtemps, les points de récupération des données sont trop anciens ou la reprise elle-même échoue.

Un outil spécialement conçu pour la cyber-résilience

Cyber Incident Recovery, basé sur IBM Resiliency Orchestration, est conçu pour permettre la reprise rapide des données et des fichiers de configuration d'une plateforme en cas de cyber-incident. Spécialement conçu pour la cyber-récupération, Cyber Incident Recovery offre les fonctionnalités suivantes :

- Fonction de test simple d'emploi et qui n'affecte pas les environnements de production.
- Détection plus rapide des altérations de données et réponse rapide pour réduire la durée d'indisponibilité.
- Récupération efficiente à un point de synchronisation, qui optimise la Perte de Données Maximale Admissible (PDMA en français ou RPO, Recovery Point Objective en anglais).
- Évolutivité permettant d'effectuer en quelques minutes seulement le travail de détection et de reprise à l'échelle d'un site complet.
- Visibilité et production de rapports simplifiées pour faciliter le respect des exigences réglementaires.

Les composants technologiques de l'outil Cyber Incident Recovery constituent une plateforme qui couvre les couches Données et Traitements des environnements de production et de reprise après incident, pour permettre une approche agile de la reprise après un cyber-sinistre. Cette architecture inclut les composants suivants :

Stockage non modifiable. Utiliser une technologie de stockage non modifiable pour les données de configuration ou celle du stockage non réinscriptible (WORM, write-once-read-many) pour les données des applications prévient l'altération des données et garantit leur récupérabilité en interdisant la modification des sauvegardes après leur enregistrement. Pour les données des applications, cette approche contribue également à réduire les coûts de stockage en ne sauvegardant que les modifications incrémentales aux points de synchronisation.

Protection par isolement physique. Un système d'isolement réseau sépare les environnements de production du stockage WORM qui contient les données sauvegardées, protégées et hébergées sur un site distant ou de reprise après incident. En outre, l'accès au stockage WORM n'est possible que lorsqu'il existe des données à sauvegarder. Cette approche, associée à celle du stockage non modifiable, contribue à empêcher la corruption des données qui sont ainsi protégées des logiciels malveillants capables de traverser les réseaux ou spécialement conçus pour cibler les données de sauvegarde.

Vérification des données de configuration. Ce composant aide à garantir que les fichiers de configuration ou les données protégées sont sains et récupérables. Ce processus, intégré dans Resiliency Orchestration, détecte automatiquement si les fichiers de configuration de votre système ont été modifiés et ne correspondent plus aux versions de référence. Resiliency Orchestration s'intègre également avec les scripts de validation des applications fournis par le client, afin de permettre de tester les applications et les données.

Automatisation et orchestration. En automatisant le processus de reprise de bout en bout des données, des applications, des commutateurs et de l'infrastructure de calcul, Resiliency Orchestration vous permet de restaurer rapidement votre environnement informatique. Resiliency Orchestration remplace les processus manuels classiques par des workflows prédéfinis testés et validés, ce qui vous permet de restaurer d'un seul clic l'ensemble d'un processus métier, d'une application, d'une base de données ou d'un système. Ces workflows orchestrent toutes les étapes nécessaires pour la reprise des données et des systèmes interconnectés, limitant ainsi les risques d'erreur humaine. Resiliency Orchestration vous aide à accélérer la mise en œuvre de la solution en s'appuyant sur une vaste bibliothèque de plus de 450 modèles prédéfinis, qui peuvent être combinés pour créer de nouveaux workflows.

Cyber Incident Recovery pour les fichiers de configuration de plateforme

Fonctionner 24 heures sur 24 nécessite une disponibilité continue de l'infrastructure informatique qui supporte les applications critiques : serveurs physiques, instances de machines virtuelles, systèmes de stockage et unités réseau. Les cyber-agresseurs peuvent mettre une entreprise à l'arrêt en corrompant les données de configuration de ces plateformes.

La fonctionnalité de protection des configurations de plateformes de Cyber Incident Recovery (voir Figure 1) permet de restaurer rapidement les services. Pour ce faire, elle réplique une copie de référence des données de configuration des serveurs et des périphériques sur un dispositif de stockage non modifiable physiquement isolé, situé dans un système de stockage par objets, dans le cloud ou dans un datacenter IBM. Les unités de production sont examinées afin de détecter toute modification des données de configuration. Le système analyse toute modification pour déterminer si elle est valide, et émet une alerte s'il la juge suspecte. Les alertes peuvent aussi servir de tickets pour les logiciels de gestion des contrôles des modifications.

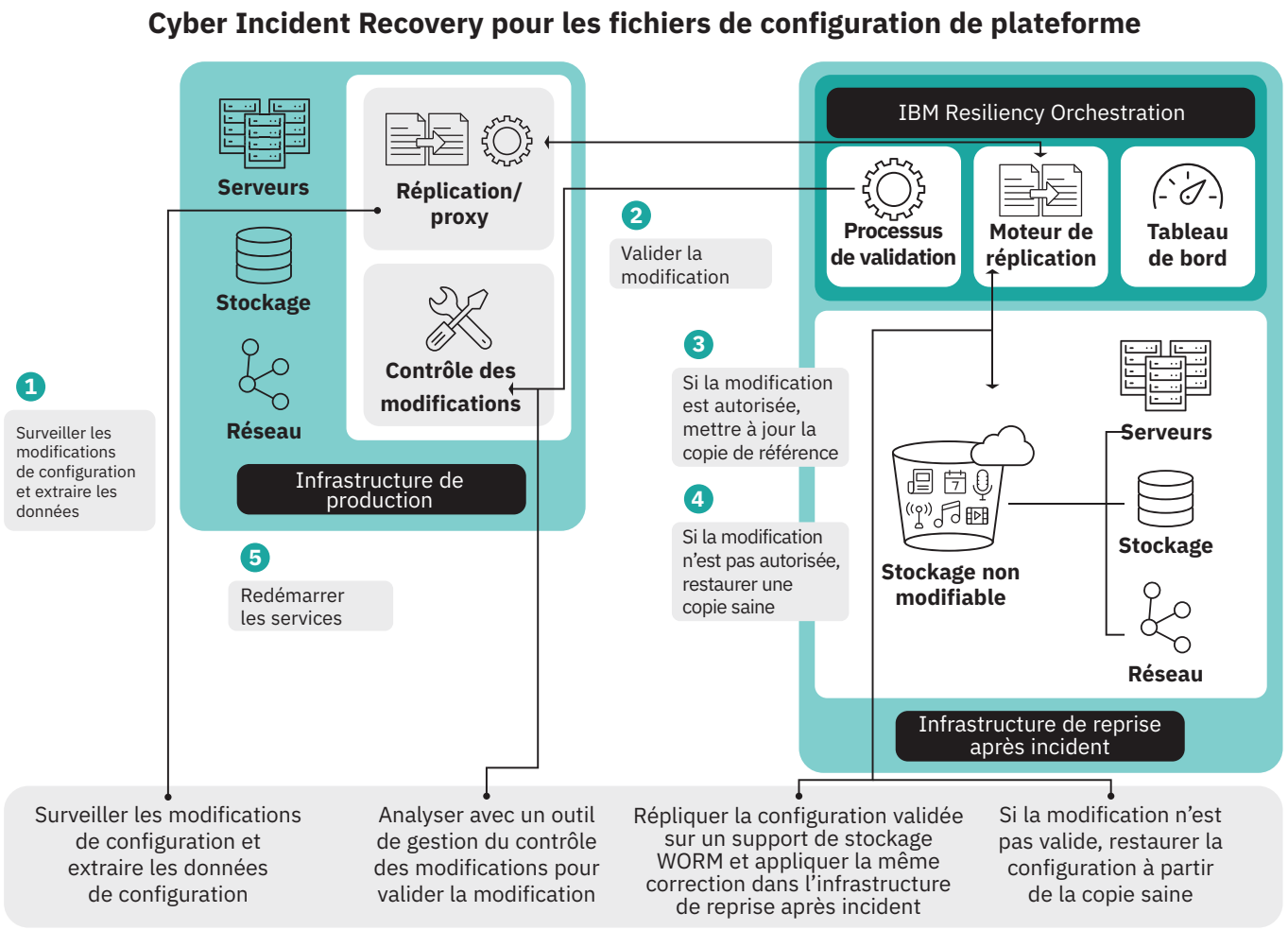

Figure 1. Cyber Incident Recovery pour les fichiers de configuration de plateforme aide à protéger les données de configuration des serveurs physiques, des serveurs virtuels, des unités de stockage et des unités réseau.

Si la modification est valide, les données de configuration sont protégées par la réplication d'une nouvelle copie de référence sur le dispositif de stockage non modifiable. Si elle ne l'est pas, Resiliency Orchestration restaure rapidement la dernière copie saine des configurations dans l'infrastructure de production, en fonction des politiques prédéfinies et avec l'accord des responsables habilités. Les configurations, y compris celles des machines virtuelles, sont restaurées dans une infrastructure de production propre.

Cyber Incident Recovery pour les données

La fonctionnalité de protection des données de Cyber Incident Recovery permet une reprise très rapide et très fiable lorsqu'une cyber-attaque a endommagé les données elles-mêmes. Elle protège les données en mettant en place un isolement physique et en utilisant un stockage non modifiable, tout en orchestrant une reprise rapide sur le site de reprise après incident du client.

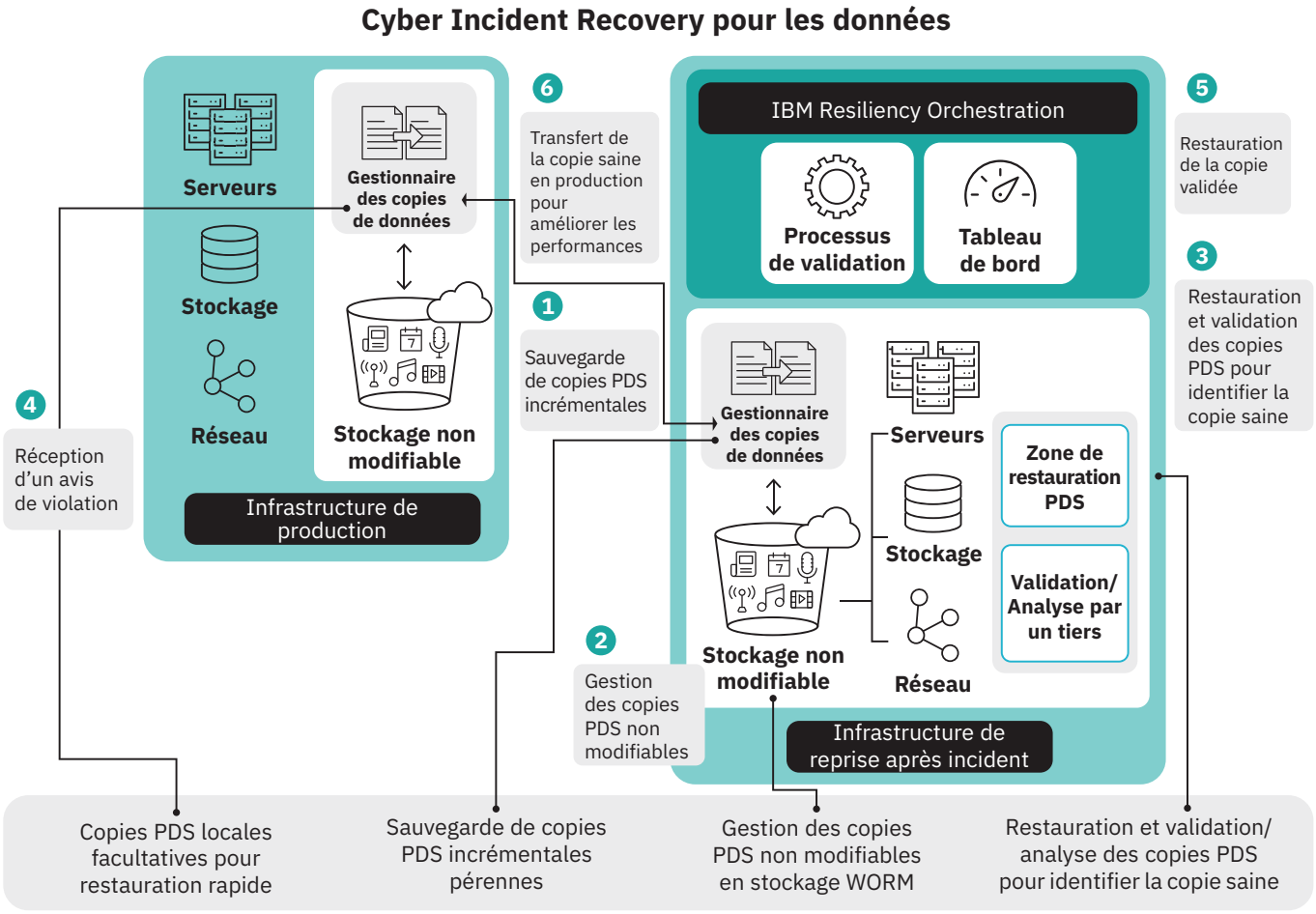

Figure 2. Cyber Incident Recovery pour les données permet de sauvegarder de façon efficiente de grands volumes de données, avec possibilité de les soumettre à des tests non disruptifs et de les restaurer rapidement.

Cyber Incident Recovery est conçu pour gérer de grands volumes de données d'application. Il utilise une technologie de gestion des copies de données pour créer et gérer des copies de données incrémentales à des points de synchronisation (PDS). Comme ces copies sont conservées dans des systèmes de stockage non modifiables, tels que le stockage par objets dans le cloud ou le stockage non réinscriptible (WORM), elles sont pérennes et immuables. Comme le montre la Figure 2, le logiciel de gestion des copies de données réplique les données sur un site de reprise après incident ou sur un site secondaire, créant ainsi des copies PDS. Eventuellement, ces dernières peuvent aussi être créées et stockées sur le site de production pour permettre leur restauration rapide.

Lorsque le responsable d'un site de reprise après incident est averti qu'une atteinte à la protection des données ou une infection par un logiciel malveillant chiffrant les données a été découverte, il lance un test automatique des copies PDS stockées sur son site pour s'assurer de la récupérabilité des données. La dernière copie « saine » identifiée par le processus de test et de vérification est ensuite restaurée dans l'infrastructure du site de reprise après incident par la fonction de reprise rapide du logiciel de gestion des copies de données. Des tests peuvent également être effectués fréquemment sur ce site afin de garantir la récupérabilité des données sans affecter le fonctionnement normal de l'entreprise. Resiliency Orchestration contribue à garantir que les plateformes peuvent être restaurées rapidement, en parallèle.

Des tableaux de bord et des rapports pour simplifier la gestion

Cyber Incident Recovery inclut des tableaux de bord (voir Figure 3) qui contribuent à surveiller les modifications apportées à la configuration des plateformes et aux données. Ils peuvent aussi fournir en temps réel aux cadres de direction ou au conseil d'administration de l'entreprise des informations cruciales sur l'état de l'opération de reprise, pour leur permettre de prendre rapidement des décisions éclairées.

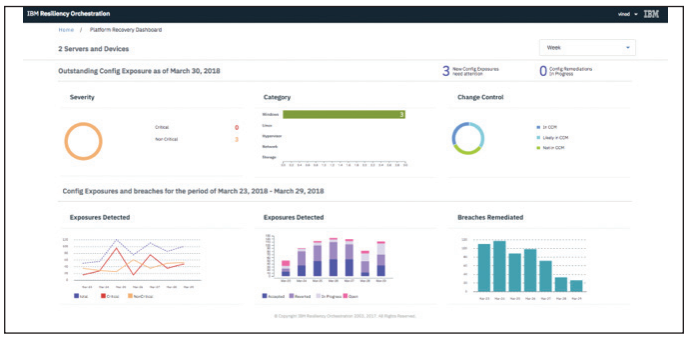

Figure 3. Tableau de bord central.

Le tableau de bord des cyber-incidents affiche des informations, telles que le nombre et le niveau de gravité des vulnérabilités, et permet de suivre les vulnérabilités ouvertes. Le tableau de bord des données offre une visibilité sur les écarts par rapport aux objectifs de Perte de Données Maximale Admissible (PDMA) et de temps de reprise, une vue instantanée des statuts et de la disponibilité de l'outil informatique.

Le module de génération de rapports intégré permet de créer une grande variété de rapports : rapports sur la cyber-résilience ou la situation de reprise après incident, qui peuvent être exportés et partagés avec les régulateurs aux fins de conformité réglementaire, ainsi que des graphiques représentatifs de moments captés pendant le fonctionnement normal de l'entreprise.

Pourquoi IBM ?

Depuis près de 60 ans, IBM Business Resiliency Services aide les entreprises du monde entier à couvrir leurs besoins en matière de sauvegarde et de reprise. Aujourd'hui, plus de 9 000 clients sont protégés par nos services de reprise après incident et de gestion de données. Aussi, nous hébergeons et gérons annuellement plus de 3,5 exaoctets de données. Plus de 300 centres de résilience IBM, répartis dans plus de 60 pays à travers le monde, fournissent des services de reprise après incident et de protection des données, et plus de 6 000 spécialistes IBM sont dédiés à la résilience dans le monde entier.

Pour plus d'informations

Pour en savoir plus sur Cyber Incident Recovery, veuillez prendre contact avec votre interlocuteur IBM ou visiter le site Web suivant :
ibm.com/services/business-continuity/cyber-resilience

En outre, IBM Global Financing propose de nombreuses options de paiement pour vous aider à acquérir la technologie dont vous avez besoin pour développer votre activité. IBM s'occupe de la gestion du cycle de vie des produits et services informatiques, de leur acquisition à leur mise au rebut. Pour plus d'informations sur IGF, visitez le site suivant : **ibm.com**/financing/fr

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex

La page d'accueil d'IBM se trouve à l'adresse :
ibm.com

Pensez au recyclage

89017289-FRFR-02