kyndryl

Resiliency Orchestration with Cyber Incident Recovery

La cyber-résilience sur mesure pour une reprise rapide, fiable et évolutive dans les environnements multicloud hybrides

Sommaire

Des changements à considérer

Pour les cyber-attaquants, lorsque vos données et vos applications transitent via une infrastructure de plus en plus interconnectée, combinant environnements sur site, publics et multicloud, les occasions d'interrompre la continuité de votre activité métier se multiplient. La complexité inhérente aux environnements multicloud hybrides expose vos données critiques et vos configurations système à des risques plus élevés que jamais, à tel point que la probabilité de réussite d'une cyber-attaque est devenue une certitude absolue. Votre équipe de sécurité IT aura beau faire preuve de vigilance, une cyberattaque finira inévitablement par provoquer une disruption de l'activité métier, que ce soit sous la forme d'une panne, d'un vol d'informations ou d'une altération des données, avec pour conséquences une atteinte à votre réputation et des retombées financières.

Il n'y a pas si longtemps, les solutions traditionnelles de reprise après incident permettaient d'atténuer les ravages causés par la plupart des cyberattaques classiques. Toutefois, ceci était le cas longtemps avant l'apparition des environnements multicloud hybrides. En effet, si les infrastructures IT sont devenues plus complexes, les cyberattaques sont pour leur part devenues plus sophistiquées. Les attaques par chiffrement des données et par logiciels malveillants sont aujourd'hui conçues pour cibler les sauvegardes de données avec des méthodes auparavant inimaginables. Les agresseurs parviennent à accéder aux emplacements réservés aux sauvegardes et à la reprise après incident, rendant inutilisables les données principales et de sauvegarde, et retardant considérablement la capacité à restaurer les opérations de production.

Kyndryl Resiliency Orchestration with Cyber Incident Recovery atténue l'impact des cyberattaques sur l'entreprise en permettant une reprise rapide, fiable et évolutive dans les environnements multicloud hybrides.

La cyber-reprise sur mesure dans un univers multicloud hybride
Kyndryl™ Resiliency Orchestration with Cyber Incident Recovery vous permet de récupérer rapidement vos configurations de données et de plateforme en cas de panne provoquée par une cyber-attaque. La solution met en place une automatisation intelligente des flux de travaux de protection et de reprise des données. Elle effectue le test de la reprise, garantit que les données sont non modifiables, et exécute la détection des anomalies, la surveillance, la gestion et le reporting dans les environnements multicloud hybrides. Elle assure une reprise automatique, fiable et rapide des charges de travail physiques et virtuelles, notamment les processus métier, les applications, les systèmes et les bases de données suite aux cyber-attaques.

Les points forts de Cyber Incident Recovery :
- Une fonctionnalité de test facile à utiliser qui n'impacte pas les environnements de production.
- Une détection accélérée de l'altération de données et une réponse rapide qui réduit les temps d'indisponibilité.
- Une reprise efficace à partir d'un point de cohérence qui optimise les objectifs de point de reprise (RPO).
- Une évolutivité lui permettant de gérer en quelques minutes une détection et une reprise de grande ampleur à l'échelle de tout un site.
- Une visibilité et un reporting simplifiés qui facilitent la conformité aux exigences en matière de réglementation.

Kyndryl Resiliency Orchestration with Cyber Incident Recovery assure une reprise automatique, fiable et rapide des charges de travail physiques et virtuelles suite aux cyber-attaques.

Une architecture permettant une approche agile de la cyber-résilience

Cyber Incident Recovery fait appel à une technologie qui inclut les couches de calcul et de données des environnements de production et de reprise après incident. Il permet une approche agile de la reprise de toutes vos charges de travail virtuelles et physiques.

Stockage non modifiable
Le recours au stockage non modifiable pour les données de configuration, ou au stockage non réinscriptible (WORM) pour les données d'application évite les altérations et garantit la capacité de reprise, en interdisant les modifications des sauvegardes une fois celles-ci effectuées. Dans le cas des données issues des applications, cette approche réduit également les coûts du stockage, en n'écrivant que les nouvelles modifications incrémentielles ponctuelles.

Protection de type air gap
L'isolement du réseau sépare les environnements de production du stockage WORM qui contient les données sauvegardées et protégées sur un site distant ou de reprise après incident. L'accès au stockage WORM est en outre réservé uniquement aux données lorsqu'elles ont besoin d'être sauvegardées. Cette approche, combinée au stockage non modifiable, évite que les données protégées ne puissent être altérées par des logiciels malveillants capables de s'infiltrer dans les réseaux ou conçus spécialement pour attaquer les données de sauvegarde.

Détection des anomalies
Kyndryl Resiliency Orchestration comprend une fonctionnalité de détection des anomalies qui utilise une identification heuristique basée sur des règles, augmentée par l'intelligence artificielle (IA).Elle est entrainée à partir de différents modèles de changement de logiciels malveillants connus. Elle capture et compare ces modèles dans des données sauvegardées pour prévoir les anomalies de données avec une grande précision. Sur un site de reprise après incident, la détection des anomalies permet d'identifier les instantanés sauvegardés anormaux et de les restaurer à partir de copies saines.

Vérification des données de configuration
Ce composant utilise la fonction intégrée de détection des anomalies basée sur l'IA afin de garantir que la configuration ou les données protégées sont saines et récupérables. Ce processus, qui est intégré à Resiliency Orchestration, détecte automatiquement les modifications de vos configurations système. Resiliency Orchestration s'intègre également aux scripts de validation d'applications fournis par les clients afin d'exécuter des tests de l'application et des données.

Automatisation et orchestration
En automatisant le processus de reprise de bout en bout des données et des applications, Resiliency Orchestration permet une restauration rapide de votre environnement IT. Resiliency Orchestration remplace les processus manuels traditionnels par des flux de travaux prédéterminés qui ont été testés et validés, et vous permettent de récupérer la totalité d'un processus métier, d'une application, d'une base de données ou d'un système discret d'un simple clic. Ces flux de travaux orchestrent les nombreuses étapes nécessaires à la reprise des systèmes et des données interconnectés, et limitent les erreurs humaines. Resiliency Orchestration accélère l'implémentation de la solution en faisant appel à une vaste bibliothèque contenant plus de 800 modèles prédéfinis qui peuvent être combinés pour créer des flux des travaux.

Cyber Incident Recovery pour la configuration de plateforme

Les logiciels malveillants modifient souvent les configurations avant d'altérer les données elles-mêmes. Il est donc fondamental de détecter les modifications de configuration avant toute infection des données. La fonction de configuration de plateforme de Cyber Incident Recovery protège les données de configuration des charges de travail virtuelles et physiques, les applications, les systèmes de stockage et les périphériques réseau dans les environnements sur site, de cloud public, de cloud hybride et multicloud.

La garantie de la continuité opérationnelle avec une «copie de référence»

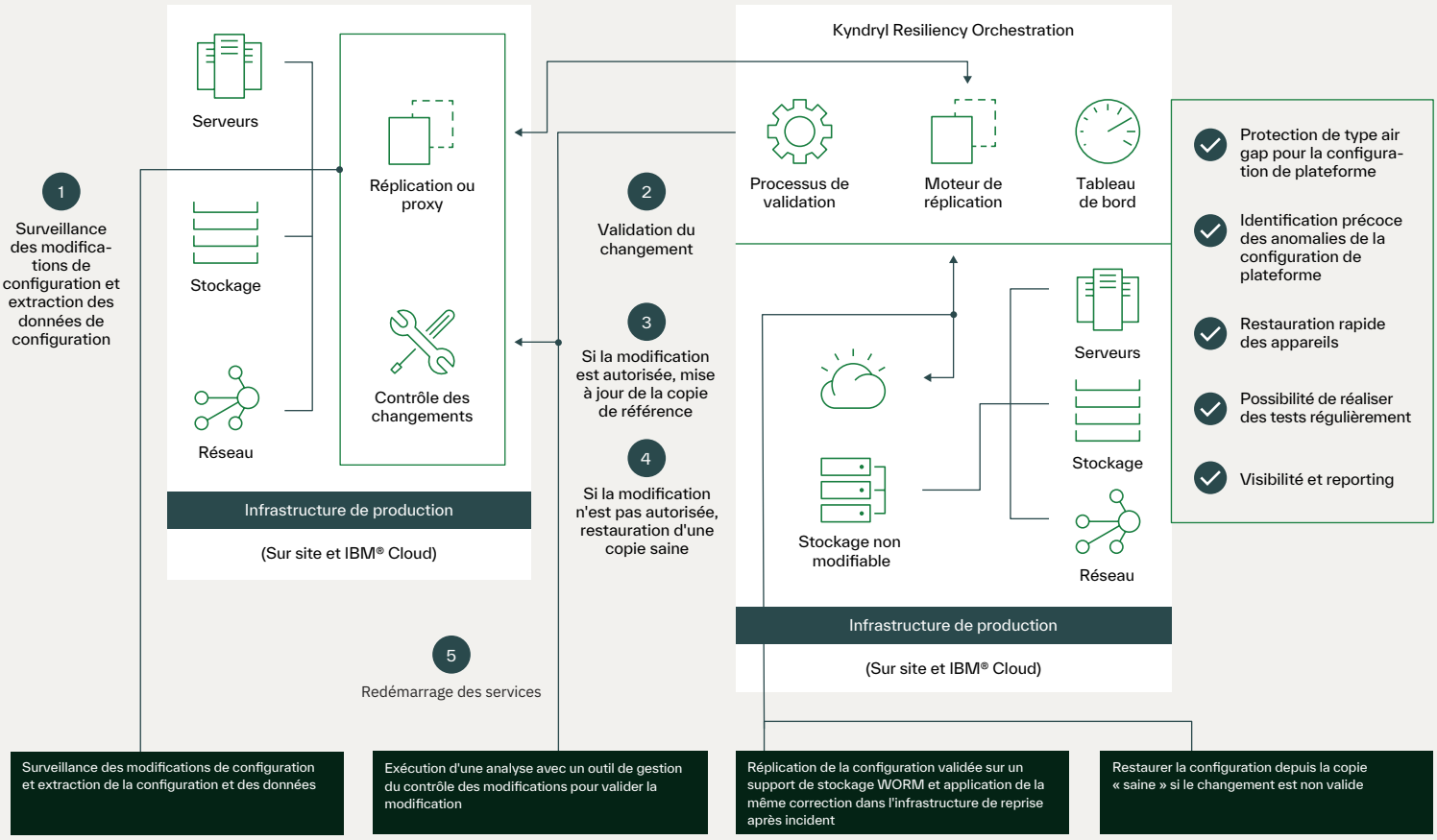
Ce composant utilise les technologies intégrées pour identifier les modifications des configurations des nœuds finaux de production et alerte l'utilisateur en cas de modification autorisée et non autorisée. Les alertes permettent également de générer les tickets à partir de logiciels de contrôle des modifications. Pour restaurer rapidement les services, Cyber Incident Recovery réplique une «copie de référence» des données de configuration du serveur et des terminaux dans du stockage non modifiable protégé par air gap.

Réponse aux modifications de configuration valides et non valides

En cas de modification valide, les données de configuration sont protégées par la réplication d'une nouvelle «copie de référence» dans du stockage non modifiable. Si une modification non valide est identifiée, la dernière copie saine de configurations de dispositif est rapidement restaurée sur l'infrastructure de production par Resiliency Orchestration, en fonction de règles pré-établies et avec l'autorisationde la direction impliquée. Les configurations des machines dédiées et virtuelles sont restaurées sur une infrastructure de production saine. En cas de modifications valides, une nouvelle «copie de référence» est créée dans le stockage non modifiable.

Kyndryl Cyber Recovery as a Service

Reprise après cyber-incident pour la configuration de la plateforme



*Isolement non pris en charge pour le stockage non modifiable hébergé sur le Cloud

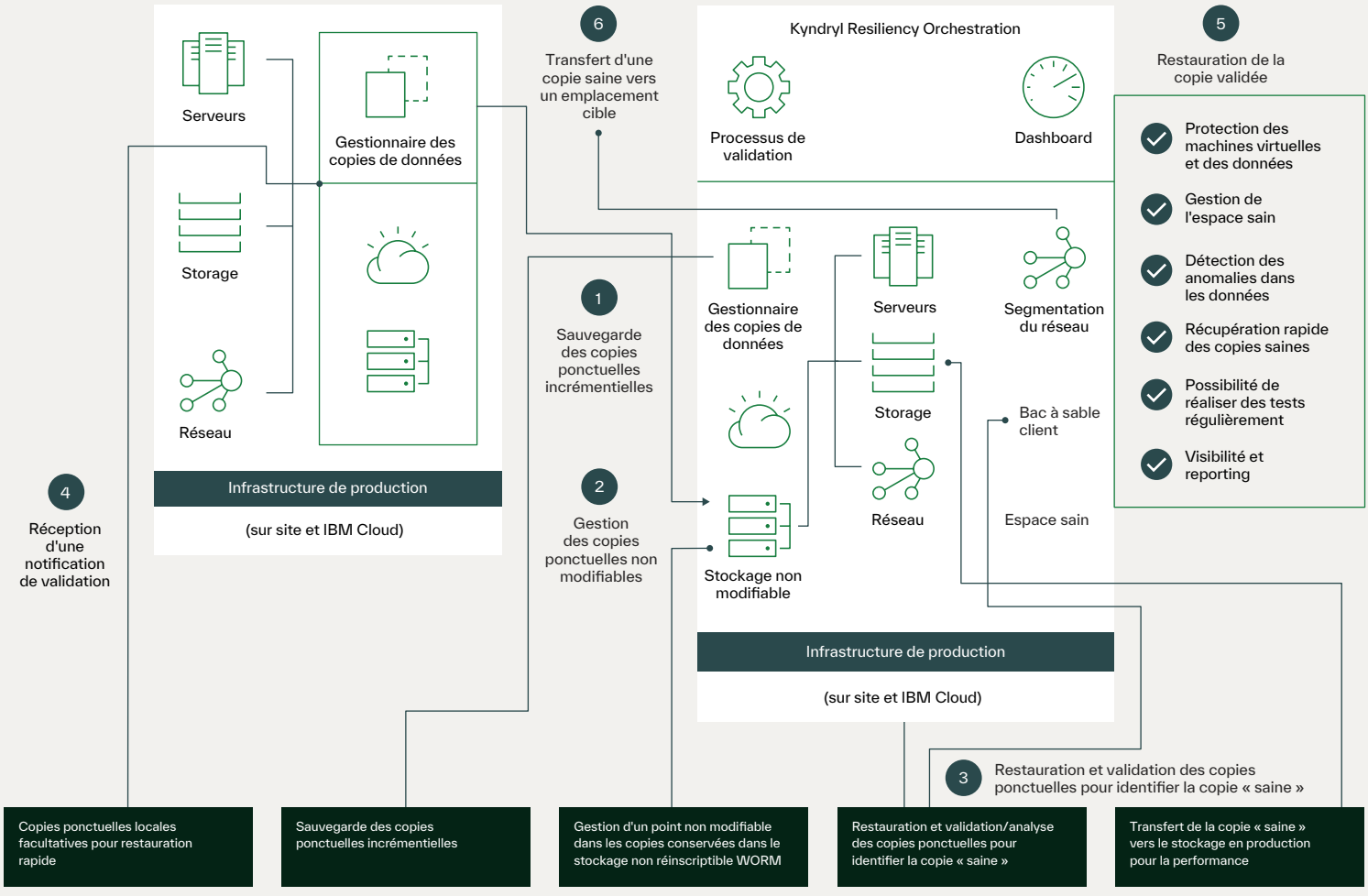
Cyber Incident Recovery pour les données

La fonctionnalité de données de Cyber Incident Recovery permet une reprise rapide et ultra-fiable contre les cyberattaques qui altèrent les données. Elle protège les données grâce à une protection de type air gap et un stockage non modifiable, tout en orchestrant la reprise rapide sur le site de reprise après incident.

Protection de gros volumes de données dans tous les environnements
Cyber Incident Recovery est prévu pour gérer de gros volumes de données d'application, quel que soit leur emplacement. Il est basé sur une technologie de gestion des copies de données qui crée et gère des copies de données ponctuelles incrémentielles. Comme ces copies sont conservées dans du stockage non modifiable, par exemple du stockage objet sur le cloud ou du stockage WORM, ce sont des copies «immuables» qui ne peuvent pas être modifiées. Le logiciel de gestion des données de copie réplique les données sur un site de reprise après incident ou un autre site, et crée les copies ponctuelles incrémentielles. Ces copies peuvent aussi être effectuées et stockées sur le site de production pour permettre une restauration rapide.

Réponse rapide aux cyberattaques pour préserver la continuité des opérations
Lorsque le responsable de la reprise après incident est averti de la découverte d'une infection par logiciel malveillant ou par chiffrement des données, un test automatique des copies ponctuelles incrémentielles est réalisé sur le site de reprise après incident pour vérifier que les données sont récupérables. La dernière copie «saine» identifiée par le processus de test et de vérification est alors récupérée sur l'infrastructure de reprise après incident par le logiciel Resiliency Orchestration. Des tests peuvent aussi être réalisés fréquemment sur le site de reprise après incident. Ils garantissent la possibilité de récupérer les données sans impacter les opérations métier. Resiliency Orchestration assure une reprise rapide et en parallèle des plateformes.

Kyndryl Cyber Recovery as a Service
Reprise après cyber-incident pour les données



Des tableaux de bord et un reporting simplifiant la gestion

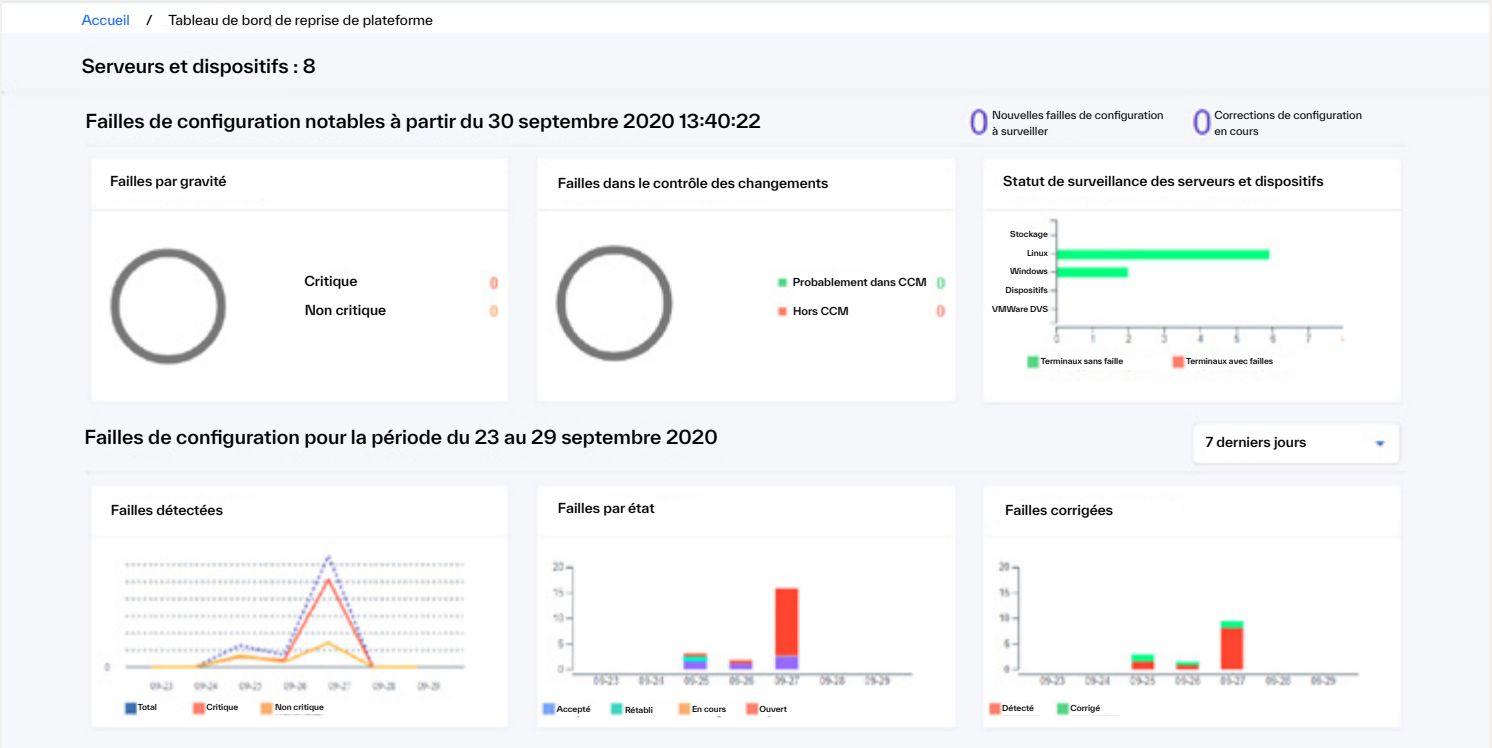
Cyber Incident Recovery comprend un tableau de bord qui simplifie la gestion de Cyber Recovery, ainsi que la surveillance des modifications de la configuration de la plateforme et des modifications des données. Il permet la visibilité en temps réel des écarts de l'objectif de point de reprise (RPO) et de l'objectif de temps de reprise (RTO), du statut de validation des instantanés et des mises à jour critiques de Cyber Recovery.

Pour sa part, l'équipe de direction ou les membres du conseil d'administration peuvent recevoir des mises à jour critiques de Cyber Recovery leur permettant de prendre des décisions plus rapides et mieux informées.

Meilleur suivi des vulnérabilités et visibilité accrue
Le tableau de bord de Cyber Incident Recovery vous indique le nombre de vulnérabilités dans vos environnements, et précise le degré de gravité de chacun d'entre eux. Vous pouvez effectuer le suivi des vulnérabilités ouvertes et prendre des décisions basées sur une bonne visibilité des écarts de l'objectif de point de reprise (RPO) et de l'objectif de temps de reprise (RTO), du statut de validation des instantanés et de votre degré actuel de préparation à la cyber-résilience.

Une fonctionnalité robuste de reporting
Le module intégré de reporting comprend un riche ensemble de rapports, notamment sur la cyber-résilience ou la stratégie de reprise après incident. Ces rapports peuvent être exportés et partagés avec les autorités de réglementation à des fins de conformité, et s'accompagner de graphiques enregistrés pendant le déroulement normal des opérations métier.

Cyber Incident Recovery permet la visibilité en temps réel des écarts de l'objectif de point de reprise (RPO) et de l'objectif de temps de reprise (RTO), du statut de validation des instantanés et des mises à jour critiques.



Les services de résilience d'entreprise Kyndryl ont accumulé des dizaines d'années d'expérience à aider des clients dans le monde entier pour leurs besoins de sauvegarde et de reprise.

Avantages offerts par Kyndryl
- Expertise dans tout le cycle de vie de la résilience
- Reprise automatique des charges de travail physiques, virtuelles et cloud
- Plus de 800 modèles prédéfinis accélérant et optimisant l'implémentation et l'évolutivité
- Choix de clouds, notamment AWS, Azure et IBM Cloud, pour l'évolutivité de l'entreprise

Digne de confiance
- Plus de 9000 clients sont protégés par les services Kyndryl de reprise après incident et de gestion de données.
- Kyndryl compte plus de 3,5 exaoctets sauvegardés annuellement et sous sa gestion

Une présence internationale
- Plus 300 IBM Resiliency Centers dans plus de 50 pays du monde.
- Plus de 6 000 professionnels IBM à travers le monde se consacrent à la résilience

Pourquoi Kyndryl ?

Kyndryl possède une expertise approfondie dans la conception, l'exploitation et la gestion des infrastructures technologiques les plus modernes, efficaces et fiables, sur lesquelles notre monde s'appuie jour après jour Nous sommes profondément engagés à faire progresser l'infrastructure vitale qui alimente le progrès humain. Nous nous appuyons sur nos principes d'excellence en créant des systèmes selon de nouvelles méthodes : en faisant appel aux bons partenaires, en investissant dans nos activités et en travaillant côte à côte avec nos clients pour libérer leur potentiel.

Prêt à en apprendre plus ?

Pour en savoir plus sur ce que Kyndryl Resiliency Orchestration with Cyber Incident Recovery peut faire pour vous, veuillez contacter un représentant Kyndryl ou visiter www.kyndryl.com

kyndryl

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

Produit aux États-Unis d'Amérique
Juillet 2021