COHESITY

# Se préparer aux attaques par ransomware : guide d'évaluation détaillé

Renforcez la sécurité de vos données et votre cyber-résilience

# Sommaire

Le champ d'action croissant des ransomwares ..... 3

Actions essentielles pour contrer les ransomwares ..... 3

Protéger les données et systèmes de sauvegarde ..... 4

Les ransomwares ne sont pas près de disparaitre ..... 4

Réduire le risque d'accès non autorisé ..... 7

Voir et détecter les attaques pour empêcher les intrusions ..... 8

Renforcer sa posture de sécurité grâce une plateforme extensible ..... 10

Assurez-vous de pouvoir rapidement récupérer vos données à grande échelle ..... 12

Liste de contrôle : évaluer sa préparation aux attaques par ransomware ..... 14

Soyez prêt à faire face aux attaques par ransomware avec Cohesity ..... 15

©2022 Cohesity. Tous droits réservés.

# Le champ d'action croissant des ransomwares

Les cybercriminels s'attaquent aux données dont votre entreprise a besoin pour fonctionner. Leur capacité à vous extorquer une rançon dépendra des mesures que vous prenez aujourd'hui pour renforcer votre environnement et améliorer votre réponse en cas d'attaque.

Les menaces liées aux ransomwares ne cessent d'évoluer. Les cibles et les tactiques se développent. Vous devrez bientôt, si ce n'est déjà fait, expliquer comment vous luttez contre les différents moyens utilisés par les cybercriminels pour perturber vos opérations.

| | Ransomware 1.0 | Ransomware 2.0 | Ransomware 3.0 |
|---|---|---|---|
| **Cible des logiciels malveillants** | Données de production | • Données de sauvegarde<br>• Systèmes de sauvegarde<br>• Données de production | • Données de sauvegarde<br>• Systèmes de sauvegarde<br>• Données de production<br>• Données à supprimer illégalement |
| **Mode opératoire** | Chiffrement | Chiffrement | Chiffrement et exfiltration |
| **Comment les entreprises luttent contre les attaques** | Système de sauvegarde et de récupération | Sauvegardes inaltérables et cyber coffre-fort | Détection précoce et surveillance continue |

# Actions essentielles pour contrer les ransomwares

Ce guide est fait pour vous si vous ne savez pas comment renforcer la cyber-résilience de votre entreprise. Il regorge d'informations pratiques et de critères d'évaluation qui vous permettront de savoir quelles capacités chercher pour que votre solution de gestion des données renforce votre stratégie de sécurité des données. Il vous sera également utile pour compléter les outils de votre équipe SecOps et déterminer ensemble la meilleure façon de faire face à des menaces de ransomware qui ne cessent d'évoluer. Ce guide comprend par ailleurs une liste de contrôle qui vous sera utile pour comparer l'efficacité de vos solutions existantes à celle de nos solutions modernes de sécurité et de gestion des données.

Mais avant toute chose, pour mieux protéger vos données et la réputation de votre entreprise, vous devez d'abord comprendre comment ces cinq actions essentielles permettront à votre entreprise de lutter contre les ransomwares :

- Protéger vos données et systèmes de sauvegarde
- Réduire les risques d'accès non autorisés
- Visualiser et détecter les attaques pour stopper les intrusions
- Renforcer votre posture de sécurité grâce une plateforme extensible
- S'assurer de pouvoir rapidement récupérer vos données à grande échelle

©2022 Cohesity. Tous droits réservés.

## Les ransomwares ne sont pas près de disparaitre

**1 070 %**

Pourcentage d'augmentation des ransomwares entre juillet 2020 et juin 2021[1]

**82 %**

Augmentation du pourcentage des rançons moyennes payées depuis 2020, avec un record de 570 000 € au premier semestre 2021[2]

**> 1,85 M€**

Coût moyen actuel pour récupérer d'une attaque par ransomware *sans* payer de rançon[3]

**> 265 Md€**

Montant que les coûts mondiaux des dommages causés par les ransomwares (pertes de revenus et de productivité, remise en état) devraient dépasser d'ici 2031[4]

# Protéger les données et systèmes de sauvegarde

Il est essentiel de protéger vos données pour préserver la confiance de vos clients et conserver votre avantage concurrentiel. Ces mesures de protection stoppent les menaces en constante évolution, notamment les nouveaux ransomwares de type « Locker », qui verrouillent entièrement l'accès d'une entreprise à ses fichiers et applications système, et affiche un compte à rebours indiquant la date et l'heure auxquelles le paiement de la rançon est attendu. Si vous n'améliorez la protection de votre infrastructure, votre entreprise n'a aucun moyen d'empêcher les cybercriminels de chiffrer (ou pire, de voler) ses données.

Les six capacités de sécurité des sauvegardes suivantes doivent absolument être intégrées à la solution de gestion des données que vous envisagez de mettre en place si vous voulez optimiser la résilience de vos données dans les environnements hybrides et multi-cloud.

### Snapshots inaltérables

Les snapshots de sauvegarde logiciels natifs et immuables représentent une protection efficace contre les attaques par ransomware, car ils ne peuvent être ni chiffrés, ni modifiés, ni supprimés (des tactiques couramment utilisées par les cybercriminels pour obliger leurs victimes à payer une rançon). C'est extrêmement important pour protéger l'authenticité des données, en particulier les quantités massives de données non structurées, notamment les fichiers audio et vidéo, ainsi que les images requises dans certains secteurs comme la justice et la santé. Contrairement à l'immuabilité matérielle, les snapshots natifs en lecture seule hébergés sur site ou dans le cloud ne sont jamais exposés ni montés en externe sur une quelconque application, et ne peuvent pas être altérés, modifiés ou supprimés. Les logiciels malveillants ne peuvent donc pas cibler vos données de sauvegarde.

[1] FortiGuard Labs. « Rapport sur le paysage mondial des menaces » (en anglais), août 2021.
[2] Palo Alto Networks. « Les extorsions de fonds atteignent de nouveaux records alors que la crise des ransomwares s'intensifie » (en anglais), 9 août 2021.
[3] Sophos. « L'état des ransomwares en 2021 » (en anglais), 2021.
[4] Cybersecurity Ventures. « Le coût mondial des dommages causés par les ransomwares devrait dépasser 265 milliards d'euros d'ici 2031 » (en anglais), 3 juin 2021.

©2022 Cohesity. Tous droits réservés.

### WORM

Des mécanismes tels que la technologie WORM (write once, read many) offrent une autre couche de protection contre les attaques par ransomware. Ils permettent aux équipes de mettre en place des stratégies pour créer et appliquer un verrouillage temporel des données, puis de les affecter à certaines tâches pour renforcer l'immuabilité des données protégées. Cette protection ne peut être modifiée ou supprimée ni par les responsables de la sécurité ni par les administrateurs de la sécurité. Vous n'avez donc pas à vous préoccuper outre mesure des menaces internes potentielles.

### Chiffrement des données

Il y a le chiffrement standard, et le chiffrement logiciel, validé par la norme FIPS AES-256, pour les données en transit et au repos. Vous avez besoin du module cryptographique validé par le NIST (National Institute of Standards and Technology) américain selon la norme FIPS (Federal Information Processing Standards) 140-2 level 1. Cette norme développée et publiée par le gouvernement des États-Unis est conçue pour valider les modules cryptographiques. Elle garantit que la conception du module et la mise en œuvre des algorithmes cryptographiques sont correctes et sécurisées. Le chiffrement validé par la FIPS est plus sécurisé car les produits doivent avoir réussi une série de tests rigoureux pour être certifiés. Cette norme est d'ailleurs aujourd'hui reconnue à l'échelle mondiale.

### Audit et analyse de la configuration

Votre équipe informatique exploite probablement aujourd'hui un grand nombre de systèmes et d'outils différents, qui possèdent tous leur propre configuration, leurs propres stratégies et leur propre interface de gestion. Les processus manuels qui permettent de les faire fonctionner sont souvent à l'origine d'erreurs humaines qui pourraient être évitées. N'y aurait-il pas une solution plus efficace ? Un système automatisé avec analyse guidée qui audite différents paramètres de sécurité des données et de contrôle d'accès vous permet d'éviter de coûteuses erreurs humaines et de simplifier l'exploitation des données (qu'il s'agisse des processus de mise en place, de stratégie, ou de gestion).

### Tolérance aux pannes

La résilience des données doit toujours être au cœur de la sécurité. Vous avez donc également besoin d'un système tolérant aux pannes qui garantisse l'intégrité des données et la réussite des sauvegardes, même dans les conditions les plus difficiles. C'est notamment le cas lorsque vos systèmes sont proches de leur pleine capacité de calcul, de mémoire ou de stockage, si le réseau est très encombré, ou en cas de défaillance matérielle inattendue. Cherchez une solution tolérante aux pannes, qui permette de poursuivre les sauvegardes malgré la défaillance d'un composant/nœud.

©2022 Cohesity. Tous droits réservés.

### Cyber coffre-fort moderne et flexible

Lorsque vous modernisez votre approche de la gestion des données, vous devez également mettre à jour votre stratégie de cyber coffre-fort. Les entreprises ont toujours conservé des copies de leurs données sécurisées via air-gap sur bandes. Cette méthode ne permet pourtant plus de respecter les accords de niveau de service (SLA) exigeants d'aujourd'hui en ce qui concerne les délais de récupération, notamment lors d'une attaque par ransomware de grande ampleur. Le terme « air gap » est aujourd'hui largement utilisé à tort pour décrire des techniques qui n'isole pas réellement les données, mais ne vous laissez pas induire en erreur. Assurez-vous que votre solution de sécurité et de gestion des données offre à la fois une véritable protection par air gap et des options modernes de cyber coffre-fort. Celles-ci concilient les besoins modernes d'objectif de délai de récupération et d'objectif de délai de récupération (RTO/RPO) avec des contrôles de sécurité appropriés en stockant les données de sauvegarde dans le cloud ou ailleurs à l'aide d'une connexion temporaire très sécurisée. Vous obtenez alors un environnement inviolable, qui permet d'éviter les perturbations dues aux ransomwares et aux menaces internes, mais également de respecter au mieux vos accords de niveau de service (SLA) organisationnels. Et surtout, vous conservez toujours une copie inaltérable de vos données.

## 4 QUESTIONS CLÉS À POSER SUR LES SYSTÈMES ET LES DONNÉES DE SAUVEGARDE

- Comment votre solution de gestion des données protège-t-elle vos données sauvegardées contre les attaques par ransomware ?
- Comment votre solution assure-t-elle la sauvegarde continue des charges de travail, même après la défaillance d'un composant matériel ou logiciel ?
- Comment votre solution concilie-t-elle les besoins d'une sécurité renforcée avec les RTO/RPO toujours plus rapides des entreprises numériques qui respectent les SLA ?
- Quelle visibilité votre solution offre-t-elle sur les lacunes de sécurité au niveau de la configuration du système et de sa conception opérationnelle ?

©2022 Cohesity. Tous droits réservés.

# Réduire le risque d'accès non autorisé

Les acteurs malveillants travaillent pour leur compte, pour des groupes et pour des états-nations. Votre entreprise a donc tout intérêt à se doter d'une solution de gestion des données dotée de contrôles d'accès stricts. Ces capacités permettent d'empêcher plus efficacement que des pirates externes accèdent au système et aux données sans autorisation, ou que des professionnels internes malhonnêtes exploitent des identifiants compromis.

Pour réduire le risque de vol et de perte de données, cherchez une solution qui intègre les principes du moindre privilège et de la séparation des tâches avec une sécurité granulaire, notamment les quatre capacités indispensables suivantes. Celles-ci permettent de protéger vos données et de préserver la confiance de vos clients

### Authentification multifacteur (MFA)

Même les mots de passe les plus créatifs sont régulièrement compromis et ne peuvent fournir aux entreprises numériques qu'une couche minimale de protection. L'authentification multifacteur (MFA) est un pas en avant dans la lutte contre les tentatives de hameçonnage et autres piratages de mots de passe. Cette fonctionnalité impose que toute personne qui accède à votre solution de sauvegarde ou de gestion des données se soumette à un processus de vérification en plusieurs étapes. Celles-ci doivent s'authentifier avec à la fois quelque chose qu'elles « savent » (par exemple, un mot de passe) et quelque chose qu'elles « ont » (par exemple, une empreinte digitale validée par un fournisseur d'authentification unique (SSO)) pour prouver qu'elles sont bien qui elles prétendent être. Insistez pour que toutes les solutions que vous sélectionnez nécessitent le MFA.

### Modification surveillée

Un observateur peut suffire à déjouer une attaque. Vous avez donc besoin d'une capacité qui empêche un identifiant ou un individu compromis de modifier les éléments essentiels de votre solution de gestion des données. Insistez pour avoir une plateforme qui vous permette d'appliquer des mesures de protection. Protégez-vous par exemple contre les intentions malveillantes et le vol d'identifiant en exigeant que toute modification au niveau de la racine et tout changement critique du système soient autorisés par plusieurs personnes.

### Contrôle d'accès granulaire basé sur les rôles

En matière de données, il est désormais admis qu'une bonne cyber-hygiène passe par une gestion efficace des identités et des accès. Pour réduire les risques de ransomware et les menaces internes, les équipes informatiques doivent désormais accorder à chaque personne un niveau d'accès à toutes les données de l'entreprise dont elle a besoin pour effectuer une tâche particulière et, en même temps, répartir les processus et fonctions de données critiques entre les rôles informatiques pour éviter qu'un seul administrateur ne puisse compromettre toute votre entreprise. Les entreprises dotées de solutions de gestion des données qui simplifient les approches RBAC parviennent mieux à contrecarrer les accès non autorisés et à déjouer les risques pour les données, tout en accordant efficacement à leurs utilisateurs les privilèges nécessaires pour qu'ils puissent travailler.

©2022 Cohesity. Tous droits réservés.

### 3 QUESTIONS CLÉS À POSER SUR LA RÉDUCTION DU RISQUE D'ACCÈS NON AUTORISÉ

- Comment votre solution de sauvegarde ou de gestion des données empêche-t-elle l'accès non autorisé aux données de l'entreprise ?
- Comment votre solution protège-t-elle à la fois contre les ransomwares et la menace interne ?
- Comment configurer une approbation multi-utilisateurs pour les opérations critiques ?

# Voir et détecter les attaques pour empêcher les intrusions

Le monde des entreprises numériques évolue rapidement. Les chefs d'entreprise ont de plus en plus besoin de savoir quelles sont leurs données sensibles, où elles se trouvent et qui y a accès. Ces informations sont essentielles pour se conformer aux réglementations sectorielles ou gouvernementales, maintenir la confiance et répondre rapidement aux attaques de double extorsion (ou exfiltration de données).

Pour minimiser le champ d'action potentiel des ransomwares, recherchez une solution de gestion des données qui intègre de l'intelligence. Vous pourrez ainsi découvrir et classer automatiquement vos données sensibles tout en bénéficiant d'une détection des menaces en temps quasi réel. Trouvez une solution qui permette à votre équipe de travailler plus intelligemment, et non davantage, et qui comprenne quatre capacités essentielles pour apporter une réponse proactive, quelles que soient les menaces qui pèsent sur votre entreprise.

**Alimenté par l'intelligence artificielle (IA) et le machine learning (ML)**

Votre entreprise a besoin de données pour prospérer.  Celles-ci augmentent de façon exponentielle, si bien que certaines solutions de gestion des données sont incapables d'effectuer un pattern matching (filtrage par motif) et une classification des données efficaces, qui vous permettent de savoir lesquelles sont les plus importantes.  En revanche, avec une solution moderne de sécurité et de gestion des données alimentée par l'intelligence artificielle et l'apprentissage automatique (IA/ML), votre entreprise peut détecter plus précisément les variations et réduire les faux positifs sans avoir besoin de plus de personnel. Vous pouvez exploiter les techniques d'IA/ML pour faire correspondre des ensembles de données « connus et fiables » de manière plus efficace et efficiente, car vos « données sensibles connues » sont mises en correspondance et renvoyées à l'algorithme d'IA/ML. C'est un peu comme vouloir trouver une aiguille dans une botte de foin sans faire d'effort.

©2022 Cohesity. Tous droits réservés.

### Détection d'anomalies en temps quasi réel

Plus vite vous trouvez une intrusion, moins elle peut nuire à votre entreprise, et moins vos équipes informatiques sont sollicitées les nuits et les week-ends. Une  solution de gestion des données qui intègre une puissante capacité de détection d'anomalies automatisée en temps quasi réel suit en permanence les opérations normales du système pour repérer rapidement les irrégularités et les comportements anormaux des utilisateurs susceptibles d'indiquer une attaque par ransomware. Ces capacités, associées à des alertes, permettent non seulement de signaler un danger potentiel, mais aussi de lancer des mesures correctives. La détection d'anomalies en temps quasi réel vous permet de découvrir rapidement les attaques en cours de type chiffrement et exfiltration de données, et ainsi de minimiser l'impact des ransomwares.

### Comprendre l'impact d'une attaque

Lorsqu'une anomalie est détectée, utilisez le ML/NLP (natural language processing, ou traitement automatique des langues)  pour déterminer si des données sensibles ont été exposées et définir les processus de correction et de conformité appropriés. Assurez-vous de pouvoir prendre en charge des déploiements à l'échelle mondiale grâce à des modèles préétablis et personnalisables.

### Identifie les menaces potentielles dans les données de récupération

Assurez-vous que vos données de sauvegarde sont exemptes de logiciels malveillants et réduisez le risque de récupération  grâce à une détection des menaces alimentée par des renseignements sur les menaces et le deep learning.  Exploitez les flux et les renseignements sur les menaces pour rechercher les indicateurs de compromission (IOC) susceptibles de signaler une attaque imminente.

### Découverte de cyber-vulnérabilités

Les cybercriminels accèdent à votre environnement de production en exploitant les vulnérabilités logicielles et informatiques (souvent dues à des logiciels non corrigés).  Les solutions de sauvegarde et de gestion des données les plus efficaces devraient permettre à votre équipe de connaître ces vulnérabilités.  Elles devraient également vous permettre de les corriger de manière proactive et d'éviter de réinjecter dans votre environnement de production des cyber-vulnérabilités déjà corrigées lorsque vous récupérez d'une attaque.

©2022 Cohesity. Tous droits réservés.

## 4 QUESTIONS CLÉS À POSER POUR EMPÊCHER LES INTRUSIONS

- Comment votre solution permet-elle de classer les données et d'identifier les informations sensibles susceptibles d'être menacées ?
- Comment votre solution de sauvegarde ou de gestion des données parvient-elle à fournir une visibilité approfondie qui permette d'identifier les vulnérabilités logicielles et informatiques, et à offrir une détection d'anomalie en temps quasi réel ?
- Comment votre solution intègre-t-elle l'IA/le ML pour détecter les anomalies susceptibles d'indiquer une menace ou une attaque par ransomware ?
- Comment votre solution détecte-t-elle les anomalies du système et du comportement des utilisateurs qui révèlent différents vecteurs d'attaque ?

# Renforcer sa posture de sécurité grâce une plateforme extensible

Les ransomwares ne sont pas une menace unique. Ils évoluent et deviennent de plus en plus sophistiqués à chaque itération. Cela signifie que votre solution de gestion des données ne peut pas être rigide ni fonctionner de manière isolée. Elle doit être évolutive et extensible. Les solutions intégrées et interopérables permettent à votre entreprise de détecter les menaces, d'enquêter et de réagir plus rapidement et en toute confiance. Elles sont également les plus à même de tenir les acteurs malveillants en échec.

Recherchez une solution de gestion des données moderne, qui prenne en charge la collaboration avec des tiers afin de renforcer la sécurité de vos données, qui soit flexible, et qui offre des moyens sécurisés de simplifier vos opérations et de rendre vos données productives. Pour créer une posture de sécurité solide, la solution que vous envisagez doit inclure ces trois capacités indispensables et s'intégrer aux autres solutions existantes.

### Intégrations préconçues

Les problèmes de sécurité des données inquiètent les dirigeants d'entreprise. Ils seraient plus sereins s'ils étaient certains que les produits de sécurité auxquels ils font confiance fonctionnent parfaitement ensemble pour lutter contre la cybercriminalité. Cherchez une solution de gestion des données qui soit déjà étroitement intégrée aux principales solutions SOAR (security orchestration, automation and response) et SIEM (security information and event management). Cela permettra d'accélérer les délais de découverte, d'enquête et de correction des attaques par ransomware. Assurez-vous également que cette solution propose des flux de travail intégrés, prédéfinis et extensibles que l'équipe SecOps puisse enrichir pour automatiser la réponse aux incidents et unifier les opérations entre les équipes sécurité, informatique et réseau.

©2022 Cohesity. Tous droits réservés.

### Intégrations personnalisables

Tout change en permanence.  Mais toutes les plateformes de gestion des données ne vous permettent pas de suivre le rythme. Votre entreprise a besoin d'une solution cyber-résiliente qui fonctionne pour lutter contre les ransomwares et qui réponde également à ses besoins particuliers. Outre les intégrations préconçues, assurez-vous que la solution que vous choisissez dispose d'un kit de développement logiciel (SDK) sécurisé et d'API de gestion personnalisables qui vous offrent la flexibilité nécessaire pour exploiter votre environnement comme vous le souhaitez.

### Interopérabilité des applications à valeur ajoutée

Vous avez besoin d'intégrations préconçues et personnalisables dans une architecture riche en API qui vous permette de rationaliser vos opérations, mais aussi d'une plateforme pérenne qui renforce la sécurité de vos données. Au lieu de faire des copies des données et de les déplacer, trouvez une solution qui vous permette de réutiliser les données sur place en leur apportant des applications à valeur ajoutée pour les tâches quotidiennes et plus complexes (par exemple l'analyse de virus, le masquage de données, l'analyse des journaux d'audit de fichiers et la classification des données). Une plateforme extensible vous permettra de réduire l'empreinte de vos données et la surface d'attaque, et de tirer davantage de valeur de vos investissements.

## 4 QUESTIONS CLÉS À POSER POUR GARANTIR L'EXTENSIBILITÉ ET L'INTEROPÉRABILITÉ

- Quelles intégrations de sécurité votre solution de sauvegarde ou de gestion des données prend-elle en charge ?
- Comment votre solution fonctionne-t-elle avec d'autres produits et plateformes de sécurité de premier plan ?
- Comment votre solution permet-elle d'extraire des informations tout en assurant la sécurité des données ?
- Comment votre solution de sauvegarde ou de gestion des données améliore-t-elle la collaboration en éliminant les silos entre les plateformes, les personnes et les processus ?

©2022 Cohesity. Tous droits réservés.

# Assurez-vous de pouvoir rapidement récupérer vos données à grande échelle

Si le pire devait se produire et qu'un ransomware réussisse à s'introduire dans votre environnement de production, il vous faut une solution qui vous permette de refuser de payer une rançon. Recherchez une solution dotée de ces trois capacités de récupération de données indispensables pour avoir cette sérénité.

### Récupération instantanée à grande échelle

Les attaques par ransomware ne visent plus une ou deux machines virtuelles (VM) ou bases de données. Elles cherchent plutôt à verrouiller la plus grande quantité possible de données et systèmes. Les entreprises ont donc aujourd'hui besoin d'une solution de gestion des données capable de récupérer rapidement des centaines de systèmes. Une capacité de récupération instantanée à grande échelle vous permet de restaurer rapidement des centaines de VM, de grosses bases de données ou de larges volumes de données non structurées à grande échelle, à n'importe quel point dans le temps et à n'importe quel emplacement.

### Récupération propre

### *Récupération sur place

Mettre en place un environnement propre après une attaque peut prendre du temps, et restaurer l'environnement d'origine peut compromettre les efforts d'investigation. Cela peut ralentir le processus de récupération (chose que vous devez absolument éviter lorsque vous cherchez à reprendre vos activités). Trouvez une solution de gestion des données qui vous permette de récupérer vos données directement sur place, sur la même plateforme, sans avoir à installer un nouveau serveur ou une nouvelle base de données. Cela vous fera gagner du temps et de l'argent.

©2022 Cohesity. Tous droits réservés.

## 4 QUESTIONS CLÉS À POSER POUR CONFIRMER QUE VOUS POUVEZ RÉCUPÉRER RAPIDEMENT VOS DONNÉES À GRANDE ÉCHELLE

- Comment votre solution de sauvegarde ou de gestion des données vous permet-elle de récupérer rapidement, proprement et de manière prévisible des données à grande échelle ?
- Votre système de sauvegarde possède-t-il suffisamment de ressources pour permettre une récupération rapide à n'importe quel point dans le temps et à n'importe quel emplacement ?
- Quelles capacités votre solution prend-elle en charge pour évaluer la santé d'un snapshot et récupérer des données non structurées sans investissement supplémentaire ?
- Comment votre solution de gestion des données procède-t-elle pour récupérer sur place les données non structurées afin de réduire les temps d'arrêt ?

©2022 Cohesity. Tous droits réservés.

# Liste de contrôle : évaluer sa préparation aux attaques par ransomware

Les cybercriminels travaillent sans relâche. Vous avez besoin d'une stratégie de gestion et de sécurité des données qui vous permette de faire face à l'évolution des menaces et de minimiser l'impact des ransomwares. Commencez par repenser votre solution de gestion des données. Utilisez cette liste de contrôle des capacités clés pour évaluer les options qui s'offrent à vous. Elle vous permettra ainsi de choisir la solution la mieux adaptée à votre entreprise.

| Action | Capacité clé | Fournisseur 1 | Fournisseur 2 | Fournisseur 3 | Fournisseur 4 |
|---|---|---|---|---|---|
| Protéger les données et systèmes de sauvegarde | Snapshots inaltérables | | | | |
| | WORM | | | | |
| | Chiffrement des données | | | | |
| | Audit et analyse des configurations | | | | |
| | Tolérance aux pannes | | | | |
| | Cyber coffre-fort moderne et flexible | | | | |
| Réduire le risque d'accès non autorisé | Authentification multifacteur (MFA) | | | | |
| | Modification surveillée | | | | |
| | Contrôle d'accès granulaire basé sur les rôles (RBAC) | | | | |
| Voir et détecter les attaques pour empêcher les intrusions | Alimenté par l'IA/le ML | | | | |
| | Détection d'anomalies en temps quasi réel | | | | |
| | Alertes automatisées | | | | |
| | Découverte de cyber-vulnérabilités | | | | |
| Renforcer sa posture de sécurité grâce une plateforme extensible | Intégrations préconçues | | | | |
| | Intégrations personnalisables | | | | |
| | Interopérabilité des applications à valeur ajoutée | | | | |
| Assurez-vous de pouvoir rapidement récupérer vos données à grande échelle | Récupération instantanée à grande échelle | | | | |
| | Récupération propre | | | | |
| | Récupération sur place | | | | |

©2022 Cohesity. Tous droits réservés.

# Soyez prêt à faire face aux attaques par ransomware avec Cohesity

Avec Cohesity, votre entreprise peut facilement sauvegarder, gérer, sécuriser et valoriser ses données dans le centre de données, à la périphérie et dans le cloud. Utilisez le logiciel Cohesity pour gérer directement votre infrastructure de données, confiez cette tâche à un service SaaS Cohesity, ou faites les deux. Cohesity résout le problème de la fragmentation massive des données, simplifie la mise en conformité des données et permet aux entreprises de déjouer les attaques par ransomware.

Cohesity a été nommée Leader dans le rapport Magic Quadrant Gartner sur les solutions de sauvegarde et de récupération dans les centres de données, et Leader dans le rapport « The Forrester Wave™ : solutions de résilience des données. » L'entreprise figure au classement Forbes Cloud 100 de l'année 2022 (pour la quatrième fois), au classement CRN des entreprises cloud les plus innovantes en 2022 (pour la troisième fois), et arrive en tête du classement des Leaders parmi 16 fournisseurs dans le GigaOm Radar pour la gestion des données non structurées.

**Modernisez dès aujourd'hui votre plateforme de gestion et de sécurité des données cohesity.com/fr/**

Pour en savoir plus, consultez cohesity.com/fr/

COHESITY

© 2023 Cohesity Inc. Tous droits réservés.

Cohesity, le logo Cohesity, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, le logo Helios, DataGovern, SiteContinuity et les autres marques Cohesity sont des marques commerciales ou déposées de Cohesity, Inc. aux États-Unis et/ou dans d'autres pays. Les noms d'autres sociétés et produits peuvent être des marques commerciales des sociétés respectives auxquelles elles sont associées. Ce document (a) est destiné à vous fournir des informations sur Cohesity, son activité et ses produits ; (b) est réputé exact et à jour au moment de sa rédaction, mais est susceptible de modification sans préavis ; et (c) est fourni « TEL QUEL ». Cohesity rejette toutes les conditions, représentations et garanties expresses ou implicites de quelque nature que ce soit.