COHESITY

Se préparer face aux ransomwares : Guide d'évaluation détaillé

Renforcez la sécurité de vos données et votre cyber-résilience

Sommaire

La portée accrue des attaques par ransomware 3

Mesures essentielles pour contrer les ransomwares 3

Les ransomwares ne sont pas près de disparaitre 4

Protégez vos données et systèmes de sauvegarde 4

Réduisez les risques d'accès non autorisés 7

Visualisez et détectez les attaques pour stopper les intrusions 8

Renforcez votre stratégie en matière de sécurité grâce une plateforme extensible 10

Assurez-vous de pouvoir rapidement récupérer vos données à grande échelle 11

Checklist : Évaluation du degré de préparation aux ransomwares 13

La portée accrue des attaques par ransomware

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

La menace des ransomwares ne cesse d'évoluer, tandis que les cibles et les tactiques se multiplient. Si cela ne s'est pas déjà produit, on vous demandera bientôt comment vous pensez vous défendre contre les différentes manières dont les cybercriminels cherchent à perturber vos opérations.

	Ransomware 1.0	Ransomware 2.0	Ransomware 3.0
Cible des logiciels malveillants	Données de production	• Données de sauvegarde • Systèmes de sauvegarde • Données de production	• Données de sauvegarde • Systèmes de sauvegarde • Données de production • Données à supprimer illégalement
Mode opératoire	Chiffrement	Chiffrement	Chiffrement et exfiltration
Comment les entreprises stoppent l'attaque	Système de sauvegarde et de restauration	Sauvegardes immuables et isolation des données	Détection précoce et surveillance continue

Mesures essentielles pour contrer les ransomwares

Si vous ne savez pas quoi faire en premier lieu pour renforcer la cyber-résilience de votre organisation, ce guide est fait pour vous. Vous y trouverez de nombreuses informations pratiques et des critères d'évaluation sur ce qu'il faut rechercher dans une solution de gestion des données pour renforcer 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 checklist qui vous sera utile pour comparer l'efficacité de vos solutions existantes avec des solutions de gestion des données de nouvelle génération.

Mais avant toute chose, pour mieux protéger vos données et la réputation de votre entreprise, il est indispensable de bien comprendre comment ces cinq mesures essentielles aideront votre organisation à lutter contre les ransomwares :

- Protégez vos données et systèmes de sauvegarde
- Réduisez les risques d'accès non autorisés
- Visualisez et détectez les attaques pour stopper les intrusions
- Renforcez votre stratégie en matière de sécurité avec des intégrations et des API
- Assurez-vous de pouvoir rapidement récupérer vos données à grande échelle

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 Million $

Coût moyen actuel pour se remettre de l'impact d'une attaque par ransomware *sans* payer la rançon[3]

> 265 Milliards $

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

Protégez vos données et systèmes de sauvegarde

Les mécanismes de protection des données sont essentiels pour préserver la confiance de vos clients et conserver votre avantage concurrentiel. Ces mécanismes stoppent les menaces en constante évolution des ransomwares, y compris les nouvelles menaces telles que les « Lockers », qui vous empêchent complètement d'accéder à vos fichiers et applications système, tout en affichant un compte à rebours jusqu'à la date et l'heure prévues du paiement de la rançon. Si vous n'améliorez pas ces mécanismes, votre entreprise n'a aucun moyen de protéger ses données contre le chiffrement, ou pire, le vol par des cybercriminels.

Pour une résilience optimale des données dans les environnements hybrides et multiclouds, assurez-vous que ces six fonctionnalités de sécurité des sauvegardes non négociables font partie de toute solution de gestion des données que vous envisagez sérieusement.

Snapshots immuables

Les snapshots de sauvegarde immuables et natifs reposant sur une méthode logicielle constituent un mécanisme de défense efficace contre les attaques par ransomware, car ils ne peuvent pas être chiffrés, modifiés ou supprimés, autant de tactiques courantes utilisées par les cybercriminels pour obliger leurs victimes à payer une rançon. Ceci est extrêmement important pour protéger l'authenticité des données, en particulier les quantités massives de données non structurées telles que les fichiers audio et vidéo, ainsi que les images requises dans certains secteurs comme la justice et les soins de santé. Contrairement à la stratégie d'immuabilité basée sur le matériel, les snapshots natifs en lecture seule hébergés sur site ou dans le cloud ne sont jamais exposés ni montés en externe pour une application quelconque, et ne peuvent donc pas être altérés, modifiés ou supprimés. Il est donc difficile pour les logiciels malveillants de cibler vos données de sauvegarde.

[1] FortiGuard Labs. « Global Threat Landscape Report », août 2021.
[2] Palo Alto Networks. « Extortion Payments Hit New Records as Ransomware Crisis Intensifies », 9 août 2021.
[3] Sophos. « The State of Ransomware 2021 », 2021.
[4] Cybersecurity Ventures. « Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031 », 3 juin 2021.

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 sécurité de créer et d'appliquer un verrouillage limité dans le temps sur les données grâce à des règles, puis de les affecter à certaines tâches pour renforcer l'immuabilité des données protégées. Comme il s'agit d'une protection que ni les responsables ni les administrateurs de la sécurité ne peuvent modifier ou supprimer, vous n'avez pas à vous préoccuper autant d'éventuelles menaces internes.

Chiffrement des données

Il y a bien sûr le chiffrement standard, mais il y a aussi le chiffrement logiciel basé sur la norme AES-256 validée par les FIPS pour les données en transit et au repos. Ce dont vous avez besoin, c'est d'un module cryptographique validé par le National Institute of Standards and Technology (NIST) des États-Unis selon la norme 140-2 niveau 1 des Federal Information Processing Standards (FIPS). La publication FIPS 140-2 est une norme du gouvernement américain pour les modules cryptographiques qui garantit que la conception du module et la mise en œuvre des algorithmes cryptographiques sont parfaitement sûres. Le chiffrement validé par les FIPS est plus sûr car les produits qui portent cette distinction ont subi un ensemble de tests rigoureux pour être certifiés et que la norme est reconnue à l'échelle mondiale.

Audit et analyse des configurations

Votre équipe informatique utilise probablement de nombreux systèmes et outils différents, tous avec leurs propres configurations, politiques et interfaces de gestion. Malheureusement, les processus manuels pour les exécuter sont souvent à l'origine d'erreurs humaines évitables. Ne pourrait-on pas trouver un moyen plus efficace ? Un système automatisé avec analyse guidée qui vérifie les différents paramètres de sécurité des données et de contrôle d'accès vous aide à éviter les erreurs humaines coûteuses tout en simplifiant vos opérations liées aux données, de la configuration aux politiques en passant par les processus de gestion.

Tolérance aux pannes

Parce que la résilience des données doit toujours être un principe directeur de la sécurité, vous avez également besoin d'un système tolérant aux pannes qui garantit l'intégrité des données et des sauvegardes réussies, même dans les conditions les plus difficiles. Certaines de ces situations peuvent survenir lorsque vos systèmes atteignent leurs limites de capacités de calcul, de mémoire ou de stockage, lorsque le réseau est particulièrement congestionné ou lorsque vous subissez une panne matérielle inattendue. Dotez-vous d'une solution intégrant une technologie de tolérance aux pannes, afin de poursuivre les sauvegardes malgré la défaillance d'un composant/nœud.

Isolation des données moderne et flexible

Lorsque vous repensez votre approche de la gestion des données, vous devez également envisager la mise à jour de votre stratégie d'isolation des données. Si les organisations utilisent traditionnellement des bandes pour conserver des copies isolées de leurs données, cette méthode ne permet plus de respecter les accords de niveau de service (SLA) exigeants d'aujourd'hui quant aux délais de restauration, en particulier en cas d'attaque par ransomware généralisée. Le terme « air gap », qui désigne la mesure de sécurité consistant à isoler physiquement un système, est aujourd'hui largement utilisé pour décrire des techniques qui ne maintiennent toutefois pas une réelle isolation, ne vous y trompez pas. Assurez-vous que votre prochaine solution de gestion des données offre à la fois une véritable protection « air gap » et des options modernes pour isoler les données. Celles-ci concilient les exigences modernes de durée maximale d'interruption admissible et d'objectif de point de restauration (RTO/RPO) avec des contrôles de sécurité appropriés en stockant les données de sauvegarde dans le cloud ou un autre emplacement, avec une connexion temporaire et hautement sécurisée. Vous obtenez alors un environnement inviolable qui empêche les ransomwares et les menaces internes tout en optimisant le respect des SLA. Et mieux encore, vous conservez toujours une copie de vos données dans un format immuable.

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

- Que fait votre solution de gestion des données pour protéger vos données sauvegardées contre les attaques par ransomware ?
- Comment votre solution sauvegarde-t-elle en continu les charges de travail, même après la panne d'un composant matériel ou logiciel ?
- Comment votre solution équilibre-t-elle la nécessité d'une sécurité renforcée avec des RTO/RPO d'entreprise numérique toujours plus rapides qui respectent les SLA ?
- De quelles manières votre solution offre-t-elle une visibilité sur les failles de sécurité dans la configuration et la conception opérationnelle du système ?

Réduisez les risques d'accès non autorisés

Les acteurs malveillants travaillent pour eux-mêmes, des organisations et des États-nations. C'est pour cette raison qu'il est de plus en plus stratégique pour votre entreprise de disposer d'une solution de gestion des données avec des contrôles d'accès stricts. De tels contrôles peuvent en effet bloquer plus efficacement les accès non autorisés des pirates externes ou des professionnels internes mal intentionnés qui tirent parti d'identifiants compromis.

Pour réduire le risque de vol et de perte de données, recherchez une solution qui intègre les principes du moindre privilège et de la séparation des tâches avec une sécurité granulaire, y compris les quatre fonctionnalités indispensables suivantes. Elles vous permettront de garantir la sécurité de vos données et de conserver la confiance de vos clients.

Authentification multifactorielle

Régulièrement compromis, même les mots de passe les plus créatifs ne peuvent fournir qu'une couche de protection minimale aux entreprises numériques. L'authentification multifactorielle (MFA) est un pas en avant dans la lutte contre les tentatives de phishing et autres techniques de piratage des mots de passe. Cela nécessite 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. Les personnes 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 vos solutions retenues exigent l'authentification multifactorielle.

Modification surveillée

Étant donné qu'une personne qui assure la surveillance du système peut suffire à stopper une attaque, vous avez besoin d'une fonctionnalité qui empêche un identifiant ou un individu compromis de modifier les éléments critiques de votre solution de gestion des données. Insistez pour avoir une plateforme qui permet d'appliquer des mesures de protection strictes, par exemple en exigeant qu'une modification au niveau de la racine ou tout autre changement critique du système soit autorisé par plus d'une personne afin de vous protéger contre les intentions malveillantes et le vol d'identifiants de connexion.

Contrôle d'accès granulaire basé sur les rôles

En matière de données, une gestion efficace des identités et des accès est de plus en plus incontournable pour une bonne cyber-hygiène. Pour réduire efficacement les attaques par ransomware et les menaces internes, l'équipe IT doit désormais accorder à chaque personne un niveau minimum d'accès à toutes les données de l'organisation nécessaires pour effectuer un travail particulier, et en même temps répartir les processus et fonctionnalités qui utilisent des données critiques entre différents rôles informatiques, de sorte qu'aucun administrateur ne puisse compromettre toute votre entreprise. Les organisations qui peuvent compter sur une solution de gestion des données qui simplifie les approches du contrôle d'accès granulaire basé sur les rôles (RBAC) parviennent à mieux lutter contre les accès non autorisés et la mise en danger des données, tout en accordant efficacement à leurs utilisateurs les privilèges appropriés pour faire leur travail.

LES 3 QUESTIONS CLÉS À POSER SUR LA RÉDUCTION DES RISQUES D'ACCÈS NON AUTORISÉS

- Que fait votre solution de sauvegarde ou de gestion des données pour empêcher l'accès non autorisé aux données de l'entreprise ?
- Comment votre solution vous protège-t-elle à la fois contre les ransomwares et les menaces internes ?
- Comment configurer l'approbation multi-utilisateur pour les opérations critiques ?

Visualisez et détectez les attaques pour stopper les intrusions

Le monde des entreprises numériques évolue rapidement. De plus en plus, les chefs d'entreprise doivent savoir quelles données sensibles ils possèdent, où elles se trouvent et qui y a accès. C'est là quelque chose d'essentiel pour se conformer aux réglementations du secteur ou gouvernementales, conserver la confiance du public et des investisseurs, et répondre rapidement aux attaques par double extorsion, ce qu'on appelle aussi l'exfiltration de données.

Pour minimiser la portée potentielle des attaques par ransomware, recherchez une solution de gestion des données avec intelligence intégrée, de sorte à pouvoir découvrir et classer automatiquement les données sensibles tout en bénéficiant d'une détection des menaces en temps quasi réel. Dotez-vous d'une solution qui aide votre équipe à travailler plus intelligemment, et non davantage, et qui inclut les quatre fonctionnalités essentielles suivantes pour une réponse proactive quelles que soient les menaces auxquelles vous devez faire face.

Optimisée par l'intelligence artificielle et le machine learning

Pour se développer, votre organisation a besoin de données. Ces données augmentent toutefois de manière exponentielle, ce qui rend impossible pour certaines solutions de gestion des données d'effectuer une mise en correspondance et une classification efficaces des données pour déterminer lesquelles sont les plus essentielles. À l'inverse, une solution de gestion des données de nouvelle génération optimisée par l'intelligence artificielle et le machine learning (IA/ML) permet à votre organisation de détecter plus précisément les variations et de réduire les faux positifs sans avoir recours à plus de personnel. Vous pouvez tirer parti des technologies d'IA/ML pour faire correspondre des ensembles de données « connus pour être sans danger » et le faire de manière plus efficace, car vos « données sensibles connues » sont mises en correspondance et renvoyées à l'algorithme d'AI/ML. C'est un peu comme trouver une aiguille dans une botte de foin sans devoir tout mettre sens dessus dessous.

Détection des anomalies en temps quasi réel

Plus vite vous détectez une intrusion, moins elle cause de dommages à votre entreprise et moins vous devez retenir votre équipe IT la nuit et les week-ends. Intégrée à une solution de gestion des données, une puissante fonctionnalité de détection automatisée des anomalies en temps quasi réel permet de suivre en permanence les opérations normales du système pour détecter rapidement les irrégularités et les comportements anormaux des utilisateurs pouvant indiquer une attaque par ransomware. Associée à un système d'alerte, cette fonctionnalité ne se contente pas de signaler un danger potentiel, elle peut également initier des mesures correctives. Grâce à la détection des anomalies en temps quasi réel, vous pouvez rapidement identifier les attaques en cours par chiffrement des données et par exfiltration des données, ce qui vous permet de minimiser l'impact des ransomwares.

Alertes automatisées

Ce n'est pas parce que c'est simple et rapide qu'il n'y a pas de la puissance et de la complexité opérationnelle derrière les alertes de gestion des données. Cherchez une solution avec à la fois des alertes anti-ransomware et des alertes basées sur l'analyse prédictive et les risques. Les premières vous informent non seulement qu'on a accédé aux données, mais aussi ce que ces données contenaient et où elles se trouvaient. Les secondes vous aident à identifier les comportements suspects des utilisateurs pouvant justifier une enquête plus approfondie pour savoir qui a accédé aux données sensibles, quand et ce qu'il en a été fait.

Détection des cyber-vulnérabilités

Les cybercriminels sont connus pour exploiter les logiciels et les cyber-vulnérabilités, c'est-à-dire les vulnérabilités créées en n'apportant pas les correctifs nécessaires aux logiciels, pour accéder à votre environnement de production. Les solutions de sauvegarde et de gestion des données les plus efficaces devraient aider votre équipe à gagner en visibilité sur ces vulnérabilités. Elles devraient également vous aider à résoudre les problèmes de manière proactive et à éviter de réinjecter des cyber-vulnérabilités déjà résolues dans votre environnement de production lors de la récupération après une attaque.

LES 4 QUESTIONS CLÉS À POSER POUR ÉVITER LES INTRUSIONS

- Comment votre solution vous aide-t-elle à classer les données et à identifier les informations sensibles pouvant présenter un risque ?
- Que fait votre solution de sauvegarde ou de gestion des données pour vous offrir une visibilité détaillée des logiciels vulnérables et autres cyber-vulnérabilités, et fournir une détection des anomalies en temps quasi réel ?
- Comment votre solution intègre-t-elle l'intelligence artificielle/le machine learning pour détecter les anomalies qui peuvent signifier une menace ou une attaque par ransomware ?
- Comment votre solution détecte-t-elle les anomalies au niveau du système et du comportement des utilisateurs pouvant indiquer différents vecteurs d'attaque ?

Renforcez votre stratégie en matière de sécurité grâce une plateforme extensible

Les ransomwares ne se résument pas à un seul type de menace. C'est une menace qui évolue et devient plus complexe 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. Une solution intégrée et interopérable offre à votre organisation la capacité de détecter et d'évaluer les menaces plus rapidement et en toute confiance. C'est également la solution la plus efficace pour lutter contre les acteurs malveillants.

Recherchez une solution de gestion de données moderne qui prend en charge la collaboration avec des tiers pour améliorer la sécurité de vos données, une solution qui garantit la flexibilité de l'environnement tout en vous offrant les moyens de simplifier les opérations et de rendre vos données productives en toute sécurité. Pour établir une stratégie solide en matière de sécurité, toute solution que vous envisagez doit inclure ces trois fonctionnalités clés et s'intégrer parfaitement aux autres.

Intégrations préconçues

Les problèmes de sécurité des données sont les pires ennemis des dirigeants d'entreprise. Ils seraient plus sereins s'ils avaient la certitude que les produits de sécurité auxquels ils font confiance fonctionnaient ensemble de manière transparente pour lutter contre la cybercriminalité. Cherchez une solution de gestion des données qui soit déjà étroitement intégrée aux principales solutions d'orchestration, d'automatisation et de réponse en matière de sécurité (SOAR) et de gestion des informations et événements de sécurité (SIEM). Cela accélérera les délais de découverte, d'investigation et de neutralisation des attaques par ransomware. Assurez-vous par ailleurs qu'elle propose également des workflows intégrés, préconçus et extensibles que l'équipe SecOps peut augmenter pour une réponse automatisée aux incidents et des opérations unifiées entre les équipes IT, réseau et sécurité.

Intégrations personnalisables

Si le changement ne s'arrête jamais, toutes les plateformes de gestion des données ne permettent pas de suivre le rythme. Votre organisation a besoin d'une solution cyber-résiliente qui lutte contre les ransomwares tout en répondant aux exigences uniques de votre entreprise. Assurez-vous qu'en plus des intégrations préconçues, la solution que vous sélectionnez 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

En plus des intégrations préconçues et personnalisables au sein d'une architecture riche en API permettant de rationaliser les opérations, vous avez besoin d'une plateforme qui vous offre des moyens d'évoluer tout en améliorant la sécurité des données. Plutôt que de faire des copies des données et de les déplacer, cherchez une solution qui vous permette de réutiliser les données sur place en leur apportant des applications à valeur ajoutée pour les tâches de routine et plus difficiles, telles que la recherche de virus, le masquage des données, l'analyse des journaux d'audit de fichier ou encore le classement des données. Une plateforme extensible vous aidera à réduire votre empreinte de données et votre surface d'attaque, tout en vous permettant de tirer davantage de valeur de vos investissements.

LES 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 extrait-elle des informations exploitables tout en protégeant les 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 ?

Assurez-vous de pouvoir rapidement restaurer vos données à grande échelle

Au cas où le pire scénario se produirait et qu'un ransomware s'introduirait dans votre environnement de production, vous avez besoin d'une solution qui vous donne les moyens de refuser de payer une rançon. Recherchez une solution avec ces trois fonctionnalités non négociables de restauration des données pour agir en toute confiance.

Restauration instantanée à grande échelle

En cas d'attaque par ransomware, ce ne sont plus une ni deux machines virtuelles (VM) ni des bases de données qui sont ciblées, mais autant de données que possible dans vos systèmes. C'est pour cette raison que les organisations ont aujourd'hui besoin d'une solution de gestion des données capable de restaurer rapidement des centaines de systèmes. Une fonctionnalité de restauration instantanée à grande échelle vous permet de restaurer sur-le-champ des centaines de VM, d'importantes bases de données ou d'importants volumes de données non structurées à grande échelle, à tout moment et en tout lieu.

Restauration propre

Lors du processus de restauration, vous devez savoir que les données que vous récupérez ne contiennent pas d'éventuels logiciels malveillants. Votre solution de gestion des données doit vous aider à identifier les snapshots compromis. Cherchez une solution avec un moteur de machine learning (ML) intégré pour recommander la dernière copie propre et ainsi vous assurer, lorsque vous effectuez la restauration, que les données des snapshots ne présentent pas d'anomalies ni de menaces potentielles pour la cybersécurité. Cela accélérera le temps de restauration et vous donnera la certitude de ne pas réinjecter de possibles logiciels malveillants dans votre environnement de production.

Restauration sur place

Allouer des ressources pour créer un environnement propre après une attaque peut prendre du temps, et la restauration de l'environnement d'origine peut compromettre les efforts d'investigation. Cela peut ralentir le processus de restauration (ce qu'il faut absolument éviter lorsqu'il s'agit de redémarrer l'activité au plus vite). Cherchez une solution de gestion des données qui vous permet de restaurer les données sur la même plateforme, sans devoir utiliser un nouveau serveur ou une nouvelle base de données. Cela vous fera gagner du temps et économiser de l'argent.

LES 4 QUESTIONS CLÉS À POSER POUR CONFIRMER QUE VOUS POUVEZ RAPIDEMENT RESTAURER VOS DONNÉES À GRANDE ÉCHELLE

- Que fait votre solution de sauvegarde ou de gestion des données pour vous aider à restaurer rapidement, proprement et de manière prévisible vos données à grande échelle ?
- Votre système de sauvegarde dispose-t-il de ressources suffisantes pour prendre en charge une restauration rapide à tout moment et en tout lieu ?
- Quelles fonctionnalités votre solution prend-elle en charge pour évaluer l'état d'un snapshot et restaurer des données non structurées sans investissement supplémentaire ?
- Comment votre solution de gestion des données effectue-t-elle la restauration sur place des données non structurées pour réduire les temps d'arrêt ?

Checklist : Évaluation du degré de préparation aux ransomwares

Les cybercriminels ne s'arrêtent jamais. Vous avez besoin d'une stratégie de gestion et de sécurité des données qui peut vous aider à suivre l'évolution des menaces et à minimiser l'impact des ransomwares. Repenser votre solution de gestion des données est un bon point de départ. À mesure que vous évaluez vos options, cette checklist des fonctionnalités clés peut vous aider à identifier la solution la mieux adaptée à votre organisation.

Mesure	Fonctionnalité clé	Fournisseur 1	Fournisseur 2	Fournisseur 3	Fournisseur 4
Protégez vos données et systèmes de sauvegarde	Snapshots immuables				
	WORM				
	Chiffrement des données				
	Audit et analyse des configurations				
	Tolérance aux pannes				
	Isolation des données moderne et flexible				
Réduisez les risques d'accès non autorisés	Authentification multifactorielle (MFA)				
	Modification surveillée				
	Contrôle d'accès granulaire basé sur les rôles (RBAC)				
Visualisez et détectez les attaques pour stopper les intrusions	Intelligence artificielle/ Machine learning				
	Détection des anomalies en temps quasi réel				
	Alertes automatisées				
	Détection des cyber-vulnérabilités				
Renforcez votre stratégie en matière de sécurité grâce une plateforme extensible	Intégrations préconçues				
	Intégrations personnalisables				
	Interopérabilité des applications à valeur ajoutée				
Assurez-vous de pouvoir rapidement restaurer vos données à grande échelle	Restauration instantanée à grande échelle				
	Restauration propre				
	Restauration sur place				

Préparez-vous aux attaques par ransomware avec la gestion des données de nouvelle génération de Cohesity

Cohesity permet à votre organisation de facilement sauvegarder, gérer et sécuriser ses données, et de générer de la valeur à partir de celles-ci dans le datacenter, sur un site distant et dans le cloud. Le logiciel Cohesity vous permet de gérer votre infrastructure de données directement, ou de confier cette gestion à Cohesity par le biais d'un service Saas, ou de faire les deux. Cohesity résout la fragmentation massive des données, accélère leur mise en conformité et aide les entreprises à stopper les attaques par ransomware.

Cohesity a été désigné parmi les Leaders du Magic Quadrant Gartner pour les solutions de sauvegarde et de restauration des données en datacenter et parmi les Leaders du « The Forrester Wave™ » dans la catégorie des solutions de résilience des données. La société a été classée au Forbes Cloud 100 de l'année 2020, parmi les Coolest Cloud Companies de CRM en 2020, et est arrivée en tête de liste parmi les 16 meilleurs fournisseurs classés au GigaOm Radar pour la gestion des données non structurées.

Découvrez comment Cohesity vous aide à défendre votre entreprise contre les attaques sophistiquées par ransomware www.cohesity.com/fr/next-gen-data-management/threat-defense/.

Apprenez-en plus sur Cohesity.com/FR.

COHESITY