5 façons de protéger, détecter et récupérer pour renforcer la cyber-résilience

On estime que le coût mondial des dommages causés par les ransomwares, notamment la perte de revenus et de productivité, dépassera 265 milliards de dollars d'ici 2031.[2]

Présentation

Les pirates s'attaquent aux données. En témoigne la hausse annuelle de 1 070 % des attaques par ransomware[1]. Et les acteurs malveillants d'aujourd'hui ne se contentent pas de chiffrer les données. Ils détruisent les sauvegardes et exfiltrent les données pour en tirer profit et nuire à la réputation des marques. C'est ce qui augmente la portée des attaques par ransomware. Ne laissez pas les pirates informatiques gagner. Renforcez plutôt votre environnement et améliorez votre stratégie de réponse en appliquant les principes de protection, de détection et de récupération.

1. Protégez vos données et systèmes de sauvegarde

Les sauvegardes traditionnelles ne sont pas conçues pour protéger les données contre les ransomwares. C'est pourquoi les entreprises continuent de payer des rançons. Vous avez besoin de protections des données intégrées à votre sauvegarde pour préserver la confiance des clients ainsi que votre avantage concurrentiel. Cherchez une solution proposant des snapshots de sauvegarde natifs inaltérables, qui ne peuvent donc pas être chiffrés, modifiés ou supprimés, pour protéger l'authenticité de vos données. Vous pouvez également ajouter des couches de protection en veillant à ce que votre sauvegarde soit dotée d'un chiffrement certifié FIPS basé sur un logiciel WORM (write once, read many). Atteignez vos objectifs de récupération et respectez vos accords de niveau de service (SLA) organisationnels grâce à une isolation moderne et flexible des données sur site et dans les clouds publics. Enfin, cherchez des solutions tolérantes aux pannes qui vous permettent d'une part de fonctionner malgré la défaillance d'un composant, et d'autre part de configurer des contrôles de sécurité automatisés, notamment l'audit et l'analyse, pour éliminer les erreurs humaines.

2. Réduisez les risques d'accès non-autorisés

Les acteurs malveillants s'attaquent désormais en premier lieu à la compromission des identifiants des utilisateurs. Une plateforme de gestion des données dotée de capacités de contrôle d'accès strictes empêche plus efficacement les personnes non-autorisées de tirer parti d'identifiants compromis. Contrez les pirates informatiques et les menaces internes avec des principes de Zero Trust. Ceux-ci incluent des contrôles d'accès basés sur les rôles, l'authentification multifactorielle, l'approbation par quorum pour empêcher les changements administratifs unilatéraux, et la surveillance avec évaluation automatique de la sécurité de votre environnement.

3. Stoppez les intrusions et détectez les attaques

Les experts de Cybersecurity Ventures estiment que toutes les 11 secondes, une entreprise est victime d'une attaque par ransomware.[1] Aucune entreprise n'a suffisamment d'employés pour réagir. Vous avez donc besoin d'une solution basée sur l'IA/ML qui vous permette de détecter les attaques émergentes et les activités inhabituelles, et de mettre en lumière les données sensibles. Cherchez une solution dotée d'une intelligence intégrée, et non pas ajoutée, qui permette à votre équipe de découvrir et de classer automatiquement les données sensibles et de profiter de la détection des menaces en temps quasi réel. Les informations de base de la solution permettent à votre équipe de recevoir des alertes basées sur l'analyse prédictive et de détecter rapidement les anomalies en cas d'attaques de type chiffrement et d'exfiltration de données.

4. Intégrez en toute transparence la solution aux systèmes de sécurité existants

La menace des ransomwares n'est pas près de disparaître et continue d'évoluer. Il appartient donc à vos équipes internes (Infrastructure et opérations (I&O), Opérations de sécurité (SecOps) et Gestion/conformité) de mieux travailler ensemble pour prévenir les violations et y répondre rapidement. Cherchez une solution de gestion des données qui vous permette d'éliminer les silos de données et les obstacles fonctionnels. Trouvez une solution intégrée et extensible qui permette à votre entreprise de détecter les menaces, de les analyser et d'y répondre plus rapidement. La solution que vous choisissez doit vous permettre de tirer parti des principaux outils de sécurité et donner à vos développeurs un riche ensemble d'API RESTful pour continuer à ajouter de la valeur tout en luttant contre les menaces.

5. Récupérez rapidement vos données à l'échelle

Les cyber-escrocs faisant preuve d'une inventivité sans borne, le pire des scénarios est à craindre. Vous avez donc besoin d'une solution de gestion des données qui vous permette de récupérer rapidement suite à une attaque et de refuser de payer une rançon. Celle-ci doit permettre de restaurer rapidement des centaines de VM, de larges bases de données et de gros volumes de données non structurées, instantanément, à l'échelle, à tout moment et en tout lieu. De plus, pour être sûr de ne pas réinfecter votre environnement avec des logiciels malveillants, vous devez trouver une solution qui évalue l'état de santé du snapshot, vous permette de récupérer vos données de façon propre et prévisible directement sur place, sur la même plateforme, et donc de vous faire économiser du temps et des ressources.

Renforcez votre cyber-résilience grâce à Cohesity

Les entreprises doivent désormais absolument trouver une solution pour lutter contre les ransomwares. La gestion des données nouvelle génération fournit à votre entreprise les capacités de sécurité des données, de récupération suite à une attaque par ransomware et de cyber-résilience dont elle a besoin pour rester compétitive et refuser en toute confiance de payer une rançon.

1. Global Threat Landscape Report, FortiGuard Labs, premier semestre 2021
2. Cybersecurity Ventures

Pour en savoir plus sur la gestion des données nouvelle génération, visitez Cohesity.com/fr

COHESITY