Détection des ransomwares en temps réel

La plupart des entreprises modernes savent qu'elles doivent lutter contre les ransomwares en déployant un ensemble de solutions de sécurité proactives et réactives multicouches, ce que l'on appelle la défense en profondeur. Mais quelles solutions et comment les associer pour maximiser vos chances à chaque étape de la chaîne de sécurité ?

Les outils de cybersécurité préventifs peuvent être excellents pour détecter et stopper les attaques, mais les ransomwares peuvent toujours s'infiltrer malgré toutes ces barrières. Les solutions de reprise peuvent être essentielles dans ces scénarios, mais comment savoir quelles sont les données qui doivent être restaurées ? Quels points de reprise ne présentent aucun risque et sont non chiffrés ? Et quels sont ceux qui sont compromis ?

Les défis de la détection périodique

Malheureusement, les méthodes traditionnelles de détermination des points de reprise ne présentant aucun danger ne sont pas assez rapides face à l'évolution du paysage de la sécurité. Les solutions existantes analysent généralement les copies de sauvegarde. Malheureusement, les données datent déjà de plusieurs heures (et remontent probablement à la tâche de sauvegarde de la veille) et le processus d'analyse des logiciels malveillants lui-même prend quelques heures de plus. Pire encore, vous risquez d'être bloqué par les outils d'analyse de sécurité d'un fournisseur - qui vous coûteront plus cher - qu'il a intégrés à un produit existant ou dont il a acquis la licence auprès d'une tierce partie.

Passer à la détection en temps réel

Zerto, société du groupe Hewlett Packard Enterprise, a mis au point une nouvelle technologie innovante pour offrir un accès en temps réel à la détection du chiffrement. La solution logicielle de Zerto applique une intelligence algorithmique pour vous alerter en quelques secondes lorsqu'il y a une anomalie de chiffrement qui pourrait signaler le début de la phase de déclenchement d'un ransomware. Comme vous n'avez plus besoin d'attendre des heures ou des jours pour savoir si une restauration est nécessaire, vous êtes en mesure de réduire radicalement les pertes de données et les temps d'arrêt à la suite d'une attaque, et ce, sans payer la moindre rançon.

« Zerto 10 jouera un rôle clé dans la protection efficace des données et la reprise après sinistre dans un contexte de cybermenaces accrues. Sa détection en temps réel des ransomwares nous place dans une position beaucoup plus forte pour identifier et atténuer les attaques de ransomwares. Cela nous donne la certitude de pouvoir répondre de manière proactive aux risques présentés par les ransomwares et d'atteindre les objectifs commerciaux que nous avons définis. »

- Steve Smith, administrateur réseau chez Unverferth Manufacturing

Différentiateurs clés

L'analyseur de chiffrement breveté de Zerto 10 se distingue radicalement des autres alternatives disponibles sur le marché de la protection et de la reprise des données :

- **En temps réel et non périodique :** La détection en ligne et en continu surveille en permanence toutes les données qui circulent dans vos environnements numériques. Vous êtes averti presque instantanément. Ainsi, les équipes informatiques ou SecOps peuvent intervenir immédiatement plutôt qu'après plusieurs heures ou jours.
- **Aucun impact sur la production :** Grâce à des composants légers (avec un encombrement faible et des frais d'entretien bas) et à des architectures uniques, vos charges de travail restent performantes sans ralentissement. Ces composants garantissent une réplication constante et continue, essentielle à la reprise. Ainsi, aucune installation supplémentaire n'est nécessaire pour bénéficier de cette technologie de détection en temps réel performante.

- **L'approche « API-First » :** Évitez la boîte noire trop souvent utilisée par les concurrents en exploitant les API REST ouvertes de Zerto, basées sur Swagger, afin d'intégrer nos analyses de chiffrement à votre stack de sécurité ou d'observabilité existant. Diffusez la détection en temps réel et toutes les alertes associées vers le SIEM ou le SOAR de votre choix, notamment de puissantes visualisations à l'aide de logiciels libres tels que Prometheus et Grafana ; un exemple gratuit est disponible sur GitHub.

- **Aucun coût supplémentaire :** La détection du chiffrement en temps réel de Zerto est incluse d'office. Pas de modules complémentaires payants, pas d'abonnements supplémentaires, pas de logiciels additionnels à acheter, à installer, à configurer et à gérer. La menace est trop réelle pour que la détection du chiffrement reste enfermée dans un module payant au lieu d'être au cœur de la reprise et de la résilience face aux ransomwares.

« Alors que les entreprises continuent de se concentrer sur la résilience et la disponibilité continue, les capacités de détection des ransomwares en temps réel offertes par Zerto 10 sont de plus en plus essentielles pour maintenir une posture de sécurité efficace et réduire le risque de perte de données et de temps d'arrêt. Nos recherches montrent que le ransomware n'est pas une question de probabilité, mais une question d'échéance. En se concentrant sur la détection et la restauration rapides, Zerto offre des fonctionnalités essentielles conçues pour aider les organisations à identifier, atténuer et résoudre les menaces liées aux ransomwares ».

- Christophe Bertrand, directeur de pôle, Enterprise Strategy Group (ESG)

Principaux résultats commerciaux

Réduisez les pertes de données et les temps d'arrêt : Tirez parti du système d'alerte le plus rapide pour réduire l'impact total du ransomware en refusant les demandes de rançons et en restaurant rapidement vos données.

Réduisez les risques et les coûts : Évitez de payer un supplément pour la sécurité de votre solution de protection des données, sans parler des coûts liés aux rançons, des dommages à votre marque et à votre réputation, ainsi que de la perte de productivité.

Améliorez l'efficacité opérationnelle : Unifiez les efforts des équipes de sécurité et d'infrastructure en détectant le chiffrement malveillant en quelques secondes et en permettant une restauration des données en quelques minutes.

Accélérez le délai de valorisation : Complétez votre système de sécurité existant en détectant immédiatement les anomalies sans déployer de nouvelle infrastructure, sans engendrer de nouveaux coûts, ni de solutions supplémentaires.

Découvrez comment la détection du chiffrement en temps réel peut s'associer à la protection des données en temps réel pour assurer la résilience face aux ransomwares avec Zerto.

EN SAVOIR PLUS

À propos de Zerto

Zerto, une société Hewlett Packard Enterprise, permet à ses utilisateurs de gérer une activité permanente en simplifiant la protection, la restauration et la mobilité des applications sur site et sur cloud. Zerto élimine les risques et la complexité associés à la modernisation et à l'adoption du cloud dans les déploiements privés, publics et hybrides. Cette plateforme logicielle simple utilise la protection continue des données à grande échelle pour assurer la résilience face aux ransomwares, la reprise après sinistre et la mobilité multicloud. Déjà plus de 9 500 clients dans le monde font confiance à Zerto. Zerto est compatible avec Amazon, Google, IBM, Microsoft et Oracle et plus de 350 autres fournisseurs de services gérés. **www.zerto.com**

RITM0095279