Récupération accélérée suite à une attaque par rançongiciel avec Dell PowerProtect Backup Services

Remettez-vous d'une attaque par rançongiciel en quelques heures, au lieu de plusieurs jours

Fonctionnalités clés

Les attaques par rançongiciel sont de plus en plus fréquentes, perfectionnées et onéreuses

- Incapacité à identifier et restaurer rapidement les sauvegardes ou les fichiers non infectés
- Propagation de la contamination et réinfection à partir des données de récupération
- Perte de données, incapacité à restaurer un jeu de données complet
- Difficultés à coordonner l'orchestration de la réponse aux incidents
- Demande de RPO/RTO plus rapides
- Coûteuses interruptions de service entraînant une perte de chiffre d'affaires et une atteinte à la réputation de la marque
- Amendes légales et réglementaires dues à une protection inadéquate des données

Le défi

Les rançongiciels représentent une menace sérieuse pour toutes les entreprises. Les cyberattaques sont fréquentes et peuvent causer des dégâts catastrophiques. 79 % des entreprises craignent de subir un événement perturbateur au cours des 12 prochains mois1. Les entreprises qui perdent leurs données risquent de déclarer faillite après un sinistre. Les attaques par rançongiciel ne sont pas seulement plus fréquentes, mais sont également devenues plus coûteuses et perfectionnées sur le plan technologique.

La solution

Une solution de récupération rapide et fiable vous fera oublier l'idée de payer une rançon. Cependant, lorsqu'un incident de sécurité ou une cyberattaque se produit, les entreprises doivent comprendre son degré d'impact et sa cause première avant de lancer le processus de restauration. Grâce à des snapshots vierges et isolés des charges applicatives et des machines virtuelles disponibles 24 h/24, 7j/7, à une surveillance continue des anomalies des utilisateurs et des données, à l'intégration aux outils de sécurité et à la récupération automatisée de données inaltérées, vous pouvez améliorer votre posture de sécurité et transformer cette terrible épreuve en un incident loin d'être fatal.

Fonctionnalités

Pour toutes les charges applicatives :

• Bénéficiez de sauvegardes immuables, hors ligne, disponibles 24 heures sur 24, 7 jours sur 7

• Récupérez des données inaltérées sur site ou dans le Cloud avec un RPO/RTO de quelques heures, au lieu de plusieurs jours ou semaines

• Le service Managed Data Detection and Response (MDDR) assure une surveillance en temps réel des environnements de sauvegarde 24 heures sur 24, 7 jours sur 7 et 365 jours par an

• Lorsque vous restaurez les charges applicatives et les machines virtuelles d'un compte/d'une région AWS à l'aide des données de votre organisation de production et que vous en créez de nombreuses copies, stockées à plusieurs endroits, vous mettez votre organisation en danger.

Récupération accélérée suite à une attaque par rançongiciel pour les principales charges applicatives :

• Surveillez et détectez les anomalies en amont grâce à des algorithmes d'apprentissage automatique

• Orchestrez les activités de réponse et de récupération via les intégrations SIEM et SOAR

• Analysez les snapshots pour détecter tout logiciel malveillant avant la récupération et supprimez les snapshots et les fichiers infectés des sauvegardes

• Restaurez automatiquement la version inaltérée la plus récente de chaque fichier au cours d'une période donnée à partir d'un golden snapshot

Protection

La première étape pour éviter les dommages causés par les rançongiciels consiste à vous assurer que vous disposez d'une copie isolée et immuable de vos données. La solution Dell PowerProtect Backup Services, basée sur une infrastructure Cloud hautement résiliente, empêche les rançongiciels de chiffrer les données de sauvegarde. L'architecture Zero-Trust, qui inclut l'authentification multifacteur, le chiffrement d'enveloppe et l'accès via un compte distinct, garantit que les rançongiciels ne peuvent pas utiliser les informations d'identification compromises de l'environnement principal pour altérer l'environnement ou les données de sauvegarde. Enfin, les fonctionnalités de prévention des suppressions excessives et de suppression réversible (corbeille) renforcent la sécurité afin d'éviter toute suppression des sauvegardes.

Détection

En détectant une attaque par rançongiciel au plus tôt, les équipes de réponse aux incidents peuvent empêcher la contamination de se propager. Le module de récupération accélérée suite à une attaque par rançongiciel Dell PowerProtect Backup Services fournit un centre de commande permettant de surveiller la posture de sécurité de votre environnement de sauvegarde. Grâce aux informations sur les accès et à la détection des anomalies, vous pouvez rapidement identifier les activités inhabituelles dans votre environnement et vos données. Consultez les informations sur l'emplacement, l'identité et l'activité pour toutes les tentatives d'accès des utilisateurs et des API. Détectez les anomalies à l'aide d'algorithmes d'apprentissage automatique propriétaires qui déclenchent des alertes en cas d'activité inhabituelle liée aux données (ex. : suppression, chiffrement, etc.). L'algorithme apprend à reconnaître des schémas de votre environnement de sauvegarde spécifique et ne nécessite ainsi aucune configuration ni aucun ajustement des règles. Il utilise également des informations basées sur l'entropie pour réduire le nombre de faux positifs

Réponse

Lorsqu'un analyste IT ou un analyste de la sécurité détecte un événement suspect ou, pire encore, confirme qu'un incident impliquant un rançongiciel s'est produit, la rapidité de la réponse devient essentielle. Même si de nombreux outils de sécurité efficaces peuvent être utilisés dans l'environnement principal pour détecter et orchestrer la réponse, les analyses et les données des journaux des modifications des données secondaires (systèmes de sauvegarde) améliorent les activités d'investigation, de réponse et d'analyse. Le module de récupération accélérée suite à une attaque par rançongiciel Dell PowerProtect Backup Services offre des intégrations d'API robustes et prêtes à l'emploi qui facilitent l'intégration de la solution à votre écosystème de sécurité global. L'orchestration des activités de réponse à l'aide de solutions SIEM et SOAR peut considérablement réduire votre temps moyen de réponse (MTTR) en exécutant automatiquement des actions telles que la mise en quarantaine des systèmes infectés ou des snapshots, ou la recherche d'IOC dans les sauvegardes en fonction d'un playbook anti-rançongiciel prédéterminé.

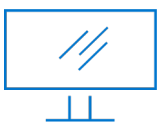
Récupération

Une fois la phase de réponse initiale terminée, le difficile travail de récupération peut commencer. Il s'agit d'un processus manuel et chronophage pour de nombreuses entreprises. Le temps de présence

des acteurs malveillants et des rançongiciels peut s'étaler de plusieurs semaines à plusieurs mois, il est donc difficile de savoir jusqu'à quel moment remonter pour trouver des données inaltérées. Même une fois le meilleur snapshot identifié, un logiciel malveillant caché peut entraîner une nouvelle infection. Un point de récupération datant d'il y a 2 semaines n'est pas acceptable pour la plupart des utilisateurs professionnels. De plus, trouver et valider des données plus récentes après un incident causé par un rançongiciel est une tâche manuelle, fastidieuse et souvent insurmontable.

Dell PowerProtect Backup Services facilite cette tâche grâce à une architecture de sauvegarde efficace et à des outils automatisés permettant d'accélérer la récupération. La plateforme Cloud Dell PowerProtect Backup Services sauvegarde les charges applicatives directement dans le Cloud, ce qui vous permet de les restaurer immédiatement en cas d'attaque par un rançongiciel.

Le module de récupération accélérée suite à une attaque par rançongiciel vous permet de rétablir vos données en toute confiance en les protégeant contre toute altération. Vous pouvez rechercher la présence de logiciels malveillants et d'IOC dans vos snapshots à l'aide de la détection antivirus intégrée ou de l'intelligence sur les menaces de vos propres flux d'analyse ou de renseignements sur les menaces. L'analyse des snapshots avant la récupération élimine le risque de réinfection.



En savoir plus à propos de PowerProtect Backup Services

Contacter un expert Dell Technologies