Examen technique

Récupération rapide et efficace suite à une attaque par rançongiciel grâce à l'architecture immuable de la plate-forme de gestion des données Rubrik

Date : Mai 2020 **Auteur :** Vinny Choinski, analyste senior de la validation, et Christophe Bertrand, analyste senior

Résumé

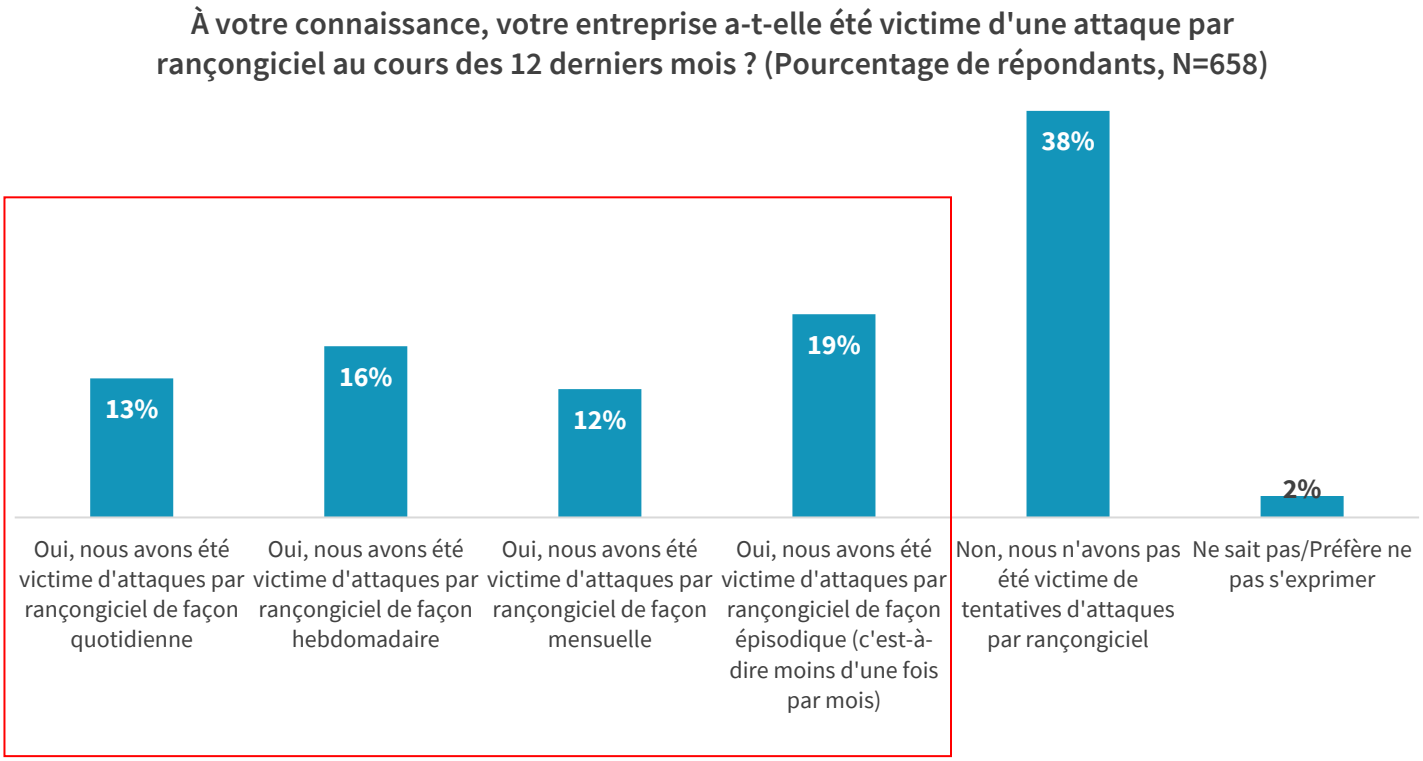
Cet examen technique ESG documente l'analyse pratique et l'examen de l'architecture Rubrik. Nous y étudions comment Rubrik protège les données contre les attaques par rançongiciel et accélère le processus de récupération après attaque grâce à son architecture immuable.

Les défis

Les rançongiciels sont omniprésents et représentent une menace importante pour les entreprises, quelle que soit leur taille. Selon le FBI, les entreprises versent plus d'un milliard de dollars par an aux cybercriminels à l'origine des rançongiciels afin de récupérer leurs données. ESG a récemment mené son enquête annuelle portant sur les intentions de dépenses consacrées aux technologies auprès de 651 décideurs informatiques de haut rang travaillant dans des entreprises de taille moyenne (de 100 à 999 employés) et dans des grandes entreprises (1 000 employés ou plus) d'Amérique du Nord et d'Europe de l'Ouest.[1] D'après la Figure 1, bien que 40 % d'entre elles n'aient pas subi d'attaque par rançongiciel (ou préfèrent ne pas s'exprimer à ce sujet), la majorité des entreprises ont indiqué avoir dû gérer une telle situation en 2019. Plus précisément, 60 % des personnes interrogées ont déclaré avoir été victimes d'une attaque par rançongiciel à un moment donné sur une période de 12 mois, et 29 % ont signalé que les attaques se sont produites chaque semaine (ou même plus fréquemment). Plus inquiétant encore, 13 % des entreprises ont été confrontées à des menaces de rançongiciel au quotidien ! Les entreprises ayant déclaré une pénurie de compétences en cybersécurité étaient beaucoup plus susceptibles (67 % contre 54 %) d'avoir été ciblées par une attaque par rançongiciel au cours des 12 derniers mois. Les recherches menées par ESG en 2020 sur les intentions de dépenses en technologie indiquent également que 62 % des entreprises prévoient d'augmenter la part des dépenses en cybersécurité en 2020, et on peut raisonnablement supposer, dans de nombreux cas, les préoccupations liées aux rançongiciels ont au moins contribué à influencer ces positions d'investissement en matière de sécurité.

[1] Source : Résultats de l'enquête ESG Master Survey, *Enquête 2020 sur les intentions de dépenses consacrées aux technologies*, janvier 2020. Sauf indication contraire, toutes les autres références et les graphiques de la recherche ESG inclus dans cet examen technique sont issus de l'ensemble des résultats obtenus au cours de cette enquête principale.

Figure 1. Taux des attaques par rançongiciel en 2019



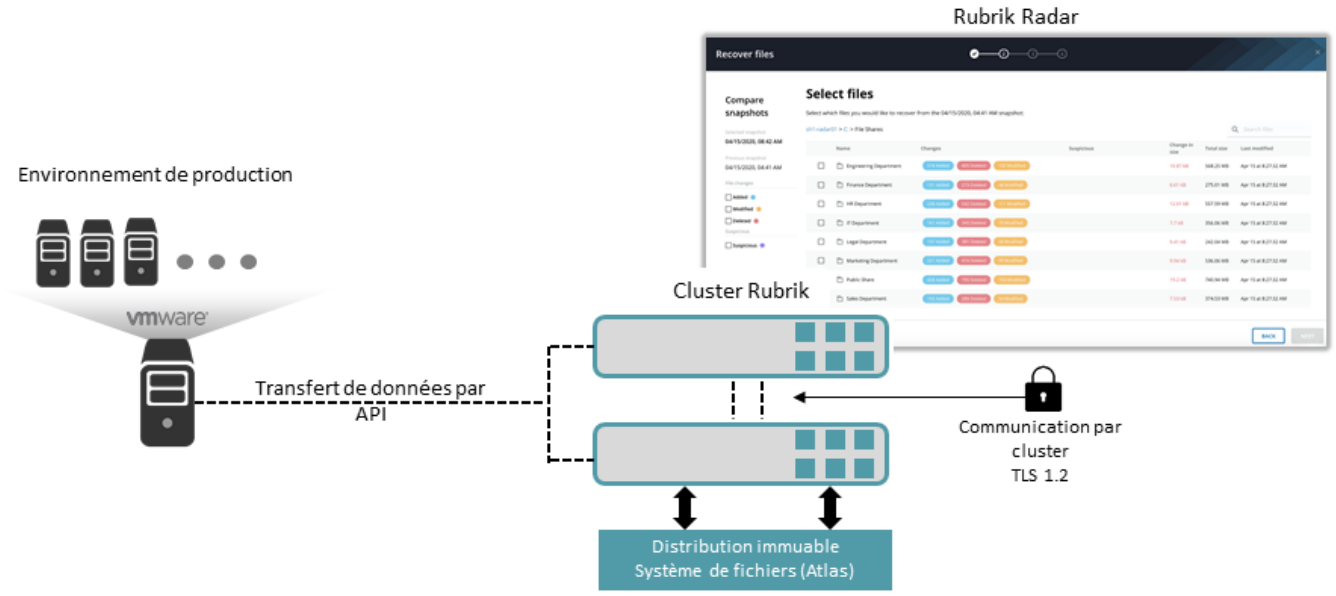
Source : Enterprise Strategy Group

La solution : Récupération en cas d'attaque par rançongiciel de Rubrik

Quand on évoque les rançongiciels, les gens se demandent souvent la raison qui pousse les victimes à payer la rançon. Ne pourraient-elles pas plutôt se remettre de ces attaques grâce à leurs sauvegardes ? En réalité, de nombreuses solutions ne disposent pas des capacités de protection dont les entreprises ont vraiment besoin pour se protéger contre les programmes malveillants et, une fois en place, les scénarios de récupération deviennent rapidement limités. Lorsque les données sont compromises, la plupart des entreprises se retrouvent à effectuer une analyse rapide de leurs options en matière de coûts et de bénéfices. Par conséquent, si l'entreprise ne dispose d'aucune solution adéquate de protection des données, elle n'a souvent plus le choix que de payer la rançon. Une grande partie de l'analyse consiste à prendre en compte le fait qu'en moyenne, il faut au moins sept jours à une entreprise pour récupérer ses données, ce qui souvent est une durée suffisante sans systèmes stratégiques pour qu'une entreprise fasse faillite. Les rançongiciels les plus sophistiqués ciblent désormais les sauvegardes en les chiffrant ou en les supprimant complètement. Cela signifie que la récupération à partir de sauvegardes hors site, telles que les sauvegardes sur bandes, prend souvent trop de temps, ce qui oblige au final les entreprises à payer la rançon. La plupart des entreprises n'ont également aucune visibilité sur leurs sauvegardes pour leur permettre de savoir ce qu'elles sont en mesure de restaurer sans réintroduire le logiciel malveillant.

La conception de la solution Rubrik protège vos données de sauvegarde contre les rançongiciels. La solution garantit la sécurité multicouches des données en chiffrant toutes les données inactives et en transit. Comme le montre la Figure 2, chaque cluster Rubrik transfère les données vers et depuis une application client de protection par le biais d'API s'authentifiant par des mots de passe complexes et aléatoires. Elle s'appuie sur le protocole TLS 1.2 pour les transferts de données et la certification des communications de nœud à nœud. Toutes les données de sauvegarde sont stockées dans un format immuable, rendant les données inaltérables, et empêchant ainsi le rançongiciel d'accéder aux sauvegardes et de les chiffrer ou les supprimer. Cet aspect est essentiel à toute stratégie de protection moderne. En quelques clics seulement, une entreprise peut récupérer rapidement d'une attaque en revenant au point de sauvegarde fonctionnel le plus récent grâce au schéma de sauvegarde incrémentale permanente de Rubrik.

Figure 2. Présentation de la solution de récupération en cas d'attaque par rançongiciel de Rubrik



Source : Enterprise Strategy Group

Les principales fonctionnalités de la solution sont les suivantes :

- **Immuabilité :** Une fois écrites, les données ne peuvent pas être lues, modifiées ou supprimées. Une véritable immuabilité est essentielle pour toute stratégie efficace de protection contre les rançongiciels. L'architecture Rubrik est conçue pour protéger les sauvegardes dans leur intégralité.
- **Visibilité de l'impact :** Une des clés de la réussite d'une récupération consiste à connaître le point de restauration ponctuel exact considéré comme exempt de tous les programmes malveillants et à utiliser comme sauvegarde à restaurer. Une visibilité rapide et précise permet de gagner un temps précieux.
- **Récupération instantanée :** Après une attaque, le temps, c'est de l'argent et de la réputation. L'objectif de temps de restauration (RTO) doit être minimal. Rubrik y parvient grâce à des sauvegardes incrémentales permanentes et à des options de restauration ponctuelles, permettant une récupération simple et rapide.

ESG validé

Cet examen technique ESG documente l'analyse pratique de la solution Rubrik conçue spécialement pour les rançongiciels. Nous avons validé la solution en nous appuyant sur plusieurs sessions de démonstration organisées par Rubrik, en examinant des études de cas, en assistant à un briefing sur l'architecture et en parcourant les différents composants de Rubrik, qui, combinés, forment une stratégie de protection intégrée contre les rançongiciels.

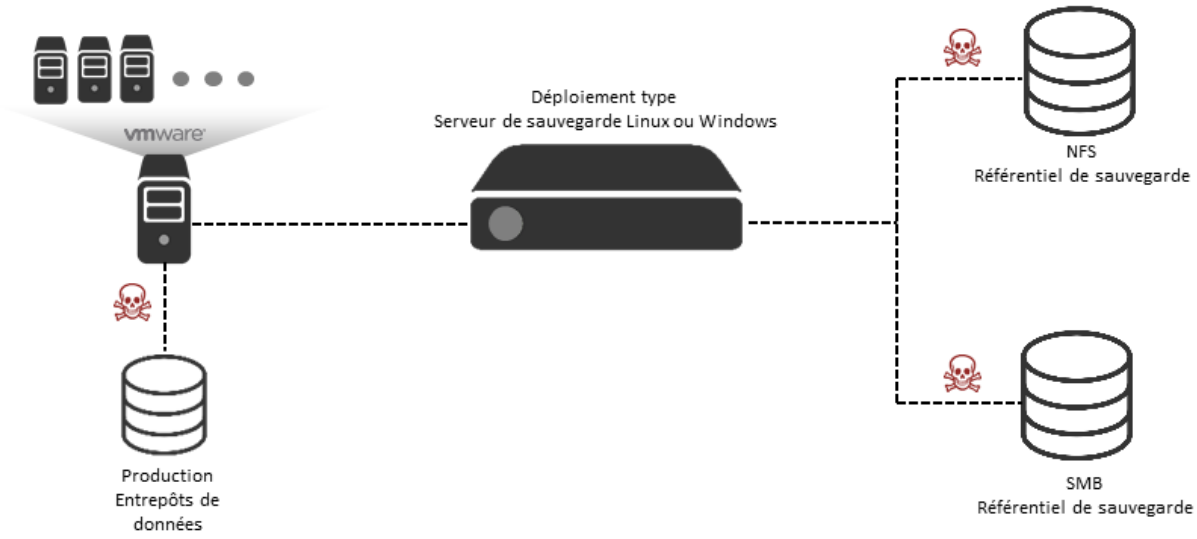
Principes de base de la résilience de l'architecture de protection des données

ESG a commencé ses tests en examinant les architectures de sauvegarde et de restauration dites « traditionnelles » et en comprenant où se trouvent les vulnérabilités, comme l'illustre la Figure 3. En résumé, notre objectif est de comprendre plus précisément comment il est possible d'attaquer une sauvegarde et d'installer un rançongiciel. Les rançongiciels sont une sous-catégorie de programme malveillant, c'est-à-dire tout code ou programme malveillant qui permet au pirate d'avoir un contrôle explicite sur votre système. Ces logiciels comprennent les virus, les bogues, les vers, les robots, les rootkits, les logiciels espions, les logiciels publicitaires et les chevaux de Troie. Ils se comportent comme un agent interne qui installe du code malveillant sur votre ordinateur ou vous incite à lancer un programme par le biais de pièces jointes malveillantes, de messages Web ou d'une fausse mise à jour d'application. En conséquence, le pirate prend le contrôle de votre système et ce dernier ne répond plus à vos commandes. Les rançongiciels vont encore plus loin en chiffrant votre base de données et vos fichiers. Une fois que cela se produit, le pirate

demande alors un paiement afin de déchiffrer vos fichiers. Il existe trois grandes catégories de rançongiciel. Les crypto-rançongiciels ciblent les fichiers critiques et empêchent les utilisateurs d'y accéder. Les crypto-verrouilleurs ne chiffrent pas les fichiers, mais bloquent l'accès de la victime à son système. Les divulgiciels sont des rançongiciels qui extorquent de l'argent aux victimes en les menaçant de divulguer des informations sensibles s'ils ne payent pas la rançon.

Comme le montre la Figure 3, ESG a étudié les composants d'une solution de protection de données lambda déployée en interne à l'aide d'outils téléchargés sur les sites Web des fournisseurs. Au centre se trouve le serveur Windows ou Linux sur lequel l'application de sauvegarde est déployée. Il s'agit généralement d'un serveur disponible dans le centre de données connecté au même réseau local que les clients de sauvegarde. De la même manière que les clients qu'il est censé protéger, il dispose généralement d'un accès à Internet pour la gestion des correctifs et l'administration à distance. Le serveur est l'endroit où l'application de sauvegarde est installée et il hérite généralement du même schéma d'identification uniformisé par le service informatique. Pour cette raison, et parce qu'elle se sert souvent des systèmes de fichiers (NFS et SMB) que le rançongiciel connaît et qu'elle privilégie pour stocker les images de sauvegarde, l'application de sauvegarde peut se retrouver tout aussi vulnérable que les systèmes qu'elle est censée protéger.

Figure 3. Architecture de sauvegarde traditionnelle



Source : Enterprise Strategy Group

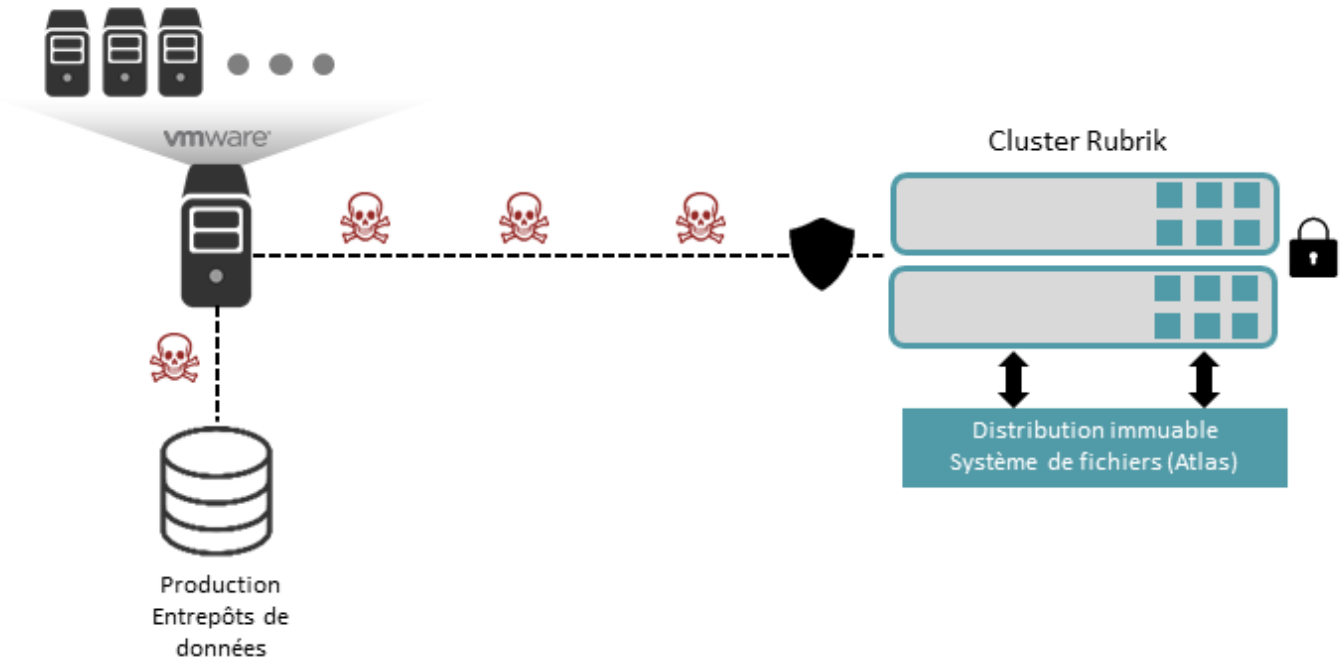
Il est difficile de bloquer une attaque par rançongiciel avant qu'elle ne se produise, car les pirates sont constamment à la recherche de vulnérabilités. La restauration à partir de vos sauvegardes est tout aussi importante que la prévention des attaques. Le moyen le plus sûr de garantir la réussite d'une restauration consiste à disposer d'une solution de sauvegarde immuable. Si une sauvegarde est immuable, une fois les données écrites, elle ne peut être ni lue, ni modifiée ou supprimée. ESG a constaté que, dans une architecture traditionnelle de sauvegarde et de récupération où le logiciel de sauvegarde n'est pas dissocié du système de stockage classique, il peut exister des vulnérabilités par lesquelles peut s'introduire le rançongiciel. La plupart des solutions de sauvegarde utilisent un système de stockage NFS. Si le rançongiciel cible le système de fichiers NFS, les sauvegardes deviennent alors vulnérables. Une fois en place, il peut alors chiffrer la sauvegarde et bloquer l'accès. Ce problème peut s'avérer fréquent avec certains des principaux fournisseurs de solutions de sauvegarde. Alors qu'en faisant appel à Rubrik, le stockage est parfaitement intégré à l'équipement de sauvegarde et à son schéma de sécurité, éliminant ainsi les vulnérabilités exploitables par les cybercriminels utilisant des rançongiciels.

La Figure 4 illustre les fonctionnalités de résilience de la solution Rubrik. Dans des conditions normales de fonctionnement, sans véritable immuabilité, les solutions de sauvegarde sur disque présentent un risque d'être infectées par un rançongiciel. Il peut s'agir de sauvegardes en cours d'écriture ou de sauvegardes existantes. Avec l'architecture basée sur les API de Rubrik, l'accès au stockage

de protection est dissimulé par rapport au réseau client, contrairement à certaines conceptions traditionnelles qui s'appuient sur des protocoles de stockage standard pour la connectivité. La conception de l'architecture de Rubrik se base sur l'approche API-First, qui nécessite l'authentification de tous les terminaux utilisés pour faire fonctionner la solution. L'authentification peut être gérée sous forme d'identifiants ou de jeton sécurisé. Cet aspect comprend les environnements ayant recours au contrôle d'accès basé sur les rôles (RBAC) ou des fonctions multientités afin de répartir logiquement les rôles, les fonctionnalités et les ressources à gérer. L'ILC, les kits de développement et les autres outils de Rubrik font appel aux API et sont tenus aux mêmes exigences de sécurité.

Les points terminaux des API qui contrôlent le comportement sous-jacent du système nécessitent un niveau d'autorisation supplémentaire qui ne peut être accordé que par un ingénieur qualifié en assistance technique. Un cybercriminel ne pourra donc pas modifier le comportement d'un cluster Rubrik. Cette conception élimine les vulnérabilités et permet à Rubrik de prétendre à une véritable immuabilité, avec la possibilité de restaurer rapidement une sauvegarde après une attaque par rançongiciel sans avoir à payer de rançon.

Figure 4. Présentation de la résilience de la solution Rubrik

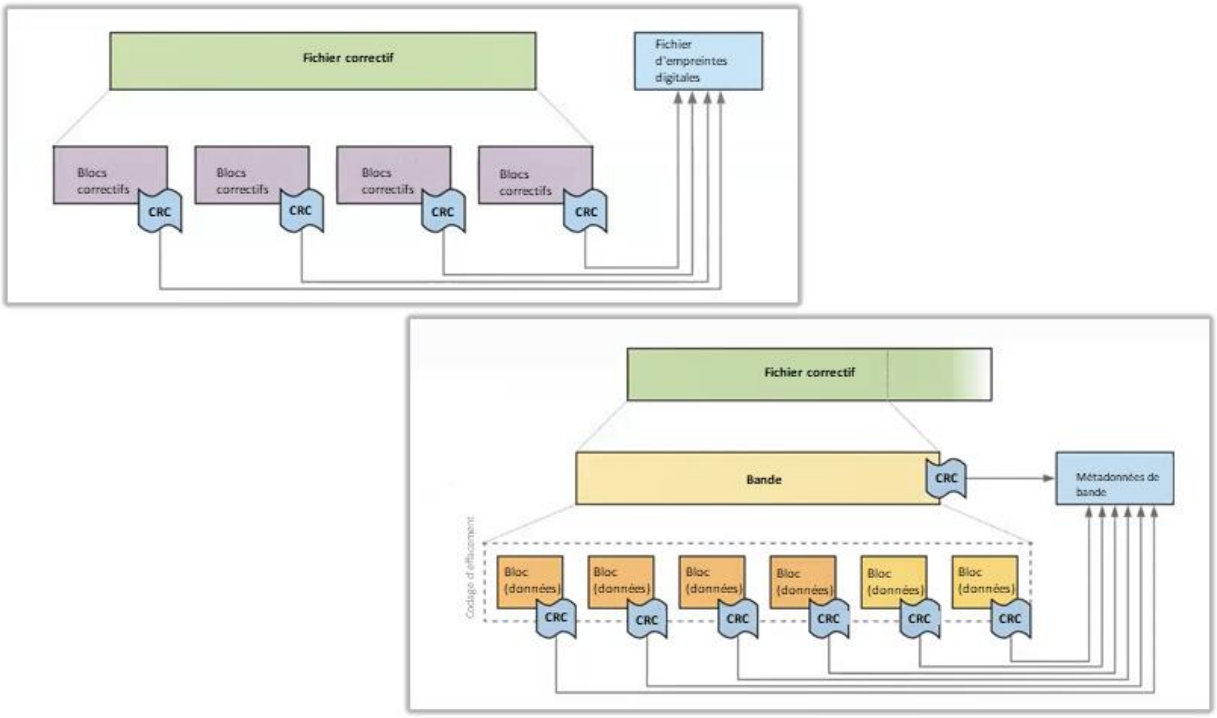


Source : Enterprise Strategy Group

Ensuite, comme illustré à la Figure 5, ESG a examiné plus en détail la conception du système de fichiers Rubrik. Lors de l'exécution d'une sauvegarde, la solution Rubrik procède aux étapes suivantes au niveau de la couche logique. Toutes les données client sont écrites dans des fichiers propriétaires fragmentés appelés fichiers correctifs. Les fichiers à ajout uniquement (Append-only file ou AOF) conservent un enregistrement des modifications de données en écrivant chaque modification à la fin du fichier. Ce faisant, il n'est possible de récupérer l'ensemble des données qu'en relisant le journal d'ajout du début à la fin.

La somme du contrôle de redondance cyclique (CRC) et les empreintes digitales sont ensuite utilisées pour vérifier l'intégrité d'un transfert de données ou d'un fichier. Les sommes de contrôle apparaissent sous forme de longues chaînes alphanumériques de caractères servant d'empreintes digitales numériques et comparent un fichier original à une version copiée de ce fichier afin de s'assurer qu'elles sont identiques.

Figure 5. Informations détaillées sur l'immuabilité du système de fichiers Rubrik



Source : Enterprise Strategy Group

Les principales caractéristiques de résilience au niveau de la couche physique sont les suivantes :

- L'AOF calcule une somme de contrôle au niveau des bandes, qu'il stocke dans chaque bande de métadonnées.
- Une somme de contrôle de bloc est calculée et stockée dans les métadonnées des bandes en même temps que la liste des blocs.
- La réplication et le codage d'effacement s'effectuent au niveau du bloc.
- Si une reconstruction de données est nécessaire, la résilience fournie par le codage d'effacement est automatiquement utilisée en arrière-plan.

Pourquoi est-ce important ?

Le passage d'une bande à isolement physique à une sauvegarde numérique a créé une vulnérabilité pour les pirates exploitant des rançongiciels qui ciblent les systèmes de sauvegarde. Dans le contexte des sauvegardes sur bande, des protocoles tels que TAR ont été utilisés pour transférer des données des serveurs et du stockage vers des supports à bande physiques et amovibles. Une bande physique était alors utilisée dans le cas où une récupération était nécessaire. Désormais, avec les sauvegardes numériques, on utilise des protocoles tels que NFS et SMB. Dans de nombreux cas, cela a permis de mettre en place un processus non immuable face aux défis que représentent les couches physiques et logiques, notamment tout problème de couche de transport inhérent aux protocoles NFS et SMB.

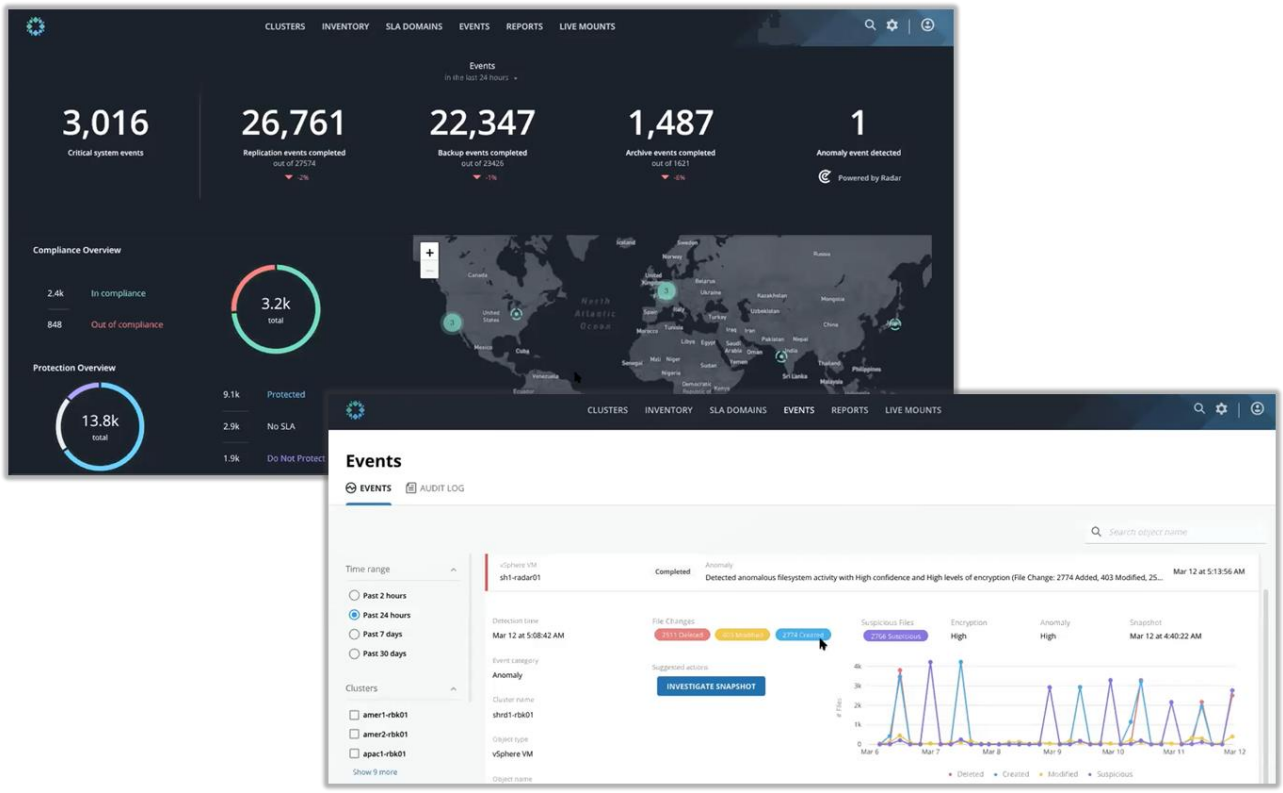
En revanche, la conception API First de Rubrik a permis de s'affranchir des protocoles tels que NFS et SMB. Les API permettent de créer un système interconnecté entre les serveurs de production, le stockage, les bases de données, les applications et les machines virtuelles. Les sauvegardes étant déclenchées et gérées à l'aide d'API, le système Rubrik est donc naturellement immuable et résistant aux attaques par rançongiciel visant à empêcher une récupération à partir de fichiers de sauvegarde. Cette approche est également combinée à une somme de contrôle renforcée des couches logiques et physiques et à un processus d'empreintes digitales permettant de garantir l'intégrité des données.

Processus de récupération en cas d'attaque par rançongiciel

La récupération après une attaque par rançongiciel nécessite une gestion et des contrôles proactifs des données. Dans les sections précédentes, nous avons mis l'accent sur l'importance de l'immuabilité pour gérer les sauvegardes en vue d'une attaque et pour initier une restauration rapide. La récupération après une attaque nécessite également d'avoir une visibilité sur l'ensemble des données et des systèmes de l'entreprise. Avec Rubrik, une entreprise peut utiliser Polaris, une plate-forme SaaS qui organise les informations de l'entreprise et les rend accessibles et exploitables. Rubrik Polaris fournit des informations basées sur l'apprentissage machine avec des applications SaaS spécialement conçues pour la protection des données, la gouvernance, la sécurité et la mobilité afin de garantir la continuité de l'activité, d'accélérer le délai de rentabilisation et d'améliorer la prise de décision.

Comme on peut le voir en haut à gauche de la Figure 6, Radar est l'application de Rubrik intégrée à sa plate-forme Polaris et qui permet d'identifier un comportement anormal, tel que les rançongiciels, et de faciliter et d'accélérer la récupération après une attaque. Il convient de noter que l'application Radar n'est pas nécessaire pour la récupération après une attaque par rançongiciel, mais elle fournit un niveau de visibilité plus précis quant aux options de récupération. Radar surveille le comportement de tous les groupes et crée un référentiel. Les référentiels sont des analyses des comportements historiques et tiennent compte des fréquences, de l'heure et des volumes. Il recherche ensuite les écarts par rapport au référentiel dans le but de détecter les anomalies telles qu'une augmentation du nombre de fichiers ajoutés, supprimés ou modifiés. En bref, tout changement des comportements de sauvegarde habituels. Rubrik détecte les anomalies de deux manières : l'analyse du système de fichiers et l'analyse du contenu des fichiers, un élément indispensable pour renforcer la confiance du modèle de détection. Si une alerte d'anomalie est générée, les entreprises peuvent utiliser l'analyse de Radar pour parcourir plus en détail le contenu des fichiers et rechercher des signes de chiffrement malveillant. La solution peut alors calculer une probabilité de chiffrement à l'aide d'un modèle statistique. Cela permet au processus d'analyse de calculer les caractéristiques entropiques afin de mesurer le niveau de chiffrement dans le système de fichiers sans perdre de temps à recourir à un flux de travail de type « force brute ».

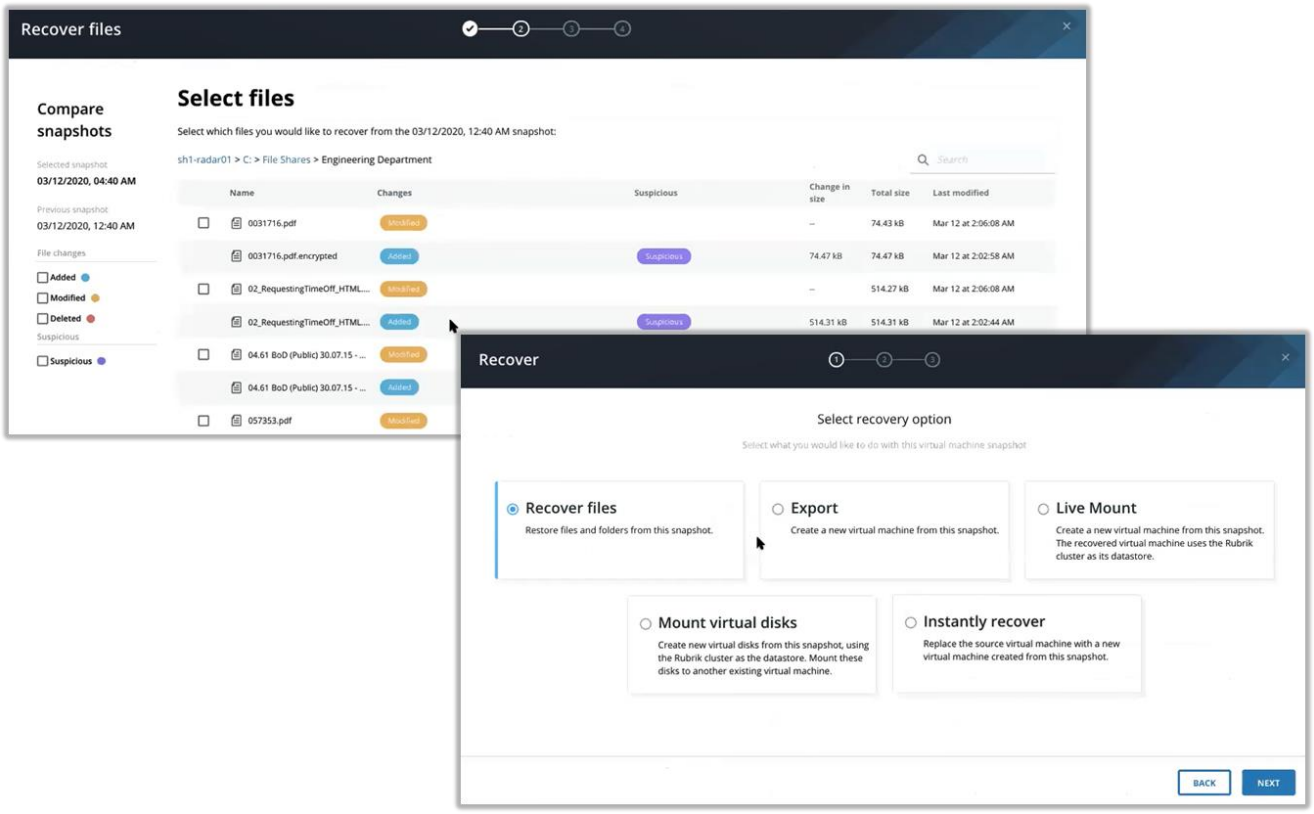
Figure 6. Visibilité Rubrik



Source : Enterprise Strategy Group

Après une attaque sur le système principal d'une entreprise, un administrateur peut accéder à Radar et lancer le processus de récupération. Comme on peut le voir en bas à droite de la Figure 6, un administrateur peut utiliser la page des événements pour déterminer rapidement les sauvegardes les plus utiles et les mesures à prendre quant à la restauration. Au centre de la page des événements, on retrouve trois identificateurs à code couleur. Le rouge représente les fichiers supprimés, le bleu les fichiers créés et le jaune les fichiers modifiés. L'administrateur peut examiner ces valeurs et l'historique pour déterminer si le comportement a changé. Radar signale une activité suspecte en violet en cas d'anomalie et l'administrateur peut déterminer si elle est due à une activité normale ou malveillante. Comme on peut le voir en haut à droite de la Figure 7, si les volumes semblent suspects, l'administrateur peut effectuer une analyse approfondie au niveau du fichier. Pour les administrateurs, les questions clés à prendre en compte sont les suivantes : Une attaque a-t-elle eu lieu ? Quand et comment s'est-elle produite ? Quel est le point de restauration à utiliser et faut-il procéder à une restauration des fichiers ou à une restauration complète ? Comme on peut le voir en bas à droite de la Figure 7, les administrateurs disposent de nombreuses options de restauration, notamment Restaurer les fichiers, Exporter, Montage dynamique, Monter des disques virtuels et Récupération instantanée. La méthode la plus sûre consiste à revenir au point de sauvegarde instantané le plus ancien, mais il existe des options permettant d'utiliser un point de sauvegarde plus récent après avoir vérifié les anomalies ou les problèmes, puis récupéré les fichiers suspects d'un autre horodatage afin d'obtenir le meilleur RPO.

Figure 7. Processus de récupération en cas d'attaque par rançongiciel de Rubrik



Source : Enterprise Strategy Group

Pourquoi est-ce important ?

Les entreprises s'appuient fortement sur leurs fournisseurs de protection des données afin de garantir les capacités de restauration et de réduire le temps nécessaire à la restauration en cas d'événement relatif à l'intégrité des données. Pour éviter qu'une victime récupère ses données sans avoir à payer de rançon, les nouvelles attaques des programmes malveillants ciblent non seulement les données de production, mais elles s'étendent à présent aux ensembles de données de sauvegarde. Rubrik permet aux entreprises de protéger les sauvegardes de données contre les programmes malveillants et les attaques de rançongiciel.

ESG a confirmé que Rubrik, grâce à ses sauvegardes immuables, et la visualisation fournie par Polaris et Radar, permet à une entreprise de récupérer ses données rapidement et facilement suite à une attaque par rançongiciel. La visibilité granulaire des éléments impactés permet une précision chirurgicale lors de la récupération afin de minimiser la perte de données résultant de l'attaque. Si le rançongiciel affecte uniquement une partie de l'environnement, les entreprises peuvent alors récupérer cette partie. Le RTO devient également critique pendant ces périodes et la gestion proactive des données de sauvegarde grâce à Rubrik peut préparer une entreprise à limiter les dégâts.

La vérité supérieure

La gestion d'une attaque par rançongiciel est l'un des événements les plus stressants auxquels une entreprise dépendante des données peut faire face. Elle perturbe l'entreprise à tous les niveaux et, si cette dernière n'est pas préparée, les coûts de la récupération peuvent atteindre des montants exorbitants et porter atteinte à la réputation d'une entreprise dans des proportions inimaginables. Il n'est pas toujours possible d'éviter une attaque par rançongiciel et on a toujours l'impression d'avoir une courte longueur d'avance sur les pirates potentiels. Si les pirates parviennent à s'introduire dans les systèmes des entreprises, celles-ci doivent pouvoir compter rapidement sur leur processus de sauvegarde et de restauration.

ESG a vérifié que, contrairement à de nombreux autres fournisseurs qui dépendent de produits matériels et logiciels tiers ou de solutions sur bandes pour mettre en place une protection contre les rançongiciels, la plate-forme de gestion de données Rubik, de par ses éléments de conception, hérite de puissantes fonctionnalités pour gérer les rançongiciels. Le recours massif aux API, aux sauvegardes immuables et à la visualisation de Polaris Radar a créé une stratégie de réponse aux rançongiciels holistique conçue pour protéger les entreprises de toutes tailles. Notre analyse a été validée par des études de cas réelles de clients capables de se remettre instantanément des attaques par rançongiciel, ainsi que d'autres qui n'avaient pas encore adopté une stratégie Rubrik et qui ont dû en payer le prix.

Nous avons constaté que certaines entreprises croient même que payer la rançon peut s'avérer être une stratégie viable. Toutefois, chacun doit garder en tête que cela ne fait qu'encourager les attaques, et ce n'est pas parce que vous versez de l'argent à un cybercriminel qu'il se gênera pour en demander plus, et pire encore, qu'il prenne juste votre argent sans jamais déverrouiller vos fichiers. Votre seul plan d'urgence valable doit être mis en place par un fournisseur de sauvegarde et de restauration éprouvé qui comprend les défis associés à ce genre de situation et qui a développé une technologie vous offrant les résultats dont vous avez besoin. Si vous cherchez à vous préparer à une récupération rapide et transparente suite à une attaque par rançongiciel, ESG estime que la solution Rubrik vaut la peine d'être sérieusement prise en considération.