rubrik | Zero Trust Data Security™

WHITE PAPER

Guide complet de la solution Zero Trust Data Security

Sommaire

Rubrik est une entreprise de cybersécurité. Nous sommes les pionniers en matière de Zero Trust Data Security™. Des entreprises du monde entier font confiance à Rubrik pour assurer la résilience de leurs activités face aux cyberattaques, aux menaces internes et aux interruptions opérationnelles. Piloté par l'intelligence artificielle, Rubrik Security Cloud permet à nos clients de sécuriser leurs données dans leurs datacenter, le cloud et en mode SaaS. Nous fournissons une protection contre les cyberattaques, nous surveillons les risques et nous assurons la récupération rapide des données et applications.

Pour en savoir plus, visitez notre site www.rubrik.com/fr et suivez notre compte @rubrikInc sur X (anciennement Twitter) et Rubrik, Inc. sur LinkedIn.

RUBRIK_eebk-definitive-guide-ztds_FR / 20240221

Introduction

Les attaques par ransomware se multiplient à un rythme alarmant – pas un jour ne passe sans que les médias ne se fassent l'écho d'une nouvelle entreprise victime. Aujourd'hui, ces attaques représentent donc une menace sérieuse pour tout type de structure.

Pour ne rien arranger, leur volume ne cesse d'augmenter. Selon la Harvard Business Review, le nombre d'attaques par ransomware a bondi de 150 % en 2020, tandis que les rançons versées par les victimes ont connu une inflation de plus de 300 %.

Dans un récent rapport intitulé *Détecter, protéger, récupérer : comment les applications de sauvegarde modernes peuvent vous protéger contre les ransomwares*, Gartner note que « d'ici 2025, au moins 75 % des Direction des systèmes d'information (DSI) auront fait face à une ou plusieurs attaques ». Dans la lutte contre les ransomwares, les approches traditionnelles de sécurisation et de protection des données sont dépassées.

- **La sécurité du périmètre ne suffit plus à repousser les assauts des cybergangs.** Malgré des investissements massifs dans la sécurité du périmètre informatique, des terminaux et de la couche applicative, les attaquants parviennent encore à s'introduire et faire main basse sur de précieuses données d'entreprise.
- **Les sauvegardes traditionnelles sont vulnérables.** Les sauvegardes représentent à la fois la dernière et la plus importante ligne de défense contre les ransomwares. Le problème, c'est que les cybercriminels en ont parfaitement conscience. C'est pourquoi de nombreuses attaques prennent ces sauvegardes pour cible afin d'empêcher la restauration et de contraindre les entreprises à payer la rançon. Or, si les méthodes classiques sont parfaites pour récupérer ses données après une catastrophe naturelle ou une défaillance opérationnelle, elles n'ont pas été conçues pour faire face aux cybermenaces. Elles sont donc vulnérables.

Confrontées à cette triste réalité, les équipes IT se tournent vers les méthodes Zero Trust pour protéger leurs données des ransomwares et autres cybermenaces. L'architecture Zero Trust part du principe selon lequel aucun utilisateur, aucun appareil ni aucune application n'est fiable.

Cet eBook fait le point sur les méthodes Zero Trust destinées à protéger les données de sauvegarde et minimiser l'impact des attaques par ransomware. Il détaille les principales techniques pour :

- Réduire le risque d'intrusion
- Sécuriser les données de sauvegarde

- Détecter les comportements anormaux
- Identifier et gérer les données sensibles pour en garantir la conformité
- Endiguer les incidents
- Récupérer rapidement, avec un minimum de temps et d'efforts

Enfin, cet eBook présente les technologies fondatrices de Rubrik Zero Trust Data Security et décrit comment Rubrik sécurise les données et en facilite la restauration.

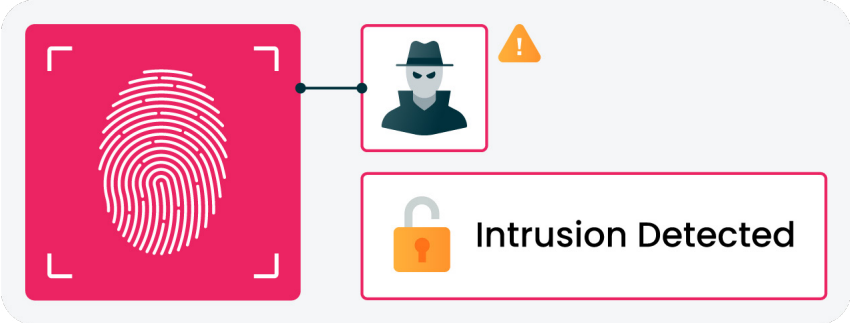
L’importance du Zero Trust pour votre entreprise

La sécurité du périmètre et la sauvegarde de données traditionnelle ont leurs limites ; c’est la raison pour laquelle une approche Zero Trust est nécessaire. Dans une architecture Zero Trust, aucun utilisateur, aucun appareil ni aucune application n’est considéré comme fiable, car tous sont susceptibles d’être compromis. Seuls les utilisateurs vérifiés via une authentification multifacteur (MFA) peuvent accéder aux données, et uniquement à celles dont ils ont besoin. Les autorisations et les accès sont soumis à de strictes restrictions, et les utilisateurs ne peuvent pas commettre d’actes malveillants sur les données stockées.

Le modèle Zero Trust est défini par le National Institute of Standards (NIST) dans la spécification NIST SP 800-207 Zero Trust Architecture. Comme l’indique le NIST, le modèle Zero Trust se compose d’un *« ensemble évolutif de paradigmes de cybersécurité qui déplace le système de défense du périmètre réseau statique et le recentre sur les utilisateurs, les actifs et les ressources ».*

Pour protéger vos données de sauvegarde, Zero Trust Data Security s’appuie sur cinq fonctionnalités distinctes.

Réduire le risque d'intrusion



Dans l'approche Zero Trust, la première ligne de défense consiste à empêcher les assaillants d'accéder aux données. Il existe de multiples moyens de limiter les accès non autorisés :

- **L'authentification multifacteur (MFA).** Cette méthode consiste à valider plusieurs facteurs que l'utilisateur doit fournir, à commencer les plus courants : ses identifiants. Il peut également s'agir d'un mot de passe à usage unique et à durée définie (TOTP), d'une identification biométrique ou d'une carte d'accès. À cela peuvent s'ajouter des facteurs d'authentification supplémentaires qui viennent encore renforcer la sécurité. En combinant une information que vous savez et une information que vous détenez, la MFA limite les cyberattaques et réduit le risque d'accès non autorisé. En ce sens, elle doit être considérée comme indispensable sur les systèmes et données de sauvegarde.
- **Le contrôle d'accès basé sur les rôles (RBAC).** Cette méthode limite les accès en fonction du rôle de l'individu au sein de l'entreprise ou de la fonction d'un service donné (des comptes de service sont créés pour accorder aux outils tiers les privilèges nécessaires à l'exécution de leur fonction). Les différents comptes utilisateurs et comptes de service ont donc des privilèges d'accès différents. Limiter les accès sur la base des rôles peut réduire considérablement la quantité de données affectées en cas d'attaque par ransomware ou d'autre intrusion.
- **Le principe du moindre privilège.** Les employés et les services n'ont accès qu'aux ressources strictement nécessaires à la réalisation des missions qui leur sont confiées. Même lorsqu'un utilisateur s'est correctement authentifié, s'il n'est pas affecté à une tâche donnée conformément aux règles établies (sur la base de différents facteurs : autorité, responsabilité, compétences), les droits d'accès correspondants ne lui sont pas accordés.

Protéger les données de sauvegarde de toute compromission

La ligne de défense suivante consiste à protéger vos données de sauvegarde dans toute la mesure du possible, même lorsqu'un ransomware parvient à y accéder. Là encore, plusieurs méthodes peuvent être employées :

- **Le chiffrement.** Chiffrer les données de sauvegarde permet de s'assurer qu'un malware ou un hacker qui y aurait obtenu un accès ne pourra pas les lire. Le chiffrement réduit ainsi le risque de compromission d'informations sensibles (données clients, RH, propriété intellectuelle, etc.). Idéalement, les données de sauvegarde sont chiffrées à la volée et au repos.
- **L'immutabilité.** Un ransomware ou un hacker étant capable de chiffrer des données déjà chiffrées afin de les rendre inaccessibles, l'immutabilité s'impose comme un impératif absolu à la protection de vos données de sauvegarde. Une fois enregistrée, une sauvegarde immuable ne peut plus être modifiée ni supprimée — soit pour une période définie, soit indéfiniment. Les technologies sous-tendant le stockage de données immuables sont souvent désignées par l'acronyme WORM (Write Once Read Many).

En associant chiffrement et immutabilité, vous prenez toutes les dispositions nécessaires pour que, même si un ransomware s'introduit dans votre système, il ne pourra jamais rendre vos sauvegardes illisibles ni exfiltrer des données pour compromettre votre entreprise, vos collaborateurs ou vos clients.

Détecter les activités anormales pour accélérer les investigations

La détection précoce constitue une autre ligne de défense importante contre les ransomwares pour toutes les organisations. Plus l'attaque est détectée tardivement, plus les hackers ont de temps pour trouver et exploiter vos failles opérationnelles, et plus une restauration complète risque d'être longue.

Les technologies modernes basées sur des modèles de machine learning aident à détecter les menaces par une analyse approfondie des systèmes de fichiers et des comportements d'accès. Les sauvegardes sont susceptibles de contenir de précieuses métadonnées qu'une technologie ML peut analyser pour déceler des activités anormales et déclencher des alertes. En cas de comportement inhabituel, l'équipe IT est alertée immédiatement afin de pouvoir mener une investigation, ce qui accélère le processus de reprise si nécessaire.

Certaines solutions utilisent la *détection basée sur les signatures* pour comparer les schémas et les séquences détectés à des malwares connus. Cependant, cette approche n'est pas toujours efficace en soi, car les ransomwares peuvent muter. En outre, la détection basée sur les signatures fonctionne seulement si vous n'êtes pas la première victime. Or, la plupart des attaques par ransomware recourent à des techniques de mutation et d'obfuscation du code qui font d'eux des Zero Day. C'est pourquoi les solutions basées sur la détection des comportements sont souvent plus efficaces, car capables d'identifier de telles attaques.

Identifier et gérer les données sensibles

Une autre ligne de défense cruciale consiste à identifier et à gérer les données sensibles en amont de toute compromission. A minima, il s'agit de garantir la conformité aux législations et réglementations applicables dans la ou les régions où vous exercez vos activités (telles que le RGPD et le CCPA), aux règlementations sectorielles (telles que l'HIPAA et le PCI-DSS) et à vos propres politiques internes. Lorsque vous subissez une attaque par ransomware, tout défaut de conformité ne fait qu'ajouter à vos problèmes.

Dans la pratique, assurez-vous de :

- Protéger correctement tous les nouveaux workloads
- Mettre en place des périodes de rétention des données
- Pouvoir identifier rapidement toutes les données sensibles susceptibles d'avoir été exfiltrées.

À l'heure où les équipes IT sont surchargés, l'automatisation garantit le respect de ces exigences, notamment par le biais d'audits et de rapports de conformité. Tout problème est ainsi rapidement corrigé.

Endiguer les incidents et assurer une reprise rapide

Une protection intégrale contre les ransomwares doit également permettre d'endiguer tout incident et de reprendre rapidement le cours normal des activités. Lorsqu'une attaque se produit, son endiguement rapide permet de l'enrayer et d'éviter toute réinfection. Une fois le ransomware introduit sur vos systèmes, il est essentiel de déterminer rapidement l'étendue de l'infection, d'isoler les systèmes touchés et de remonter la piste jusqu'au point d'infiltration. Dans cette optique, le machine learning peut vous aider à identifier le moment auquel vous êtes certain de retrouver des données saines à restaurer.

La rapidité du processus est essentielle pour reprendre rapidement vos activités, avec une perturbation minime de vos capacités opérationnelles. Aucune entreprise n'est à l'abri des cyberattaques. Et lorsque l'inévitable se produit, une restauration trop longue peut avoir un impact considérable sur votre entreprise et sa réputation. La vitesse de la reprise après incident et la limitation des pertes de données représentent donc un véritable enjeu financier. D'où l'importance d'un plan de sauvegarde complet et testé régulièrement.

Votre solution de sauvegarde et de restauration doit être conçue de manière à accélérer et fiabiliser la reprise après sinistre. Même en cas d'attaque par ransomware, il doit être relativement simple d'identifier et de restaurer la version saine la plus récente de vos données. Si votre équipe dispose de technologies capables d'évaluer automatiquement les impacts d'une attaque et de visualiser clairement la nature et les emplacements des applications et fichiers infectés, elle aura toutes les cartes en main pour les restaurer à un niveau de granularité très fin.

Rubrik Zero Trust Data Security

Conçue à partir du modèle d'implémentation défini par le NIST, Rubrik Zero Trust Data Security intègre toutes les fonctionnalités que nous venons d'évoquer. Elle assure ainsi une protection maximale contre les hackers et une reprise rapide après une attaque par ransomware.

Les données enregistrées dans le système Rubrik ne peuvent être modifiées, supprimées ou chiffrées lors d'une attaque. Ainsi, une sauvegarde fiable est toujours disponible, prête à être récupérée. Live Mount, restauration massive, restauration orchestrée des applications… plusieurs options de restauration sont à votre disposition pour récupérer rapidement vos fichiers et workloads affectés par une attaque.

Atouts de Rubrik Zero Trust Data Security

Équipes IT

- Données critiques protégées contre les attaques par ransomware
- Récupération rapide des données et applications
- Paiement de rançons

Équipes de sécurité

- Utilisation des données de sauvegarde sécurisées à des fins d'analyse forensique
- Reprise lancée depuis le centre des opérations de sécurité (SOC)

Propriétaires d'applications

- Garantie sérénité quant à la protection des données de l'entreprise
- Applications restaurées rapidement pour garantir la continuité des activités

DSI et directeurs financiers

- Zero Trust appliqué à la restauration post-ransomware
- Réduction du montant des primes de cyberassurance
- Prévention de l'atteinte à la réputation de l'entreprise

Rubrik Zero Trust Data Security s'inscrit au cœur de la protection des données en bloquant tout accès des hackers votre système de sauvegarde, en identifiant les activités liées au ransomware et en garantissant une sauvegarde saine de toutes vos données, restaurable à tout moment.

L'approche Zero Trust de Rubrik est fondée sur un système de fichiers dédié, qui n'expose jamais les données de sauvegarde via des protocoles réseau ouverts. Le stockage n'est ni en ligne, ni accessible via le réseau. Les données sont donc isolées par un air-gap logique qui empêche de les découvrir et d'y accéder. Cette approche assure un niveau de protection similaire à un air-gap physique, sans imposer un délai de récupération aussi long.

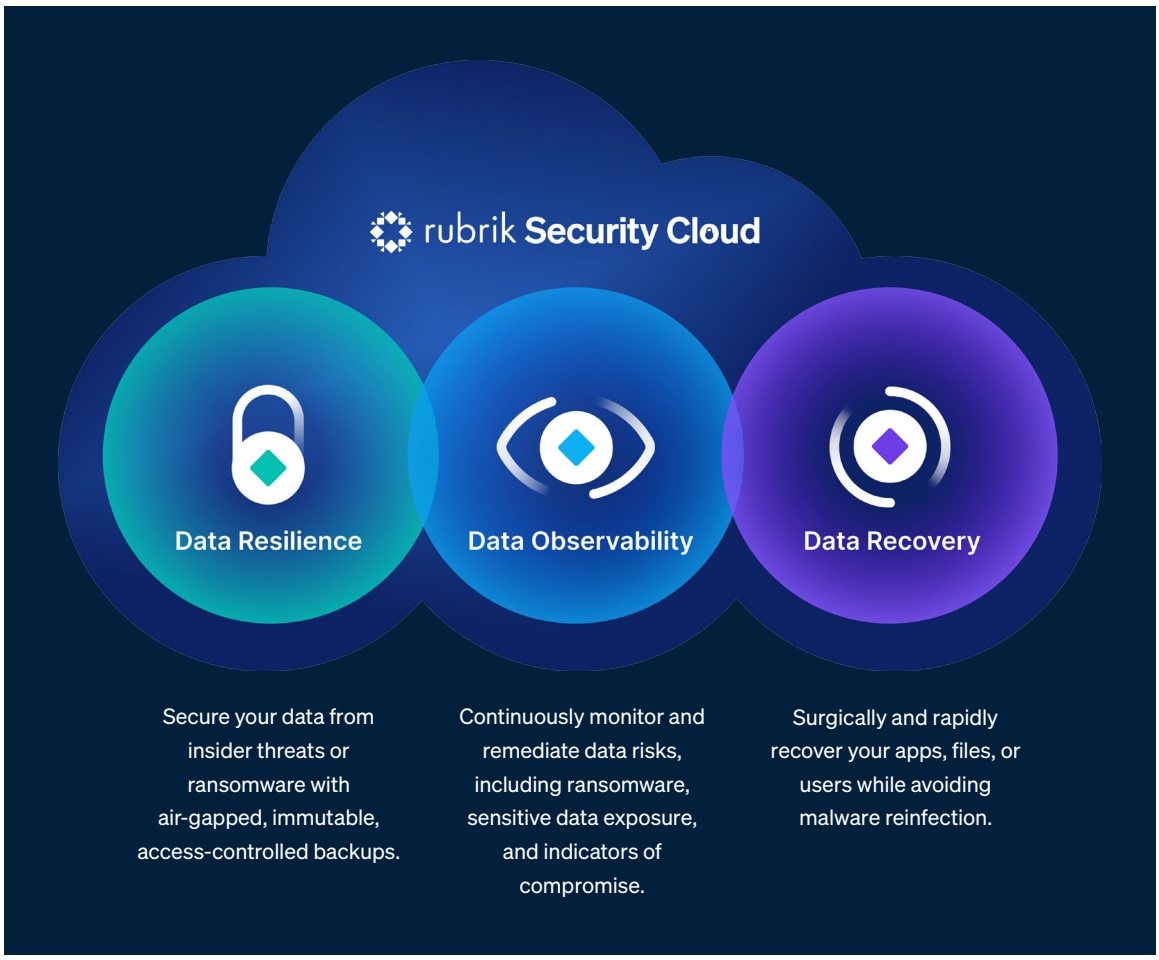
Le rapport Gartner mentionné en introduction recommande d'installer des fonctions de détection précoce, de protection du système de sauvegarde et de reprise rapide. Pour repousser les assauts directs contre les systèmes de sauvegarde, Gartner recommande vivement de prendre un certain nombre de mesures, parmi lesquelles : stockage de fichiers immuable, suppression du recours aux protocoles de fichiers réseau pour les sauvegardes, authentification multifacteur (MFA), la séparation des rôles, et application des autorisations

multipartites pour valider les modifications apportées au système de sauvegarde. Ces fonctions sont toutes intégrées à la solution Rubrik.

La suite de cet eBook décrit les différentes technologies sur lesquelles s'appuie Rubrik Zero Trust Data Security. Ces dernières se répartissent en trois catégories :

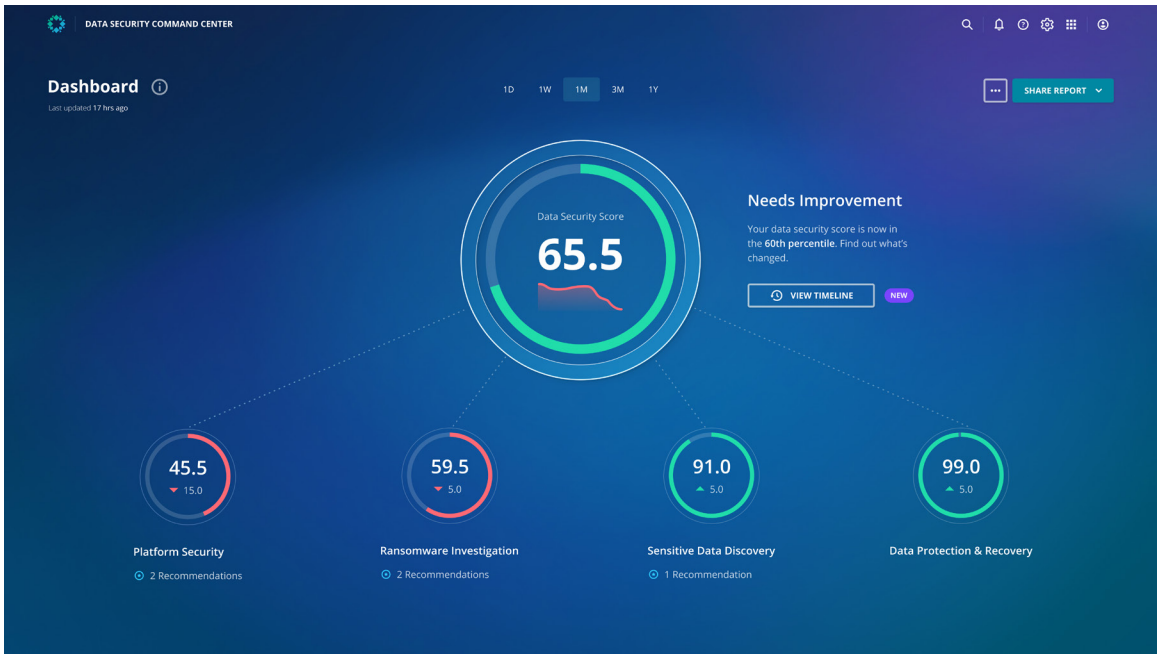
- **Résilience des données.** Prévention et protection contre les infections par ransomware.
- **Observabilité des données.** Détection et identification rapides des attaques par ransomware.
- **Restauration des données.** Endiguement des ransomwares post-infection et récupération rapide des données.

L'ensemble de ces fonctionnalités sont accessibles sur Rubrik Security Cloud, ainsi que via les API Rubrik pour une intégration simplifiée.



Data Security Command Center

Grâce au Data Security Command Center (DSCC), votre équipe accède à toutes les fonctionnalités de Rubrik Security Cloud pour s'assurer de la bonne protection de vos données. Un score de sécurité des données est calculé sur la base de quatre catégories de risque majeures, chacune apportant tous les détails nécessaires pour évaluer rapidement les menaces.



Fourni sous forme de service SaaS pratique et facile à utiliser, le DSCC vous donne une vue d'ensemble du risque pour les données et des failles de sécurité de votre entreprise, le tout assorti de recommandations pour renforcer votre posture de sécurité globale. En fournissant un hub central de visibilité et de collaboration, le DSCC simplifie radicalement la gestion du risque data. Vous évitez ainsi les coûts inutiles et disposez de données fiables pour prendre les bonnes décisions opérationnelles en matière de sécurité des données.

Résilience des données

En matière de protection contre les ransomwares, les sauvegardes constituent un point de vulnérabilité considérable.

- **Une gestion manuelle des sauvegardes** sur des centaines d'applications génère bien trop d'opportunités d'erreurs (et fait perdre un temps précieux à vos collaborateurs).
- **L'accès aux sauvegardes** est parfois trop permissif, tandis que les identifiants peuvent être facilement compromis.
- **Le manque voire l'absence totale de protection sur les applications** renforce le risque de voir une attaque réussir.
- **Des outils de sécurité inadaptés** laissent les données de sauvegarde vulnérables.

Rubrik automatise et simplifie la gestion des données pour relever ces défis.

- Une plateforme évolutive gère l'ensemble du cycle de vie des données, assurant ainsi un avantage économique et des opérations simplifiées.
- Rubrik élimine la surcharge de gestion des tâches de sauvegarde traditionnelles en les remplaçant par quelques règles simples à définir et à gérer.
- La plateforme Rubrik s'intègre facilement à votre environnement.

Rubrik garantit la résilience et la sécurité de vos données critiques grâce aux outils suivants :

- **Rubrik Zero Trust Data Protection.** Protégez vos données contre les menaces internes et externes.
- **Rubrik Cloud Vault.** Stockez une copie saine de vos données hors site, aisément accessible et disponible pour être rapidement restaurée.

Rubrik Zero Trust Data Protection

Rubrik Zero Trust Data Protection assure la sécurité de vos applications et données critiques. Rubrik :

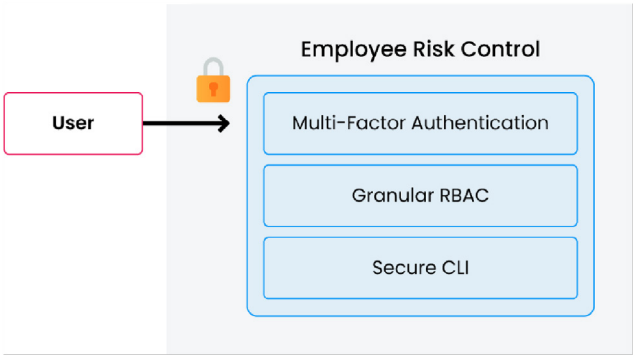
- Empêche les attaquants d'accéder à vos sauvegardes
- Protège vos données de sauvegarde contre les tentatives de chiffrement
- Contrôle les accès aux sauvegardes des machines virtuelles, des bases de données et bien davantage.

La solution Rubrik Zero Trust Data Protection s'appuie sur le principe du Zero Trust : elle unifie la protection des environnements on-prem, multi-cloud et SaaS, et protège vos données grâce au *contrôle du risque d'intrusion* et à une *couche de données sécurisée*.

Rubrik Intrusion Risk Control

Le contrôle du risque d'intrusion est un composant critique de Rubrik Zero Trust Data Protection. Il inclut :

- L'authentification multifacteur
- Le contrôle granulaire des accès en fonction des rôles
- La désactivation de la restauration des paramètres d'usine
- Une interface en ligne de commande (ILC) sécurisée.



Ces techniques de sécurité limitent les risques inhérents aux systèmes rattachés à plusieurs comptes utilisateurs et de service.

Authentification multifacteur

L'approche Zero Trust impose de vérifier l'identité de chaque utilisateur, au-delà de ses simples noms d'utilisateur et mots de passe. Lorsqu'un collaborateur doté de droits d'accès privilégiés est victime d'une attaque de phishing, ses identifiants compromis peuvent permettre à l'assaillant de pénétrer des systèmes critiques, y compris vos systèmes de sauvegarde, compromettant ainsi la capacité de votre entreprise à se remettre d'un ransomware.

Rubrik inclut authentification multifacteur (MFA) native qui évite tout recours à un fournisseur d'identité SAML tiers tel qu'Okta. À l'aide d'un mot de passe à usage unique et à durée définie (TOTP), notre algorithme génère automatiquement un code d'authentification qui change au bout d'un laps de temps défini.

Comme son nom l'indique, ce code est unique et a une durée limitée. Par conséquent, même si un attaquant obtient le mot de passe d'un utilisateur, il ne pourra pas accéder au système de sauvegarde et aux données qu'il contient. La MFA est disponible pour le protocole d'accès LDAP et pour les comptes à authentification unique (SSO).

Les entreprises utilisant un fournisseur d'identité SSO doivent mettre en œuvre à la fois la SSO *et la* MFA. Les deux ne sont pas mutuellement exclusives. Grâce à l'authentification TOTP, les attaquants ne peuvent pas accéder à vos données de sauvegarde et ce, même lorsqu'ils sont parvenus à compromettre votre serveur Active Directory, à obtenir des noms d'utilisateurs et mots de passe, et qu'ils tentent de contourner la SSO via des comptes locaux. Combiner la SSO et la MFA renforce ainsi la sécurité des systèmes.

Contrôle d'accès granulaire basé sur les rôles (RBAC)

Avec Rubrik, il est facile d'affecter des autorisations RBAC granulaires et de les intégrer à Active Directory. Dans un premier temps, la MFA assure la vérification d'identité. Ensuite, le moteur de règles accorde des droits d'accès sur le principe du moindre privilège, en fonction du rôle de l'utilisateur ou du service. Ainsi, si un attaquant parvient à voler des identifiants dotés de droits d'accès à vos données, le contrôle d'accès basé sur des rôles limite considérablement sa capacité de nuisance, en particulier pour les ransomwares

Désactivation de la restauration des paramètres d'usine

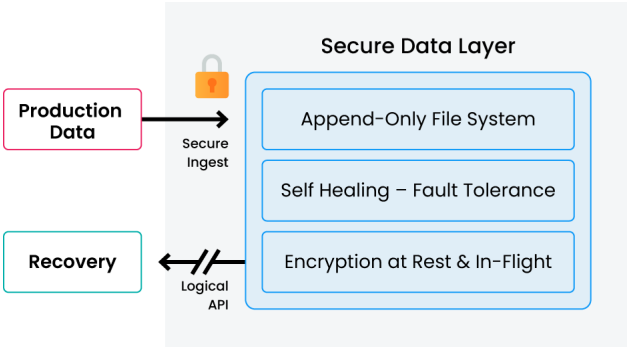
Les commandes de réinitialisation sur les paramètres d'usine sont volontairement désactivées pour plus de sûreté. De cette manière, même si un hacker parvient à accéder à un système Rubrik grâce à des identifiants volés, il ne pourra pas réinitialiser le système pour bloquer l'accès aux données ou leur récupération. Lorsqu'un nœud ou un cluster Rubrik donné doit être réinitialisé, l'administrateur doit contacter le support Rubrik et d'autres preuves d'identité vérifiables.

Interface en ligne de commande sécurisée

La solution Rubrik est conçue pour sécuriser toutes les interfaces du système. Elle protège donc notamment l'interface en ligne de commande (ILC) à l'aide d'une fonction de mot de passe à usage unique. L'authentification TOTP de l'ILC crée une couche de sécurité supplémentaire contre des vulnérabilités de type attaques par injection de commande sur le système d'exploitation, susceptibles de lancer à distance l'exécution d'un code arbitraire sur les systèmes gérés par Rubrik.

Couche de données sécurisée de Rubrik

La couche de données sécurisée de Rubrik applique les bonnes pratiques de sécurité en matière d'ingestion, de gestion et de stockage de données immuables, assurant donc la dernière ligne de défense contre les ransomwares. Rubrik utilise des techniques de pointe pour préserver vos données de sauvegarde contre les menaces.



Air Gap **Immutability** **Retention Lock** **Data Encryption**

Chiffrement

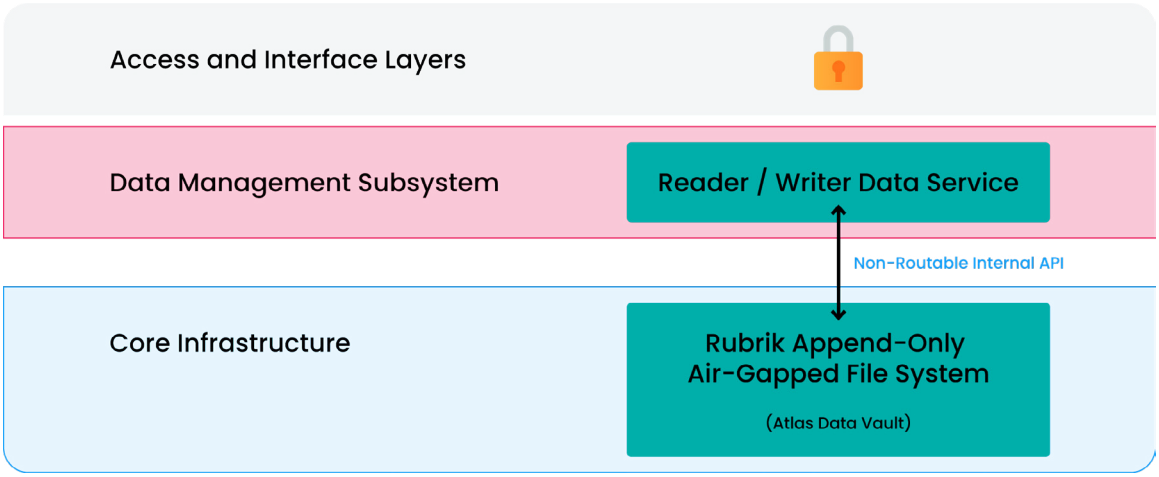
Rubrik chiffre les données au repos et à la volée, de sorte qu'elles ne sont jamais exposées à des utilisateurs non approuvés. Si votre entreprise subit une intrusion, le chiffrement est la meilleure manière d'empêcher toute lecture ou abus de vos données par des personnes malveillantes. Il garantit la confidentialité de ces données en les rendant illisibles aux regards indiscrets qui ne disposeraient pas des clés de déchiffrement nécessaires.

Immutabilité

Avec Rubrik, l'immutabilité ne se résume pas à l'octroi de droits d'accès aux fichiers, à une liste de contrôle d'accès aux dossiers ou à des protocoles de stockage. Notre architecture allie un système de fichiers immuable et une conception en cluster Zero Trust.

Système de fichiers immuable. Le système de fichiers Rubrik empêche tout accès non autorisé et toute suppression des sauvegardes. Votre équipe est ainsi en mesure de restaurer rapidement les données saines les plus récentes, limitant par là même la perturbation des activités.

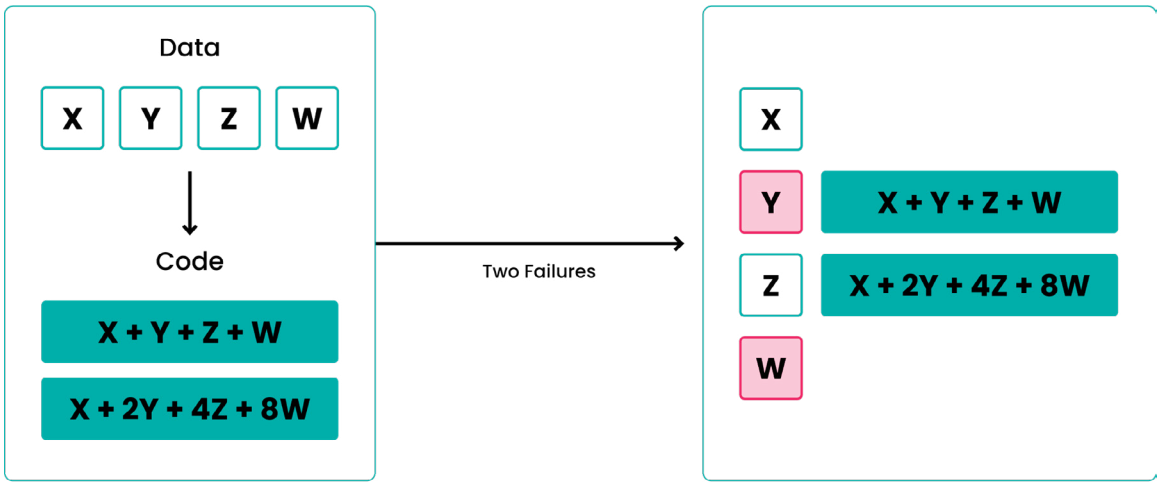
Avec Rubrik, l'immutabilité n'est pas une simple fonctionnalité à activer ou non sur des workloads, applications ou jeux de données spécifiques : elle est intégrée au cœur même du système de fichier, si bien qu'elle s'applique par défaut à toutes les données gérées par Rubrik et ne peut être désactivée. D'autres solutions nécessitent que l'administrateur active et désactive l'immutabilité ou le mécanisme WORM sur les jeux de données concernés, puis planifie et gère l'utilisation des autres. Rubrik réalise toutes ces tâches de manière native et transparente.



Conception en cluster Zero Trust. Grâce à la conception en cluster Zero Trust de Rubrik, les opérations au sein d'un cluster donné ne peuvent être réalisées qu'à l'aide d'API authentifiées. D'autres modèles s'appuient sur un principe de confiance dans lequel tous les membres d'un cluster peuvent communiquer librement entre eux. Parfois, tous disposent d'une autorité au niveau root et d'une autorisation à consulter ou à modifier les données conservées dans le système de fichiers, sans aucun contrôle d'authentification mutuel. En cas d'intrusion sur un nœud d'un tel cluster, les données de sauvegarde risquent d'être altérées de manière à rendre toute restauration impossible.

Codes d'effacement

Pour enregistrer des données sur disque, le système de fichiers Rubrik utilise des codes d'effacement, à savoir une méthode de stockage des données redondantes qui garantit une récupérabilité intégrale après la défaillance d'un système de stockage. Ces codes permettent ainsi de trouver un juste équilibre entre la disponibilité et la surcharge liée aux redondances. Le volume total de stockage disponible pour protéger les données est ainsi plus important, ce qui réduit le coût total de possession (TCO) tout en renforçant la tolérance du système aux défaillances.



Four equations and four variables – everything can be recovered!

En cas de panne de disques ou de nœuds de cluster, les codes d'effacement assurent une résolution automatique qui garantit la disponibilité des données. Généralement, Rubrik s'autorépare en moins d'une heure, réduisant ainsi la probabilité de défaillance simultanée de plusieurs nœuds dans les vastes systèmes distribués.

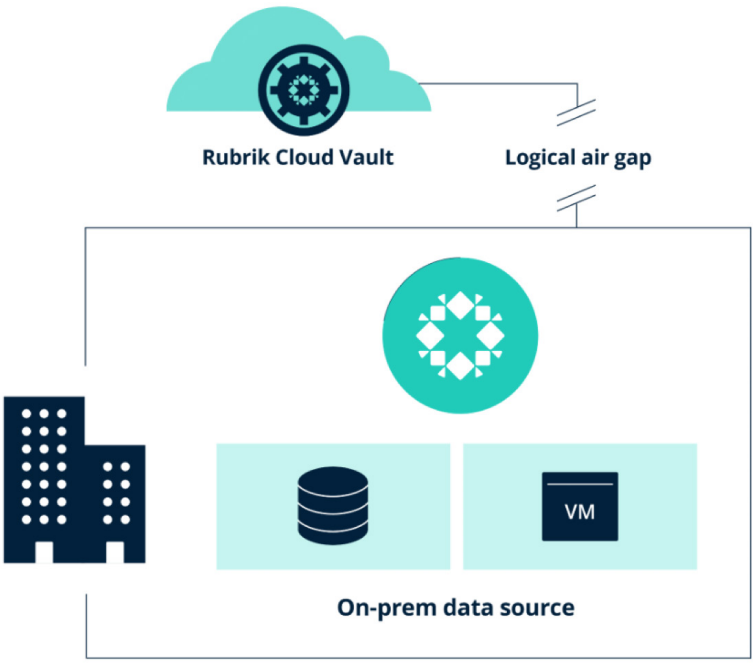
Domaines SLA

Certaines personnes pensent que le stockage sur bande est moins vulnérable aux ransomwares que d'autres formes de sauvegarde. Dans certains cas, cela peut être exact. Mais combien de temps faut-il pour récupérer des bandes hors site et effectuer la restauration ? Après une attaque par ransomware, plus le retour à la normale est long, plus l'impact est élevé sur les plans financier et opérationnel. D'où l'importance capitale d'une orchestration intégrée et intelligente pour relancer efficacement l'activité. Avec les domaines SLA robustes de Rubrik, vos données se trouvent toujours au bon endroit, au bon moment. Rubrik assure ainsi des reprises rapides, avec en prime la garantie sécurité qu'apportent le chiffrement et le système de fichiers immuable.

Rubrik Cloud Vault

Rubrik Cloud Vault étend les fonctionnalités de Rubrik Zero Trust Data Protection et de la couche de données sécurisée à l'archivage isolé sur un cloud hors site. Ce service 100 % managé simplifie les opérations tout en proposant une solution d'archivage isolée par un air-gap logique, pour un coût prévisible. Basée sur Azure Storage, la solution Cloud Vault génère des copies immuables de vos données et les isole intégralement dans le cloud. Elle facilite ainsi la reprise en cas de cyberattaque ou de catastrophe naturelle.

Une fois Cloud Vault configuré, il vous suffit de créer un ou plusieurs SLA. Toutes les données protégées par ces SLA sont automatiquement stockées sur site et dans le cloud, assurant ainsi la redondance des sauvegardes et des archives. L'intégralité des frais de stockage et de sortie sont inclus.



Observabilité des données

Vous avez créé un environnement de sauvegarde sûr et résilient. L'étape suivante consiste à assurer une détection rapide de toute tentative d'attaque. Avec une approche traditionnelle, cela peut représenter un véritable défi :

- **L'impossibilité d'identifier les données sensibles** en amont augmente les risques et les coûts.
- **Trouver où et quand la menace a pénétré** votre environnement peut prendre beaucoup de temps.
- **Une réinfection des systèmes de production** peut se produire au moment de la reprise.
- **Les risques liés aux données** prolifèrent hors de tout contrôle.

Rubrik Zero Trust Data Security relève ces défis à travers des fonctions complètes qui permettent de limiter les risques et d'économiser du temps :

- **Surveillance des données sensibles.** Classifiez les données et évaluez le risque d'exfiltration.
- **Surveillance et investigation des ransomwares.** Détectez les anomalies à l'aide du machine learning.
- **Surveillance des menaces et Threat Hunting.** Localisez le malware et évitez de nouvelles infections.

Surveillance des données sensibles

Le manque de visibilité sur les données sensibles peut entraîner une vulnérabilité et augmenter inutilement les coûts de réponse aux incidents. Rubrik Sensitive Data Monitoring analyse les sauvegardes et localise les données sensibles dans les fichiers et les applications pour vous aider à rester en conformité avec la réglementation.

Avec Rubrik, vous êtes en mesure de visualiser ce que contiennent vos données, où elles se trouvent et qui a le droit d'y accéder. En cas de compromission, les équipes IT qui savent quelles données sont susceptibles d'avoir été exfiltrées disposent de meilleurs éléments pour négocier avec les cybercriminels.

Lorsqu'une entreprise est victime d'une attaque par ransomware, sa capacité à répondre aux questions opérationnelles urgentes et à déterminer si des données précieuses ou sensibles ont été affectées représente une part importante du processus de reprise. Ce sont là autant de composantes fondamentales de l'architecture Zero Trust de Rubrik.

Avec Rubrik, la découverte, la classification et le reporting des données ont un impact nul sur votre environnement de production. Concrètement, Rubrik traite les données de sauvegarde et les métadonnées, sans aucune infrastructure supplémentaire ni agent logiciel à installer. Rubrik vous permet d'identifier les données à risque et de mieux résister à une compromission des données ou à une attaque par ransomware. Résultat : vous limitez le préjudice financier, juridique et réputationnel en cas d'incident.

Découverte et protection des actifs

Rubrik Sensitive Data Monitoring identifie l'intégralité de vos données sur tous vos environnements (des data centers internes au cloud public), tout en appliquant automatiquement des règles SLA pour protéger les actifs tout juste créés. Vous réduisez ainsi votre vulnérabilité aux attaques. Un rapport sur les objets non gérés est exécuté régulièrement afin d'identifier les machines virtuelles, bases de données ou workloads cloud dépourvus de tout SLA, puis d'y appliquer des niveaux de protection adéquats.

Verrou de conservation

Rubrik aide à prévenir les actes malveillants de certains utilisateurs en vérifiant que personne ne peut supprimer ou restreindre les règles de rétention, ni supprimer les emplacements d'archivage ou de réplication. La sécurité des SLA verrouillés pour rétention est vérifiée à travers un processus de validation. Si une modification est demandée pour un SLA verrouillé, deux personnes désignées au sein de votre organisation doivent confirmer leur identité et faire valider les modifications auprès de l'équipe d'assistance de Rubrik. C'est un point particulièrement important dans les secteurs très réglementés, notamment ceux soumis à une obligation de conformité WORM en application des réglementations SEC 17a-4(f) ou FINRA 4511(c).

Reporting de conformité

Pour vous aider à limiter l'exposition des données sensibles, Rubrik analyse activement les sauvegardes de manière à identifier ces données et ainsi faciliter la conformité aux législations applicables en matière de confidentialité (RGPD, HIPAA ou encore PCI-DSS). Rubrik vous permet d'obtenir des informations précieuses sur l'emplacement des données et génère rapidement des rapports sur les données réglementées ou les éventuelles entorses aux politiques en place.

Surveillance et investigation des attaques par ransomware

Rubrik a conscience du fait qu'une attaque par ransomware représente un scénario catastrophe pour la plupart des entreprises. Lorsque le pire se produit, vous risquez d'être confronté simultanément à des difficultés informatiques, opérationnelles et logistiques généralisées. C'est pourquoi Rubrik a mis au point une série de bonnes pratiques pour vous aider à anticiper, identifier et résoudre les attaques par ransomware.

Nos fonctions de surveillance et d'investigation vous permettent de détecter rapidement les attaques par ransomware afin de les endiguer au plus vite. Pour ce faire, nous surveillons les activités de chiffrement, analysons les accès inhabituels et signalons immédiatement les signes d'activité potentiellement malveillante sur vos données de sauvegarde. Rubrik :

- **Utilise la détection des anomalies basées sur le machine learning** pour identifier automatiquement les menaces éventuelles
- **Détermine l'onde de choc d'une attaque** et recommande les points de reprise les plus récents
- **Assure une intégration par API** aux outils SecOps les plus répandus, renforçant ainsi la collaboration entre les équipes IT et sécurité pour accélérer la réponse à incident.

Rubrik permet à vos équipes d'identifier et de localiser rapidement les applications et les fichiers touchés par le ransomware, de sorte que vous ne restaurez que ces derniers.

Détection des anomalies basée sur le machine learning

Les données de sauvegarde contiennent quantité d'informations : leur contenu en lui-même, mais aussi des métadonnées telles que le chemin d'accès, la taille, la liste de contrôle d'accès détaillée, les identifiants utilisateur et de groupe, et autres attributs. Rubrik Zero Trust Data Security transmet ces informations à un moteur ML qui génère des éclairages précieux pour rationaliser le processus décisionnel lors d'une restauration post-ransomware.

Chez Rubrik, dès qu'un snapshot de sauvegarde est réalisé, un fichier FMD est créé. Ce dernier contient une liste des entrées correspondant aux fichiers créés, supprimés ou modifiés depuis la dernière sauvegarde. Un réseau neuronal profond (DNN) reconstitue alors une vue complète de chaque workload.

Entraîné grâce à une méthode d'apprentissage supervisé, le réseau neuronal profond est capable d'identifier les tendances à partir de tous les échantillons et de classifier les nouvelles données en fonction de leur similarité avec les données existantes, le tout sans aucune intervention humaine.

L'analyse DNN s'appuie sur un modèle de détection des anomalies et un modèle de détection du chiffrement :

- **Analyse du comportement du système de fichiers.** Cette fonction assure une analyse comportementale des métadonnées du système de fichiers en se basant sur des éléments tels que le nombre de fichiers ajoutés ou supprimés.
- **Analyse du contenu des fichiers.** En cas d'anomalie comportementale du système de fichiers, une seconde analyse est réalisée pour déterminer l'existence ou non d'une nette augmentation de l'entropie des fichiers, laquelle est généralement le symptôme d'une attaque par ransomware. Ce modèle recherche également les signes d'un éventuel chiffrement et en calcule la probabilité.

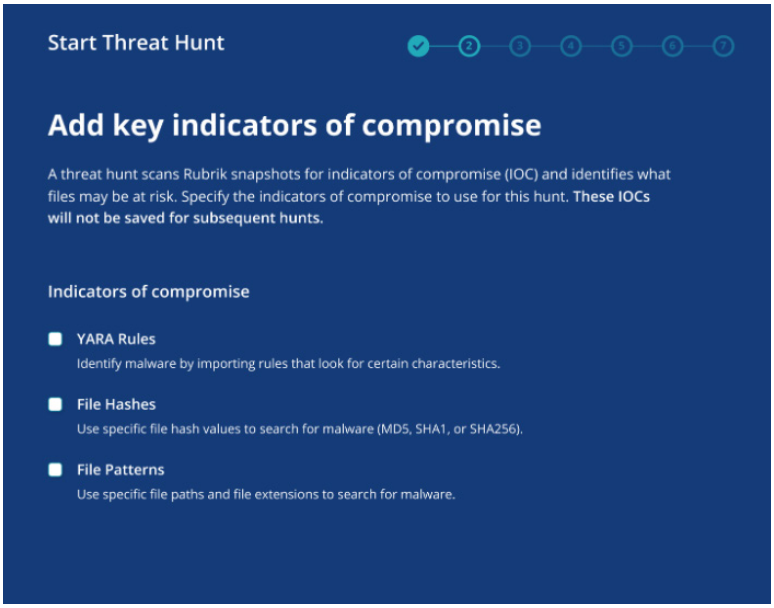
Chaque fois que vous effectuez une sauvegarde, Rubrik utilise le machine learning pour rechercher les signes de ransomware et autres anomalies, de manière à détecter les attaques et à lancer la reprise plus rapidement.

Surveillance des menaces et Threat Hunting

Rubrik Threat Monitoring & Hunting est conçu pour vous aider à détecter les malwares et à éviter toute réinfection. Cette solution consulte vos sauvegardes sans imposer de restauration préalable, de manière à retracer la chronologie des événements sur vos machines virtuelles et vos fichiers. Vous identifiez ainsi le moment de l'infection initiale et empêchez toute réinfection pendant la reprise.

Rubrik Threat Monitoring & Hunting permet :

- **L'identification des menaces.** Rubrik analyse les données de sauvegarde et fournit des informations qui évitent toute réinfection par le malware.
- **La localisation du malware.** Analysez les sauvegardes à partir de modèles, de hashs de fichiers et de règles YARA afin de détecter d'éventuels indicateurs de compromission (IoC) sur l'ensemble des objets sauvegardés.
- **L'établissement d'un point de reprise sûr.** Analysez l'historique de vos sauvegardes pour identifier le ou les meilleurs snapshots à restaurer.
- **La documentation des preuves à des fins d'investigation Exploitez les analyses IoC pour fournir les indices utiles aux investigations cyber internes et externes.**



Rubrik Threat Monitoring & Hunting se démarque des solutions concurrentes par son absence totale d'impact sur votre environnement de production. Elle est capable de traiter plusieurs règles sur différents points dans le temps. Quant à son interface utilisateur intuitive, elle élimine le temps de formation nécessaire à la prise en main d'autres produits. Elle permet ainsi d'exécuter des recherches complexes et d'obtenir davantage d'informations en moins de temps.

Récupération des données

Lorsqu'elle est victime d'une cyberattaque en général, et d'un ransomware en particulier, votre entreprise doit pouvoir récupérer ses données aussi rapidement et aisément que possible. C'est à l'aune de ses capacités de restauration que l'on juge une solution de lutte contre les ransomwares. Malheureusement, de nombreuses solutions de sauvegarde déçoivent en la matière, et ce pour plusieurs raisons :

- **Les approches de reprise peuvent différer** entre les data centers, les environnements SaaS ou le cloud.
- **Les menaces ne sont pas mises en quarantaine** à partir de la sauvegarde active.
- **Il est difficile de récupérer les données** au niveau fichier, utilisateur, objet ou système.
- **La réussite de la restauration est incertaine** et le processus est chronophage.

Rubrik Zero Trust Data Security vous permet de mettre les malwares en quarantaine et d'automatiser la reprise afin de rétablir vos activités avec plus de rapidité et moins d'incertitudes. Rubrik assure les fonctions suivantes :

- **Endiguement des menaces.** Mettez les données en quarantaine pour éviter les réinfections
- **Restauration massive.** Identifiez les données affectées et lancez la reprise en quelques minutes.
- **Restauration orchestrée des applications.** Récupérez aisément vos données et applications grâce à des workflows guidés.

Endiguement des menaces

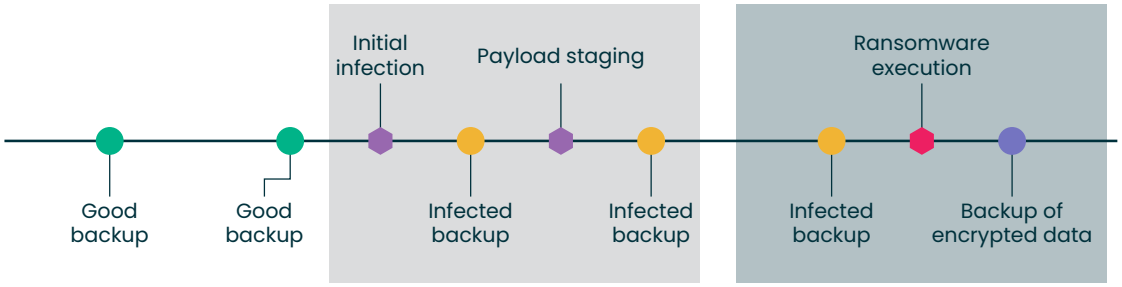
E-mails suspects, malwares connus, communications avec des adresses IP externes associées à des cybercriminels ou à des botnets… votre organisation repère parfois les signaux faibles d'une attaque par ransomware en cours. Plus vous détectez et circonscrivez rapidement l'attaque, moins elle aura d'impact sur vos opérations et plus vous pourrez reprendre rapidement vos activités.

L'endiguement des attaques par ransomware revêt un caractère vital et ce, pour deux raisons. Premièrement, les hackers continuent souvent à étendre leur emprise et à chiffrer de nouveaux systèmes, même après avoir paralysé un premier ensemble de systèmes et signalé leur présence. Deuxièmement, certaines des mesures prises les empêchent de revenir et de lancer une nouvelle attaque.

Analyser l'impact d'une menace

Rubrik analyse en continu l'intégralité de votre environnement pour déterminer comment vos données évoluent dans le temps. En cas d'attaque, des visualisations simples et intuitives vous permettent de rapidement identifier quelles applications et quels fichiers ont été impactés et où ils se situent. Grâce à cette IU, vous pouvez explorer l'ensemble de la hiérarchie de dossiers et cibler votre recherche sur ce qui a été ajouté, supprimé ou modifié au niveau des fichiers. Rubrik vous aide à comprendre plus rapidement le déroulé des événements et assure une visibilité fine sur les fichiers affectés.

En cas de compromission ou de menace, les opérateurs de la solution Rubrik peuvent suspendre l'intégralité des accès et des activités . Vous confinez ainsi les données affectées afin qu'elles ne réinfectent pas votre environnement. Rubrik vous permet de rechercher les indicateurs de compromissions (IoC), sur de multiples systèmes et par ordre chronologique, ce qui vous aide à identifier les sauvegardes saines à restaurer.



Restauration massive

En cas de sinistre informatique ou d'attaque par ransomware, une procédure de restauration simple et évolutive est essentielle pour éviter des interruptions coûteuses. C'est pourquoi la restauration massive de Rubrik vous permet d'assurer la continuité de vos activités grâce à une récupération sécurisée de vos données et de vos applications, dans le respect des objectifs de temps de restauration (RTO) les plus stricts.

Avec la restauration massive de Rubrik, vous pouvez :

- **Minimiser les interruptions d'activité.** Récupérez des centaines de machines virtuelles ou restaurez des dizaines de milliers de fichiers sains en quelques minutes.
- **Empêcher les réinfections.** En identifiant les fichiers et les applications infectés par le ransomware, Rubrik vous permet de trouver rapidement un snapshot sain et de restaurer des données intègres, sans risque de réinfection.
- **Restaurer uniquement les données touchées.** Récupérez uniquement les données affectées grâce à des workflows qui vous guident dans la restauration de fichiers, d'objets, d'applications ou de systèmes individuels.

Souvent, après un ransomware, la récupération prend du temps, car il incombe aux quelques « experts » en interne de définir un plan et de décider comment procéder aux restaurations. L'assistant de restauration en masse de Rubrik utilise le machine learning pour identifier rapidement le ou les derniers snapshots sains. Votre équipe peut ainsi exécuter facilement la reprise en toute fluidité, sans dépendre d'experts internes ni maîtriser des connaissances et compétences pointues dans ce domaine.

Restauration orchestrée des applications

Garantir la sécurité et la résilience des données et des services face aux cyberattaques et autres catastrophes est une responsabilité considérable. L'exécution de plans de restauration manuelle des applications, sur plusieurs couches et avec de multiples interdépendances, ralentit le processus et génère des risques d'erreurs.

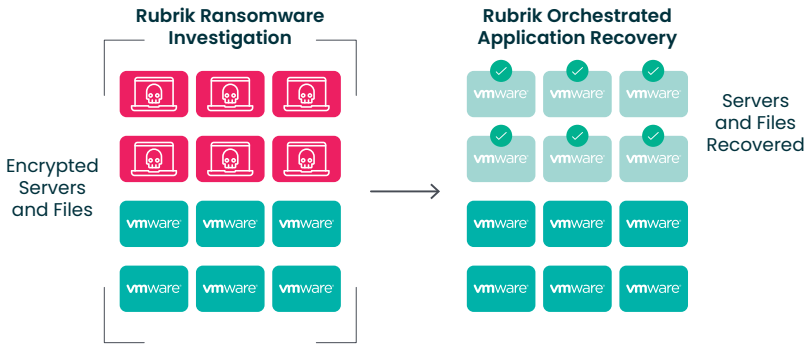
Rubrik Orchestrated Application Recovery est un service de reprise automatisé et étroitement intégré, garant de l'orchestration des tests de reprise après sinistre, mais aussi du basculement lorsqu'un incident réel se produit. Il utilise pour cela des fonctions de surveillance et d'investigation des ransomwares axées sur les applications, ce qui en simplifie considérablement la reprise.

Rubrik utilise des blueprints d'application contenant des informations sur la séquence de reprise de la machine virtuelle correspondante, ainsi que sur les configurations de mappage des ressources (traitement, stockage et réseau) pour une orchestration au niveau des applications.

Imaginez une application à trois niveaux, avec un serveur web frontal, un serveur de middleware et une base de données en back-end. Une reprise basée sur un blueprint vous permet de restaurer une version saine des différents serveurs, indépendamment les uns des autres. Selon la date de l'infection, vous pouvez ainsi restaurer votre serveur de middleware tel qu'il était il y a 2 jours et vos systèmes frontaux et back-end tels qu'ils étaient il y a 3 jours. Les blueprints peuvent englober des centaines de machines virtuelles pour effectuer des récupérations à grande échelle. De même, des groupes de blueprints peuvent former le socle d'un plan de reprise d'un data center entier.

Avec cette méthode, vous pouvez basculer vers un site de secours on-prem ou vers le cloud public en quelques clics. Dès que vous êtes prêt, vous pouvez rétablir le data center principal on-prem tout en maintenant les chaînes de snapshots existantes et des points de restauration CDP pour garantir la conformité aux SLA tout au long de l'événement.

Ensemble, les fonctionnalités Rubrik de surveillance et d'investigation des ransomwares et ses capacités d'endiguement des menaces analysent, puis sélectionnent les applications et fichiers touchés pour en restaurer la version saine la plus récente, le tout en quelques clics. Rubrik vous aide ainsi à accélérer la récupération de vos données après une attaque par ransomware. Orchestrated Application Recovery automatise le processus de restauration.



Pour en savoir plus sur Orchestrated Application Recovery, consultez notre livre blanc de *présentation de Rubrik Orchestrated Application Recovery*.

L’heure est au Zero Trust

Le message des experts en sécurité et des plus hautes sphères de l’État est on ne peut plus clair : les acteurs malveillants sont capables de percer les défenses classiques et ciblent désormais vos données de sauvegarde pour mieux étendre leur emprise. Si ce n’est déjà le cas, il est temps de repenser votre stratégie de protection des données, de créer de nouvelles exigences de sauvegarde et de reprise basées sur les principes Zero Trust, et de procéder aux investissements informatiques nécessaires pour préserver vos données et vous assurer que votre entreprise n’aura jamais à payer de rançon.

Rubrik Zero Trust Data Security vous dote des fonctionnalités essentielles pour protéger votre environnement de sauvegarde contre les attaques par ransomware, tout en vous permettant d’accélérer la reprise. Rubrik vous aide à réduire le risque d’intrusion et à sécuriser vos données de sauvegarde dans un format immuable, tout en simplifiant nettement la détection de comportements anormaux et en assurant le respect des lois, réglementations et politiques clés.

Et pour davantage de sérénité, Rubrik propose également une garantie unique de récupération en cas d’attaque par ransomware. Pour découvrir comment Rubrik peut vous aider à assurer une protection maximale de vos données face aux hackers et à récupérer rapidement d’une attaque par ransomware, rendez-vous sur rubrik.com/fr/ransomware

Autres ressources consacrées aux ransomwares

Ne manquez pas de consulter toutes nos ressources sur les ransomwares (inscription requise) :

- Mise en œuvre d’un plan complet de récupération après une attaque par ransomware
- Guide de bonnes pratiques : préparation et récupération des données après une attaque par ransomware avec Rubrik

Zero Trust Data Security™