the GORILLA GUIDE® to...

Cyber-résilience dans le cloud

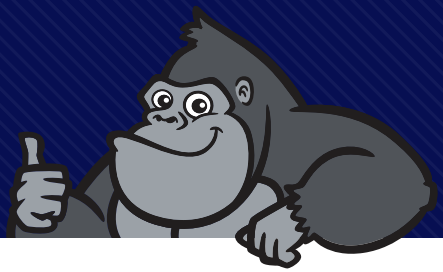
Comment protéger les données de votre organisation dans les environnements multicloud et hybrides

LAWRENCE MILLER

rubrik

POWERED BY ActualTech MEDIA

the GORILLA GUIDE® to...



Cyber-résilience dans le cloud

Comment protéger les données de votre organisation dans les environnements multicloud et hybrides

Par Lawrence Miller

POWERED BY ActualTech MEDIA

Copyright © 2024 Future US LLC
Full 7th Floor
130 West 42nd Street
New York, NY 10036

Tous droits réservés. Cet eBook ne peut être reproduit ou utilisé, en tout ou en partie et de quelque manière que ce soit, sans la permission expresse par écrit de l'éditeur, sauf citations brèves dans le cadre d'une critique. Imprimé aux États-Unis.

www.actualtechmedia.com

REMERCIEMENTS DE L'ÉDITEUR

RESPONSABLE DE LA DIFFUSION DE CONTENU

Wendy Hernandez

GRAPHISTE

Olivia Thomson

PRÉSIDENTE DE SMARTSTUDIO

Katie Mohr

AVEC LA PARTICIPATION SPÉCIALE DE RUBRIK

Daniel Lu
MARKETING PRODUIT POUR LE CLOUD

Amanda O'Callaghan
DIRECTRICE DU CONTENU MARKETING

À PROPOS DE L'AUTEUR

Lawrence Miller, CISSP, est un professionnel de la sécurité de l'information comptant à son actif plus de 20 ans d'expérience dans divers secteurs. À ce jour, il a écrit plus de 200 livres sur une variété de sujets liés à l'IT et à la sécurité.

S'AVENTURER DANS LA JUNGLE

Chapitre 1 : Pourquoi la prévention ne suffit pas 7

Les cyberattaques sont parties pour durer 7

Cyber-résilience : définition et enjeux 10

Continuité opérationnelle en situation de crise : repensez votre stratégie 11

Chapitre 2 : Les défis de la protection des données dans le cloud 12

L'expansion du cloud étend considérablement votre surface d'attaque 12

Le cloud, cible privilégiée d'un nombre croissant d'attaques 13

Chapitre 3 : Cyber-résilience : comment font les autres ? 15

Inaction 15

Méthode maison (DIY) 17

« Lift-and-shift » des outils on-prem existants 18

Outils de sauvegarde cloud natifs des CSP 20

Chapitre 4 : Une meilleure solution pour la cyber-résilience cloud 23

Protection simplifiée et unifiée 24

Cyber-résilience holistique 25

Architecture pensée pour le cloud 25

Récupération rapide 26

Réduction du TCO 27

Conclusion 27

LÉGENDES UTILISÉES DANS CE GUIDE

SCHOOL HOUSE

La légende « School House » signale des informations sur des sujets qui peuvent s'éloigner du thème principal, mais restent importants.

FOOD FOR THOUGHT

La légende « Food for Thought » vous permet d'en apprendre davantage sur les sujets complémentaires présentés dans le guide.

BRIGHT IDEA

Lorsque nous avons une idée lumineuse, nous l'exposons dans un encadré « Bright Idea ».

DEEP DIVE

La légende « Deep Dive » sert à approfondir un sujet en particulier.

EXECUTIVE CORNER

La légende « Executive Corner » aborde des sujets d'intérêt stratégique pour les dirigeants.

DÉFINITION

Définition d'un mot, d'une phrase ou d'un concept.

GPS

Nous vous dirigeons vers la bonne information.

CONTRÔLE DES CONNAISSANCES

Testez vos connaissances sur ce que vous venez de lire.

ATTENTION !

Lisez bien cet encadré afin de ne pas commettre d'erreur majeure !

IMPORTANT

Ne passez pas à côté de ces informations !

CONSEIL

Conseil utile basé sur ce que vous venez de lire.

INTRODUCTION

Bienvenue dans le Gorilla Guide® : cyber-résilience dans le cloud ! Ce guide vous invite à découvrir pourquoi, face à des menaces en constante évolution, une stratégie de cyber-résilience basée uniquement sur la prévention ne suffit pas à protéger les données de votre organisation dans le cloud.

Après un tour d'horizon des approches les plus courantes, nous vous présenterons une meilleure solution pour préserver les données de votre organisation dans le cloud et garantir une cyber-résilience optimale.

Sur ce, entrons dans le vif du sujet !

CHAPITRE 1

Pourquoi la prévention ne suffit pas

À l'heure où les entreprises migrent leurs applications et leurs données critiques vers le cloud, les cybercriminels adaptent leurs techniques pour cibler cet environnement aux multiples points d'entrée potentiels. Face à une telle prolifération de menaces, les organisations doivent partir du principe qu'elles sont ou seront forcément victimes d'une compromission. Par conséquent, une stratégie de cybersécurité axée uniquement sur la prévention ne suffit plus à assurer la sécurité de vos données, et encore moins la viabilité de vos activités. Ce qu'il vous faut, c'est une approche holistique de la cybersécurité et de la cyber-résilience dans le cloud.

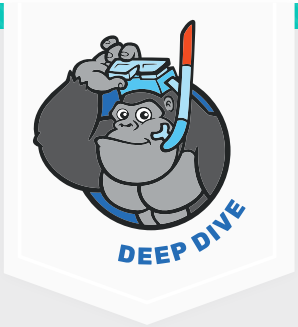
Les cyberattaques sont parties pour durer

Les cybercriminels sont prêt à tout pour faire main basse sur de précieuses données d'entreprise, recourant pour cela à des techniques toujours plus sophistiquées. En témoignent les chiffres alarmants d'un rapport Rubrik Zero Labs récent : 94 % des organisations ont été la cible de cyberattaques. Facteur aggravant, ces attaques ne se limitent pas à un seul point de vulnérabilité. D'après le rapport, elles s'étendent la plupart du temps à plusieurs environnements, notamment le SaaS (67 %), le cloud (66 %) et le réseau on-prem (51 %).

Par leur complexité, les infrastructures cloud de nouvelle génération exacerbent ce phénomène. De même, le foisonnement incontrôlé de l'environnement cloud, appelé « cloud sprawl », élargit considérablement la surface d'attaque d'une organisation. Cette expansion complexifie la protection des données et exige une expertise en sécurité bien souvent absente des entreprises.

Pour compliquer un peu plus l'équation, les ransomwares sont devenus de plus en plus dévastateurs au cours des dernières années. Pour l'année 2021, le coût global de ces incidents est estimé à 20 milliards de dollars. Un chiffre qui devrait exploser d'ici 2031, avec des prévisions tablant sur un coût total de 265 milliards de dollars.

DORA – Non non, pas l'exploratrice



Le règlement européen sur la résilience opérationnelle numérique (DORA) a pour but d'accélérer la mise en place de capacités de cyber-résilience au sein des sociétés de services financiers. Qu'elles soient situées dans un État membre ou entretiennent des relations commerciales avec l'UE, elles sont tenues d'améliorer leur réponse face aux perturbations opérationnelles, à commencer par les cyberattaques. Mais elles vont pour cela devoir se projeter au-delà de l'approche de détection/protection pour s'inscrire dans une démarche de résilience/restauration.

Les prestataires de services essentiels à ces sociétés sont soumis à ces mêmes exigences réglementaires. Tout manquement à leurs obligations peut entraîner des amendes représentant jusqu'à 2 % du total de leur chiffre d'affaires mondial annuel.

Interruptions de service, perte de revenus, coûts de restauration, érosion de l'image de marque, amendes pour infraction à la réglementation… l'onde de choc d'un ransomware s'étend bien au-delà du seul coût de la rançon. Toutefois, ne comptez pas sur les cybercriminels pour suivre un quelconque code d'honneur. Autrement dit, même si l'attaquant vous fournit la clé de déchiffrement pour restaurer vos données sensibles, vous n'aurez aucune garantie qu'elles ne seront pas revendues sur le dark web.

En général, le coût total d'une cyberattaque se chiffre en millions de dollars. Une restauration complète des données (lorsqu'elle est possible) peut prendre des semaines, voire des mois entiers, et laisse des séquelles durables dans l'organisation.

Cette année, les entreprises et acteurs publics sont en passe d'investir plus de 200 milliards de dollars dans leur cybersécurité. Rien d'étonnant quand on sait que dans le cadre de leurs activités de prévention, les équipes de sécurité utilisent parfois plus de 75 outils. Malheureusement, ces investissements massifs n'empêchent pas les attaquants de s'introduire dans les réseaux pour y semer le chaos et réduire à néant des réputations, des carrières et même des entreprises tout entières.

- En février 2024, le ransomware qui a touché UnitedHealth Group (UHG) aurait coûté plus de 872 millions de dollars et devrait représenter au total plus de 1 milliard de dollars en coûts directs.
- En septembre 2023, la compromission des données de MGM Resorts International a entraîné une interruption de service de 10 jours, soit une perte de 100 millions de dollars sur ses résultats du troisième trimestre.
- Révélée en août 2023, la cyberattaque contre le fabricant de détergents Clorox lui a coûté près de 500 millions de dollars en pertes de revenus, plus de 3 milliards de dollars en dépréciation, des ruptures de la chaîne d'approvisionnement et le départ de son responsable sécurité des systèmes d'information (RSSI).

Ces exemples illustrent combien l'incapacité à revenir rapidement à la normale augmente de façon exponentielle le coût d'une cyberattaque. Dans un monde digital « always on », la cyber-résilience doit donc constituer une priorité absolue.

Cyber-résilience : définition et enjeux

La cyber-résilience désigne la capacité d'une organisation à se préparer, à gérer et à récupérer d'une cyberattaque ou d'une compromission de données, tout en continuant à opérer avec efficacité. L'Institut national des normes et de la technologie (NIST) des États-Unis définit la cyber-résilience comme « la capacité d'anticipation, de résistance, de récupération et d'adaptation face à des conditions hostiles, des pressions, des attaques ou des compromissions de systèmes qui utilisent ou dépendent de ressources cyber ».

Pour contrer les menaces actuelles, les entreprises doivent impérativement se doter de capacités robustes de cyber-résilience. Lorsque les mesures préventives ne suffisent pas à bloquer une cyberattaque, la viabilité de l'entreprise dépend de sa capacité à répondre et à rebondir rapidement.

Dans une enquête réalisée en *2024 sur le coût horaire des interruptions de service*, le cabinet Information Technology Intelligence Consulting (ITIC) a découvert que le coût moyen d'une seule heure d'interruption dépasse désormais 300 000 $ pour plus de 90 % des grandes et moyennes entreprises.

Outre les dégâts causés par l'attaque elle-même, il est impossible d'éviter les interruptions de service, qu'elles découlent directement de l'attaque (dans le cas d'un ransomware ou d'une attaque par déni de service), des mesures de réponse à incident déclenchées (notamment l'endiguement et l'éradication) ou des deux. Pour preuve, lors de l'attaque par ransomware contre l'acteur de l'énergie Colonial Pipeline en mai 2021, le PDG a décidé, à juste titre, de débrancher immédiatement les systèmes critiques touchés afin d'endiguer la propagation du ransomware. Malgré une réponse rapide et efficace, combinée au paiement d'une rançon de 4,4 millions de dollars, l'entreprise a mis plusieurs jours à reprendre des activités normales. Et les répercussions ont

perturbé toute la côte Est américaine, où les pénuries de carburant ont forcé quatre États (Virginie, Caroline du Nord, Géorgie et Floride) à déclarer l'état d'urgence.

En somme, plus l'entreprise met du temps à se relever, plus le coût de l'attaque est élevé. Les interruptions de service ont un impact négatif non seulement sur vos activités et vos clients, mais aussi parfois sur l'ensemble de la chaîne d'approvisionnement, comme le démontre la mésaventure de Colonial Pipeline. **Ainsi, qui dit résilience du cyber, dit résilience de toute l'entreprise.**

Continuité opérationnelle en situation de crise : repensez votre stratégie

Les acteurs de la cybersécurité ont toujours travaillé d'arrache-pied pour renforcer les murailles et élargir les douves autour des différentes couches d'infrastructure (terminaux, réseau, applications, etc.) dans l'espoir de bloquer les attaques. Pour chaque méthode d'attaque identifiée, un nouvel outil de prévention soi-disant indispensable voit le jour. Sauf que la prévention ne se suffit pas à elle-même, aussi vitale soit-elle. Aujourd'hui, les applications sont décentralisées et distribuées entre des environnements multicloud et hybrides, ce qui les rend particulièrement difficiles à sécuriser au moyen de défenses traditionnelles. Pour mieux récupérer après une cyberattaque, les organisations doivent faire de la cyber-résilience une priorité, sans toutefois la limiter à la seule sécurité de l'infrastructure. Ce sont les données elles-mêmes qui doivent être sécurisées, car de leur sécurité et de leur disponibilité dépend la continuité opérationnelle de l'entreprise.

CHAPITRE 2

Les défis de la protection des données dans le cloud

Dans le cloud, la protection des données présente des difficultés inhérentes à l'environnement lui-même. L'un des attraits du cloud est la facilité avec laquelle il permet de déployer des ressources. Or, c'est cette flexibilité même qui favorise l'éparpillement de données entre de multiples comptes, régions, services et clouds. Il devient alors difficile de savoir quels assets sont protégés et par quels moyens. Mais surtout, il est très compliqué d'identifier les assets non protégés. Les cyberattaquants le savent. Et c'est exactement pour cela qu'ils ciblent de plus en plus les données situées dans le cloud.

L'expansion du cloud étend considérablement votre surface d'attaque

Même en matière de cloud, il ne faut pas abuser des bonnes choses. Malgré les nombreux avantages de la technologie, son expansion constitue aujourd'hui un véritable fléau pour les entreprises. En plus d'être coûteux, ce phénomène accroît grandement la surface d'attaque et le risque d'erreur de configuration, deux facteurs qui tendent à faciliter la compromission des données.

Le « cloud sprawl » découle généralement de données « fantômes » (Shadow Data), c'est-à-dire de données créées, stockées ou partagées sans gestion ni protection formelle de la part des équipes IT et sécurité. Au sein d'une même entreprise, les différents métiers ou services peuvent faire appel à des fournisseurs cloud distincts pour répondre à leurs besoins spécifiques. Par exemple, les développeurs préfèrent l'écosystème robuste de Google Cloud Platform (GCP), tandis que l'équipe marketing s'oriente plutôt vers Amazon Web Services (AWS) pour la facilité d'utilisation et la familiarité de l'Amazon Marketplace. Quant à l'équipe infrastructure et opérations (I&O), elle tend à déployer ses systèmes sur Microsoft Azure pour profiter de la large gamme de services Windows.

Conséquence : des comptes, des tenants et des abonnements silotés, conjugués à des contrôles d'accès utilisateur et des politiques de sécurité disparates. Sans une image claire et unifiée de la posture de sécurité pour tous les services cloud, les failles deviennent inévitables. Au-delà du danger pour les données, ce manque de visibilité et de contrôle complique aussi le respect des réglementations en vigueur.

Le cloud, cible privilégiée d'un nombre croissant d'attaques

Aujourd'hui, malheureusement, la question n'est pas de savoir si, mais bien quand votre entreprise sera victime d'une cyberattaque. Le cloud ne fait hélas pas disparaître ces problèmes d'un coup de baguette magique. En 2022, 94 % des tenants cloud ont été ciblés chaque mois par des attaques, et 62 % d'entre eux ont été compromis. Les ransomwares, en particulier, sont de plus en plus répandus. D'après Gartner Inc., 75 % des organisations seront confrontées à une attaque par ransomware d'ici 2025.

Les cybercriminels emploient de plus en plus des techniques de « double extorsion », qui consistent à menacer de publier les données sensibles d'une organisation si cette dernière refuse de payer une somme supplémentaire. Certains vont encore plus loin : ils lancent une attaque par déni de service

(DoS) ou extorquent une rançon supplémentaire directement auprès des individus dont les données personnelles ont été compromises lors du premier assaut. On parle alors de « triple extorsion ».

Autre mauvaise nouvelle, l'essor du Ransomware-as-a-Service (RaaS) abaisse les barrières à l'entrée aux apprentis cybercriminels peu versés dans les techniques du ransomware. Des prestataires RaaS peuvent ainsi monter et/ou exécuter une attaquant pour un commanditaire contre une somme forfaitaire ou une commission sur les gains. Beaucoup vont même jusqu'à proposer un support technique, des services de recouvrement et d'autres prestations à valeur ajoutée.

Certaines entreprises décident de payer la rançon pour récupérer leurs données. Un choix risqué. En effet, le paiement de la rançon ne garantit pas que le cybercriminel tiendra sa promesse. Loin de là : dans son rapport 2023, Rubrik Zero Labs observe que seules 16 % des entreprises ayant versé une rançon ont pu récupérer la totalité de leurs données. Pour 46 % d'entre elles, seule la moitié ou moins des données ont été restaurées. Avant de prendre une telle décision, demandez conseil à des juristes et aux pouvoirs judiciaires.

Toutes les mesures de prévention que vous prenez maintenant détermineront 1) les chances de réussite d'une attaque et 2) son impact sur votre entreprise si elle parvient à percer vos défenses. Une stratégie de cyber-résilience est l'un des meilleurs remparts contre les effets des cyberattaques.

CHAPITRE 3

Cyber-résilience : comment font les autres ?

Force est de constater que la prévention ne se suffit pas à elle même et qu'il devient de plus en plus difficile de protéger les données dans le cloud. D'où la question : comment font les autres ? Dans ce chapitre, nous verrons les quatre approches les plus courantes de la cyber-résilience à l'heure actuelle.

Inaction

La première solution de sauvegarde et de récupération n'est pas vraiment à considérer comme telle. Pourtant, de nombreuses organisations pensent, à tort, qu'il suffit de migrer leurs données vers le cloud pour assurer leur protection et leur cyber-résilience. Bref, elles décident de ne rien faire. Un postulat dangereux, qui s'appuie sur des idées reçues malheureusement courantes :

- **Un modèle de partage de responsabilité.** Tous les fournisseurs de cloud public suivent un modèle de partage de responsabilité (voir exemple à la **FIGURE 1**) qui définit qui, du fournisseur ou du client, est garant de quels composants de la stack technologique – infrastructure physique, réseau, virtualisation, systèmes d'exploitation, applications, données, etc.

> Naturellement, ses spécifications varient quelque peu selon les fournisseurs et les modèles de service, à savoir Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) ou Infrastructure-as-a-Service (IaaS). On observe néanmoins une constante : le client est toujours responsable de ses propres données.

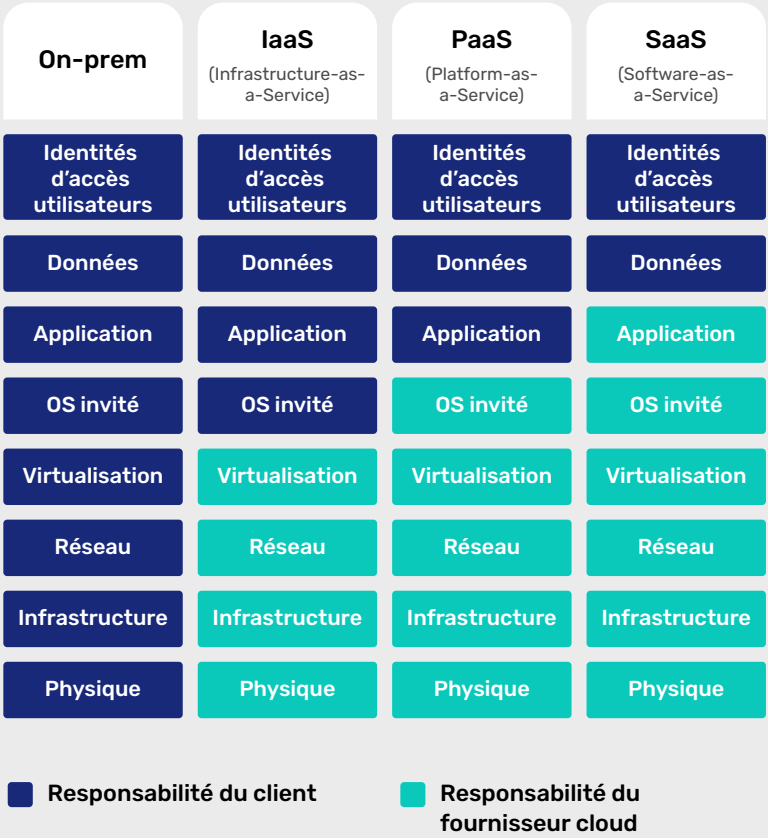


FIGURE 1 : Exemple de modèle de partage de responsabilité

- **Une haute fiabilité.** Les principaux fournisseurs de services cloud (CSP) offrent tous une infrastructure et des services robustes, avec une disponibilité à 99,999 % (ou plus) et une durabilité à 99,999999999 % pour garantir l'intégrité des données. Avec un tel niveau de fiabilité, impossible de perdre des données, n'est-ce pas ? Faux : fiabilité n'est pas forcément synonyme de cyber-résilience. La première réduit au minimum les interruptions des systèmes critiques dues aux pannes matérielles (par exemple, d'un disque dur ou d'un serveur). La seconde, en revanche, permet de s'assurer que votre entreprise est capable de détecter, de gérer et de récupérer d'un incident de sécurité. C'est là qu'est toute la différence.

- **Un manque de préparation de votre part ne constitue pas une urgence pour le CSP.** Certes, ce dernier sauvegarde les données et les réplique dans d'autres data centers et régions. Mais ne vous y méprenez pas : il le fait seulement pour remplir ses accords de niveau de service (SLA) et garantir sa propre cyber-résilience, pas la vôtre. De plus, les fournisseurs cloud ne font rien pour assurer la validité des données. Si vos données originales ont déjà été chiffrées par un cybercriminel, alors la copie de sauvegarde répliquée le sera aussi. Un acteur interne a volontairement supprimé des fichiers critiques ? Un hacker externe a détourné un compte privilégié pour chiffrer vos données ? Votre CSP ne vous aidera pas à les récupérer.

Méthode maison (DIY)

Plutôt que de ne rien faire, certaines entreprises choisissent de concevoir elles-mêmes leur solution de sauvegarde et de récupération. Ces outils maison se composent de logiciels développés sur mesure et de solutions basées sur des scripts, lesquels ont été pensés pour répondre précisément aux exigences

de l'entreprise. Toutefois, leur complexité et leur fonctionnalité varient grandement. Mis à part une personnalisation et un contrôle granulaires, ils présentent néanmoins des désavantages non négligeables :

- **Coût (direct et indirect).** Du développement à la maintenance et aux mises à jour, ces outils mobilisent d'énormes ressources pendant toute la durée du cycle de vie des données. Pire encore, ils détournent des compétences rares et coûteuses (vos développeurs d'applications) des missions stratégiques qui sous-tendent vos cœurs de métier.

- **Scalabilité.** Beaucoup de solutions développées en interne sont spécifiquement conçues pour résoudre un problème précis, comme la sauvegarde d'un type de données dans un environnement déterminé. L'architecture applicative étant susceptible d'évoluer, voire de migrer vers un autre cloud, les outils et les scripts doivent être adaptés à chaque compte, tenant et abonnement cloud. Voilà qui complique leur scalabilité à mesure que les volumes de données augmentent et que l'infrastructure se complexifie. Enfin, n'oubliez pas que la sauvegarde de données n'a rien de très difficile en soi. Ce qui l'est davantage, c'est de programmer et gérer l'expiration de ces sauvegardes pour ne pas payer indéfiniment des frais de stockage injustifiés.

- **Sécurité et conformité.** Les solutions maison sont rarement dotées des fonctionnalités de sécurité avancées nécessaires à la réduction des risques et à la conformité réglementaire.

« Lift-and-shift » des outils on-prem existants

D'autres organisations tenteront de simplement faire migrer vers le cloud leurs outils de sauvegarde et de restauration on-prem, qu'ils soient conçus en interne ou achetés à un éditeur de logiciels. C'est ce qu'on appelle le « lift-and-shift ». Malheureusement, cette approche est souvent un frein à l'agilité et à l'élasticité qui font l'attrait même du cloud, car ces

outils d'ancienne génération ne sont pas conçus ni optimisés pour cet environnement. Ils sont par conséquent inaptes à libérer les potentialités des services cloud-native, entraînant une perte de performances et une hausse des coûts. L'autre défaut du lift-and-shift, c'est de créer un environnement fragmenté, qui requiert toute une panoplie d'outils pour protéger les données dans ses différents clouds et applications. Difficile, dans ces conditions, d'assurer une protection homogène de toutes les données d'entreprise où qu'elles soient situées. L'intégration au cloud des outils de sauvegarde on-prem d'ancienne génération présente encore d'autres problèmes, notamment :

- **Les sauvegardes traditionnelles sont vulnérables aux cyberattaques.** Les sauvegardes traditionnelles disposent rarement de fonctions robustes d'authentification et de contrôle d'accès basées sur une architecture Zero Trust garante de l'immutabilité des données. Elles constituent ainsi des vulnérabilités que les acteurs malveillants ne manquent pas d'exploiter afin d'accéder aux données sensibles, compromettant de ce fait toute la posture de sécurité de l'organisation. De plus, ces systèmes emploient souvent des protocoles de stockage ouverts, qui exposent les données à des accès non autorisés et aux acteurs malveillants susceptibles de les manipuler.

- **Les sauvegardes traditionnelles ne fournissent aucune information ni aucune visibilité sur les données à risque ou les données touchées lors d'une cyberattaque.** Résultat : en cas de cyberattaque, il peut être extrêmement compliqué de déterminer les éléments à récupérer, le moment et la portée de l'attaque, ainsi que l'étendue des dommages occasionnés. Le travail nécessaire à la reconstitution de toutes les pièces du puzzle est à la fois méticuleux et chronophage, ce qui peut sérieusement retarder le processus de restauration. Or, faute de pouvoir identifier des sauvegardes intègres à une date antérieure précise, les organisations risquent d'être réinfectées par des sauvegardes compromises.

- **Les sauvegardes traditionnelles ne sont pas prévues pour le cloud.** Alors que le cloud est ultra dynamique par nature, les environnements on-prem sont relativement statiques.

> Prise en charge nulle ou limitée des opérations par API et de l'Infrastructure-as-Code (IaC) ; incompatibilité avec les configurations cloud-native, les métadonnées et les composants sans état ; absence d'optimisation pour les contraintes de latence réseau et de bande passante du cloud… toutes ces lacunes rendent les outils de sauvegarde d'ancienne génération particulièrement inadaptés au cloud.

Outils de sauvegarde cloud natifs des CSP

Enfin, de nombreuses organisations s'en remettent simplement aux outils natifs de sauvegarde et de restauration offerts par leur fournisseur cloud. L'avantage étant qu'ils sont spécialement conçus et optimisés pour la sauvegarde de données dans les environnements du fournisseur cloud. En plus d'offrir des fonctionnalités basiques, voire avancées, de sauvegarde et de récupération, ces outils s'assimilent facilement aux autres services du CSP. Ils représentent donc le choix privilégié des entreprises voulant se doter de capacités essentielles de sauvegarde dans le cloud. Cette simplicité est l'une des principales raisons pour lesquelles les organisations se tournent vers les outils natifs de leur fournisseur cloud. Mais la facilité ne fait pas tout, loin s'en faut.

Certaines organisations pensent pouvoir se contenter du minimum en optant pour les outils de sauvegarde et de restauration fournis par leur CSP. Sauf que votre entreprise et ses données critiques exigent mieux que le minimum pour se protéger contre les menaces.

S'il peut sembler pratique et logique d'adopter la solution de sauvegarde native à la plateforme cloud dans laquelle vous avez investi, ce type d'outil pèche souvent par son manque de flexibilité, d'évolutivité et de fonctionnalités – des atouts pourtant essentiels à la cyber-résilience des données critiques dans le cloud. De plus, les outils natifs peuvent être eux aussi peu intuitifs, voire complexes. Sans oublier, évidemment, qu'ils ne protègent que les données dans l'environnement cloud en question, négligeant celles stockées dans les autres clouds ou dans les data centers on-prem. Parmi les autres défauts des outils de sauvegarde natifs figurent :

- **Le manque de support des environnements multicloud ou hybrides.** En général, les outils cloud-native sont conçus et optimisés pour leur propre environnement, qu'il s'agisse d'AWS, de GCP ou de Microsoft Azure. Or, cette restriction constitue souvent un obstacle à la gestion des sauvegardes et à une restauration transverse à plusieurs clouds, applications SaaS et infrastructures on-prem. Et si certains prennent en charge d'autres environnements cloud, leur fonctionnalité reste néanmoins limitée, sans compter les frais occasionnés pour la sortie des données.

- **Une gestion fragmentée.** Même au sein d'un même environnement cloud, leur approche fragmentée de la gestion des workloads impose une administration et une configuration individuelles de chaque compte cloud, ce qui rend difficile la protection complète des données. Par ailleurs, ces outils peuvent changer d'approche en fonction des types de workload. Ainsi, certaines sauvegardes ressemblent à des snapshots, d'autres à des sauvegardes de base ; certaines sont immuables, d'autres non ; certaines peuvent être stockées à long terme, d'autres non… Bref, un vrai casse-tête.

- **Des analyses de sécurité limitées.** Les outils de sauvegarde cloud-native ne possèdent pas les fonctions d'analyse des menaces et de gestion de la posture de sécurité nécessaires à la détection d'activités suspectes, de cyberattaques potentielles ou de risques pour les données sensibles.

- **Les coûts de stockage des sauvegardes.** Rares sont les outils cloud-native optimisés pour stocker les données de sauvegarde de façon économe. Résultat, la facture finit parfois par dépasser celle du stockage des données originales. À titre d'exemple, le service AWS Backup coûte 0,05 $/Go/mois pour les données de sauvegarde S3, soit plus du double du coût de stockage des données originales (0,022 $/Go/mois).

CHAPITRE 4

Une meilleure solution pour la cyber-résilience cloud

Inaction, méthode maison, lift-and-shift des solutions existantes, services natifs du CSP… les approches traditionnelles de la protection des données sont rarement à la hauteur des besoins des organisations. Ce dont ces dernières ont besoin, ce sont des fonctionnalités de recherche et de récupération de fichiers individuels, de sauvegarde protégée par air-gap logique, sans oublier des capacités de sécurité avancées comme la détection de données sensibles – soit autant d'atouts indispensables à une vraie cyber-résilience dans le cloud. Le constat est sans appel : un changement d'approche s'impose. Mais quels sont les critères de sélection d'une solution de cyber-résilience cloud ? Dans l'idéal, elle devrait être conçue pour offrir les fonctionnalités suivantes :

- Protection simplifiée et unifiée
- Cyber-résilience holistique
- Récupération rapide
- Faible coût total de possession (TCO)

Protection simplifiée et unifiée

Avec l'essor des services de cloud public en entreprise, il devient plus difficile de créer une sauvegarde de référence (baseline) pour des dizaines, voire des centaines, de comptes et d'abonnements cloud. Une mesure pourtant nécessaire à la cyber-résilience et à la conformité réglementaire. Dans des environnements d'une telle envergure, l'implémentation de politiques implique inévitablement de faire appel à l'équipe IT pour effectuer des tâches manuelles chronophages de programmation ou d'écriture de scripts. Afin de satisfaire les exigences propres aux différentes composantes de leurs métiers, les entreprises recourent à de multiples solutions, donnant ainsi naissance à des environnements multicloud et hybrides. Un tel patchwork requiert toutefois des compétences spécialisées. Il faut en effet pouvoir configurer et jongler avec des outils et des ressources cloud disparates, ce qui hélas se traduit souvent par des erreurs de configuration, des pertes d'efficacité opérationnelle et des failles dans la protection des données.

Par contraste, la solution de cyber-résilience cloud idéale se présente sous la forme d'une plateforme unique couvrant les environnements multicloud et hybrides, y compris les applications SaaS et les data centers on-prem. Bien sûr, une compatibilité avec les plus grands fournisseurs de cloud public est essentielle, notamment AWS, GCP et Microsoft Azure, entre autres. Par ailleurs, la solution doit détecter et sécuriser de façon automatique les workloads cloud, ainsi que les applications SaaS et on-prem. Un centre de commande, en somme, pour paramétrer vos politiques de protection des données, visualiser les sauvegardes, restaurer les données, mais aussi assurer la conformité et la préparation aux audits. Enfin, optez pour une solution qui permette une administration hors bande, afin que votre stack de protection des données s'exécute indépendamment de celle de production.

Selon une enquête menée par Rubrik Zero Labs en 2023, neuf organisations sur dix ont été victimes d'une cyberattaque impliquant une tentative d'accès à leurs données de sauvegarde. Plus terrifiant encore, les cybercriminels y sont parvenus (au moins en partie) dans 73 % des cas.

Cyber-résilience holistique

Votre solution de cyber-résilience cloud doit garantir l'intégrité et la disponibilité de vos données cloud. Comment ? Par des sauvegardes automatiques et immuables, sous contrôle d'accès, protégées par air-gap et conçues pour résister aux cyberattaques, aux acteurs internes malveillants et aux perturbations opérationnelles, quelle que soit la source de données. Impossible d'instaurer une cyber-résilience solide sans des fonctionnalités d'identification précise des données sensibles et de surveillance continue des données à la recherche d'anomalies et de menaces (ransomwares, destruction, indicateurs de compromission, etc.), tout en vous informant sur les données exposées et à risque. Autant d'atouts qui maximisent la posture de sécurité des données et permettent de déterminer le périmètre d'une attaque et les éventuelles données exposées, ce qui s'avère crucial lorsque l'entreprise est soumise à des réglementations telles que le Règlement général pour la protection des données (RGPD) dans l'Union européenne et le California Consumer Consumer Privacy Act (CCPA) aux États-Unis. Les deux textes imposent en effet de notifier les autorités compétentes de toute compromission de données sensibles à caractère personnel dans des délais très courts.

Architecture pensée pour le cloud

Votre solution de cyber-résilience cloud doit non seulement être cloud-native, mais aussi conçue selon les principes suivants :

- **Software-Defined** – Consolidez des composants matériels et logiciels disparates en une fabric unifiée et flexible, qui couvre aussi bien les appliances plug-and-play on-prem, que les logiciels sur des équipements tiers ou les applications cloud.

- **Simplicité à grande échelle** – Gérez facilement des volumes d'informations à croissance exponentielle grâce à une architecture à scalabilité linéaire qui élimine toute complexité d'administration.
- **Mobilité cloud** – Qu'elles soient déployées on-premise ou dans un cloud public, Rubrik protège vos applications cloud-native, décortique vos applications et fichiers à la recherche de données, et démarre rapidement des instances de test et de développement ou de reprise après sinistre.
- **Conception API-first** – Facilement extensible, votre solution doit simplifier l'exploitation des API grâce à une documentation OpenAPI standard, des échantillons de code et des intégrations clé en main à divers outils d'automatisation
- **Sécurité intégrale** – Protégez l'ensemble du cycle de vie des données à l'aide d'une approche multidimensionnelle de la sécurité : chiffrement des données en transit et au repos, nombre illimité de snapshots immuables, contrôles d'accès granulaires et plus encore.

Récupération rapide

Pour restaurer une seule instance de workload dans le cloud, les équipes IT doivent souvent s'engager dans un processus manuel en plusieurs étapes, qui diffère selon le service et le fournisseur. Plus les processus requièrent d'interventions, plus ils sont longs et s'exposent au risque d'erreur humaine, retardant la restauration des données et le retour à la normale.

Pour sortir de cette impasse, choisissez une solution de cyber-résilience cloud dotée de fonctionnalités de recherche globale et de récupération individuelle des fichiers sur l'ensemble des données de sauvegarde cloud. À la clé, une restauration granulaire des applications, des fichiers et des objets en quelques clics, pour un RTO quasi instantané. L'équipe de réponse à incident a besoin d'identifier rapidement la première sauvegarde saine, sans devoir valider chaque instance à la main, afin que les workloads soient restaurés en toute confiance et l'environnement de production protégé de toute réinfection.

Réduction du TCO

À l'heure où les services de cloud public ont le vent en poupe, le phénomène de « cloud sprawl » s'impose comme un problème majeur, notamment par la hausse des coûts associés au stockage cloud. Face à une telle envolée, les entreprises cherchent à optimiser leur utilisation du cloud pour maîtriser leurs dépenses, y compris les coûts directs tels que les ressources de calcul nécessaires à la sauvegarde, l'indexation, l'archivage et la récupération des données. Pour les accompagner dans cette démarche, la solution de cyber-résilience idéale devra permettre de stocker les sauvegardes dans des environnements plus économiques de type AWS S3 Glacier et Azure Blob Archive, de réaliser des sauvegardes incrémentielles et non complètes, mais aussi de capitaliser sur des fonctionnalités de réduction des données comme la compression et la déduplication.

Coté baisse des coûts indirects, il existe également plusieurs leviers de rationalisation au niveau de la configuration des politiques de sécurité, de la gestion de la restauration des données, de la surveillance des menaces et du reporting de conformité. Le temps et les ressources ainsi économisés peuvent être réaffectés à d'autres priorités stratégiques.

Conclusion

Ce guide démontre à quel point la cyber-résilience cloud est indispensable à la protection des données d'entreprise dans les environnements multicloud et hybrides. Entre des menaces qui ne cessent d'évoluer et des surfaces d'attaque en constante expansion, les cybercriminels ont toutes les chances de leur côté pour parvenir à leurs fins. D'où l'importance d'un changement radical dans les approches de la protection de données. La nouvelle réalité impose une plateforme cloud-native simple et unifiée, avec des fonctionnalités de cyber-résilience holistique et de récupération rapide, tout en enrayant la spirale des coûts associés au cloud.

Pour continuer d'explorer l'approche Rubrik de la cyber-résilience cloud, retrouvez nos articles, webinaires, démonstrations et autres contenus sur la page https://www.rubrik.com/solutions/cloud-solutions.

À PROPOS DE RUBRIK

Rubrik aide les entreprises à contrôler leurs données pour renforcer leur résilience, améliorer leur mobilité cloud et les accompagner dans leurs obligations de conformité. Grâce à sa structure « software-defined » et son plan de gestion unifié pour l'ensemble de vos données, sur site comme dans le cloud, Rubrik fait le lien entre les infrastructures installées on-prem et le cloud en découplant les données du data center. L'accès instantané, l'orchestration automatisée et les fonctions professionnelles de protection et de résilience des données permettent une gestion in extenso.

À PROPOS D'ACTUALTECH MEDIA

Entreprise du groupe Future B2B, ActualTech Media se spécialise dans le marketing B2B pour mettre en relation les fournisseurs de solutions informatiques d'entreprise et les acheteurs par le biais de programmes innovants de lead generation et de services de contenus personnalisés à fort impact.

L'équipe d'ActualTech Media parle la langue des professionnels de l'IT, car elle a été à leur place.

Notre équipe dirigeante est composée d'anciens DSI, responsables informatiques, architectes, spécialistes et professionnels du marketing. Ainsi, nos clients passent moins de temps à expliquer en quoi consistent leurs technologies pour se concentrer sur la création de stratégies génératrices de résultats.

Vous êtes spécialiste du marketing IT et voudriez un Gorilla Guide® sur votre entreprise ? Rendez-vous sur actualtechmedia.com.