O'REILLY®
Report

Le bilan de la cyber-résilience

Une nouvelle stratégie pour survivre dans un environnement de menaces agentiques

Govind Rangasamy

Commvault

Visit commvault.com

97 9 834 18 5 986 5

Le bilan de la cyber-résilience

Une nouvelle stratégie pour survivre dans un environnement de menaces agentiques

Govind Rangasamy

O'REILLY®

Le bilan de la cyber-résilience
par Govind Rangasamy

Publié par O'Reilly Media, Inc., 141 Stony Circle, Suite 195, Santa Rosa, CA 95401.

Les livres O'Reilly peuvent être achetés à des fins pédagogiques, commerciales ou promotionnelles. Des éditions en ligne sont également disponibles pour la plupart des titres (https://oreilly.com). Pour plus d'informations, contactez notre service commercial entreprises / institutions : + 1 800-998-9938 ou corporate@oreilly.com.

Responsable des acquisitions: Simina Calin
Concepteur éditorial: Michele Cronin
Éditeur de production: Jonathon Owen
Réviseur: Paula L. Fleming
Concepteur de couverture : Susan Brown
Illustrateur de couverture: Ellie Volckhausen
Concepteur de contenu: David Futato
Illustrateur de contenu: Kate Dullea

Septembre 2025: Première édition

Historique des révisions de la première édition
2025-09-19: Première version

Ce travail s'inscrit dans le cadre d'une collaboration entre O'Reilly et Commvault. Voir notre déclaration d'indépendance éditoriale.

979-8-341-65986-5

[LSI]

Table des matières

Remerciements

Je tiens à remercier Katherine Demacopoulos pour ses efforts fantastiques dans tous les aspects de ce livre ; Anna Griffin pour avoir reconnu la nécessité de cet ouvrage sur le marché et pour l'avoir sponsorisé ; et Chris DiRado pour son expertise et son assistance en matière de sécurité.

À ma femme, Bhuvana, et à mes incroyables fils, Pranav et Sanjit : vous me rappelez chaque jour ce qui compte vraiment. Votre amour, votre curiosité, vos blagues et vos câlins m'ont donné la joie et l'énergie nécessaires pour continuer.

CHAPITRE 1

La cyberattaque se profile. Êtes-vous en mesure de procéder à une récupération en toute confiance

L' élément vital d'une organisation transite par ses réseaux, ses applications et ses magasins de données. Ces systèmes vitaux sont confrontés à des menaces croissantes, car les cyberattaques deviennent plus fréquentes et plus sophistiquées. Les cybercriminels déploient déjà des outils sophistiqués optimisés par l'IA, mais une menace bien plus dangereuse est en train d'émerger. L'intelligence artificielle (IA) agentique, capable de raisonner, de planifier et d'agir de manière autonome, va révolutionner les tactiques de la cybercriminalité, rendant les attaques plus évolutives et plus efficaces.

Contrairement aux ransomwares classiques, qui suivent des scénarios préprogrammés, l'IA agentique peut adapter sa stratégie en temps réel, en apprenant des réponses défensives et en faisant évoluer les attaques plus rapidement que les défenseurs humains ne peuvent riposter.

Des incidents très médiatisés montrent qu'aucun secteur ni aucune région du monde n'est à l'abri. Nous avons observé des exemples allant de l'empoisonnement d'une usine de traitement de l'eau en Floride et de la fermeture pendant 11 jours du système d'oléoduc américain Colonial Pipeline, jusqu'à la paralysie de districts scolaires causée par des attaques de ransomwares et au cryptage en masse des systèmes d'hôtels et de casinos.

Même les défenses périmétriques les plus renforcées et les programmes avancés de renseignement en matière de menaces, comme le Financial Services Information Sharing and Analysis Center (FS-ISAC) et la US Cybersecurity & Infrastructure Security Agency (CISA), ne représentent que la partie émergée de l'iceberg. Les adversaires d'aujourd'hui sont bien financés, extraordinairement patients et focalisés sur la désactivation de la capacité de récupération de l'organisation visée.

Comprendre l'environnement actuel des cybermenaces : l'industrialisation de la cybercriminalité

Il y a quelques années encore, les attaques par ransomware étaient largement limitées à une poignée de groupes de hackers sophistiqués. Aujourd'hui, les plateformes de *ransomware en tant que service* (RaaS) sont disponibles sur le darknet et peuvent être louées par tout criminel moyennement qualifié. Le modèle économique RaaS fonctionne comme n'importe quelle plateforme de logiciel en tant que service (SaaS) d'entreprise, offrant des frais d'abonnement et des accords de partage des revenus qui rendent la cybercriminalité accessible à toute personne disposée à payer.

Ces entreprises criminelles fournissent un accès clé en main à des cadres d'extorsion sophistiqués, complété par des centres d'appels pour l'assistance aux victimes, une aide à la négociation des rançons et même des « garanties » de suppression des données si les victimes refusent de payer. Cette approche à l'échelle industrielle a entraîné une explosion des attaques. Les criminels n'ont plus besoin de développer leurs propres logiciels malveillants. Ils peuvent simplement faire leur choix dans un menu : LockBit, REvil, DarkSide, Conti, BlackCat et des dizaines d'autres.

Chaque option offre différentes fonctionnalités spécialisées conçues pour maximiser les dommages et l'effet de levier. Les variantes de

ransomwares modernes exfiltrent régulièrement les données avant le chiffrement pour menacer la divulgation publique, ciblent et détruisent systématiquement les systèmes de sauvegarde pour éliminer les options de récupération et déploient des charges utiles capables d'effacer des réseaux entiers ou des comptes cloud en quelques minutes.

Ransomware d'IA agentique : quand les attaques pensent, apprennent et s'adaptent

L'émergence de l'I. agentique marque un changement fondamental au-delà des plateformes RaaS classiques. Contrairement à l'IA générative, qui aide à accomplir des tâches spécifiques, l'IA agentique est proactive, peut résoudre des problèmes complexes et prendre des décisions de manière autonome. Ces agents d'IA ne se contentent pas d'exécuter simplement des attaques préprogrammées. Ils apprennent et adaptent leurs stratégies en fonction de l'environnement spécifique qu'ils rencontrent. Par exemple, lors de tests contrôlés, les chercheurs d'Unit 42 ont démontré une attaque complète, du compromis initial à l'exfiltration des données, en seulement 25 minutes. Le différentiel de vitesse est stupéfiant : alors que les attaquants humains ont eu besoin de deux jours (en moyenne) pour effectuer l'exfiltration des données, les attaques assistées par l'IA ont atteint le même objectif environ 100 fois plus rapidement.

Double extorsion et au-delà : Des attaques qui vont encore plus loin

Les ransomwares modernes suivent souvent un scénario en deux phases :

1. Exfiltrer les données sensibles.
2. Chiffrer les systèmes critiques.

Même si une victime dispose de sauvegardes dans un deuxième cloud régional hors site, la menace d'une exposition publique des données sensibles exerce une pression immense pour payer. Fin 2024, la violation de LastPass a exposé les sauvegardes de coffres-forts chiffrés de millions d'utilisateurs, et même si les mots de passe principaux sont restés en sécurité, le fait même qu'un attaquant détienne une copie de chaque coffre-fort a créé une crise de confiance.

Pendant ce temps, les acteurs étatiques déploient des ransomwares non pas à des fins lucratives, mais pour avoir un impact stratégique, par exemple en fermant les opérations clés des pipelines, des services publics, des systèmes de santé et des services gouvernementaux à grande échelle, affectant directement les technologies opérationnelles

L' attaque par ransomware WannaCry de 2017 en est une illustration frappante. Elle a gravement perturbé les systèmes hospitaliers du National Health Service du Royaume-Uni, entraînant l'annulation de procédures médicales et le détournement d'ambulances. Cette attaque démontre clairement comment les cyberattaques peuvent mettre des vies en danger lorsque des infrastructures critiques tombent en panne.

L'omniprésence des cibles

La démocratisation de l'IA agentique par le biais de plateformes accessibles a brisé toute illusion selon laquelle certaines industries pourraient être à l'abri des attaques. L'IA agentique peut aider à planifier les attaques et à les mener de manière autonome, ce qui rend les attaques plus évolutives et plus efficaces tout en réduisant la barrière d'entrée pour les cybercriminels :

- *Éducation:* En 2022, Vice Society a pris en otage les données du district scolaire unifié de Los Angeles, touchant plus de 1 000 écoles et 600 000 élèves.

- *Énergie:* La même année, Suncor Energy au Canada a vu des ransomwares mettre hors service ses systèmes de cartes Petro-Canada, bloquant les conducteurs aux pompes à essence dans tout le pays.

- *Hôtellerie:* En 2024, BlackCat a attaqué MGM Resorts, mettant hors service les machines à sous et les réservations dans 30 établissements.

- *Commerce de détail et services:* En avril 2025, Marks & Spencer au Royaume-Uni a dû fermer des magasins lorsque DragonForce a chiffré ses systèmes commerciaux, et Mailchimp et SendGrid ont subi des campagnes d'hameçonnage mondiales.

La morale est claire : nos adversaires ont à la fois les outils et les motivations pour frapper n'importe où. À mesure que la transformation numérique s'accélère, connectant toujours plus d'appareils, de processus et de partenaires, la surface d'attaque augmente. L'époque où l'informatique pouvait isoler les « systèmes critiques » derrière un pare-feu semblable à une forteresse est révolue. Chaque point de terminaison, chaque service de cloud et chaque intégration tierce est un point d'entrée potentiel. En outre, l'interface humaine elle-même, que ce soit par le biais d'un appel deepfake convaincant généré par l'I.A. ou d'un employé utilisant un appareil personnel compromis pour le travail, peut devenir une passerelle efficace pour un attaquant.

Pourquoi les entreprises sont-elles encore surprises par les attaques

Malgré les preuves croissantes d'une vulnérabilité accrue face aux cybermenaces, de nombreuses entreprises continuent d'être prises au dépourvu. Cette vulnérabilité persistante découle d'hypothèses profondément ancrées sur la cybersécurité, qui ne correspondent plus à la réalité actuelle. Trois angles morts critiques (un état d'esprit axé uniquement sur la prévention, des équipes et des runbooks en silos, et une croyance en la résilience du cloud) rendent vulnérables même les entreprises les mieux protégées.

Une mentalité uniquement axée sur la prévention : quand la confiance devient trompeuse

Historiquement, la cybersécurité a évolué par vagues distinctes. Pour chacune d'entre elles, les experts en cybersécurité pensaient avoir enfin maîtrisé la protection des informations de leurs entreprises. Le tableau 1-1 décrit cette trajectoire évolutive.

Une mentalité uniquement axée sur la prévention : quand la confiance devient trompeuse

Historiquement, la cybersécurité a évolué par vagues distinctes. Pour chacune d'entre elles, les experts en cybersécurité pensaient avoir enfin maîtrisé la protection des informations de leurs entreprises. Le tableau 1-1 décrit cette trajectoire évolutive.

Tableau 1-1. Évolution de la cybersécurité à travers des vagues distinctes

Époque	Objectif	Fausse promesse	Réalité
Années 1990	Défenses périmétriques	Les pare-feux et les routeurs périphériques empêchent les accès non autorisés.	Les attaques ont contourné les protections par le biais de l'hameçonnage, de l'ingénierie sociale et des initiés.
Années 2000	Sécurité des e-mails	Le filtrage permettrait d'éliminer les messages malveillants.	Les logiciels malveillants se cachaient dans des flux de trafic et des pièces jointes légitimes.
À partir de 2005	Sécurité du réseau	La surveillance détectait les anomalies.	Les menaces sophistiquées semblaient inoffensives jusqu'à ce qu'elles déclenchent des violations.
À partir de 2010	Protection des terminaux	L'antivirus bloquait l'exécution.	Les logiciels malveillants sans fichier et les exploits zero-day ont contourné la détection de signature.
À partir de 2015	Sécurité de l'identité	La confiance zéro n'autorise que l'accès authentifié.	Les jetons volés, les clés API et les autorisations mal configurées ont créé des lacunes.
À partir de 2020	Sécurité du cloud	Les fournisseurs s'occupaient de la sécurité.	Les attaques ciblaient les autorisations cloud et les registres de conteneurs mal configurés.

Malgré la recrudescence des cybermenaces, de nombreuses entreprises restent enfermées dans un état d'esprit mettant la priorité sur la prévention. Nous investissons massivement dans les pare-feux de nouvelle génération, la détection et la réponse des points de terminaison (EDR), les plateformes de gestion des informations et des événements de sécurité (SIEM), les flux de menaces et les exercices d'équipe rouge (red team), pour finalement découvrir que ces contrôles sont nécessaires mais pas suffisants.

Dès qu'un attaquant s'implante, que ce soit en volant des informations d'identification, en exécutant des exploits zero-day, en pratiquant l'hameçonnage ou en compromettant la chaîne d'approvisionnement, la défense périmétrique s'effondre. La figure 1-1 illustre le modèle de défense en couches sur lequel repose la confiance de l'industrie de la cybersécurité.

Pourquoi les entreprises sont-elles encore surprises par les attaques

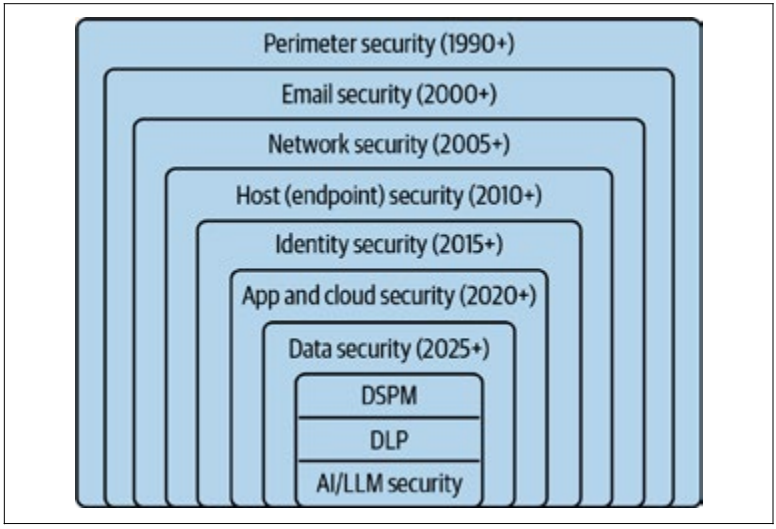

Figure 1-1 La défense en couches du secteur de la cybersécurité

Cela soulève un paradoxe : en nous concentrant excessivement sur la prévention, nous sous-investissons dans la récupération et en particulier dans les tests de récupération. Nous considérons les sauvegardes comme une simple case à cocher pour la conformité plutôt que comme un atout stratégique, et nous traitons les tests de cyber-récupération comme un exercice annuel de récupération après sinistre (DR), si nous le faisons.

Lorsque l'alarme retentit, nous nous efforçons de suivre les conseils des runbooks ad hoc, pour nous rendre compte qu'ils sont obsolètes, incomplets, non testés et incompatibles avec les environnements dynamiques d'aujourd'hui.

Équipes en silos et runbooks déconnectés

Les équipes de cybersécurité, d'exploitation du cloud, de développement d'applications, d'architecture d'entreprise et de continuité des activités travaillent souvent en silos, chacune avec ses propres processus, outils et priorités.

Le résultat ? Les politiques et les runbooks sont conservés dans des présentations PowerPoint, des documents Word et des systèmes de tickets et sont rarement, voire jamais, utilisés lors d'une véritable crise. Les connexions et les dépendances entre les applications, les configurations réseau, les systèmes d'identité, les référentiels GitHub, les registres de conteneurs, les serveurs de base de données et les copies de sauvegarde des données sont rarement documentées.

Il n'y a rien de pire que de découvrir un élément manquant lors de votre première tentative de reconstruction.

Illusions de la résilience du cloud

De nombreux DSI, DTO et RSSI pensaient que le passage au cloud au prétexte de la transformation numérique résoudrait comme par magie le problème de la récupération organisationnelle. Les fournisseurs hyperscale annoncent des multizones, des régions, des instantanés, des copies répliquées et des outils de sauvegarde intégrés qui promettent de réduire considérablement les temps de récupération. Pour garantir une résilience adéquate, les équipes doivent souvent associer plus d'une dizaine d'outils et de services.

L' échelle amplifie le problème. Les entreprises ne gèrent pas correctement leur posture de sauvegarde des données sur tous leurs comptes cloud. La culture du « shift left » (ou glissement vers la gauche), qui donne aux développeurs une plus grande responsabilité opérationnelle, a sans doute créé plus de risques qu'elle n'en a atténué.

Les fournisseurs hyperscale continuent de publier davantage de services et d'outils pour faciliter le modèle de libre-service, mais ce modèle même a conduit à des processus défaillants, laissant finalement les entreprises exposées à des risques encore plus grands. Ces lacunes deviennent évidentes sous pression. Dans un cas récent, une société de

services financiers a tenté de basculer vers une deuxième région après une violation simulée, mais elle a constaté que les clés de chiffrement des données et les rôles d'identité n'avaient pas été répliqués. Le script de « basculement de région » a échoué, laissant le site de récupération dans un état inutilisable.

Le cloud à lui seul n'est pas la solution miracle. Il exige des reconstructions entièrement testées à l'échelle de l'environnement applicatif pour s'assurer que chaque configuration, chaque identifiant et chaque objet est en place.

La résilience est impossible sans récupération

La dure réalité est que la plupart des entreprises ont bâti toute leur stratégie de cybersécurité sur une illusion dangereuse, selon laquelle elles peuvent empêcher toute attaque. Cet état d'esprit axé sur la prévention d'abord crée un faux sentiment de sécurité qui s'effondre dès qu'un attaquant franchit le périmètre.

Sans une capacité éprouvée à récupérer rapidement et complètement, même les défenses les plus sophistiquées deviennent dénuées de sens. En effet, la résilience ne consiste pas à éviter l'échec, mais à rebondir dès lors qu'il intervient.

Pourquoi les entreprises sont-elles encore surprises par les attaques

Redéfinir la résilience comme la « restauration de la confiance »

La résilience rime avec confiance. La confiance de pouvoir rallumer les lumières quand elles s'éteignent. La cyber-résilience n'est pas la disponibilité du pare-feu, ni la cadence des correctifs. C'est notre capacité à récupérer les services d'application critiques pour l'entreprise (par exemple, les portails clients, les systèmes de paiement, les lignes de production ou les dossiers médicaux électroniques) en quelques minutes ou en quelques heures plutôt qu'en quelques jours ou en quelques semaines.
La devise « La reconstruction est impérative » exige trois changements fondamentaux :

- *De la sauvegarde à la reconstruction complète de l'environnement applicatif:* L'accent doit être mis au-delà de la création de copies de fichiers et d'instantanés de blocs, pour avoir la capacité à reconstruire chaque composant de l'application (c'est-à-dire le réseau, le calcul, le stockage, l'identité et en particulier leurs dépendances) dans le but de restaurer des services critiques entiers et de les rendre opérationnels.
- *Des exercices de reprise après sinistre peu fréquents aux tests de récupération réguliers:* Au lieu d'exercices de basculement une fois par an, les équipes devraient exécuter des « exercices de reconstruction » automatisés mensuels dans des comptes cloud isolés de la production.
- *Des playbooks en silos à la récupération interfonctionnelle en tant que code (RaC):* Les équipes de sécurité, de cloud, d'architecture, de développement et de reprise après sinistre devraient s'entendre sur des runbooks partagés qui sont versionnés en tant que code et testés à l'unisson.

Et si la RaC pouvait être créée automatiquement et mise à jour régulièrement ?

Le coût de la complaisance

Lorsque des minutes d'indisponibilité peuvent coûter des milliers d'euros à une entreprise, réaliser ce qu'une journée complète hors ligne signifie vraiment s'apparente à une douche froide. Une seule journée peut avoir des conséquences dévastatrices : des pertes de revenus chiffrées en millions d'euros, des amendes réglementaires paralysantes et de graves atteintes (souvent irréparables) à la réputation.

Les détaillants sont fermés, empêchés de vendre ; les fabricants sont hors service, empêchés d'expédier ; et les hôpitaux sont paralysés, empêchés d'accéder aux dossiers vitaux des patients. Chaque minute perdue peut avoir pour conséquence un client en colère, un partenaire trahi et une marque gravement endommagée.

En revanche, les entreprises qui adoptent des stratégies de reconstruction cohérentes font état d'une réduction de leurs temps de récupération moyens de 48 heures (environ 2 jours) à moins de 2 heures et la confiance que même l'attaque la plus sophistiquée ne peut pas les empêcher de fonctionner.

C'est le retour sur investissement de la reconstruction : pas seulement une économie en numéraire, mais aussi un regain de la confiance. Le chapitre suivant approfondira le développement d'une fonction de reconstruction.

CHAPITRE 2

L'illusion de la sécurité : Pourquoi les anciennes méthodes de récupération échouent-elles et pourquoi le cadre de cybersécurité du NIST doit-il intégrer *la reconstruction*

On ne peut pas éteindre un feu de forêt avec une tasse d'eau.

—Inspiré de la sagesse des pompiers de forêt

À la fin du XIXe siècle, les ingénieurs ont construit d'imposantes digues entre les villes frontalières et le fleuve Mississippi, convaincus que leur masse pouvait retenir toute inondation. Les familles pique-niquaient au sommet de ces digues, croyant que la bataille contre l'eau était gagnée. Pourtant, lorsque le dégel printanier a déclenché des torrents sans précédent, les digues se sont fissurées comme des coquilles d'œufs et l'eau s'est déversée, inondant toute la ville.

La leçon à tirer de leurs fondations détrempées : aucune défense, aussi grande soit-elle, n'est imprenable lorsqu'elle repose sur des hypothèses erronées.

L'infrastructure numérique actuelle est confrontée à une crise similaire de confiance mal fondée. Les secteurs de la cybersécurité et de la sauvegarde ont construit leurs propres digues, chacun étant convaincu de l'adéquation de sa solution :

- Le secteur de la cybersécurité érige des barrières : périmètres, pare-feux, défenses des points de terminaison, sécurité du cloud et cadres d'identité.
- Le secteur de la sauvegarde se concentre sur les coffres-forts de données, les archives sur bande, les instantanés et les stratégies de réplication.

Pourtant, des violations de données et des incidents de ransomwares très médiatisés ont brisé cette illusion. Quelle que soit la hauteur des murs, les attaquants trouvent toujours un moyen de passer. De même, les méthodes de sauvegarde traditionnelles s'avèrent terriblement inadéquates lorsqu'il s'agit d'essayer de restaurer des écosystèmes entièrement compromis après des attaques de ransomwares modernes. Ce chapitre explorera pourquoi les approches de sauvegarde conventionnelles sont insuffisantes et pourquoi une fonction de reconstruction peut considérablement améliorer les résultats de la récupération.

La dangereuse complaisance de la sauvegarde et de la protection des données

Pendant plus de 50 ans, nous avons cru qu'il suffisait de protéger les données. Les systèmes de protection des données ont mis l'accent sur une conservation rentable et à long terme, et non pas sur la protection de l'ensemble de l'écosystème des applications. Par conséquent, lorsque les entreprises tentent une restauration après un événement de ransomware, elles découvrent fréquemment une cascade de défaillances critiques qui rendent leurs sauvegardes presque inutiles.

Par exemple, les coffres-forts de bandes préservent les fichiers, mais la restauration des serveurs prend des jours. Les sauvegardes sur disque améliorent la vitesse, mais restent exposées à des réseaux vulnérables. Les sites de récupération après sinistre promettent un basculement transparent, mais échouent systématiquement en raison de procédures obsolètes, de dérives de configuration et de lacunes dans les connaissances.

Le défaut fondamental ne réside pas dans la protection des données, mais dans l'illusion que la sauvegarde des données équivaut à la capacité de restaurer des systèmes fonctionnels. Une véritable récupération nécessite non seulement un stockage de données hors ligne, mais également des capacités complètes de restauration du système que la plupart des stratégies de sauvegarde ne parviennent pas à fournir.

Ransomware moderne : « Sauvegarde et restauration » : une stratégie obsolète

Les attaques par ransomware ne consistent pas simplement à découvrir les sauvegardes : elles les traquent d'abord, s'assurant que votre plan B est compromis avant le début de la deuxième phase.

Une fois que les attaquants obtiennent des droits d'administrateur de domaine, ils démantèlent systématiquement les capacités de récupération de l'organisation en désactivant ou en supprimant les instantanés, en falsifiant les politiques de conservation des sauvegardes et en corrompant les coffres-forts supposément immuables. Ils compromettent même les couches d'orchestration qui gèrent ces systèmes, faisant de chaque chemin de récupération potentiel une impasse.

La menace s'étend au-delà de la simple destruction. Les gangs de double extorsion ont mis au point une approche calculée : ils volent d'abord des données sensibles pour menacer de les divulguer publiquement, puis chiffrent ce qui reste pour paralyser les opérations. Cette attaque en deux volets maximise l'effet de levier, car les entreprises sont confrontées à la fois à un arrêt opérationnel et à une catastrophe pour leur réputation.

Le mirage du stockage immuable

Le stockage immuable est conçu de manière à ce que les instantanés, une fois écrits, ne puissent pas être modifiés. Pourtant, les attaquants ont développé des contre-stratégies sophistiquées qui exposent les limites fondamentales de la technologie. Les cybercriminels détournent le plan de gestion ou la couche de contrôle pour modifier les politiques et les paramètres d'immuabilité avant que les instantanés ne soient terminés, neutralisant ainsi la protection avant qu'elle ne prenne effet. Ils exploitent également les vulnérabilités de configuration pour s'accorder le pouvoir de purger ou de rechiffrer les archives, retournant les propres contrôles de sécurité de l'organisation contre elle.

Même lorsque les coffres-forts restent techniquement sécurisés, leur champ de protection reste dangereusement limité, protégeant les données mais laissant les configurations réseau, les maillages de micro-services et les arbres d'identité complètement exposés aux attaques.

Outils de sécurité des données : utiles mais incomplets

Les progrès récents en matière de sécurité ont permis de mettre en place des outils sophistiqués tels que la gestion de la posture de sécurité des données (DSPM) pour une visibilité complète des données, la prévention des pertes de données (DLP) pour la surveillance des mouvements de données, et des outils de sécurité basés sur l'IA qui permettent une détection et une réponse intelligentes aux menaces.

Bien que ces technologies représentent des progrès considérables en matière de cybersécurité, elles se concentrent principalement sur la prévention et la détection plutôt que sur la récupération complète, laissant les entreprises vulnérables lorsque les attaquants parviennent à percer leurs défenses.

Les promesses et les pièges cachés de la récupération dans le cloud

Les fournisseurs de cloud hyperscale ont promis une capacité infinie, des captures instantanées répliquées dans toutes les régions et des pipelines de reprise après sinistre en libre-service. De nombreuses entreprises, convaincues que leurs données seraient plus en sécurité, ont migré des téraoctets en quelques semaines. Cependant, ces promesses masquaient des lacunes fondamentales qui n'ont ressurgi que lorsque les entreprises ont eu le plus besoin de leurs capacités de récupération.

Au-delà de la sauvegarde classique

Les méthodes traditionnelles ne parviennent pas à capturer les dépendances complexes qui couvrent les services cloud ; la dérive de configuration inévitable qui se produit dans les domaines du réseau et de l'identité ; et les logiciels malveillants ou les mauvaises configurations qui se cachent dans les conteneurs, les fonctions sans serveur ou les bibliothèques d'applications. Sans copies de référence (copies d'applications et de données entièrement numérisées, multi-composants, ponctuelles et propres), les restaurations reposent sur du sable.

L'ancienne approche consistant à « espérer que la sauvegarde fonctionne » est aussi risquée que de parier votre entreprise sur un seul parachute non testé.

La pièce manquante cruciale : tests de reconstruction réguliers et complets

La cybersécurité basée sur la défense et les stratégies classiques de sauvegarde des données reste fondamentalement incomplète. La solution réside dans des tests réguliers et en conditions réelles des capacités de reconstruction complètes.

Les tests de reconstruction représentent un changement fondamental, passant de l'espoir que les sauvegardes fonctionnent à la vérification de leur efficacité grâce à une validation globale. Cette approche reconstruit l'ensemble de l'environnement numérique exactement tel qu'il existait à un moment connu comme étant propre, offrant une récupération holistique de l'environnement qui va bien au-delà de la simple restauration des données.

Le processus consiste à rembobiner chaque couche de l'infrastructure de l'entreprise – pas seulement ses données, mais aussi ses configurations réseau, ses ressources de calcul, ses cadres d'identité, ses conteneurs, ses configurations sans serveur et ses passerelles API – afin que l'environnement restauré reflète l'original.

Plus important encore, les tests de reconstruction intègrent une analyse complète des logiciels malveillants, des vulnérabilités, des dérives de configuration et des modifications non autorisées qui peuvent avoir infiltré l'environnement avant que l'instantané n'ait été pris. Cette étape de validation transforme la restauration de sauvegarde, la faisant passer d'un acte de foi à un processus de récupération vérifié et sécurisé auquel les entreprises peuvent se fier lorsque leur survie en dépend.

L'angle mort du cadre de cybersécurité du NIST

Le cadre de cybersécurité du National Institute of Standards and Technology (NIST) fournit une structure élégante à travers six fonctions principales : identifier, protéger, détecter, répondre, récupérer et gouverner. Cependant, sa fonction de récupération est dangereusement mal comprise, créant un angle mort critique qui laisse les entreprises vulnérables même lorsqu'elles se pensent protégées.

Récupérer vs. Reconstruire : deux fonctions distinctes

La fonction de récupération du NIST se concentre sur la restauration pour remettre les systèmes dans un état fonctionnel après un incident. Cette approche traite la récupération comme un contrôle des dommages, en mettant l'accent sur la rapidité plutôt que sur la validation. Les entreprises restaurent à partir de sauvegardes, exécutent des scripts de reprise après sinistre et se réjouissent lorsque les applications semblent fonctionner, souvent sans vérifier l'intégrité ou l'exhaustivité de ce qu'elles ont restauré.

La reconstruction, en revanche, représente un changement de paradigme vers une reconstruction en toute confiance. Plutôt que de simplement restaurer ce qui a été perdu, la fonction « Reconstruire » est conçue pour créer un environnement d'application vérifié et propre à partir de composants connus et fiables. C'est la différence entre réparer un mur endommagé et en construire un nouveau à partir de plans fiables. Les deux murs peuvent sembler fonctionnels, mais un seul peut maintenir l'intégrité structurelle.

Les limites de la récupération

Dans la pratique, la récupération n'est souvent rien de plus qu'une série d'activités de conformité sommaires, qui fournissent une assurance minimale de la capacité de récupération réelle. Les entreprises effectuent des exercices annuels de reprise après sinistre sur table, qui testent les procédures sur papier, mais ne valident jamais la restauration réelle du système. Elles effectuent des restaurations sporadiques de bases de données et testent périodiquement des rotations de machines virtuelles (VM) qui ne touchent que des fragments de leur infrastructure, tout en ignorant les interdépendances complexes requises par les applications modernes.

Plus important encore, les entreprises effectuent rarement des restaurations d'application complètes à grande échelle avec une validation régulière pour vérifier que tous les composants correspondent aux données instantanées et fonctionnent ensemble comme un système intégré.

. Le tableau 2-1 identifie les points où le cadre actuel du NIST ne répond pas aux exigences modernes et montre comment la reconstruction comble ces lacunes critiques.

En érigeant la reconstruction sur son propre pilier, une extension vivante de récupération, nous concentrons les défenseurs sur un test de résilience plus rigoureux : la capacité de revenir à un moment précis, de sélectionner une copie de référence sûre et de reconstruire l'application depuis le réseau jusqu'à la couche de données à la demande.

Tableau 2-1. Lacunes dans le cadre actuel du NIST et comment la fonction Reconstruire comble ces lacunes

Fonction	Force tradition-nelle	Lacune actuelle	Comment la Reconstruction comble la lacune
Identifier	Inventaires d'actifs, BIA	Pas de confiance de récupération régulière	Catalogue historique des copies de référence
Protéger	IAM, chiffrement, pare-feux	Impossible d'arrêter les attaques de type « zero-day » ou les attaques internes	Instantanés immuables pour reconstruire les artefacts
Détecter	SIEM, XDR, UEBA	Alerte ≠ restauration assurée	Tests de reconstruction automatisés déclenchés par des flux d'événements
Répondre	Playbooks de réponse à un incident (IR), quarantaine	Les playbooks valident rarement une restauration complète	La reconstruction intégrée s'exécute dans le cadre de la réponse
Récupérer	Scripts de sauvegarde et de basculement	Restaurations partielles et manuelles ; runbooks non testés	Orchestration définie par code de la re-construction de l'environnement complet
Reconstruire			Exercices de reconstruction ponctuels réguliers et automatisés

Le cadre élargi

Pour maintenir la résilience, nous devons ajouter la fonction de reconstruction au cadre du NIST. La récupération reste la politique, le plan et l'analyse rétrospective : le cadre stratégique qui définit ce qui doit se produire en cas de catastrophe. La reconstruction est le cœur battant qui peut faire de la récupération une réalité prouvée plutôt qu'une possibilité théorique, comme le montre la figure 2-1.

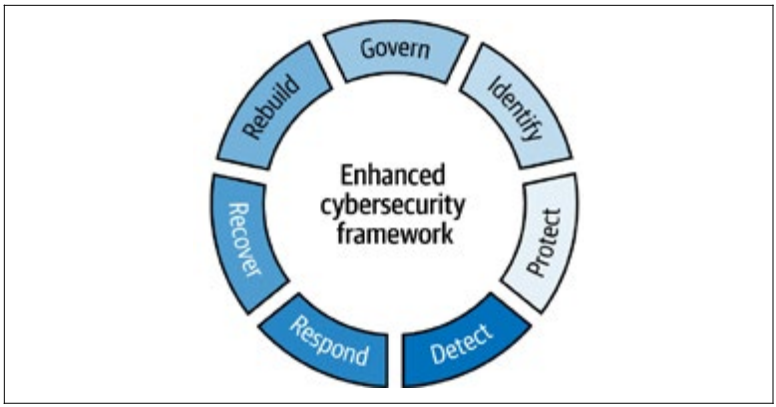

Figure 2-1 Le cadre du NIST avec l'ajout de la fonction Reconstruction

La fonction Reconstruction comporte un certain nombre d'éléments :

Récupération de l'infrastructure à un instant donné
: Celle-ci capture des instantanés complets des composants de l'infrastructure, y compris les configurations réseau, les ressources de calcul, les images d'application et leurs interdépendances. Contrairement aux sauvegardes classiques qui se concentrent sur les données, ces instantanés sont conçus pour recréer le contexte d'infrastructure dont les applications ont besoin pour fonctionner correctement.

Les copies de référence
: Il s'agit d'images ponctuelles qui ont fait l'objet d'une analyse complète à la recherche de logiciels malveillants, de mauvaises configurations et de vulnérabilités de sécurité et qui fournissent ainsi des points de récupération validés et propres. Il ne s'agit pas seulement de copies de données, mais d'instantanés vérifiés et propres de piles d'applications entières auxquelles vous pouvez faire confiance implicitement, éliminant ainsi la crainte que la restauration ne réintroduise précisément les problèmes que vous essayez d'éviter.

Récupération en tant que code
: La RaC transforme les procédures de restauration ad hoc en processus automatisés, versionnés et reproductibles. Au lieu de s'appuyer sur des runbooks obsolètes, la RaC traite les procédures de reconstruction comme des logiciels vivants qui évoluent avec votre infrastructure, de sorte que les capacités de récupération s'améliorent au fil du temps plutôt que de se dégrader par négligence.

La reconstruction transforme le « J'espère que la sauvegarde fonctionne » en « J'ai la certitude que cette reconstruction réussira ». C'est parce que vous l'avez testée, affinée et éprouvée qu'elle fonctionne des dizaines de fois avant que vous n'en ayez réellement besoin.

CHAPITRE 3

Exploiter les avantages de la reconstruction: tester l'inattendu dans le cloud

Au début du XXe siècle, la sécurité automobile s'est considérablement améliorée, non seulement parce que les voitures sont devenues plus robustes, mais parce que les crash tests sont devenus essentiels au processus de développement des véhicules, faisant de la sécurité un résultat assuré et non plus un simple espoir. De même, dans les premières heures de l'aviation, les pilotes croyaient que maîtriser le vol signifiait construire des avions plus solides.

Pourtant, lorsque la catastrophe a frappé dans les airs, ce n'est pas la seule résistance de l'avion qui a sauvé des vies, mais plutôt la capacité du pilote à récupérer d'événements inattendus. Quelle que soit la qualité de conception de l'avion, la survie dépendait souvent d'une formation approfondie et rigoureuse, grâce à des simulations de toutes les situations d'urgence imaginables.

Aujourd'hui, la résilience numérique est confrontée à un moment de transformation similaire. Les entreprises doivent aller au-delà de l'hypothèse que les sauvegardes et les défenses de cybersécurité fonctionneront. Le test régulier constitue l'un des éléments manquants, et peut-être même l'élément le plus critique. Des tests réguliers permettent aux entreprises de reconstruire de manière fiable leurs environnements numériques après des défaillances catastrophiques. Ce chapitre se concentrera sur la manière dont les entreprises peuvent mettre en œuvre des tests de reconstruction continus.

Histoires vraies de sauvegardes qui n'ont pas fonctionné et de plans de récupération qui ont échoué

Les incidents récents révèlent la fragilité de nos écosystèmes numériques malgré les investissements considérables que les entreprises ont réalisés dans la cybersécurité et les sauvegardes de données. L'ampleur et l'intensité des attaques par ransomware ont considérablement augmenté au cours des dernières années, ce qui prouve que même les plans de reprise après sinistre complets échouent lorsqu'ils n'ont pas été testés par rapport aux réalités des cybermenaces modernes.

Pensez à la façon dont les grandes entreprises ont souffert au cours des dernières années lorsque leurs plans de reprise, malgré une documentation méticuleuse et des investissements importants, ont échoué de manière spectaculaire.

MGM Resorts et Caesars Entertainment
: Ces entreprises ont été confrontées à des attaques débilitantes à la fin 2023, provoquant des perturbations importantes. Malgré leurs plans complets de reprise après sinistre, les deux entreprises ont eu du mal à rétablir rapidement les fonctions critiques de l'entreprise. Une documentation solide existait, mais la restauration réelle a échoué en raison de dépendances non testées, de configurations obsolètes et d'intégrations manquantes entre les sauvegardes de données et la récupération des applications

National Health Service (NHS), Londres, Royaume-Uni
: Une attaque de 2024 avec le ransomware Qilin a révélé une dure réalité : près d'un million de dossiers de patients et de systèmes de données de santé critiques ont été compromis, malgré des sauvegardes robustes. Le NHS a dû apprendre à ses dépens que la restauration des bases de données à elle seule était insuffisante : sans procédures de restauration vérifiées pour les applications, les identités et les architectures de réseau, les sauvegardes se sont révélées inutiles.

Attaques de compartiments buckets S3 d'AWS
: Dans cet édifiant scénario de 2025, le ransomware Codefinger a ciblé les compartiments de stockage dans le cloud de l'entreprise, rendant inefficaces les stratégies classiques de sauvegarde dans le cloud. De nombreuses entreprises, malgré des sauvegardes

régulières dans le cloud, se sont réveillées pour découvrir que ces sauvegardes étaient verrouillées derrière un chiffrement de ransomware. De tels incidents mettent en évidence le besoin critique d'une approche de test complètement nouvelle pour restaurer les procédures.

Ces histoires illustrent une réalité troublante : nos hypothèses traditionnelles sur la protection des données et la cybersécurité sont incomplètes. L'augmentation exponentielle des ransomwares sophistiqués, associée à des pannes de plus en plus fréquentes dans les régions de cloud, exige une nouvelle discipline en matière de résilience numérique : tester les reconstructions d'environnements complets de manière régulière, complète et rigoureuse.

Au-delà de la récupération classique : Le défi moderne de la reconstruction des clouds

La reconstruction des environnements cloud implique bien plus que la simple restauration des données à partir de sauvegardes. Les applications modernes fonctionnent dans des écosystèmes extrêmement dynamiques, composés de nombreux services natifs du cloud, qui évoluent constamment à travers de multiples pipelines DevOps simultanés. Aujourd'hui, ces mêmes pipelines sont de plus en plus pilotés par l'IA.

Dépendances cachées et dérive de configuration

Chaque pipeline DevOps peut indépendamment mettre à jour les configurations, déployer des micro-services et ajuster les politiques de sécurité, ce qui exacerbe le risque de dérive de la configuration et obscurcit les dépendances critiques. Les équipes qui utilisent des outils d'intégration et de déploiement continus (CI/CD) comme AWS CodeDeploy CodePipeline et CodeBuild, modifient fréquemment les environnements sans avoir une visibilité claire sur l'impact de leurs changements. Ainsi, elles créent souvent des vulnérabilités cachées ou des dépendances négligées, rendant difficile une reconstruction complète et précise en cas de crise.

Le cadre stratégique de viabilité minimale : rendre la reconstruction réalisable

La réalité pratique à laquelle la plupart des entreprises sont confrontées est que tout reconstruire simultanément n'est ni pratique

ni nécessaire. C'est là que le concept de viabilité minimale (ou « entreprise minimale viable ») devient le pont stratégique entre la théorie de la reconstruction et une mise en œuvre réussie.

Le cadre de viabilité minimale reconnaît que les entreprises ont besoin d'une compréhension approfondie de leurs actifs les plus critiques et de ce qu'il faut pour restaurer leur état de fonctionnement. Plutôt que de tenter l'immense tâche de tester des reconstructions complètes de l'environnement, les entreprises peuvent mettre en œuvre la fonction de reconstruction de manière progressive en se concentrant sur ce qui compte vraiment pour la survie de l'entreprise.

Les entreprises peuvent mettre en œuvre la fonction de Reconstruction de manière efficace en hiérarchisant leurs applications et leurs services à l'aide de cadres établis tels que la norme ISO 22301 (systèmes de gestion de la continuité des activités) ou les directives d'analyse d'impact sur les activités du NIST. Ces cadres aident les entreprises à classer les systèmes en fonction de leur criticité opérationnelle :

- *Critiques pour la mission:* les systèmes sans lesquels vous ne pouvez rien faire (par exemple, Active Directory, système de gestion des commandes, systèmes de soins aux patients). Ces applications constituent le fondement de la viabilité minimale : sans elles, l'organisation ne peut pas fonctionner du tout.

- *Critiques pour l'entreprise:* Systèmes nécessaires à la récupération complète des opérations (par exemple, e-mail, comptabilité, gestion de la chaîne d'approvisionnement). Ils permettent d'étendre la capacité opérationnelle au-delà de la survie de base.

- *Non critiques:* Tous les autres systèmes qui prennent en charge l'intégralité des fonctionnalités, mais qui ne sont pas essentiels à la continuité immédiate des activités.

Cette approche par paliers transforme la fonction de Reconstruction, la faisant passer d'un écrasant défi où « tout doit fonctionner » en un processus de récupération stratégique et progressif. Les entreprises peuvent atteindre une viabilité minimale en concentrant d'abord les tests de reconstruction sur les systèmes critiques pour l'entreprise, puis

en les étendant systématiquement aux applications critiques pour la mission et non critiques.

Cette approche réduit considérablement les objectifs de délais de récupération initiaux (RTO) pour les fonctions essentielles à l'entreprise, tout en maintenant l'objectif de restauration complète de l'environnement.

La reconstruction complète : métadonnées, automatisation et orchestration

Une reconstruction efficace implique la capture de toutes les métadonnées pertinentes – non seulement les données d'application, mais aussi les configurations détaillées, les dépendances des ressources, les politiques de gestion des identités et des accès (IAM), les topologies de réseau et les points de terminaison API. Il est essentiel que les entreprises répliquent ces métadonnées complètes de manière sécurisée et immuable sur plusieurs régions cloud ou comptes isolés afin de minimiser les points de défaillance individuels et de renforcer la sécurité contre les ransomwares et les modifications non autorisées.

La reconstruction doit tirer parti des techniques automatisées d'infrastructure en tant que code (IaC), en intégrant les processus de récupération précédemment fragmentés dans des pipelines d'automatisation exécutables. Cette approche permet aux opérations de résilience de rester adaptables, cohérentes et vérifiables. La centralisation et la mise à jour continue du code de récupération permettent aux équipes de gérer la résilience de manière proactive plutôt que de répondre aux crises de manière réactive. Par conséquent, un processus de reconstruction complet signifie non seulement de restaurer les données, mais aussi d'orchestrer l'ensemble de l'environnement cloud de manière transparente et cohérente.

Opérationnalisation de la fonction de reconstruction : récupération de l'infrastructure à un instant donné et récupération en tant que code

Cloud Rewind de Commvault (anciennement Appranix) remédie aux faiblesses critiques des pratiques classiques de reprise après sinistre grâce à deux concepts innovants pour la reconstruction à la demande des environnements d'application : la restauration de l'infrastructure à un instant donné (PITR) et la RaC.

Historiquement, les entreprises ont lutté avec des runbooks de récupération fragmentés, chaque runbook étant géré indépendamment par les équipes de sécurité, d'application, d'architecture d'entreprise et de sauvegarde. En cas de crise, les équipes affectées à la continuité des activités subissaient des retards importants lorsqu'elles rassemblaient ces documents de récupération dispersés, ce qui avait pour conséquence l'augmentation des temps d'arrêt.

La récupération de l'infrastructure à un instant donné résout ce problème en fournissant un instantané automatisé et complet de tout un écosystème numérique : pas seulement les données, mais la pile d'applications complète, les micro-services, les fonctions sans serveur, les configurations d'identité et d'accès, les topologies de réseau ainsi que leurs dépendances.

En capturant régulièrement ces états ponctuels complets, sur la base des politiques données, la PITR (Figure 3-1) permet aux entreprises de conserver des copies de référence validées et complètes, qui sont rapidement disponibles à la fois pour la restauration de la viabilité minimale et pour les reconstructions complètes de la pile d'applications.

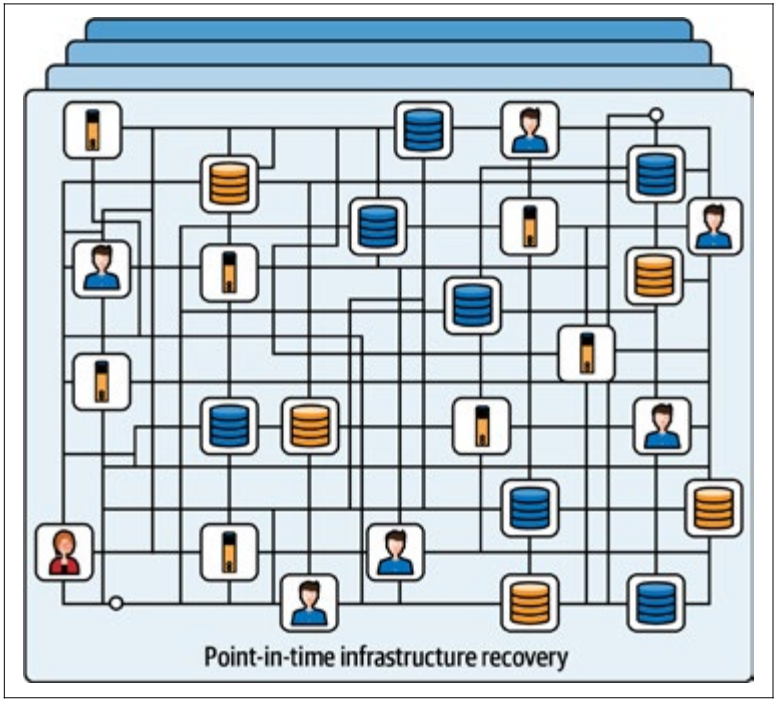

Figure 3-1 Illustration de la façon dont la PITR fournit un instantané complet d'un écosystème d'application cloud entier

La capacité de la PITR à capturer des instantanés hiérarchisés devient particulièrement précieuse pour les stratégies de viabilité minimale. Les entreprises peuvent configurer des politiques qui donnent la priorité aux applications critiques pour l'entreprise afin d'obtenir des instantanés plus fréquents, fournir des systèmes critiques pour la mission avec des points de récupération vérifiés et maintenir une protection de base pour les applications non critiques.

Cette approche à plusieurs niveaux permet une restauration rapide des opérations minimales viables tout en maintenant une protection complète dans l'ensemble de l'environnement.

Tirer parti des plateformes cloud hyperscale comme AWS, Azure ou Google Cloud améliore encore cette capacité. Les vastes ressources de calcul à la demande et les fonctionnalités d'isolement intégrées des clouds hyperscale permettent aux entreprises d'exécuter fréquemment des tests à grande échelle avec facilité et efficacité.

Ces plateformes simplifient les validations de récupération complexes, transformant les exercices de reprise après sinistre coûteux et peu fréquents en exercices de reconstruction de routine et rentables.

En complément de la PITR, la récupération en tant que code transforme la récupération en un processus unifié et automatisé qui rend opérationnelle la fonction de reconstruction. Plutôt que de maintenir des runbooks distincts et encombrants, la RaC intègre toutes les étapes de récupération nécessaires directement dans des pipelines d'automatisation exécutables (Figure 3-2).

Le code contrôlé par version sert de source fiable unique pour la récupération, alignant les équipes de sécurité, les architectes, les développeurs d'applications et les spécialistes de la sauvegarde autour d'un processus centralisé et cohérent. Cette approche basée sur le code intègre de manière transparente les tests de reconstruction réguliers en flux de travail DevOps quotidiens, réduisant considérablement la complexité opérationnelle.

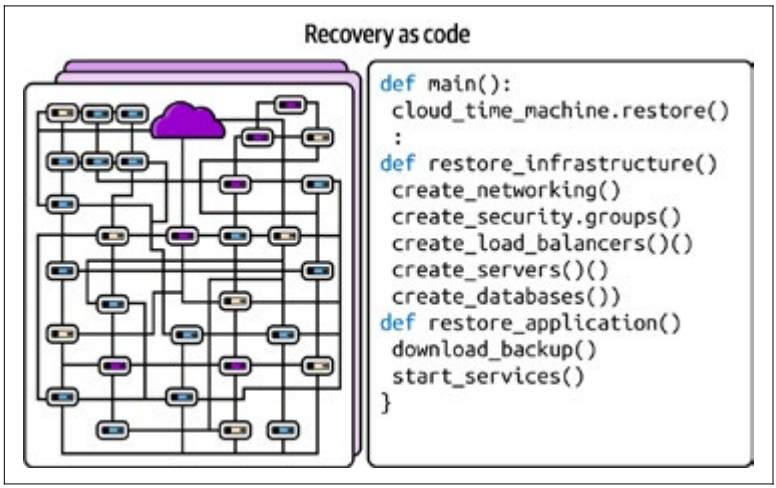

Figure 3-2 La PITR main dans la main avec la RaC, qui intègre toutes les étapes de récupération dans des pipelines d'automatisation exécutables

Utilisation stratégique de la reconstruction

La RaC peut être structurée pour prendre en charge les flux de travail de viabilité minimale, avec des pipelines d'automatisation distincts pour les niveaux d'application critiques pour l'entreprise, critiques pour la mission et non critiques. Cela permet aux entreprises d'exécuter une restauration rapide de la viabilité minimale tout en se préparant à une récupération complète de l'environnement, rendant la fonction de reconstruction à la fois stratégique et pratique.

Ensemble, la PITR et la RaC changent fondamentalement la résilience organisationnelle. Ces innovations permettent aux entreprises de passer de l'incertitude et de la gestion réactive des crises à une capacité proactive et tangible, réduisant considérablement les temps de récupération, simplifiant les exigences de conformité et l'établissement d'une confiance inégalée avec les parties prenantes. Les tests de reconstruction réguliers deviennent ainsi non seulement réalisables, mais aussi un impératif stratégique pour la résilience numérique moderne.

La valeur commerciale des tests de reconstruction réguliers avec optimisation des coûts

L'adoption de tests de reconstruction réguliers avec PITR et RaC transforme fondamentalement la résilience organisationnelle en rendant la fonction de reconstruction à la fois économiquement viable et stratégiquement précieuse. Plutôt que de s'appuyer sur des plans de reprise incertains et une gestion de crise fondée sur la peur, les entreprises peuvent acquérir des capacités de reprise claires, mesurables et tangibles.

Prenons l'exemple d'une organisation de soins de santé confrontée à une attaque par ransomware. Plutôt que d'attendre la restauration complète de l'infrastructure, la planification de la viabilité minimale permet de restaurer rapidement les systèmes de soins aux patients, les opérations des services d'urgence et les capacités de communication essentielles. L'entreprise peut restaurer ses systèmes administratifs, ses plateformes de planification et ses outils de reporting ultérieurement, sans affecter les soins aux patients.

Cette approche par paliers offre un certain nombre d'avantages commerciaux clés qui peuvent être mesurés.

Amélioration des opérations et de la confiance des clients

En donnant la priorité aux systèmes générateurs de revenus dans la planification de la viabilité minimale, les entreprises peuvent reprendre rapidement leurs activités principales tout en conservant la confiance de leurs clients. Cette confiance devient un avantage concurrentiel, en particulier dans les secteurs où la fiabilité numérique a un impact direct sur les relations avec les clients.

Avantages réglementaires et de conformité

La planification de la viabilité minimale aide les entreprises à répondre aux exigences réglementaires pour le maintien des services essentiels pendant les perturbations. Les tests de reconstruction automatisés simplifient les processus de conformité en générant régulièrement des preuves complètes, ce qui rend les préparatifs d'audit plus efficaces.

Les entreprises peuvent démontrer leur conformité aux normes réglementaires telles que la loi américaine sur la portabilité et la

responsabilité en matière d'assurance maladie (HIPAA) et aux cadres sectoriels tels que SOC 2, ISO 27001 et la loi sur la résilience opérationnelle numérique (DORA) avec un minimum d'efforts manuels, en fournissant aux auditeurs des informations immédiates sur les capacités de résilience.

Réduction des coûts et des délais

L'automatisation des reconstructions réduit aussi de façon considérable la complexité et les coûts. Les tests classiques de reprise après sinistre sont coûteux, perturbateurs et sujets aux erreurs humaines. En adoptant RaC, les entreprises peuvent reconstruire et tester efficacement à la demande en utilisant des modèles de programmabilité et de déploiement cloud hyperscale.

Elles peuvent automatiser des processus de reconstruction complexes, en transformant des runbooks manuels épars en procédures rationalisées et reproductibles basées sur du code. Cette automatisation réduit non seulement les frais généraux opérationnels et élimine les dépenses liées aux tests manuels, mais elle favorise également la cohérence et la fiabilité de chaque test.

Confiance et assurance organisationnelles

Le plus important est peut-être que les tests de reconstruction réguliers engendrent une confiance et une assurance organisationnelles inégalées. Des capacités de récupération régulièrement validées offrent aux équipes dirigeantes une assurance claire et tangible de leur préparation pour faire face aux perturbations.

Les organismes de réglementation, les clients et les partenaires sont davantage rassurés quant au fait que l'entreprise atténue les risques de manière proactive et peut rapidement récupérer de toute cyberattaque ou défaillance du cloud. Cette confiance devient un avantage stratégique, distinguant les entreprises résilientes dans un monde de plus en plus défini par les menaces et les perturbations numériques.

Rendre les tests de reconstruction pratiques : infrastructure et méthodes de validation

Après avoir établi le cadre stratégique pour une viabilité minimale, la question devient : Comment les entreprises exécutent-elles réellement des tests de reconstruction réguliers à grande échelle pour les applications critiques ? La réponse réside dans deux facteurs qui rendent les tests fréquents à la fois abordables et réalistes:

- •Premièrement, les plateformes cloud hyperscale fournissent l'infrastructure élastique nécessaire pour créer des environnements de test complets à la demande.
- Deuxièmement, les principes d'ingénierie du chaos aident ces tests à simuler des défaillances en conditions réelles plutôt que des scénarios prévisibles.

Ensemble, ces approches transforment les tests de reconstruction d'un exercice annuel coûteux en une capacité opérationnelle de routine.

Utiliser les plateformes cloud comme moteur de test

Les plateformes cloud telles qu'AWS, Azure et Google Cloud offrent un environnement idéal pour les tests de reconstruction réguliers en raison de leur flexibilité, de leur évolutivité et de leur accessibilité inégalées. Contrairement aux centres de données classiques, les clouds hyperscale permettent aux entreprises de créer instantanément des environnements de bacs à sable (sandbox) entièrement isolés, d'exécuter des tests rigoureux et de les supprimer sans affecter la production.

Cette flexibilité supprime les obstacles encombrants traditionnellement associés aux tests de reprise après sinistre, permettant des tests plus fréquents, plus approfondis et plus significatifs.

Les vastes ressources de calcul et de stockage à la demande constituent des avantages significatifs pour ces plateformes, qui permettent aux entreprises d'augmenter ou de réduire rapidement les ressources en fonction des besoins de test spécifiques. L'utilisation stratégique d'instances ponctuelles fournit une capacité de calcul de l'espace à des

coûts considérablement réduits, souvent de 70 % à 80 % inférieurs aux prix à la demande habituels, ce qui permet d'augmenter la fréquence des tests sans contraintes budgétaires supplémentaires.

L'environnement cloud permet également de simuler des défaillances partielles de l'infrastructure, de tester les capacités de basculement interrégionales pour les systèmes critiques de l'entreprise et de valider que les procédures de restauration de la viabilité minimale fonctionnent dans diverses conditions de défaillance, le tout dans des environnements de test isolés et rentables.

Les tests de reconstruction réguliers, autrefois considérés comme complexes et coûteux, sont désormais pratiques et accessibles, permettant à ce qui était autrefois une activité de conformité occasionnelle de devenir une capacité organisationnelle de base.

Tests de chaos : renforcer la résilience par l'échec intentionnel

Le test de chaos est la pratique consistant à injecter délibérément des perturbations contrôlées dans un système pour découvrir des faiblesses cachées et valider la résilience dans des conditions réalistes. Cette approche introduit intentionnellement des scénarios de défaillance, tels que des pannes d'infrastructure, une latence du réseau ou des pics de ressources inattendus, pour tester si les systèmes continuent à fonctionner de manière fiable sous contrainte.

Contrairement aux exercices de reprise après sinistre standard, qui simulent souvent des scénarios prévisibles, les tests de chaos se nourrissent de l'imprévisibilité, remettant continuellement en question les hypothèses et révélant les angles morts dans la résilience des applications et des infrastructures.

Dans le contexte des tests de reconstruction, les tests de chaos deviennent particulièrement essentiels. Parce que les environnements de production évoluent constamment, de nouveaux services sont déployés, les configurations changent et les charges de travail fluctuent.

Les tests de reconstruction statiques classiques deviennent rapidement obsolètes. Les plateformes cloud permettent aux entreprises d'exécuter des tests de reconstruction adaptatifs qui reflètent la nature dynamique des applications modernes. En intégrant les principes de l'ingénierie du chaos aux pratiques de reconstruction, les tests évoluent de manière proactive, reflétant la complexité de la production et s'adaptant continuellement aux changements.

Les tests de chaos deviennent encore plus précieux lorsqu'ils sont appliqués sous le prisme de la viabilité minimale. Plutôt que de tester des défaillances aléatoires dans des environnements entiers, les entreprises peuvent concentrer les expériences de chaos sur les systèmes critiques pour comprendre comment les défaillances pourraient se répercuter en cascade et impacter la restauration de la viabilité minimale.

Par exemple, lors d'un exercice de restauration de la viabilité minimale, le test de chaos peut délibérément désactiver les services Active Directory pour valider que les systèmes d'authentification de sauvegarde peuvent maintenir les opérations commerciales essentielles. Sinon, il peut également simuler des défaillances de partition de réseau entre des micro-services critiques pour confirmer que les applications de viabilité minimale restent fonctionnelles même lorsque les services dépendants ne sont pas disponibles.

Réaliser des tests de reconstruction réguliers : de la théorie aux résultats concrets

La mise en place de tests de reconstruction réguliers transforme la résilience organisationnelle, passant d'une simple assurance théorique à une capacité concrète et quantifiable. Tout comme le développement logiciel intègre désormais des pratiques régulières d'assurance qualité (QA), la résilience numérique doit de même adopter des tests de reconstruction réguliers. Les DSI et les RSSI peuvent s'attendre à des résultats tangibles : une capacité de récupération démontrable ; des réductions de risques quantifiables ; et un alignement clair entre les équipes de sécurité, d'exploitation du cloud et de récupération.

Mise en œuvre d'approches de test à plusieurs niveaux

Une approche structurée commence par la planification mensuelle ou trimestrielle de jours de test de reconstruction, qui intègrent à la fois des scénarios de viabilité minimale et de restauration complète de l'environnement. Ces événements doivent être soigneusement planifiés et inclure des exercices de récupération réguliers, des exercices de viabilité minimale et des expériences de chaos contrôlées.

Jours de test de viabilité minimale

Les entreprises doivent mener des exercices distincts axés spécifiquement sur la restauration des systèmes critiques pour l'entreprise dans des fenêtres temporelles définies. Ces tests permettent de valider que les fonctions essentielles pour l'entreprise peuvent rapidement être restaurées, généralement en quelques heures plutôt qu'en quelques jours.

Les indicateurs de réussite de ces tests comprennent le temps nécessaire pour restaurer les services d'identité, le temps nécessaire pour mettre en ligne les applications commerciales de base et la vérification que les opérations viables minimales peuvent être maintenues pendant que la reprise complète se poursuit.

Test de reconstruction complet de l'environnement

Il est également important de mener des exercices de plus grande ampleur qui testent la restauration complète de l'infrastructure, confirmant que les systèmes critiques à la mission et non critiques

peuvent être restaurés avec succès une fois la viabilité minimale atteinte. Ces tests valident la capacité de l'organisation à retrouver sa pleine capacité opérationnelle.

Définition des rôles et des responsabilités

La définition claire des rôles et des responsabilités devient cruciale pour des tests efficaces, en particulier lorsqu'il s'agit d'équilibrer les priorités de viabilité minimale et la restauration complète de l'environnement.

Équipes de sécurité

Les équipes de sécurité valident que les environnements récupérés sont rigoureusement analysés et débarrassés des vulnérabilités, des signatures de ransomwares et des erreurs de configuration. Lors de la restauration de la viabilité minimale, ces équipes donnent la priorité à la validation des systèmes critiques pour l'entreprise tout en effectuant des évaluations de sécurité complètes de l'environnement plus large en parallèle.

Équipes d'exploitation et d'applications cloud

Ces équipes se concentrent sur le provisionnement de l'infrastructure, l'alignement de la configuration et l'orchestration de reconstructions complètes à partir des PTIR de l'environnement. Elles gèrent l'exécution technique de la restauration de la viabilité minimale et de la reconstruction complète de l'environnement, en confirmant que les dépendances de l'infrastructure sont correctement séquencées et que les services restaurés répondent aux exigences fonctionnelles.

Équipes de récupération

Supervisant l'ensemble du processus de reconstruction, les équipes de récupération assurent la coordination entre tous les groupes et la documentation précise des résultats. Elles gèrent la transition de la viabilité minimale à la pleine capacité opérationnelle et coordonnent les différents scénarios de test.

Mesurer le succès et démontrer la valeur

Pour évaluer l'efficacité et démontrer la valeur des tests de reconstruction, des mesures claires doivent être établies et communiquées. Ces mesures vont au-delà des simples objectifs de délais de récupération (RTO) et des objectifs de point de récupération (RPO). Elles comprennent:

Les mesures de viabilité minimale

Le temps nécessaire pour restaurer l'ensemble des systèmes critiques pour l'entreprise et les dépendances associées, le taux de réussite des procédures de viabilité minimale dans des conditions de stress et la capacité à maintenir les opérations essentielles pendant la récupération complète.

Les mesures de la récupération complète

Le temps de récupération global pour des environnements complets, le taux de réussite des procédures de reconstruction complète et la vérification du bon fonctionnement de tous les systèmes après la restauration.

Les mesures de test de résilience

La fréquence et l'exhaustivité des tests de chaos effectués, le nombre de vulnérabilités ou de mauvaises configurations identifiées et résolues grâce aux tests, et l'amélioration des performances de récupération au fil du temps.

Les mesures de l'impact sur l'entreprise

La réduction de la perte de revenus potentielle lors d'incidents cybernétiques, l'amélioration des mesures de confiance des clients et la démonstration de la conformité réglementaire grâce à des tests réguliers soulignent que les DSI et les RSSI doivent s'attendre à des rapports réguliers mettant en évidence ces mesures, et ces mesures fourniront une transparence et des preuves concrètes d'amélioration au fil du temps.

Des tests de reconstruction réguliers fournissent des preuves concrètes des capacités de récupération à toutes les parties prenantes – depuis les équipes de sécurité qui souhaitent valider l'atténuation des menaces jusqu'aux dirigeants qui cherchent à démontrer la résilience opérationnelle.

Longtemps considérée comme une bonne pratique, la réalisation régulière de tests de reconstruction devient un élément fondamental de la gestion des risques de l'entreprise. En intégrant les principes de viabilité minimale à des tests complets, les entreprises peuvent démontrer en toute confiance leur capacité à restaurer rapidement les fonctions essentielles de l'entreprise tout en maintenant une résilience numérique complète. Cette capacité est devenue essentielle à la survie des entreprises, car les cybermenaces continuent d'évoluer et de s'intensifier.

CHAPITRE 4

La clé de votre victoire : mettre en œuvre la fonction de reconstruction pour une véritable cyber-résilience

La véritable cyber-résilience repose sur une capacité critique qui s'étend au-delà des cadres classiques de la cybersécurité. Comme nous l'avons établi au Chapitre 2, le cadre de cybersécurité du NIST nécessite une septième fonction : Reconstruire. Cette fonction transforme l'incertitude en confiance, rendant obsolète l'approche du « J'espère vraiment que la sauvegarde fonctionne » grâce à des tests réguliers qui témoignent des capacités de récupération.

L'approche de viabilité minimale décrite au Chapitre 3 rend cette transformation réalisable. Plutôt que de tenter de tout tester simultanément, les entreprises peuvent mettre en œuvre la reconstruction de manière systématique, en commençant par les systèmes critiques pour l'entreprise et en s'étendant à des environnements complets. Ce cadre stratégique transforme un défi écrasant en un processus gérable, étape par étape, qui apporte une valeur immédiate tout en renforçant la résilience globale.

La menace agentique : pourquoi la vitesse des attaques modifie les exigences en matière de récupération

Les experts prédisent que nous pourrions vivre dans un monde d'attaquants agentiques dès cette année, les agents d'IA représentant une perspective attrayante pour les cybercriminels, car ils sont beaucoup moins coûteux que

l'embauche de hackers professionnels et peuvent orchestrer des attaques plus rapidement et à une échelle beaucoup plus grande que les humains.

Les ransomwares agentiques représentent une collection de robots d'IA, qui exécutent toutes les étapes nécessaires à la réussite des attaques par ransomware, mais plus rapidement et mieux que les opérateurs humains. Ces systèmes ne se contentent pas d'accélérer les méthodes d'attaque existantes, ils changent fondamentalement la donne en fonctionnant à la vitesse d'une machine dotée de capacités d'apprentissage automatique.

Les implications pour la récupération sont profondes. Dans près d'un cas sur cinq, l'exfiltration des données a désormais lieu dans la première heure suivant la compromission. Les approches classiques de sauvegarde et de récupération, conçues pour des menaces à vitesse humaine qui fournissaient des jours ou des semaines d'avertissement, deviennent obsolètes lorsque les attaques passent de la reconnaissance au chiffrement en quelques minutes.

C'est pourquoi la fonction de reconstruction rapide et automatisée devient encore plus essentielle à l'ère agentique. Ce n'est que par des tests réguliers et automatisés que les entreprises peuvent garder une longueur d'avance sur des adversaires qui apprennent et s'adaptent à une vitesse surhumaine.

La voie stratégique à suivre : de la viabilité minimale à la résilience complète

Le chemin vers la confiance en la reconstruction suit le cadre de viabilité minimale qui rend les tests complets réalisables. Les entreprises commencent par identifier leurs systèmes stratégiques, ceux qui sont essentiels à une viabilité minimale en cas de crise. Elles mettent ensuite en œuvre des instantanés PITR et une automatisation RaC pour ces systèmes prioritaires en premier lieu.

Le succès avec une viabilité minimale crée une base pour l'expansion. Les entreprises peuvent ensuite étendre les capacités de reconstruction aux systèmes critiques à la mission tels que la comptabilité et la gestion de la chaîne d'approvisionnement, puis aux applications non critiques. Chaque expansion s'appuie sur des processus éprouvés et sur une

expertise organisationnelle croissante, et, en fin de compte, une capacité de reconstruction complète est atteinte dans l'ensemble de l'écosystème numérique.

Les plateformes cloud hyperscale abordées au Chapitre 3 rendent cette progression économiquement viable. Les instances ponctuelles permettent jusqu'à 90 % de réduction des coûts de test par rapport à la tarification à la demande, selon la documentation officielle d'AWS et d'Azure, tandis que l'infrastructure élastique permet une validation fréquente sans impact sur les systèmes de production.

Les tests de chaos confirment que les scénarios de test reflètent des scénarios de défaillance du monde réel, établissant ainsi une véritable confiance dans les capacités de récupération.

Surmonter les défis de la mise en œuvre

L'approche de viabilité minimale s'attaque systématiquement aux obstacles organisationnels courants à la mise en œuvre de la reconstruction. En effet, lorsque les dirigeants expriment leur inquiétude quant aux coûts, l'analyse de rentabilité devient convaincante. La restauration rapide des systèmes générateurs de revenus est rentabilisée dès le premier incident qu'elle permet d'éviter.

Considérez les cas concrets du Chapitre 3. MGM Resorts et Caesars Entertainment avaient des plans de reprise après sinistre complets, mais les deux entreprises ont eu du mal à restaurer parce qu'elles n'avaient pas de capacités de reconstruction testées. L'approche de viabilité minimale aurait pu faciliter la restauration rapide des activités de jeu et d'hébergement de base, tandis que la reprise complète se poursuivait en parallèle, minimisant les perturbations de l'activité et l'impact sur les clients.

De même, l'expérience de NHS London avec le ransomware Qilin a démontré que des sauvegardes robustes n'ont pas de sens sans des procédures de restauration vérifiées pour les applications, les identités et les architectures de réseau. Une stratégie de viabilité minimale aurait donné la priorité à la restauration du système de soins aux patients, permettant aux opérations de soins de santé essentiels de se poursuivre pendant que la reconstruction complète s'attaquait aux systèmes administratifs et de soutien.

Contraintes budgétaires et de ressources

L'automatisation RaC réduit les runbooks fragmentés en pipelines unifiés et contrôlés par version. Les équipes de sécurité, d'exploitation du cloud, d'application et de récupération collaborent sur la même base de code plutôt que de maintenir une documentation séparée et en silos. Cette consolidation élimine le besoin d'exercices séparés entre les équipes tout en assurant la cohérence et en réduisant l'effort manuel.
Le retour sur investissement devient clair lorsque les entreprises mesurent les délais de restauration d'une viabilité minimale. La réduction du RTO de 48 heures à 2 heures pour les systèmes critiques de l'entreprise produit une valeur immédiate. L'automatisation de la collecte de preuves pour la conformité SOC 2, ISO 27001 et DORA réduit les frais généraux d'audit tout en fournissant une validation continue des capacités de récupération.

Adhésion des équipes dirigeantes et alignement organisationnel

Rien ne renforce le soutien du leadership comme une capacité tangible. Les entreprises peuvent afficher des indicateurs de reconstruction en direct via des tableaux de bord, mettre des rapports d'audit à la portée des dirigeants et démontrer l'achèvement de la récupération en moins d'une heure plutôt qu'en quelques jours ou semaines.

L'approche de viabilité minimale rend l'impact commercial immédiatement visible. Lorsque la direction constate que les principaux systèmes générateurs de revenus peuvent être restaurés rapidement et de manière fiable, le financement et le soutien organisationnel suivent naturellement. Chaque test de viabilité minimum réussi renforce la confiance pour une mise en œuvre de la reconstruction à plus grande échelle.

Perspectives d'avenir : Quand la reconstruction devient une pratique courante

L'avenir de la cyber-résilience est déjà en train d'émerger, sous l'impulsion de la réalité des menaces agentiques. Avec la montée en puissance de l'IA agentique, les équipes de sécurité délégueront davantage de tâches à des agents autonomes avec un minimum d'instructions, permettant aux systèmes et aux réseaux de suivre l'évolution constante des tactiques de menace. Dans cinq ans, la fonction de reconstruction sera aussi fondamentale pour la cybersécurité que les fonctions actuelles établies dans le cadre du NIST. La planification de la viabilité minimale sera une pratique courante, les entreprises maintenant des procédures de récupération testées pour les systèmes critiques de l'entreprise aussi rigoureusement qu'elles maintiennent des contrôles financiers.

Cette transformation va remodeler la façon dont les entreprises abordent la résilience numérique :

- *Capacités de reconstruction améliorées par l'IA:* Les futurs systèmes de reconstruction tireront parti de l'IA pour identifier automatiquement les dérives de configuration, prédire les scénarios de défaillance potentiels et effectuer des tests de chaos (chaos testing) systématiques qui anticipent les nouveaux vecteurs d'attaque avant leur déploiement. Ces systèmes de récupération agentique travailleront aux côtés d'opérateurs humains pour assumer de manière autonome les tâches de routine, augmenter la prise de décision humaine et automatiser les flux de travail.
- *Réponse adaptée à la vitesse:* Les capacités de reconstruction doivent s'accélérer en réponse à l'accélération des attaques. Les entreprises mettront en œuvre des systèmes de récupération alimentés par l'IA, conçus pour exécuter une restauration complète de l'environnement plus rapidement que les attaquants agentiques ne peuvent adapter leurs stratégies.
- *Avantage concurrentiel:* Les entreprises qui peuvent démontrer une récupération rapide et fiable obtiendront des avantages concurrentiels importants. Les clients et les partenaires préféreront les fournisseurs qui peuvent démontrer une continuité de service fiable. Dans les secteurs réglementés, des capacités de reconstruction éprouvées deviendront une exigence pour le maintien des licences et des certifications.

Les entreprises qui adoptent aujourd'hui la fonction de reconstruction, en commençant par une viabilité minimale et en évoluant vers une couverture complète, deviendront celles qui non seulement survivront aux attaques de demain, mais en sortiront plus fortes. Elles transformeront les cyber-incidents de catastrophes menaçant l'entreprise en défis opérationnels gérables.

Votre cheminement : de l'espoir à la confiance

Le choix auquel chaque organisation est confrontée est clair : continuer à espérer que les méthodes classiques de sauvegarde et de récupération suffiront à faire face aux menaces modernes ou commencer à mettre en place une capacité de reconstruction démontrée qui offre une véritable confiance.

L'approche de viabilité minimale rend ce choix réalisable. Commencer par un seul système critique pour l'entreprise. Mettre en œuvre des instantanés PTIR et l'automatisation RaC. Effectuer des tests de chaos pour valider la restauration sous contrainte. Mesurer et démontrer les résultats.

Le succès d'un système jette les bases d'une expansion systématique. Chaque système supplémentaire bénéficie d'une expertise organisationnelle croissante, de processus éprouvés et d'une automatisation établie. Le passage de l'espoir de sauvegarde à la reconstruction de la confiance s'accélère à mesure que les capacités s'affinent.

Tester d'abord sa viabilité minimale, puis développe systématiquement. Récupérer en toute confiance grâce à des capacités de reconstruction éprouvées. Prospérer en faisant de la résilience un avantage concurrentiel.

Les cybermenaces de demain seront plus sophistiquées, plus persistantes et plus dévastatrices que les attaques d'aujourd'hui. Les entreprises qui attendent des solutions parfaites ou des conditions idéales seront mal préparées alors que leur survie dépend de la vitesse et de la fiabilité de la récupération.

Votre parcours commence par la compréhension des systèmes critiques de votre entreprise et la mise en œuvre du cadre de viabilité minimum. La technologie existe. Les méthodologies ont fait leurs preuves. La seule question est de savoir si vous allez commencer maintenant ou attendre que la prochaine attaque vous y oblige.

Faites le choix de la confiance. Faites le choix de la reconstruction. Faites le choix du succès dans un monde d'incertitude.

À propos de l'auteur

Govind Rangasamy est le fondateur et PDG d'Appranix, qui fait maintenant partie de Commvault, et un auteur du Forbes Technology Council. Entrepreneur en série possédant une vaste expérience dans la gestion du cloud d'entreprise, Govind a fondé Appranix pour révolutionner les modèles de résilience centrés sur l'infrastructure, qu'il estime inadéquats pour les applications cloud dynamiques et distribuées d'aujourd'hui. Il contribue régulièrement à Forbes et est fréquemment invité à des podcasts et à des conférences sur la résilience du cloud.