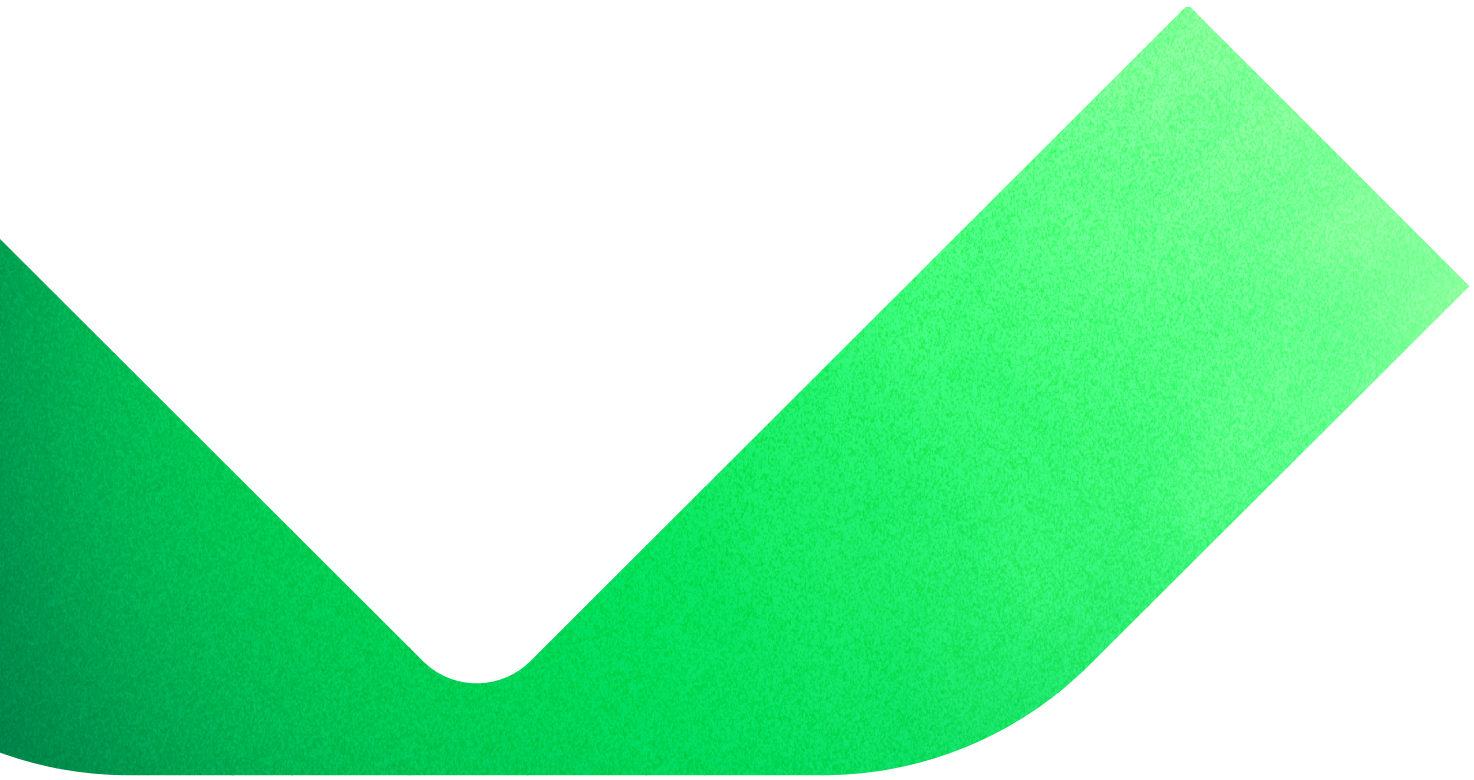
Concevoir une stratégie de restauration des données cyber-résiliente

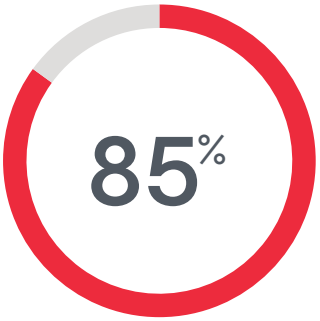


Sommaire

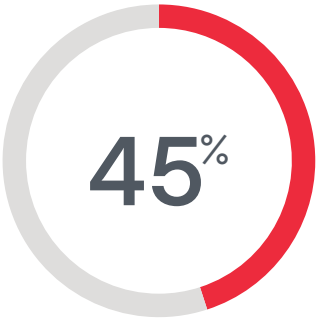
Introduction

La sécurité des données figure au premier plan des stratégies des entreprises. En effet, la menace des cyberattaques, en particulier des ransomwares, représente bel et bien un danger. Malheureusement, 85% des entreprises ont subi au moins une attaque par ransomware en 2022 (rapport Veeam sur les tendances de la protection des données en 2023). Plus alarmant encore, les ransomwares ne se contentent plus de bloquer l'accès des entreprises à leurs données : ils les exfiltrent ou les volent pour les vendre, les utilisent pour de futures attaques ou à des fins d'extorsion.

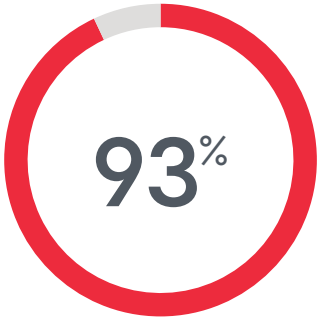
Quel qu'il soit, un plan de cybersécurité doit avoir pour objectif principal d'empêcher tout accès malveillant aux données. Néanmoins, aucune entreprise ne peut être sûre que son système de protection résistera en toutes circonstances. Il est donc tout aussi important de pouvoir restaurer les données en dernière ligne de défense. Les entreprises victimes de ransomwares ont perdu en moyenne 15% de leurs données de production (rapport Veeam sur les tendances des ransomwares en 2023). D'où l'importance d'un plan de restauration des données fiable et bien conçu.



des organisations ont été touchées par par une attaque de ransoware en 2023*.



des données de production ont été affectées par une cyberattaque*



des attaques de ransomware sauvegardes ciblées*

Source : rapport Veeam sur les tendances des ransomwares en 2023

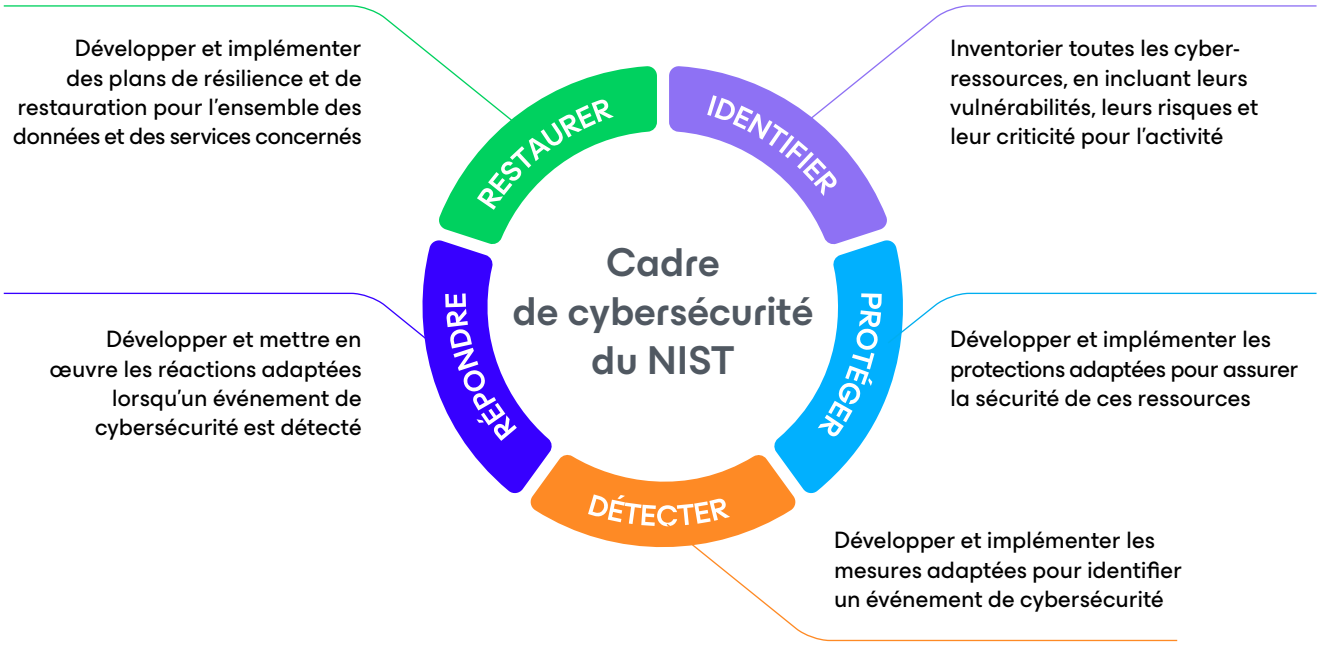
Un socle fiable pour restaurer les données

Dans le cadre d'une stratégie de disponibilité des données, la restauration des données constitue souvent le dernier rempart d'un plan de cybersécurité et doit donc être bien étudiée et planifiée. En suivant des concepts de protection des données tels que la règle du 3-2-1-1-0 et en disposant d'un outil unique qui sauvegarde les données au sein de l'infrastructure et les restaure à un état d'intégrité à tout moment et selon les besoins après un cyberincident, les entreprises détiennent la configuration parfaite pour restaurer les données en toute situation.

Les clients Veeam y parviennent de manière sécurisée, orchestrée et bien documentée, grâce à la Veeam Data Platform. En utilisant la suite complète, notamment Veeam Backup & Replication, Veeam ONE et Veeam Recovery Orchestrator, les clients atteignent des objectifs de sécurité des données qui s'alignent sur toutes les phases de l'infrastructure de cybersécurité du NIST et vont bien au-delà de la sauvegarde et la restauration des données.

Une infrastructure commune pour la planification de la cybersécurité

L'infrastructure de cybersécurité du NIST est une infrastructure éprouvée que les entreprises peuvent utiliser pour améliorer leur stratégie de cybersécurité. Organisée en un ensemble reproductible de phases et de fonctions pouvant être appliquées à de multiples disciplines informatiques et métier, cette infrastructure a pour but de guider les entreprises dans la gestion des risques liés à la cybersécurité.



Si un logiciel de disponibilité des données constitue un composant clé de la phase de restauration de l'infrastructure de cybersécurité du NIST, peu d'utilisateurs le considèrent par nature applicable aux autres phases d'une stratégie de cybersécurité. Depuis de nombreuses années, Veeam s'efforce de tirer parti de sa position en tant que plateforme de protection des données des grandes entreprises pour mieux fournir à ses clients les informations dont ils ont besoin pour protéger leurs données.

S'inspirant essentiellement du cadre de cybersécurité du NIST, ce livre blanc vise à fournir aux services IT, équipes de sécurité et décideurs les connaissances nécessaires pour utiliser la Veeam Data Platform à des fins d'identification des données stratégiques, de détection des logiciels malveillants, de protection des données, de réponse rapide aux menaces actives et de restauration rapide de données saines, tout en présentant les fonctionnalités clés utilisées pour atteindre ces objectifs.

Identifier les données stratégiques

Comme pour tout incident susceptible de toucher une entreprise, la planification constitue la première étape. En effet, la cybersécurité partage un credo essentiel avec la reprise après incident classique : **vous ne pouvez pas protéger ce que vous ne connaissez pas**. Inventorier et catégoriser les ressources à protéger peut sembler anodin comparé à la protection active et la réponse à une menace de cybersécurité, mais la première étape consiste à estimer ce qui est menacé et à quel niveau de priorité. Grâce aux fonctionnalités suivantes, Veeam peut constituer un élément essentiel d'une stratégie multicouche pour **identifier** les données stratégiques.

Inventorier les systèmes et données stratégiques

Pour créer un plan de reprise fiable, les équipes IT et de sécurité doivent travailler en étroite collaboration avec l'entreprise pour identifier, inventorier et prioriser les workloads et données de l'entreprise. Les rapports disponibles dans Veeam ONE et le catalogue des systèmes en cours de sauvegarde par Veeam Backup & Replication sont parfaits pour commencer. Toutes les données stratégiques doivent être sauvegardées, et Veeam informe l'utilisateur en cas de machines virtuelles ou données non protégées.

De même, le réseau et les outils de sécurité utilisés par l'équipe de sécurité peuvent créer une liste des systèmes au sein de l'environnement. Comparer ces différents systèmes permet souvent de détecter des données mal protégées dans chaque outil, et de garantir ainsi des plans de protection et de restauration complets.

Identifier et prioriser les données grâce au balisage et à la classification

En utilisant les fonctionnalités de balisage et de classification des données dans Veeam Backup & Replication, les clients démarrent avec un catalogue concret de workloads (leurs sauvegardes), et commencent à appliquer des balises pour identifier des métadonnées système comme la localisation, le propriétaire et la priorité de restauration. Cela permet parfois de mettre en évidence des données manquantes, d'indiquer une lacune dans la protection des données ou d'identifier des métadonnées clés nécessaires pour planifier correctement la restauration des données.

Une fois les métadonnées identifiées, l'assistant de planification des restaurations de Veeam Recovery Orchestrator permet de créer le plan de restauration et contribue ainsi à réduire le temps nécessaire à son élaboration. Le plan peut ensuite être revu avec l'entreprise pour vérifier qu'il répond précisément à ses besoins.

Mettre en évidence les lacunes et les modifications grâce aux tests de restauration automatisés

Le meilleur moyen de vérifier qu'une sauvegarde ou un plan fonctionnent en cas d'urgence consiste à les tester. Les fonctionnalités de tests automatisés de Veeam Recovery Orchestrator offrent l'avantage considérable de garantir la restauration complète de tout ou partie de l'infrastructure. Outre les avantages évidents de réduction du travail pendant l'exécution des tests, l'automatisation peut également se traduire par des tests plus fréquents, permettant de signaler des lacunes plus rapidement.

Les systèmes qui ne sont pas sauvegardés ou pris en compte figurent parmi les lacunes identifiées grâce à des tests fréquents. En vérifiant régulièrement les résultats des tests et en corrigeant rapidement les lacunes, il est possible de savoir exactement quelles ressources sont à protéger.

Protéger les données et l'infrastructure de sauvegarde

Quel que soit l'environnement IT, l'infrastructure de sauvegarde y tient une place prépondérante. Elle constitue non seulement l'ultime filet de sécurité pour les données, mais contient aussi plusieurs copies de toutes les données (plus les données sont stratégiques, plus les copies sont nécessaires), y compris des données qui ont pu être supprimées en production. Cela en fait une cible de choix pour les criminels qui n'hésitent pas à voler les données et supprimer le filet de sécurité afin d'améliorer le taux de réussite de leurs stratégies de rançon et d'extorsion. C'est pourquoi il est essentiel de **protéger** l'infrastructure de sauvegarde elle-même.

Une infrastructure de sauvegarde qui ne fait confiance à personne

Pour protéger les sauvegardes, la première étape consiste à empêcher tout accès non autorisé au système de gestion des sauvegardes. Les principes de la confiance zéro (vérification explicite, supposition de violation et moindre privilège) devraient être appliqués afin de rendre les mouvements latéraux dans l'infrastructure de sauvegarde aussi difficiles que possible.

Pour contrôler les politiques utilisateur, l'authentification multifacteur et la mise en place d'un système distinct de gestion des identités et des accès (IAM) dédié à la protection des données garantissent que les utilisateurs sont strictement contrôlés et plus difficiles à compromettre. Un contrôle d'accès basé sur le principe du moindre privilège (en séparant par exemple les comptes administrateur et opérationnel) permet de prévenir les erreurs involontaires et de minimiser l'accumulation de privilèges. Enfin, l'ensemble doit être configuré en supposant que le reste de l'infrastructure a déjà été compromis, en isolant les composants de sauvegarde sur un réseau séparé et en restreignant l'accès à la console Veeam Backup & Replication via une connexion VPN ou à distance.

Tous les niveaux de l'infrastructure de sauvegarde doivent intégrer ces approches à des degrés légèrement différents. Les systèmes d'exploitation, partages de fichiers, la gestion hors bande et toute autre application de gestion utilisée doivent suivre les mêmes principes.

Analyser la conformité de l'infrastructure de sauvegarde

Pour aider les clients à appliquer correctement les principes de la confiance zéro, la console Veeam Backup & Replication intègre un utilitaire appelé « Analyseur de sécurité et de conformité » (anciennement « Outil d'analyse des meilleures pratiques ») qui analyse l'infrastructure Veeam et signale les éléments de configuration qui n'ont pas été mis en œuvre selon les recommandations Veeam. Cette analyse doit être régulièrement exécutée et chaque élément non conforme doit être corrigé ou supprimé. Les éléments supprimés comportent le nom de l'utilisateur, ainsi que la date et l'heure de la suppression. Une fois les corrections effectuées, l'analyse doit être à nouveau effectuée et les résultats documentés.

S'assurer que des sauvegardes existent en cas de besoin

Une caractéristique courante des ransomwares consiste à supprimer des sauvegardes de manière à ce que les données ne puissent pas être restaurées. Il est donc indispensable de s'assurer que les sauvegardes ne peuvent être ni modifiées, ni supprimées.

L'inaltérabilité est un concept informatique très ancien, devenu récemment indispensable pour les sauvegardes, en particulier pour celles qui doivent rester inchangées ou exemptes d'erreurs afin de satisfaire aux exigences de rétention. Cibles renforcées, stockage objet, appliances de déduplication tierces, bandes… différents moyens existent pour stocker les sauvegardes Veeam sans même que les administrateurs puissent modifier ou supprimer les données. Comme avec n'importe quel système de sécurité, des contournements existent. Aussi est-il essentiel de considérer la pile dans son intégralité, jusqu'à la base du datacenter, pour éliminer ou contrôler strictement ces contournements.

Dans le domaine de la cybersécurité, on dit souvent que le système le plus sûr est celui qui reste éteint, déconnecté du réseau et stocké dans une pièce à laquelle personne n'a accès. Bien que tout à fait exact, voilà qui est amusant, parce que ce système n'a aucune raison d'exister. Cet adage peut toutefois s'appliquer à la sécurité des sauvegardes. Tant qu'elle reste accessible en cas de besoin, une sauvegarde stockée hors ligne est la moins susceptible d'être altérée. Veeam offre plusieurs options pour concevoir cette approche de sauvegardes physiquement isolées, des systèmes en ligne qui requièrent une authentification différente au stockage sur bande, la meilleure option hors ligne.

Aucun plan ne devrait se baser sur une seule couche de protection. Aussi, Veeam Backup & Replication peut activer le principe des « quatre yeux » pour la suppression des sauvegardes. Similaire à l'ancienne « règle des deux hommes », cette configuration requiert deux administrateurs pour autoriser la suppression d'une sauvegarde et protéger ainsi les sauvegardes contre les suppressions accidentelles ou malveillantes.

Modèle de sécurité confiance zéro

Le concept de « confiance zéro » a pour objectif d'éliminer la confiance qui a toujours prévalu au sein du périmètre de sécurité, pour éviter que les menaces circulent facilement dans un environnement. Grâce au mantra « ne jamais faire confiance, toujours vérifier », un modèle de sécurité sans périmètre est créé, qui ne compte pas sur le pare-feu pour stopper les cybermenaces. Selon ce modèle, chaque système doit vérifier toutes les nouvelles interactions, sans supposer qu'elles sont sécurisées.

Les trois principes du modèle de sécurité confiance zéro sont les suivants :

1. Vérifier explicitement
2. Fournir un accès selon le principe du moindre privilège
3. Supposer qu'une violation peut se produire

Chiffrer ses propres sauvegardes

Pour protéger les données des abus après leur exfiltration, les sauvegardes peuvent être chiffrées par Veeam afin d'empêcher quiconque d'y accéder en dehors de l'infrastructure Veeam. Si cela n'empêche pas le vol ou le verrouillage des données par un ransomware, il est très peu probable qu'elles puissent faire l'objet deplans d'extorsion. Ce chiffrement peut être géré en interne par Veeam ou confié à un système tiers de gestion des clés.

Détecter les cybermenaces

Une fois l'ensemble des données et des systèmes identifiés, l'entreprise doit mettre en place des plans et des systèmes de détection rapide des intrusions sur ses actifs. Une détection rapide réduira considérablement le temps de séjour et l'impact de la menace, qui se traduit en général par une perte d'argent. Là encore, les logiciels Veeam constituent des composants clés d'une stratégie multicouche pour **détecter** les cybermenaces.

Attirer l'attention sur les comportements anormaux

L'une des stratégies clés des logiciels malveillants consiste à éviter d'être détectés tout en accumulant des privilèges et en se déplaçant latéralement dans l'environnement, en infectant autant de systèmes que possible. Pour éviter de se faire remarquer, ils peuvent opérer très peu de changements à la fois. En outre, comme ils sont devenus plus habiles pour contrecarrer les efforts de restauration des données sur lesquelles ils souhaitent demander une rançon, les auteurs de logiciels malveillants commencent à supprimer des sauvegardes, réduire les délais de rétention des sauvegardes ou désactiver des tâches de sauvegarde. Veeam peut identifier et signaler ces types de comportements anormaux au moyen d'alertes et de rapports dans Veeam ONE.

Rechercher des logiciels malveillants pendant la sauvegarde

Grâce à la détection des logiciels malveillants à la volée, Veeam Backup & Replication peut analyser les blocs qui passent par les nœuds Veeam Proxy à la recherche de signes d'un nouveau chiffrement, indicateur clé de la présence d'un logiciel malveillant. Une recherche dans l'index de la sauvegarde permet de détecter des signatures et noms de fichiers malveillants. En cas d'élément suspect, la sauvegarde sera signalée comme suspecte.

Détecter les logiciels malveillants dans les sauvegardes

La fonctionnalité SureBackup de Veeam Backup & Replication a été conçue à l'origine pour automatiser la restauration et la validation des sauvegardes pouvant être restaurées. Les logiciels de protection des postes de travail n'étaient pas parfaits et pouvaient entraîner l'infection des sauvegardes. SureBackup intègre des fonctionnalités puissantes de détection des logiciels malveillants dans les sauvegardes.

Dans le cadre d'un test de la capacité de restauration, SureBackup peut s'associer aux outils de détection des logiciels malveillants afin d'analyser la machine virtuelle restaurée. Cela permet aux entreprises d'utiliser un outil secondaire de détection des logiciels malveillants dans une approche de la détection de type « faire confiance mais vérifier ». De plus, l'analyse SureBackup se déroule sans impact sur le workload de production, ce qui permet d'effectuer une analyse plus approfondie. SureBackup peut aussi monter des disques individuels sur une machine test qui analyse ensuite les fichiers à la recherche de logiciels malveillants. Un moyen encore plus rapide et économe en ressources dans les cas où une restauration complète n'est pas nécessaire.

Si ces analyses révèlent des éléments suspects, alors ce point de restauration particulier sera signalé comme suspect.

Tester régulièrement le plan de reprise pour détecter les altérations

Des tests réguliers des plans de reprisemettant en évidence les altérations dues aux logiciels malveillants peuvent s'avérer utiles. En effet, lors du test complet d'un plan de reprise comprenant notamment la vérification des applications, des échecs peuvent révéler des zones de l'infrastructure dans lesquelles un fichier de clé a été chiffré ou un fichier de configuration a été modifié de manière inappropriée. Cela peut être particulièrement utile pour détecter l'exécution d'un logiciel malveillant pendant une séquence de démarrage.

Reporting centralisé des journaux et corrélation

L'envoi des fichiers journaux à un service syslog externe offre à la fois un référentiel de journaux secondaire et une centralisation permettant de corréler les événements entre les systèmes. C'est la fonction principale d'un système de gestion des événements et des incidents de sécurité (SIEM) pour la plupart des équipes de sécurité. Lorsque le système SIEM est configuré en tant que destination syslog, les indicateurs d'altération découverts par Veeam peuvent être signalés directement dans le système utilisé par l'équipe de sécurité. Cela réduit le temps de réponse et offre aux analystes de sécurité une vision plus fiable de l'événement.

Temps de séjour

Le temps de séjour, c'est-à-dire la durée d'existence du logiciel malveillant dans l'environnement avant sa découverte, est la période durant laquelle il réside dans l'environnement sans exécuter l'attaque principale. Il peut passer ce temps à compromettre d'autres comptes, élever des privilèges, s'implanter plus profondément dans le système d'exploitation, s'étendre latéralement à d'autres systèmes et rassembler toutes les informations utiles pour les attaques actuelles ou futures.

Intégrations externes pour la protection des données

L'API d'incidents est un ensemble d'interfaces de programmation d'applications que les outils de cybersécurité peuvent utiliser pour informer l'infrastructure de sauvegarde d'une infection et signaler des sauvegardes suspectes ou infectées. Il est possible de configurer Veeam Backup & Recovery pour alerter les administrateurs en fonction de ces informations. Cela leur permet d'examiner, vérifier et répondre rapidement par des actions telles que la création d'une sauvegarde immédiate, l'exécution d'une action SureBackup pour vérifier qu'il n'y a pas d'infection et restaurer les fichiers sains, et la création d'une copie inaltérable d'une sauvegarde à des fins d'analyse forensique. Ce point d'intégration ouvert entre les outils de sécurité et la plateforme de protection des données améliore considérablement la communication, contribuant ainsi à réduire le temps de séjour des logiciels malveillants pour une restauration plus rapide et plus saine.

Répondre aux cybermenaces

Assurer en permanence une protection totale est impossible. Il faut donc à tout prix essayer de bloquer les logiciels malveillants et de les supprimer le plus rapidement possible. Comme pour planifier la reprise après une catastrophe naturelle, l'objectif de temps de restauration (RTO) constitue l'un des principaux objectifs vers lequel toutes les décisions devraient converger. De fait, lors d'un événement de cybersécurité, l'objectif premier consiste à bloquer le logiciel malveillant et le supprimer de l'environnement avant de remettre en service les systèmes. Si le temps laissé au logiciel malveillant pour séjourner et exfiltrer les données est réduit, l'effort de nettoyage sera moindre et la restauration plus rapide. C'est pourquoi il est indispensable de se préparer à **répondre** rapidement.

Utiliser les sauvegardes pour l'analyse forensique de cybersécurité

Tel qu'évoqué plus tôt, SureBackup est une fonctionnalité qui ne se contente pas de tester la capacité de restauration des sauvegardes : elle détecte aussi les logiciels malveillants. L'un des objectifs en phase de réponse consiste à identifier le temps de séjour. L'utilisation des alertes de la console Veeam Backup & Replication, qui indiquent si un logiciel malveillant a été détecté à un point de restauration ou décelé par un outil tiers utilisant l'API d'incidents, facilite la recherche du premier point d'infection.

Autre fonctionnalité de Veeam Backup & Replication, Secure Restore permet de monter les disques pour y détecter la présence de logiciels malveillants avant une restauration complète. Renouveler ce processus jusqu'à la découverte d'un point non infecté permet de trouver facilement l'instant précis où le logiciel malveillant est apparu sur un système donné, mais aussi d'éviter une réinfection causée par la restauration d'une partie restée dormante.

Avec Veeam Recovery Orchestrator, ce processus Secure Restore peut être exécuté dans l'ensemble de l'environnement, selon une approche de « salle blanche » orchestrée. Cela permet non seulement d'accélérer le contrôle des points de restauration sains, mais ajoute également des informations précieuses à l'analyse forensique d'un incident de cybersécurité.

Exfiltration

Si des données ont été atteintes et modifiées par un logiciel malveillant, il est probable qu'elles aient d'abord été volées. Les données exfiltrées sont envoyées aux cybercriminels depuis l'environnement de la victime.Elles peuvent être divulguées ou vendues par les cybercriminels après une violation, entraînant l'exposition de secrets d'entreprise, une atteinte à la réputation et le vol d'informations personnelles débouchant sur une fraude ou une cyberattaque.

Chasse aux menaces améliorée avec YARA

Outil très connu des traqueurs de menaces de cybersécurité, YARA s'appuie sur des règles pour identifier et classifier les logiciels malveillants. Dans le cadre d'une opération SureBackup ou Secure Restore, une règle YARA peut être identifiée et exécutée à des fins de classification initiale du logiciel malveillant pour le rechercher parmi les sauvegardes.

Suivi des incidents avec ServiceNow

Grâce aux intégrations directes dans ServiceNow, Veeam peut automatiquement créer de nouveaux tickets et mettre à jour les existants selon l'évolution de la situation. Cela permet aux différentes équipes de communiquer de manière plus efficace et de bénéficier d'un historique automatisé de l'incident.

Restaurer les données sécurisées plus vite que jamais

Selon la nature de l'incident de cybersécurité, et notamment en cas de ransomware, la restauration n'est possible que si les données sont saines. Si le temps de séjour est long, le logiciel malveillant peut être présent au niveau de nombreux points de restauration, obligeant à revenir loin en arrière pour trouver un point de restauration sain. Comme pour une reprise après incident classique, il est important de s'aligner sur des objectifs de réduction des pertes de données : le délai optimal de reprise d'activité (RPO). Étant donné l'importance de découvrir le début de l'infection dans la phase de réponse, bon nombre de ces efforts seront déployés parallèlement aux efforts de **restauration**des données.

Une sauvegarde utile est une sauvegarde qui peut être restaurée (et exempte de logiciels malveillants)

Lorsque SureBackup ou l'API d'incidents signalent des points de restauration suspects ou infectés pendant les phases de détection et de réponse, il est très facile de déterminer directement dans la console Veeam Backup & Replication si un logiciel malveillant a été détecté à chaque point de restauration. C'est un bon point de départ, qui ne garantit pas cependant que les points de restauration précédents sont totalement sains.

Pour réduire le risque de restaurer des données infectées et minimiser les duplications, des efforts de restauration doivent être déployés parallèlement aux analyses forensiques de cybersécurité menées lors de la phase de réponse. Une collaboration étroite entre les équipes IT, de sécurité et l'entreprise est essentielle pour restaurer les données appropriées sans réintroduire le logiciel malveillant.

L'utilisation d'outils de détection parfaitement à jour dans le cadre de SureBackup et Secure Restore peut permettre de détecter dans les premiers points de restauration des logiciels malveillants qui n'avaient pas été repérés jusqu'alors. Il est donc important de ne pas se fier uniquement aux indicateurs de logiciels malveillants provenant d'analyses antérieures. Dans le cas où les points de restauration sains se situent bien avant les RPO définis, il est possible d'effectuer des restaurations de données individuelles essentielles au niveau fichier, tout en évitant les logiciels malveillants dans la sauvegarde complète.

Sauvegarde ou réplication après une cyberattaque

Si la réplication fait partie d'un plan de reprise après une cyberattaque, il est important de différencier ses objectifs de ceux de la sauvegarde. La réplication consiste à déplacer des données le plus rapidement possible et à revenir au réplica sain le plus récent. Comme les sauvegardes ne s'exécutent pas en continu, elles permettent d'être plus méthodique en garantissant des données saines, qu'il est possible de restaurer. Sachant que la reprise après un événement de cybersécurité doit tenir compte du temps de séjour et s'appuyer sur des données saines au point de restauration, la sauvegarde est un mécanisme plus répandu.

Restaurer les données non infectées le plus vite possible

Pour restaurer rapidement, même les environnements les plus simples, l'automatisation est la clé. Cela dit, le mode de restauration peut aussi faire la différence. Avec des snapshots de baie de stockage et la restauration instantanée, les données restaurées peuvent être utilisées presque instantanément.

Veeam Recovery Orchestrator a été conçu pour définir un processus de restauration complet qu'il est possible d'activer d'un simple clic. Plan de reprise avec alertes en cas d'infection, Secure Restore, snapshots de baie de stockage, restauration instantanée, vérification des applications… Veeam offre une riche palette de fonctionnalités pour restaurer les données de manière rapide et efficace, tout en s'assurant qu'elles sont exemptes de logiciels malveillants.

Visualiser les anomalies d'I/O

Parfois, rien ne vaut un graphique visuel pour mettre en lumière des tendances. Dans l'interface utilisateur de Veeam Backup & Replication, des graphiques sont fournis pour toute restauration à partir d'une tâche de réplication. Ils permettent d'identifier le point de départ d'un chiffrement en masse, et facilitent ainsi la recherche d'un instant précis avant le chiffrement.

Synthèse

Aujourd'hui, la conception d'une stratégie de cybersécurité est loin d'être une tâche aisée. Les menaces sont nombreuses et une violation représente une valeur potentiellement considérable pour les cybercriminels. Aussi, les entreprises doivent utiliser tous les outils à leur disposition pour créer des couches de sécurité permettant d'atteindre un niveau d'efficacité maximal à chaque phase du cadre de cybersécurité du NIST. C'est là qu'intervient Veeam pour améliorer leur stratégie de cybersécurité :

- Créer et tester régulièrement les plans de reprise peut fournir des données précieuses en phase **d'identification**, pour garantir que les données stratégiques sont identifiées et peuvent être protégées.
- Mettre en œuvre des meilleures pratiques documentées et des fonctionnalités de sécurité natives garantit que les sauvegardes et l'infrastructure de sauvegarde sont incluses dans la phase de **protection**.
- Les sauvegardes concernent l'ensemble des données de l'infrastructure. Elles peuvent donc offrir une deuxième vérification importante pour révéler des logiciels malveillants passés inaperçus sur les postes de travail en phase de **détection**.
- Accéder rapidement à différents instants précis et environnements de « salle blanche » virtuels peut s'avérer essentiel pour rassembler des informations en phase de **réponse**.
- Des sauvegardes dont la preuve est faite qu'elles peuvent être restaurées et sont exemptes de logiciels malveillants doivent être disponibles à tout moment. Elles assurent une restauration dans un état sain et utilisable le plus rapidement possible en phase de **restauration**.

Il est temps que les équipes IT endossent un rôle plus important que celui de simples gardiens des données à restaurer, et participent activement au plan de cybersécurité de l'entreprise. À l'aide des conseils proposés dans ce guide, elles doivent être en mesure d'échanger de manière productive avec les équipes de sécurité pour intégrer une plateforme de protection des données basée sur les solutions Veeam à leur stratégie de cybersécurité globale.

Pour en savoir plus sur les fonctionnalités mentionnées dans ce document, veuillez consulter les guides de l'utilisateur disponibles dans le centre d'aide Veeam. Beaucoup de ces nouvelles fonctionnalités sont incluses dans la mise à jour 2e semestre 2023 de la Veeam Data Platform.

Mise à jour 2e semestre 2023 de la Veeam Data Platform

Essai gratuit de l'édition Premium pendant 30 jours