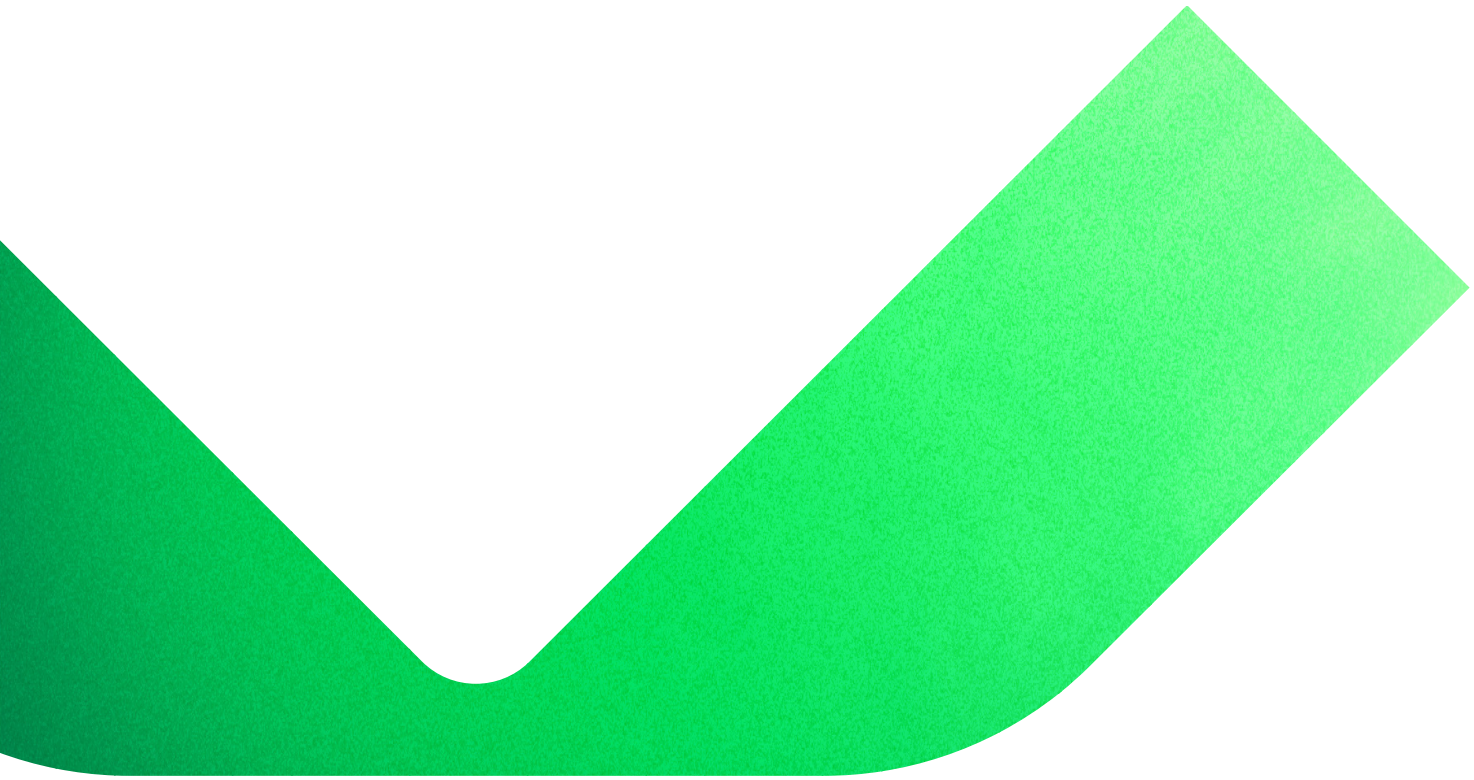
Concevoir une stratégie de restauration des données cyber-résiliente



Contenu

Introduction	**4**
Contexte du Cadre de cybersécurité du NIST	**5**
Un socle fiable pour la restauration des données	**8**
Fonction NIST « Identifier » (ID)	**9**
Inventorier les systèmes et données stratégiques	**9**
Identifier et prioriser les données grâce au balisage et à la classification	**9**
Mettre en évidence les lacunes et les modifications grâce aux tests de restauration automatisés	**9**
La fonction « Protéger » (PR) du NIST	**10**
Une infrastructure de sauvegarde qui ne fait confiance à personne	**10**
Analyser la conformité de l'infrastructure de sauvegarde	**10**
S'assurer que des sauvegardes existent en cas de besoin	**11**
Chiffrer ses propres sauvegardes	**11**
Barre latérale : Modèle de sécurité confiance zéro	**11**
Fonction NIST « Détecter »	**12**
Attirer l'attention sur les comportements anormaux	**12**
Rechercher des logiciels malveillants pendant la sauvegarde	**12**
Détecter les logiciels malveillants dans les sauvegardes	**12**
Tester régulièrement le plan de reprise pour détecter les altérations	**13**
Reporting centralisé des journaux et corrélation	**13**
Intégrations externes pour la protection des données	**13**
Barre latérale : Temps de séjour	**13**
Fonction NIST « Répondre »	**14**
Utiliser les sauvegardes pour l'analyse criminelle de cybersécurité	**14**
Chasse aux menaces améliorée avec YARA	**14**

Suivi des incidents avec ServiceNow	**15**
Barre latérale : Exfiltration	**15**
Fonction NIST « Restaurer »	**16**
Une sauvegarde utile est une sauvegarde qui peut être restaurée (et qui est exempte de logiciels malveillants)	**16**
Restaurer les données non infectées le plus vite possible	**16**
Visualiser les anomalies d'I/O	**17**
Barre latérale : Sauvegarde ou réplication pour des restaurations de cybersécurité	**17**
Fonction NIST « Gouverner »	**18**
Assurez-vous que tout est documenté	**18**
Une surveillance constante pour limiter les risques	**19**
Tableau de bord de la sécurité des sauvegardes	**19**
Conclusion	**20**

Introduction

Dans le monde numérique d'aujourd'hui, la cybersécurité est une nécessité fondamentale. Il n'est pas surprenant que chaque blog ou livre blanc sur la cybersécurité que vous lisez aujourd'hui tourne inévitablement autour des ransomwares. C'est ennuyeux d'en entendre parler (nous le savons !) mais les ransomwares sont devenus la plus grande menace pour les entreprises de toutes tailles et ciblent nos infrastructures et secteurs industriels les plus critiques. C'est un jeu du chat et de la souris et, lorsque de nouvelles menaces apparaissent, les équipes de sécurité doivent s'adapter pour suivre le rythme. La numérisation généralisée des opérations commerciales, des fonctions gouvernementales et des activités personnelles a augmenté de manière exponentielle le volume de données sensibles stockées et transmises en ligne. Malheureusement, ce changement a également élargi la surface d'attaque pour les cybercriminels, d'où l'importance de mesures de cybersécurité robustes.

Les cybermenaces, qu'il s'agisse de violations de données, d'attaques par ransomware ou de cyberespionnage sophistiqué parrainé par des États, présentent des risques importants pour l'intégrité d'infrastructures essentielles, la confidentialité de vos renseignements personnels et jusqu'à la stabilité des économies mondiales. La sécurité des données doit donc figurer au premier plan des stratégies des entreprises, car la menace de cyberattaques, en particulier de ransomware, représente bel et bien un danger. Malheureusement, 85 % des entreprises ont subi au moins une attaque par ransomware en 2022[1]. Plus alarmant encore, les attaques par ransomware ne se contentent plus de bloquer l'accès des entreprises à leurs données : elles les exfiltrent, les volent, les vendent ou les archivent pour les utiliser dans d'autres stratagèmes d'extorsion.

Quel qu'il soit, un plan de cybersécurité doit avoir pour objectif principal d'empêcher tout accès malveillant aux données. Cependant, aucune entreprise ne doit être sûre que son système de défense résistera en toutes circonstances. Il est donc tout aussi important de pouvoir restaurer vos données. Parmi les entreprises touchées par un ransomware, 15 % des données de production ont été perdues en moyenne[2] , d'où l'importance d'un plan de restauration fiable et bien conçu.

Des pratiques de cybersécurité efficaces protègent contre l'accès non autorisé aux données, assurent la continuité des opérations et préservent la confiance entre les consommateurs et les fournisseurs de services. À mesure que les cybermenaces évoluent en complexité et en envergure, on ne saurait trop insister sur l'importance de la cybersécurité dans la protection des actifs numériques, de la vie privée des individus et de la sécurité nationale. C'est un pilier essentiel de l'architecture de notre société numérique et nous permet de naviguer, d'innover et de communiquer dans ce domaine en toute confiance.

La récente mise à jour du Cadre de cybersécurité (CSF) 2.0[3] du NIST marque une évolution charnière dans l'approche standard de la cybersécurité et reflète l'évolution des paradigmes dans un monde où les menaces numériques sont de plus en plus complexes et omniprésentes.

Le présent document présente le Cadre de cybersécurité (CSF) du NIST mis à jour et les domaines dans lesquels Veeam Software peut vous aider à le mettre en place.

[1] https://go.veeam.com/wp-data-protection-trends-2024

[2] https://go.veeam.com/wp-data-protection-trends-2024

[3] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Contexte du Cadre de cybersécurité du NIST

Le Cadre de cybersécurité (CSF) du NIST a été présenté pour la première fois en 2014 pour répondre au besoin croissant d'une approche unifiée de la gestion des risques de cybersécurité. Élaboré par le National Institute of Standards and Technology (NIST) en collaboration avec des entités du secteur privé et public, il visait à fournir un ensemble de normes industrielles aux organisations afin de les aider à protéger leurs systèmes d'information. Les objectifs du CSF étaient d'aider les organisations à comprendre et à améliorer la gestion des risques liés à la cybersécurité, ce qui améliorerait également la sécurité et la résilience des infrastructures essentielles.

Le Cadre de cybersécurité (CSF) 2.0 du NIST, publié en février 2024, reprend les versions précédentes, mais introduit plusieurs changements importants qui reflètent l'évolution du paysage de la cybersécurité et prennent en compte les remarques émises par la communauté.

Le CSF 2.0 étend sa portée au-delà des secteurs critiques de l'infrastructure ; il a été révisé pour profiter à toutes les organisations, quelle que soit leur taille ou leur type, ce qui rend cette ligne directrice plus universellement applicable.

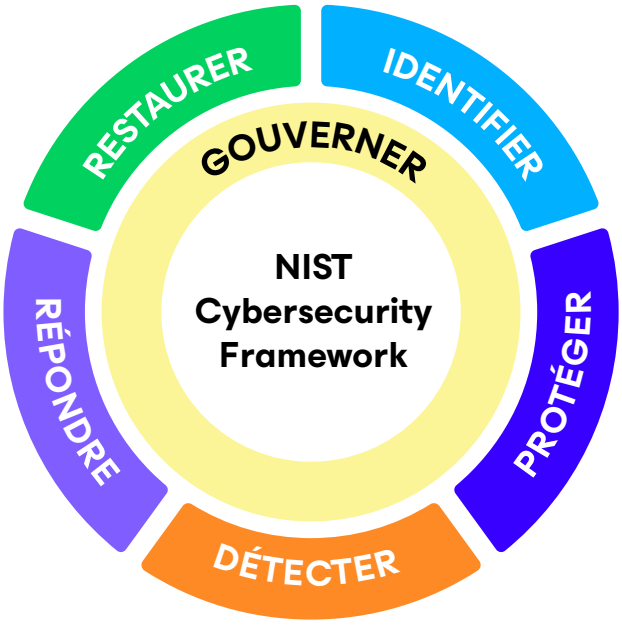


Figure 1 : Cadre de cybersécurité 2.0 du NIST

Il s'organise essentiellement autour de six grandes fonctions qui, ensemble, composent une recommandation globale qui s'inspire du cycle de vie des risques de cybersécurité.

- **Identifier :** mieux connaître les organisations afin de gérer les risques de cybersécurité pesant sur les systèmes les personnes, les actifs, les données et les fonctionnalités. Il s'agit notamment d'identifier les processus métier critiques et les actifs clés, ainsi que leurs vulnérabilités et menaces.
- **Protéger :** mettre en œuvre des mesures de protection appropriées pour assurer la prestation des services essentiels et limiter ou contenir l'impact des incidents de cybersécurité potentiels. Cela comprend la gestion des identités, le contrôle d'accès, la sécurité des données et les technologies de protection.
- **Détecter :** mettre en œuvre des mesures visant à identifier à temps la survenue d'incidents de cybersécurité. La supervision continue et la détection des menaces sont des fonctionnalités clés de cette fonction.
- **Répondre :** Agissez dès qu'un incident de cybersécurité est détecté. Cela comprend la planification, l'analyse, l'atténuation et la communication en cas d'incident.
- **Restaurer :** gérer les plans de résilience et restaurer les fonctionnalités ou les services détériorés lors d'un incident de cybersécurité. L'objectif est d'opérer cette restauration pour revenir à un fonctionnement normal dans les meilleurs délais.
- **Gouverner (nouveau) :** cette nouvelle fonction de CSF 2.0 se concentre sur la gestion globale et la gouvernance des risques de cybersécurité. C'est là que les organisations établissent leur stratégie, leurs politiques et leur supervision de la gestion des risques de cybersécurité, notamment en définissant les rôles et les responsabilités et en intégrant la cybersécurité dans la gestion des risques de l'entreprise.

La nouvelle fonction « Gouverner » relève les objectifs fondamentaux de reddition de comptes et de transparence et sert de force unificatrice pour aider les organisations à établir des priorités et atteindre les objectifs énoncés dans les cinq autres fonctions. Elle souligne également que la cybersécurité n'est pas une préoccupation isolée, mais fait partie intégrante de tout ce qui constitue un risque pour l'entreprise. En particulier, la composante de surveillance de cette nouvelle fonction aide les organisations à respecter les cadres réglementaires (par exemple, les règlements de la SEC) qui insistent sur une responsabilisation accrue des directions générales et des conseils d'administration lorsqu'ils font des choix en matière de sécurité informatique.

Pour plus de clarté et de pertinence, les cinq fonctions d'origine (Identifier, Protéger, Détecter, Répondre et Restaurer) ont été conservées et actualisées de façon à refléter l'évolution des menaces et des pratiques de cybersécurité. L'objectif est que les organisations puissent gérer et réduire efficacement leurs risques de cybersécurité dans un environnement numérique dynamique. Les éléments liés à la gouvernance ont également été transférés à la fonction « Gouverner » nouvellement créée. De plus, les objectifs principaux de chaque fonction sont désormais énoncés plus clairement. En reconnaissant que ces tâches ne sont pas séquentielles, mais constituent plutôt des éléments interdépendants d'une stratégie de cybersécurité globale, cette restructuration vise à permettre une approche de la cybersécurité plus cohérente et plus imbriquée.

L'accent mis sur la gestion des risques liés à la chaîne d'approvisionnement en matière de cybersécurité est également plus prononcé, avec de nouveaux contrôles visant à intégrer la gestion des risques de la chaîne d'approvisionnement dans l'ensemble du programme de cybersécurité d'une organisation.

Les utilisateurs de ce cadre disposent maintenant aussi d'exemples d'implémentation[4] et de guides de démarrage rapide[5] adaptés à leurs besoins spécifiques. Ils trouveront notamment un catalogue de références doté de fonctions de recherche[6], accessible via l'outil de référence. Ce catalogue permet aux organisations de relier les conseils du Cadre à plus de 50 autres documents utiles sur la cybersécurité.

[4] https://www.nist.gov/document/csf-20-implementations-pdf

[5] https://www.nist.gov/quick-start-guides

[6] https://csrc.nist.gov/projects/olir/informative-reference-catalog#

Les principaux changements sont les suivants :

1. Le CSF 2.0 étend son champ d'application au-delà des secteurs critiques de l'infrastructure. Ce cadre révisé est conçu pour bénéficier à toutes les organisations, quelle que soit leur taille ou leur secteur d'activité, en rendant les lignes directrices du CSF plus universellement applicables.
2. L'ajout de la fonction « Gouverner » est une amélioration significative de CSF 2.0. Cette fonction rehausse les objectifs fondamentaux de responsabilisation et de transparence tout en servant de force unificatrice pour aider les organisations à établir des priorités et à atteindre les objectifs énoncés dans les cinq autres fonctions. Il met l'accent sur l'intégration de la cybersécurité dans la gestion globale des risques de l'entreprise, plutôt que de la traiter simplement comme une préoccupation autonome. La composante de surveillance de la fonction « Gouverner » est particulièrement utile pour les organisations qui doivent respecter des cadres réglementaires, comme les règlements de la SEC, qui insistent sur une responsabilité accrue des conseils d'administration et des directions générales dans les prises de décisions liées à la cybersécurité.
3. Une attention accrue portée à la gestion des risques de la chaîne d'approvisionnement. CSF 2.0 met davantage l'accent sur la gestion des risques de cybersécurité dans la chaîne d'approvisionnement. De nouveaux contrôles ont également été mis en place pour intégrer la gestion des risques liés à la chaîne d'approvisionnement dans l'ensemble du programme de cybersécurité d'une organisation. Cela souligne à quel point il est important de sécuriser l'ensemble de votre écosystème de partenaires, de fournisseurs et de prestataires de services.

Ces améliorations apportées au NIST CSF 2.0 offrent aux organisations un cadre plus complet et plus adaptable pour les aider à s'y retrouver dans un paysage de cybersécurité complexe. En élargissant le champ d'application, en introduisant la fonction « Gouverner », en mettant à jour les fonctions de base et en mettant l'accent sur la gestion des risques de la chaîne d'approvisionnement, CSF 2.0 fournit aux organisations les outils et les conseils dont elles ont besoin pour renforcer leur posture de cybersécurité et leur résilience face à l'évolution des menaces.

Les utilisateurs de ce cadre disposent maintenant aussi d'exemples d'implémentation[7] et de guides de démarrage rapide[8] adaptés à leurs besoins spécifiques. Il s'agit notamment d'un catalogue de références consultable[9], accessible via l'outil de référence, qui permet aux organisations de mapper les conseils à plus de 50 autres documents pertinents sur la cybersécurité.

[7] https://www.nist.gov/document/csf-20-implementations-pdf

[8] https://www.nist.gov/quick-start-guides

[9] https://csrc.nist.gov/projects/olir/informative-reference-catalog#

Un socle fiable pour la restauration des données

Dans le cadre d'une stratégie de disponibilité des données, la restauration des données constitue souvent la dernière étape 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 capable de sauvegarder les données dans toute l'infrastructure et de leur rendre leur intégrité en cas de cyber-incident, les entreprises disposent d'une configuration idéale pour restaurer les données quelle que soit la situation.

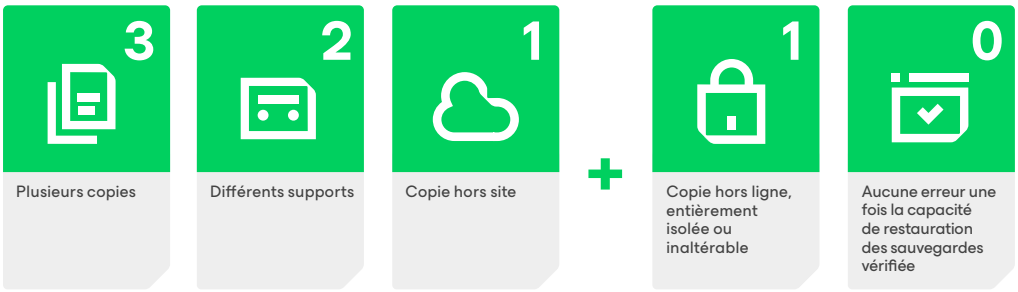


Figure 2 : règle de sauvegarde 3-2-1-1-0 de Veeam

Les clients Veeam peuvent y parvenir de manière sécurisée, orchestrée et bien documentée avec la Veeam Data Platform. En utilisant la suite complète, dont Veeam Backup & Replication, Veeam ONE et Veeam Recovery Orchestrator, les clients peuvent atteindre des objectifs de sécurité des données compatibles avec tous les niveaux du Cadre de cybersécurité du NIST et qui vont bien au-delà de la simple sauvegarde et restauration des données.

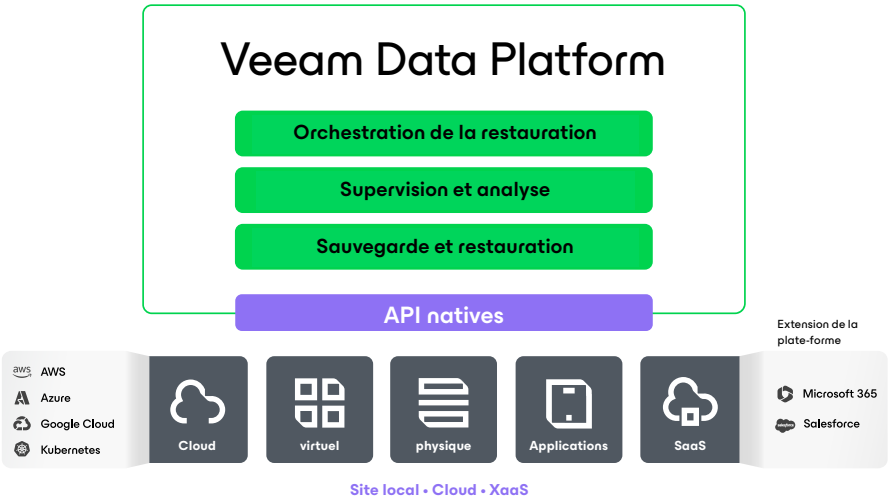


Figure 3 : Veeam Data Platform

S'inspirant fortement du Cadre de cybersécurité du NIST évoqué ci-dessus, la suite de ce document vise à fournir aux services IT, aux équipes de sécurité et aux décideurs les informations et les connaissances dont ils ont besoin pour utiliser efficacement la Veeam Data Platform conformément à ce cadre. Nous souhaitons également vous fournir une autre riche source d'informations et de fonctionnalités qui vous permettent d'identifier les données stratégiques, de détecter les logiciels malveillants, de protéger les données, de réagir rapidement aux menaces actives et de restaurer rapidement des données saines tout en mettant en évidence les fonctionnalités clés qui peuvent être utilisées pour atteindre ces objectifs.

Fonction NIST « Identifier » (ID)

Résultat souhaité en matière de cybersécurité :

Une compréhension des risques actuels de cybersécurité de l'organisation.

La cybersécurité partage un credo fondamental avec la reprise après sinistre traditionnelle (DR) : **On ne peut pas protéger ce qu'on ne connaît pas.** Inventorier et catégoriser les ressources à protéger peut sembler anodin comparé à la lutte et à la réaction actives 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 devenir un élément essentiel d'une stratégie multicouche d'identification **des** données stratégiques.

Inventorier les systèmes et données stratégiques

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

De même, les outils de réseau et de sécurité utilisés par l'équipe de sécurité peuvent créer une liste des systèmes de votre environnement. Comparer ces différents systèmes permet souvent de découvrir des cas où vos données ne sont pas correctement protégées dans chacun des outils, et de vous assurer que vos plans de protection et de restauration seront aussi complets que possible.

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

En utilisant les fonctionnalités de balisage et de classification des données de Veeam Backup & Replication, les clients peuvent démarrer avec un catalogue concret de workloads (leurs sauvegardes) et commencer à appliquer des balises pour identifier des métadonnées système comme la localisation, le propriétaire et la priorité de restauration. Cet exercice mettra parfois en évidence les données manquantes, indiquera une lacune dans votre protection des données et identifiera les métadonnées clés nécessaires pour planifier correctement la restauration des données.

Une fois les métadonnées appliquées, l'assistant de planification de restauration de Veeam Recovery Orchestrator permet de créer le plan de restauration, ce qui réduit 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 savoir si une sauvegarde ou un plan sera prêt pour une utilisation d'urgence consiste à le tester. Les fonctionnalités de tests automatisés de Veeam Recovery Orchestrator offrent l'avantage considérable de garantir la capacité de restauration complète de tout ou partie de l'infrastructure. Outre les avantages évidents de la réduction de la main-d'œuvre pendant l'exécution des tests, l'automatisation du processus de restauration des tests peut également signifier des tests plus fréquents, ce qui permet de mettre en évidence les défauts plus rapidement.

Des tests plus fréquents peuvent, par exemple, permettre d'identifier les systèmes qui ne sont pas sauvegardés ou n'ont pas été pris en compte. En vérifiant régulièrement les résultats des tests et en corrigeant les lacunes, l'entreprise aura une meilleure idée des éléments à protéger.

La fonction « Protéger » (PR) du NIST

Résultat souhaité en matière de cybersécurité :

Mettez en place des mesures de protection pour assurer la sécurité de vos actifs.

L'infrastructure de sauvegarde constitue un endroit spécial pour tout environnement informatique. Non seulement elle constitue le filet de sécurité ultime en matière de sécurité des données, mais elle contient aussi plusieurs copies de toutes vos données (plus celles-ci sont critiques, plus il y aura de copies), y compris celles qui ont pu être supprimées en production. Cela en fait une cible de choix pour les pirates qui souhaitent vous les dérober et déjouer vos mesures de sécurité afin que leurs stratagèmes de rançon et d'extorsion réussissent. 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 de ces sauvegardes. Les principes de confiance zéro (vérification explicite, supposition de violation et utilisation du moindre privilège) doivent être appliqués afin de compliquer au maximum les mouvements latéraux dans l'infrastructure de sauvegarde.

L'utilisation de l'authentification multifacteur (Multi-Factor Authentication ou MFA) 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 vos utilisateurs et leurs informations d'identification sont correctement vérifiés 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 aussi de prévenir les erreurs involontaires et de limiter l'accumulation de privilèges. Enfin, tout doit être configuré en partant de l'hypothèse que le reste de votre infrastructure a déjà été compromis. Cela signifie que les composants de sauvegarde doivent être isolés sur un réseau distinct et que l'accès à la console Veeam Backup & Replication doit être restreint via une connexion VPN ou à distance.

Chaque niveau de votre infrastructure de sauvegarde doit intégrer ces approches, mais elles peuvent sembler légèrement différentes à chaque niveau. Cela signifie que les systèmes d'exploitation, partages de fichiers, la gestion hors bande et toutes les applications utilisées pour les gérer doivent suivre les mêmes principes.

Analyser la conformité de l'infrastructure de sauvegarde

Pour aider les clients à appliquer correctement les principes de 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 de Veeam. Cette analyse doit être effectuée régulièrement et chacun de vos éléments non conformes doit être soit corrigé, soit supprimé. Les éléments supprimés se voient alors adjoindre 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 les sauvegardes de manière à empêcher la restauration des données. C'est pourquoi il est essentiel de vous assurer que vos sauvegardes ne peuvent pas être modifiées ou supprimées.

L'inaltérabilité est un concept informatique très ancien qui est récemment devenu une fonctionnalité essentielle 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 tout système de sécurité, il existe souvent des solutions de contournement. Il est donc essentiel de considérer votre pile dans son ensemble, jusqu'à l'étage du datacenter, pour vous assurer que ces solutions sont éliminées ou strictement contrôlées.

Dans le domaine de la cybersécurité, on dit souvent que le système le plus sûr est celui qui est éteint, déconnecté du réseau et stocké dans une pièce à laquelle personne n'a accès. Bien que la blague soit tout à fait exacte, la vérité est qu'un système inaccessible n'a aucune raison d'exister. Cet adage, cependant, peut parfaitement s'appliquer à la sécurité des sauvegardes. Tant qu'elle est accessible, si nécessaire, une sauvegarde stockée hors ligne est la moins susceptible d'être altérée. Veeam offre plusieurs options pour mettre en place cette vision de sauvegardes entièrement isolées, depuis les systèmes en ligne qui exigent une authentification différente jusqu'au stockage de sauvegardes sur bande, qui constitue la meilleure option hors ligne.

Cela dit, aucun plan ne devrait se baser sur une seule couche de protection. C'est pourquoi Veeam Backup & Replication™ applique le principe des « quatre yeux » à 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.

Chiffrer ses propres sauvegardes

Pour protéger vos données des abus après leur exfiltration, Veeam peut chiffrer les sauvegardes afin d'empêcher quiconque d'y accéder en dehors de votre infrastructure Veeam. Bien que cela n'empêchera pas le vol ou le verrouillage de vos données par un ransomware, il sera très peu probable qu'elles soient utilisées pour des stratagèmes d'extorsion. Ce chiffrement peut être géré en interne par Veeam ou confié à un système tiers de gestion des clés.

Barre latérale : Modèle de sécurité confiance zéro

L'objectif du principe de confiance zéro est d'éliminer la confiance qui a toujours prévalu au sein du périmètre de sécurité, réduisant ainsi la capacité des menaces à se déplacer facilement dans votre environnement. En utilisant le mantra « ne jamais faire confiance, toujours vérifier », vous créez un modèle de sécurité sans périmètre qui ne suppose pas que votre pare-feu se chargera de stopper les cybermenaces. Selon ce modèle, chaque système doit vérifier toutes les nouvelles interactions, sans présumer qu'elles sont sécurisées. Les trois principes du modèle de sécurité confiance zéro sont les suivants :

1. **Vérifiez explicitement.**

2. **Fournir un accès selon le principe du moindre privilège.**

3. **Supposer qu'une violation peut se produire.**

Fonction NIST « Détecter »

Résultat souhaité en matière de cybersécurité :

Élaborer et mettre en œuvre des mesures appropriées pour identifier un événement de cybersécurité.

Une fois l'ensemble des données et des systèmes identifiés, votre entreprise doit établir des plans et des systèmes de détection rapide des intrusions sur ses actifs. Une détection rapide réduira considérablement le temps de présence et l'impact des menaces, qui peuvent en général entraîner des pertes financières. Là encore, Veeam peut jouer un rôle clé dans une stratégie multicouche de détection **des** cybermenaces.

Attirer l'attention sur les comportements anormaux

L'une des stratégies clés des logiciels malveillants consiste à éviter d'être détectés tout en élevant les privilèges et en se déplaçant latéralement dans l'environnement, infectant ainsi autant de systèmes que possible. Pour ce faire, les logiciels malveillants peuvent n'apporter que de petites modifications à la fois pour échapper à votre attention. En outre, puisqu'ils sont devenus plus habiles pour contrecarrer les efforts de restauration de données pour lesquelles ils prévoient d'exiger une rançon, les auteurs de logiciels malveillants commencent à supprimer des sauvegardes, à réduire leurs délais de rétention ou à désactiver leurs tâches. Veeam peut identifier et vous alerter de ces types de comportements anormaux au moyen de plusieurs alertes et 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 pour y rechercher des signes de nouveaux chiffrements, indicateurs clés de la présence de logiciels malveillants. Une recherche dans l'index de la sauvegarde permet de détecter des signatures et des noms de fichiers malveillants. En cas d'élément douteux, la sauvegarde sera signalée comme suspecte.

Détecter les logiciels malveillants dans les sauvegardes

La fonctionnalité SureBackup de Veeam Sauvegarde et Réplication a été conçue à l'origine pour automatiser la restauration et la validation des sauvegardes afin d'assurer leur récupérabilité. Les logiciels de protection des postes de travail n'étaient pas parfaits et pouvaient laisser les sauvegardes être infectées. SureBackup intègre de puissantes fonctionnalités de détection des logiciels malveillants dans les sauvegardes.

Dans le cadre d'un test de la capacité de restauration, SureBackup peut également fonctionner avec les outils de détection des logiciels malveillants afin d'analyser votre machine virtuelle (VM) 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 de SureBackup s'exécute sans aucun impact sur le workload de production, ce qui permet d'effectuer des analyses plus approfondies. SureBackup peut également monter des disques individuels sur une machine test qui analyse ensuite les fichiers à la recherche de logiciels malveillants, offrant ainsi une analyse encore plus rapide et économe en ressources chaque fois qu'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

Là encore, tester régulièrement les plans de restauration peut s'avérer utile, car ils peuvent mettre en évidence les altérations causées par les logiciels malveillants. Des échecs pendant le test complet d'un plan de restauration y compris la vérification de l'application, peuvent attirer l'attention sur des zones où 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 les logiciels malveillants qui s'exécutent 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 incidents et des événements 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, ce qui réduit le temps de réponse et offre aux analystes de la sécurité une vision plus fiable des événements.

Intégrations externes pour la protection des données

L'API d'incidents est un ensemble d'interfaces de programmation d'applications (API) 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 de façon à ce qu'il alerte les administrateurs sur la base de ces informations. Ces derniers peuvent alors entreprendre des examens et des vérifications, puis répondre rapidement par des actions telles que la création d'une sauvegarde immédiate, l'exécution d'une action SureBackup pour vérifier l'absence d'infection et restaurer les fichiers sains, puis la création de la copie inaltérable d'une sauvegarde à des fins d'analyse criminelle. Ce point d'intégration ouvert entre les outils de sécurité et la plateforme de protection des données améliore considérablement la communication, ce qui contribue à réduire le temps de séjour des logiciels malveillants et favorise des restaurations plus rapides et plus saines.

Barre latérale : Temps de séjour

Le temps de séjour — la durée pendant laquelle le logiciel malveillant existe dans l'environnement avant d'être découvert — correspond au moment où le logiciel malveillant réside dans votre environnement sans exécuter l'attaque principale. Il peut passer ce temps à compromettre des comptes supplémentaires, élever des privilèges, s'intégrer plus profondément dans votre système d'exploitation, se propager latéralement à d'autres systèmes et recueillir des informations qu'il peut utiliser pour les attaques actuelles ou futures.

Fonction NIST « Répondre »

Résultat souhaité en matière de cybersécurité :

Développer et mettre en œuvre des réactions appropriées pour un événement de cybersécurité détecté.

Il est impossible d'assurer en permanence une protection totale. Il faut donc à tout prix essayer de bloquer les logiciels malveillants et de les supprimer le plus rapidement possible. Comme pour planifier la restauration après une catastrophe naturelle, l'un des principaux objectifs vers lequel toutes vos décisions devraient converger est celui des objectifs de temps de restauration (RTO). De fait, lors d'un événement de cybersécurité, l'objectif premier consiste à bloquer le logiciel malveillant et à le supprimer de l'environnement avant de remettre les systèmes en service. 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 criminelle de cybersécurité

Tel qu'évoqué plus haut, SureBackup est une fonctionnalité qui ne se contente pas de tester la capacité de restauration des sauvegardes, mais détecte aussi les logiciels malveillants. L'un des objectifs de la phase de réponse consiste à connaître le temps de séjour. Ainsi, l'utilisation des indicateurs de Veeam Backup & Replication™, qui signalent si un logiciel malveillant a été détecté dans un point de restauration ou identifié par un outil tiers, facilite la recherche du point d'infection initial.

La restauration sécurisée est une autre fonction de Veeam Sauvegarde et Réplication qui 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 et d'éviter une réinfection causée par la restauration d'une partie restée dormante.

Avec Veeam Recovery Orchestrator, ce processus de restauration sécurisé 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 aussi d'ajouter rapidement des informations précieuses à l'analyse forensique d'un incident de cybersécurité.

Chasse aux menaces améliorée avec YARA

Outil très connu des traqueurs de menaces de cybersécurité, YARA s'appuie sur des règles pour identifier et classer 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 des logiciels malveillants pour les rechercher parmi les sauvegardes.

Suivi des incidents avec ServiceNow

Grâce aux intégrations directes dans ServiceNow, Veeam ONE peut créer automatiquement de nouveaux tickets et mettre à jour les tickets existants en fonction de 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.

Barre latérale : 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 des données qui sont envoyées de l'environnement d'une victime aux cybercriminels. Elles peuvent alors devenir des informations divulguées ou vendues par ces cybercriminels à la suite de cette violation. Cela peut entraîner la divulgation de secrets d'entreprise, la compromission de réputations et le vol d'informations personnelles avec, à terme, de futures fraudes ou cyberattaques.

Fonction NIST « Restaurer »

Résultat souhaité en matière de cybersécurité :

Élaborer et mettre en œuvre les activités appropriées pour procéder à la restauration après un événement de cybersécurité (plans, processus, personnes, technologie)

Selon la nature de votre incident de cybersécurité, la restauration de données saines sera essentielle pour rétablir les services, notamment en cas de ransomware. Si le temps de séjour est long, de nombreux points de restauration peuvent contenir des logiciels malveillants et vous devrez peut-être remonter loin dans le temps pour trouver un point de restauration sain. Comme pour la DR traditionnelle, il est important de s'aligner sur des objectifs qui minimisent les pertes de données : Vos délais optimaux de reprise d'activité (RPO). Puisqu'il est important 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 qui est 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 que vos points de restauration précédents sont totalement sains.

Pour réduire les risques de restaurer des données infectées et d'avoir travaillé en vain, les efforts de restauration doivent être menés conjointement avec les analyses criminelles de cybersécurité effectuées pendant la phase de réponse. Une collaboration étroite entre le service informatique, la sécurité et l'entreprise dans son ensemble est essentielle pour restaurer les données appropriées et éviter de 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 présents dans la sauvegarde complète.

Restaurer les données non infectées le plus vite possible

L'automatisation est la clé pour restaurer rapidement, même les environnements les plus simples, mais le mode de restauration peut aussi faire la différence. Grâce à des snapshots de baie de stockage et à la restauration instantanée, les sauvegardes 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 cumulables capables de 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 les restaurations effectuées 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 antérieur à ce chiffrement.

Barre latérale : Sauvegarde ou réplication pour des restaurations de cybersécurité

La réplication peut faire partie de votre processus de restauration de cybersécurité, mais il est important de savoir distinguer ses objectifs de ceux des sauvegardes. La réplication consiste à déplacer des données le plus rapidement possible et à les renvoyer vers le réplica sain le plus récent. Puisque les sauvegardes ne s'exécutent pas en continu, elles permettent d'être plus méthodique pour garantir des données saines capables d'être restaurées. Sachant que la reprise après un événement de cybersécurité doit tenir compte du temps de séjour et utiliser des données saines au point de restauration, la sauvegarde est un mécanisme plus répandu.

Fonction NIST « Gouverner »

Résultat souhaité en matière de cybersécurité :

La stratégie, les attentes et la politique de gestion des risques de cybersécurité de l'organisation sont établies, communiquées et surveillées.

L'introduction de la fonction « Gouverner » représente une évolution significative de la stratégie et de la supervision de la cybersécurité. Cette nouvelle fonction souligne l'importance de la gouvernance dans la gestion des risques de cybersécurité au sein d'une organisation. Il souligne également la nécessité d'établir des politiques, des stratégies et des processus de cybersécurité clairs qui s'alignent sur les objectifs globaux et la tolérance au risque de votre organisation. En intégrant la fonction « Gouverner », le NIST CSF 2.0 encourage les organisations à adopter une approche plus holistique et responsable de la cybersécurité, garantissant ainsi que les considérations de cybersécurité sont intégrées au tissu de la gouvernance organisationnelle. Il s'agit notamment de définir les rôles et les responsabilités en matière de cybersécurité, de favoriser une culture de sensibilisation à la sécurité et de veiller à ce que les décisions en matière de cybersécurité soient éclairées par les objectifs et les contraintes de l'organisation. L'ajout de cette fonction met en évidence l'évolution vers la reconnaissance de la cybersécurité non seulement comme un défi technique, mais aussi comme une composante essentielle de la gestion de l'entreprise et de la résilience opérationnelle.

Composant essentiel de la sécurité des données, votre infrastructure de sauvegarde doit être visiblement conforme aux réglementations de l'entreprise et à celles des autorités compétentes. Pour « **gouverner** » correctement, il faut documenter la stratégie de gestion des risques de cybersécurité de votre organisation, notamment en consignant la configuration, les règles, le suivi des modifications et les succès ou les échecs de chaque test. Cela permet de s'assurer que les attentes et les politiques sont communiquées et surveillées efficacement.

Assurez-vous que tout est documenté

Qu'il s'agisse d'auditeurs, de cyber-assurance, d'amélioration des processus ou d'assurance personnelle, l'importance d'une documentation précise, complète et fréquente ne peut être surestimée. La précision et la rapidité d'un plan de restauration entièrement orchestré seront du plus grand intérêt pour les administrateurs et les responsables d'entreprise, mais une documentation dynamique créée à chaque exécution complète ou chaque test sera un atout considérable pour les équipes qui doivent pouvoir vérifier que ces opérations ont réellement fonctionné, notamment les équipes de sécurité et de conformité.

Au-delà, le nombre de rapports possibles à partir de Veeam ONE vous fournira une mine d'informations sur votre infrastructure de sauvegarde et son intégrité. La documentation de la fréquence des sauvegardes, le suivi des modifications des configurations de sauvegarde, etc., font partie des rapports intégrés qui peuvent être générés manuellement ou d'après un calendrier et transmis automatiquement aux destinataires appropriés.

Une surveillance constante pour limiter les risques

Utilisez l'automatisation pour vérifier les configurations Veeam et l'environnement de sauvegarde afin de vous assurer que vos appareils et vos logiciels sont sécurisés et à jour. Veeam utilise son Analyseur de sécurité et de conformité pour effectuer automatiquement plus de 30 vérifications de sécurité. L'objectif est de s'assurer que vous êtes à jour, que les correctifs sont appliqués et que vos anciens protocoles non sécurisés sont désactivés. De plus, toutes ces informations sont compilées dans un rapport unique permettant aux équipes informatiques et de sécurité de suivre l'adhésion aux politiques de l'entreprise.

Tableau de bord de la sécurité des sauvegardes

La cybersécurité consiste souvent à détecter des tendances dans votre environnement. Veeam offre une large gamme de fonctionnalités, avec notamment de nouvelles fonctionnalités axées sur la cybersécurité. C'est le cas du tableau de bord du Centre d'évaluation des menaces de Veeam, un panneau de contrôle unique qui regroupe plusieurs sources de données sur l'interface de Veeam ONE. Les administrateurs et les spécialistes de la sécurité bénéficient ainsi d'une vue unifiée de toute leur infrastructure de sauvegarde.

Conclusion

Le NIST CSF 2.0 représente une étape importante dans l'évolution de la gestion des risques de cybersécurité et de la lutte contre l'évolution des menaces. En s'appuyant sur les solides bases du CSF 1.1, en y introduisant des améliorations fondamentales comme la fonction « Gouverner » et en mettant davantage l'accent sur la chaîne d'approvisionnement, CSF 2.0 fournit aux organisations un cadre plus complet et plus adaptable pour les aider à s'y retrouver dans un paysage de cybersécurité en constante évolution.

Le champ d'application élargi du CSF 2.0 permet aux organisations de toutes tailles et de tous secteurs de bénéficier de ses conseils, favorisant ainsi une approche plus inclusive et collaborative de la cybersécurité. Ce cadre mis à jour reconnaît également qu'une gestion efficace des risques liés à la cybersécurité nécessite la participation active et l'engagement des acteurs de toute l'organisation, que ce soit les cadres supérieurs ou les collaborateurs de première ligne.

En fin de compte, le succès de la mise en œuvre du NIST CSF 2.0 repose sur la promotion d'une culture de sensibilisation, de collaboration et de responsabilité en matière de cybersécurité. En investissant dans des programmes de formation et d'éducation, les entreprises peuvent donner à leur personnel les moyens de participer activement au processus de gestion des risques de cybersécurité. Une communication claire et un renforcement cohérent des politiques et meilleures pratiques de cybersécurité sont essentiels pour créer un sentiment partagé de responsabilité et de vigilance.

À l'avenir, il est évident que la cybersécurité continuera d'être une priorité essentielle pour les entreprises du monde entier. La sophistication et la fréquence croissantes des cybermenaces, associées à une dépendance toujours plus forte vis-à-vis des technologies numériques, soulignent la nécessité de disposer de cadres de cybersécurité performants et agiles tels que le CSF 2.0 du NIST. En adoptant ce cadre mis à jour et en s'engageant à le mettre en œuvre en permanence, les organisations peuvent renforcer leur résilience, protéger leurs actifs et conserver la confiance de leurs parties prenantes face à l'évolution des cyber-risques.

Aujourd'hui, la conception d'une stratégie de cybersécurité est loin d'être une tâche aisée. Les menaces sont nombreuses et une violation peut représenter un véritable pactole pour les cybercriminels. Aussi, les entreprises doivent utiliser tous les outils à leur disposition pour créer des couches de sécurité leur permettant d'atteindre une efficacité maximale à tous les niveaux du cadre de cybersécurité du NIST. C'est là qu'intervient Veeam pour améliorer leur stratégie de cybersécurité :

- Créer et tester régulièrement des plans de restauration peut vous fournir des données précieuses que vous pouvez utiliser dans la phase d'identification pour vous assurer que les données stratégiques sont **identifiées** et peuvent être protégées.
- La mise en œuvre des meilleures pratiques documentées et des fonctionnalités de sécurité natives garantit l'inclusion des sauvegardes et de l'infrastructure de sauvegarde dans la phase de **protection**.
- Étant donné que les sauvegardes concernent toutes les données de l'infrastructure, elles peuvent constituer une deuxième vérification importante pour détecter des logiciels malveillants qui auraient pu passer inaperçus sur les terminal lors de la phase de **détection** .
- L'accès rapide à différents points dans le temps et à des environnements de « salle blanche » virtuels peut être essentiel aux efforts de collecte d'informations dans la 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 la restauration dans un état sain et utilisable le plus rapidement possible en phase de **restauration**.
- Chacun a un rôle à jouer dans la sécurisation de son organisation et de ses données. Dans la phase de « **gouvernance** », l'élaboration, la diffusion et la supervision de la stratégie et des règles de cybersécurité de votre organisation sont essentielles.

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. En suivant les conseils proposés dans ce guide, elles doivent être en mesure d'échanger de manière productive avec les équipes de cybersécurité et les autres parties prenantes pour intégrer une plateforme de protection des données basée sur les solutions Veeam à leur stratégie de cybersécurité globale.

N'hésitez pas à nous contacter pour en savoir plus sur les fonctionnalités et les capacités de Veeam.

À propos de Veeam Software

Veeam, le leader mondial de la protection des données et de la restauration après une attaque par ransomware, s'est donné pour mission d'aider toutes les entreprises à bénéficier d'une résilience totale en garantissant la sécurité, la restauration et la liberté des données présentes dans leur cloud hybride. Basé à Seattle et possédant des bureaux dans plus de 30 pays, Veeam protège plus de 450 000 clients dans le monde entier qui font confiance à Veeam pour le maintien de leur activité. Pour en savoir plus, rendez-vous sur www.veeam.com ou suivez Veeam sur LinkedIn @veeam-software et X @veeam.

→ Regardez la Veeam Data Platform en action

→ Essai gratuit de 30 jours