Résilience des données Zero Trust (ZTDR)

Architecture de sauvegarde et de restauration sécurisée des données

Une approche pragmatique pour la mise en œuvre du Zero Trust

Aperçu

Les entreprises de toutes tailles dans tous les secteurs d'activité comprennent l'importance du Zero Trust pour assurer la sécurité de leurs données et de leur activité. Cependant, le modèle Zero Trust actuel n'a pas encore été appliqué de manière substantielle à la sauvegarde et à la restauration des données. L'extension des principes du Zero Trust à la sauvegarde et restauration des données s'aligne sur la nature holistique de la cybersécurité. De plus, la protection des informations sensibles ne se limite pas à la sécurité du périmètre.

Pour relever ce défi, Veeam a collaboré avec Jason Garbis de Numberline Security, expert en Zero Trust, sur l'infrastructure de résilience des données Zero Trust, conçue pour minimiser les risques, renforcer la protection des données et révolutionner la posture de sécurité d'une entreprise. Cette infrastructure s'appuie sur le modèle de maturité Zero Trust (ZTMM) de l'Agence de cybersécurité et de sécurité des infrastructures (CISA) et étend les grands principes du ZTMM à un scénario de sauvegarde et restauration. L'infrastructure de résilience des données Zero Trust implique qu'on ne présume jamais de la confiance et que les mesures de sécurité sont appliquées de manière cohérente tout au long du cycle de vie des données (y compris le processus de sauvegarde et restauration). Il s'agit d'un modèle pratique qui aidera les équipes IT et de sécurité à réduire considérablement les risques, à renforcer la protection des données et à améliorer considérablement la posture de sécurité de toute entreprise.

Vous voulez en savoir plus sur la résilience des données confiance zéro ? Téléchargez le livre blanc

L'approche Veeam du Zero Trust : Résilience des données Zero Trust (ZTDR)

Zero Trust est au cœur de la stratégie de sécurité d'une entreprise. En outre, des éléments clés tels que la segmentation des actifs de données les plus stratégiques, l'accès selon le principe du moindre privilège ainsi que l'authentification et l'autorisation continues avec les meilleures pratiques de gestion des identités et des accès (IAM) sont particulièrement pertinents lorsqu'il s'agit de protéger les environnements de sauvegarde. En intégrant une fonction de résilience des données Zero Trust, les entreprises peuvent relever les défis uniques posés par les solutions de protection des données et déployer une stratégie de sécurité complète, que leur environnement soit sur site, dans le cloud ou hybride.

L'un des concepts essentiels du Zero Trust est de toujours supposer une violation, quelle que soit la sécurité d'un environnement donné. Pour lutter contre ce risque, une technique essentielle consiste à séparer le logiciel d'administration des sauvegardes et leur stockage en zones de résilience distinctes ou domaines de sécurité. Les données de sauvegarde sont isolées de toute menace pesant sur le logiciel d'administration des sauvegardes, qu'elles soient internes ou externes. Veeam prend en charge plusieurs technologies pour créer des zones de résilience avec stockage hautement sécurisé et inaltérable (voir la figure 1).

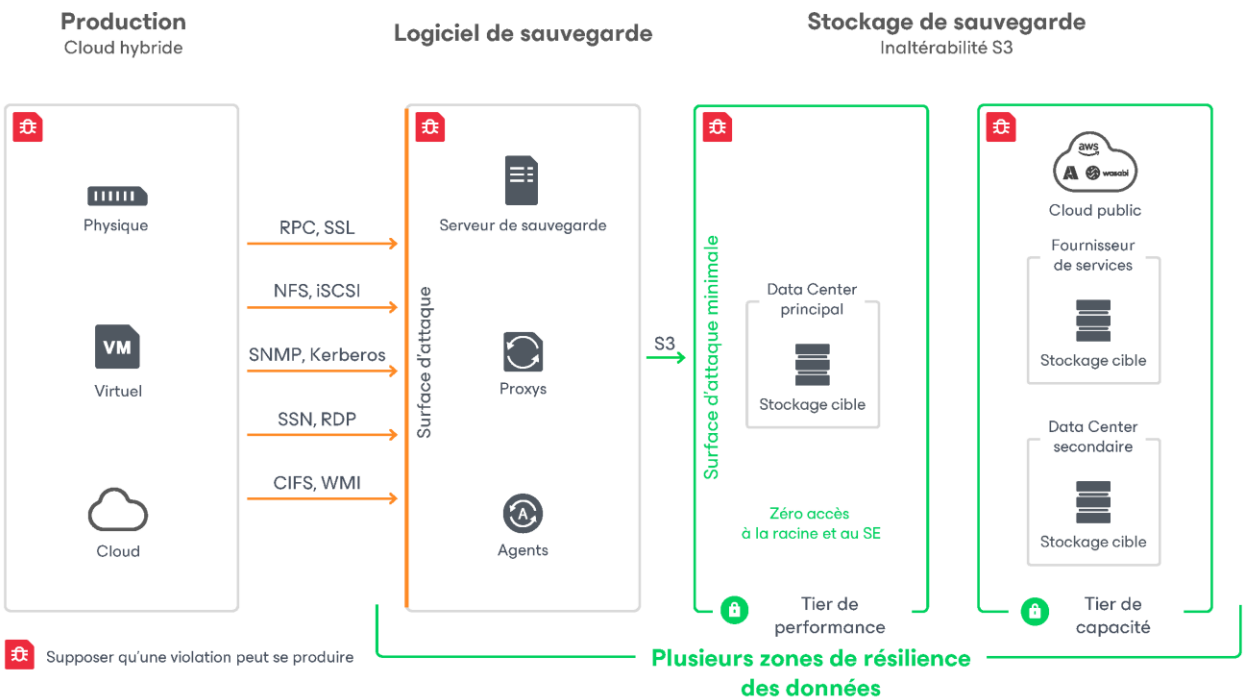

Figure 1

Étant donné que les solutions de protection des données offrent un accès en lecture et en écriture aux données de production parmi les plus élevés de toute l'entreprise, et souvent aux données les plus stratégiques, il est impératif de sécuriser et de protéger l'environnement de sauvegarde au moyen des meilleures pratiques Zero Trust.

Principes de résilience des données Zero Trust

En s'appuyant sur le modèle de maturité Zero Trust de la CISA (voir figure 2), il existe des éléments supplémentaires qu'une entreprise doit appliquer spécifiquement au pilier des données.

Modèle de maturité Zero Trust de la CISA

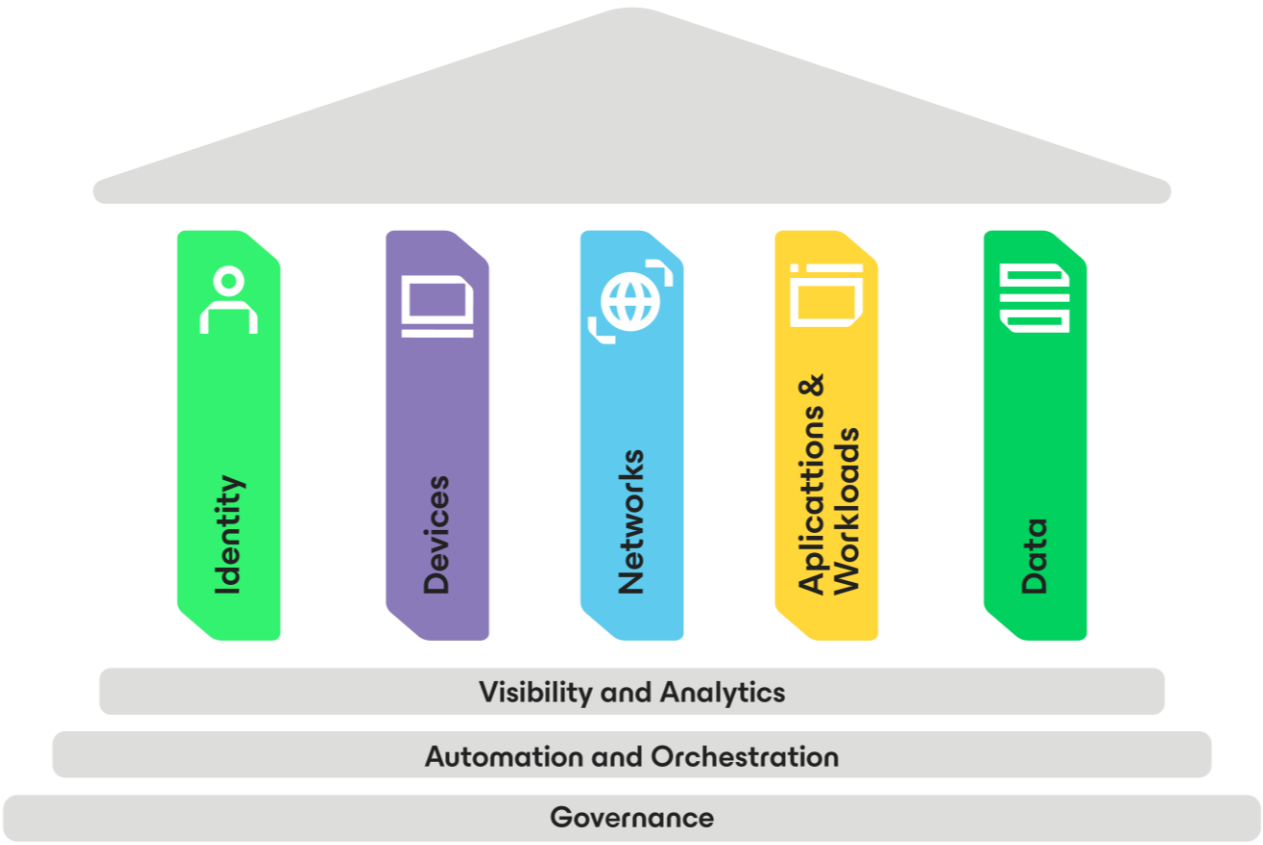

Figure 2

La synthèse d'étude sur la résilience des données Zero Trust met en évidence les 5 principes fondamentaux de la résilience des données Zero Trust (ZTDR) pour aider la stratégie globale de cyber-résilience des entreprises, en assurant la protection des actifs de données stratégiques face à l'évolution des cybermenaces.

Moindre privilège

Ce principe met l'accent sur l'octroi de l'accès à une personne, un processus, un appareil ou un workload qui est essentiel à l'exécution de sa fonction prévue.

Accès contrôlé de l'infrastructure de sauvegarde :

- L'implémentation de stratégies Zero Trust pour contrôler l'accès à l'infrastructure de sauvegarde garantit que seuls les utilisateurs validés peuvent établir une connexion avec la solution de sauvegarde. Il s'agit d'une étape cruciale pour prévenir les accès non autorisés et les violations potentielles de données.

Rôles granulaires en libre-service et rôles d'administrateur de sauvegarde restreints :

- La fourniture de rôles granulaires en libre-service et de rôles d'administrateur de sauvegarde restreints au sein de Veeam démontre un attachement au principe du moindre privilège. Cela garantit que les utilisateurs n'ont accès qu'aux fonctions spécifiques nécessaires à leurs tâches, ce qui réduit la probabilité d'une mauvaise utilisation accidentelle ou intentionnelle.

Meilleures pratiques de gestion des identités et des accès (IAM)

- Appliquer les meilleures pratiques IAM, telles que l'utilisation de l'authentification multifacteur (MFA), ajoute une couche de sécurité supplémentaire à l'environnement de sauvegarde. Il s'agit d'une mesure essentielle pour empêcher tout accès non autorisé, en particulier compte tenu du niveau élevé de privilège associé aux solutions de sauvegarde.

Principe des « quatre yeux » pour les décisions opérationnelles stratégiques :

- L'intégration du principe des « quatre yeux » pour les décisions opérationnelles stratégiques garantit que les actions clés nécessitent l'approbation ou la vérification par au moins deux personnes autorisées. Cela ajoute une couche de surveillance supplémentaire et réduit le risque d'activités malveillantes ou erronées.

Inaltérabilité

Même avec un périmètre réseau sécurisé, un concept essentiel du Zero Trust consiste à partir du principe qu'une violation est survenue. L'inaltérabilité des sauvegardes est un puissant mécanisme de défense qui empêche tout acteur malveillant, interne ou externe, de modifier ou de supprimer les données de sauvegarde stratégiques.

Segmentation pour minimiser la surface d'attaque et le rayon d'action :

- Segmenter le logiciel de sauvegarde et le stockage de sauvegarde en zones de résilience distinctes constitue le concept clé du ZTDR. Cela minimise l'impact potentiel de menaces internes ou externes en isolant les composants critiques. S'assurer que le logiciel de sauvegarde ne dispose pas d'autorisations de niveau gestion/système d'exploitation sur le stockage de sauvegarde ajoute une couche de protection supplémentaire.

Zones de résilience multiples et règle de sauvegarde 3-2-1-1 :

- Plusieurs zones de résilience des données ou domaines de sécurité offrent une sécurité multicouche. En outre, la règle de sauvegarde 3-2-1-1 constitue une meilleure pratique de stratégie de sauvegarde et s'aligne parfaitement avec les principes de résilience des données. Disposer d'au moins trois copies des données, sur deux types de supports différents, avec au moins une copie hors site et au moins une copie entièrement isolée ou inaltérable, offre une sécurité multicouche et réduit le risque de perte de données.

Zones de résilience

L'un des concepts Zero Trust de base de la mise en réseau est la micro-segmentation pour diviser les périmètres de sécurité en zones plus petites, réduisant ainsi la surface d'attaque, le rayon d'explosion de toute zone compromise et le mouvement latéral d'un attaquant. Pour le ZTDR, ce concept peut être appliqué en utilisant des zones de résilience des données. Les zones de résilience séparent le stockage de sauvegarde et isolent le plan de contrôle du stockage du logiciel de sauvegarde et de son plan de contrôle. C'est une ligne de démarcation essentielle qui assure la survie des données de sauvegarde, même en cas de logiciel de sauvegarde compromis. Cela peut se produire pour de multiples raisons, y compris les acteurs malveillants internes. Un système de sauvegarde doit garantir que les données de sauvegarde peuvent être restaurées simplement et rapidement depuis une nouvelle installation du logiciel de sauvegarde.

Infrastructure de production

Infrastructure Veeam

Données de sauvegarde autonomes

Inaltérable | Chiffré | 3-2-1-1-0

Intégrité des données et sécurité renforcée :

- Configurer une cible de sauvegarde compatible et définir une période de rétention pour les sauvegardes inaltérables sont des mesures proactives pour assurer l'intégrité des données et une sécurité renforcée. Les sauvegardes inaltérables constituent une protection contre les attaques par ransomware et d'autres formes de manipulation des données.

Résilience du système

Une approche holistique de la sécurité informatique englobe la résilience de l'ensemble de l'écosystème, y compris les plateformes, les outils, les technologies et les processus. Les diverses options de résilience de Veeam témoignent d'un engagement à fournir aux entreprises les outils nécessaires pour résister à divers types de perturbations, y compris en cas de perte complète du système.

Détection du décalage temporel pour les sauvegardes inaltérables :

- L'implémentation de la détection de décalage temporel constitue une mesure proactive visant à empêcher la suppression des sauvegardes inaltérables, même en cas de NTP (Network Time Protocol) compromis. Cette fonctionnalité renforce la sécurité et la fiabilité des cibles de sauvegarde en garantissant l'intégrité des données de sauvegarde stratégiques.

Options de restauration flexibles :

- Veeam offre des options de restauration flexibles, même vers des environnements dissemblables, et prend en charge les déploiements physiques et virtuels, ainsi que les environnements hybrides, pour s'adapter aux diverses infrastructures IT que les entreprises peuvent exploiter. Cette flexibilité permet aux entreprises une restauration rapide : par exemple, VMware local vers AWS ou Azure, ou AWS vers Azure si l'environnement d'origine n'est pas disponible.

Options de restauration granulaire des données :

- La flexibilité de restauration des données dans différents environnements et à différentes granularités améliore la résilience globale des données. Cette capacité d'adaptation permet aux entreprises d'adapter leurs processus de restauration en fonction des besoins spécifiques de différents scénarios.

Validation proactive

Il est essentiel de valider en permanence les aspects fonctionnels et les processus pour s'assurer que les données sont protégées et que toute anomalie est détectée et traitée rapidement.

Supervision et validation en continu :

- L'accent mis sur la supervision des systèmes 365/24/7 reflète la compréhension que les menaces de cybersécurité peuvent émerger à tout moment. Grâce aux informations en temps réel sur l'état de l'environnement, les administrateurs peuvent détecter précocement les anomalies et donner aux entreprises les moyens d'enquêter et d'intervenir avant qu'une cyberattaque ou une perte de données ne se produise.

- Tirer parti d'outils tels que Veeam ONE pour la supervision constitue une approche proactive pour maintenir l'intégrité et la sécurité des environnements de sauvegarde et restauration. La capacité de Veeam ONE à superviser divers paramètres, notamment l'utilisation de la CPU, le taux d'écriture dans le datastore, le taux de transmission sur le réseau et la taille des sauvegardes incrémentielles, fournit aux entreprises des informations précieuses sur les problèmes potentiels.

Visibilité de bout en bout :

- Le concept de visibilité de bout en bout sur l'ensemble de l'infrastructure de protection des données est essentiel. Il assure que les entreprises ont une compréhension complète de l'intégrité et de l'état de leurs systèmes de sauvegarde et restauration, ce qui leur permet de prendre des décisions éclairées et d'agir rapidement en cas de nécessité.
- Inclus dans la récente version 12.1 de Veeam, le nouveau centre d'évaluation des menaces de Veeam rassemble des informations provenant de l'ensemble de la plateforme et de l'infrastructure, qu'il combine dans un panneau de contrôle unique pour mettre en évidence les menaces, identifier les risques et fournir aux entreprises une fiche de sécurité simple et puissante pour l'ensemble de leur environnement de protection des données.

Simplicité opérationnelle

L'importance de la simplicité opérationnelle pendant les incidents ou les événements de cybersécurité est une reconnaissance du rôle stratégique que la simplicité joue dans une restauration efficace. Plus le temps d'arrêt est long, plus l'impact sur l'exploitation et le résultat financier de l'entreprise est important.

Temps d'arrêt moyen des attaques par ransomware :

- Selon le rapport de Veeam sur les tendances des ransomwares en 2023, le temps d'arrêt à la suite d'une attaque par ransomware est de trois semaines en moyenne. Cela souligne l'urgence et l'importance d'une restauration rapide, particulièrement critique dans les situations sous haute pression où chaque instant compte.

Équilibrer les outils, les personnes et les processus :

- Trouver le juste équilibre entre les outils, les personnes et les processus est un défi majeur, en particulier lorsque les organisations sont confrontées à une catastrophe ou à une cyberattaque. La simplicité opérationnelle implique de rationaliser les workflows, d'optimiser les processus et de s'assurer que les bons outils sont en place pour une restauration efficace.

Investissement dans la simplification des fonctionnalités de restauration :

- Les leaders du marché tels que Veeam investissent de manière proactive pour offrir des fonctionnalités de restauration en traitant les complexités de la restauration. La capacité de restaurer les données d'une plateforme à une autre et de tirer parti d'outils tels que Recovery Orchestrator de Veeam témoigne d'une volonté de simplifier les scénarios de restauration complexes et de maintenir à jour les plans de basculement, automatisés et entièrement testés, afin de garantir la disponibilité en cas de scénarios sous haute pression.

Découvrez les dernières fonctionnalités de sécurité de la version 12.1

Conclusion

Notre paysage numérique évolue et s'élargit, tout comme les cyberattaques et les capacités des auteurs de menaces. Par conséquent, nous avons un besoin urgent d'unifier et de renforcer la collaboration et l'efficacité des technologies de l'information et de la sécurité afin de mieux protéger et défendre les données, les appareils et le personnel de nos organisations. Ce voyage vers la maturité ne se fera pas du jour au lendemain, mais il est impératif que cela commence à se produire le plus tôt possible. La première étape est le Zero Trust. Le modèle de maturité Zero Trust (ZTMM) de la CISA fournit des principes fondamentaux qui sont essentiels à la sécurisation et à la protection d'une entreprise, mais ne couvre pas tout. L'introduction de la résilience des données Zero Trust (ZTDR) en tant qu'extension du modèle de maturité Zero Trust (ZTMM) de la CISA est une approche stratégique et avant-gardiste pour faire face à l'évolution du paysage des cybermenaces.

L'intégration des principes du ZTDR, notamment l'accès selon le principe du moindre privilège, l'inaltérabilité, la résilience du système, la validation proactive et la simplicité opérationnelle, met en évidence une stratégie complète de sécurisation et de protection des données d'entreprise. En adoptant le ZTDR, les entreprises disposeront d'une voie claire et concrète pour renforcer leur posture de sécurité. Il en résulte des opérations plus efficaces et un meilleur alignement entre les équipes IT et de sécurité. Au final, cela conduira à une restauration plus rapide et plus sûre.

À propos de Veeam Software

Veeam, le leader mondial de la protection des données et de la restauration anti-ransomware, s'est donné pour mission d'aider toutes les entreprises à se relever après une panne ou une perte de données et, surtout, à aller de l'avant. Avec Veeam, les entreprises garantissent une résilience totale en assurant la sécurité, la restauration et la liberté des données au sein de leur cloud hybride. La Veeam Data Platform offre une solution unique pour les environnements cloud, virtuels, physiques, SaaS et Kubernetes et garantit aux décideurs informatiques et responsables de la sécurité que leurs données et applications sont protégées et toujours disponibles. Basé à Columbus dans l'État américain de l'Ohio, et possédant des bureaux dans plus de 30 pays, Veeam protège plus de 450 000 clients dans le monde, dont 73 % des entreprises du Global 2000, qui font confiance à Veeam pour le maintien de leur activité. La résilience totale commence avec Veeam. Pour en savoir plus, rendez-vous sur www.veeam.com/fr ou suivez Veeam sur LinkedIn @veeam-software et X @veeam.