Choisir sa cible Veeam Backup & Replication en fonction du niveau de protection anti-ransomware souhaité

Franck Guéné
Ingénieur avant-vente senior

Table des matières

À l'heure de la transformation numérique et du multicloud, toute entreprise se doit de répondre aux questions suivantes :

- **Quelle valeur représentent les données pour nous ?**
- **Sommes-nous préparés à subir une attaque informatique de quelque nature que ce soit (attaque externe de type ransomware, attaque interne compromettant le système d'information) ?**

La question n'est plus de savoir si l'entreprise sera un jour victime d'un acte cybercriminel, mais plutôt quand celui-ci se produira.

État des lieux de la cybercriminalité

Les infrastructures de sauvegarde sont conçues pour protéger les données des entreprises. C'est pourquoi les actes malveillants ciblent de plus en plus souvent les archives de sauvegarde.

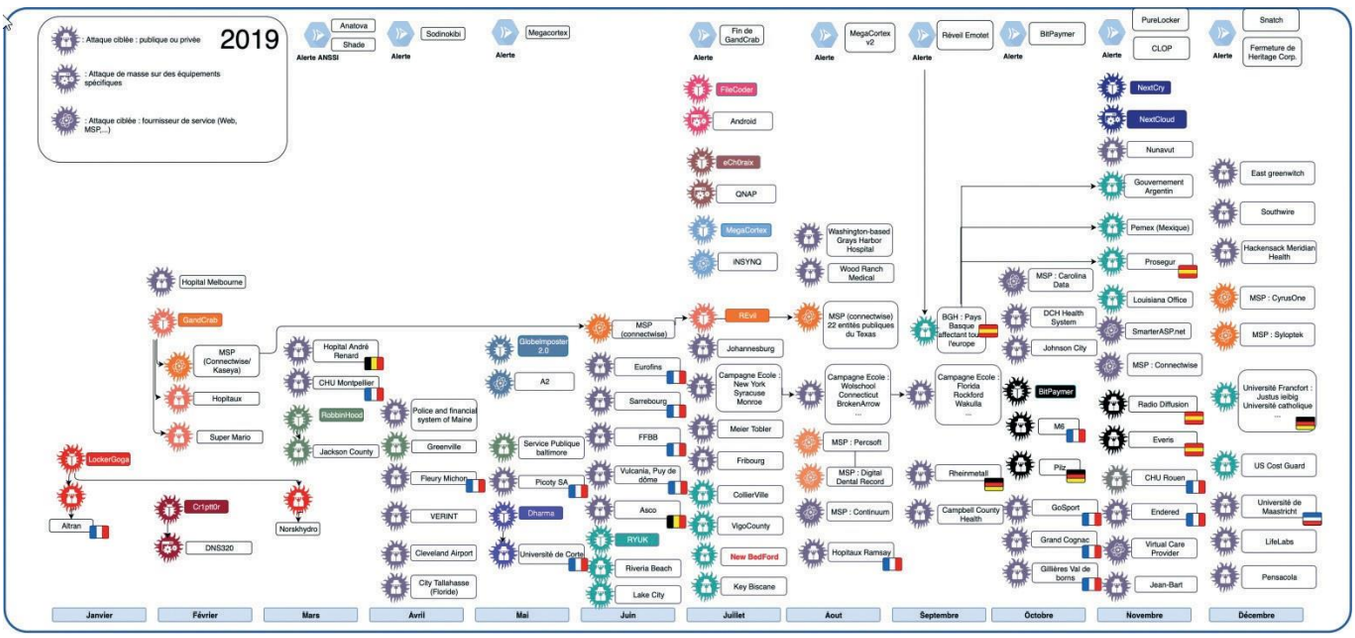
« Les premiers ransomware fonctionnaient un peu comme des spams. Les cybercriminels arrosaient les messageries en espérant que quelqu'un 'mordrait à l'hameçon' », explique Kurt Baumgartner, chercheur spécialiste de la sécurité chez Kaspersky.

Depuis quelques temps, on observe toutefois une modernisation du mode de fonctionnement et un changement de cible des pirates. Ceux-ci préfèrent maintenant s'attaquer à des organismes gouvernementaux (villes, hôpitaux), mais aussi à des entreprises, de la TPE aux grands groupes internationaux.

« S'il en coûte à un particulier seulement 300 ou 400 dollars pour récupérer ses données, ces organisations payent parfois des millions, en partie parce que les compagnies d'assurances le leur permettent », ajoute Kurt Baumgartner.

À l'occasion de son évènement Panocrim 2020 (https://clusif.fr/conferences/panorama-de-la-cybercriminalite-annee-2019/), le CLUSIF (Club de la Sécurité de l'Information Français) vient de publier son retour d'expérience pour l'année 2019.

Dans une illustration, il répertorie les attaques de type ransomware rendues publiques au cours de l'année 2019.



- **Un hôpital de Melbourne, le Melbourne Heart Group, a vu les dossiers de 15000 patients chiffrés, l'empêchant d'accéder à leurs données pendant environ trois semaines. En échange du déchiffrement des fichiers, les pirates ont exigé le règlement d'une rançon en cryptomonnaie. Celle-ci a été payée, mais certains fichiers n'ont jamais pu être récupérés.**

- **Le 7 mai 2019, des pirates informatiques ont verrouillé les données de 10000 ordinateurs de la ville de Baltimore et exigé environ 80 000 dollars US de rançon en bitcoins pour les restituer. la ville ayant refusé de payer la rançon, il lui a fallu un mois pour mettre progressivement en place des solutions manuelles puisque ni les fonctionnaires ni les administrés ne pouvaient accéder à des services essentiels comme les sites Web permettant de régler les factures d'eau, les taxes foncières et les contraventions de stationnement. Le maire et son cabinet estiment que le retour à la normale aura coûté 10 millions de dollars US, sans compter les 8 millions perdus en raison de revenus différés ou de l'incapacité de la ville à traiter les paiements.**

- **Norsk Hydro, l'un des plus grands producteurs mondiaux d'aluminium, a été victime d'une cyberattaque massive qui a paralysé une partie de son infrastructure et l'a contraint à mettre en place des opérations manuelles sur certains sites de production. Une semaine après l'infection par ransomware, Norsk Hydro évaluait ses pertes totales à 40 millions de dollars US, somme qui peut paraître modérée par comparaison avec les attaques dirigées contre Mondelez (100 millions) et Maersk (300 millions).**

- **Attaqué en juin 2019, le groupe de laboratoires Eurofins estime ses pertes à près de 62 millions d'euros, soit plus de 35 % de son bénéfice net. la police britannique a suspendu ses relations avec la société peu après que celle-ci a révélé l'incident. la National Crime Agency du Royaume-Uni a déclaré qu'elle participait à l'enquête pour retrouver la trace des attaquants. L'attaque pourrait remettre en question la validité auprès des tribunaux britanniques des analyses et tests sanguins et d'ADN réalisés par le laboratoire à la suite de l'incident.**

Quelques chiffres :

- Une attaque de ransomware se produit toutes les 14 secondes
- 700 % de croissance depuis 2016
- 35 % des cybercriminels ont obtenu une rançon
- 2 milliards de dollars de pertes financières
- 11 milliards de dollars de pertes financières, de productivité et de temps d'arrêt

Kurt Baumgartner juge que payer autant est une erreur. « Ça rend le crime attractif et ça crée un effet boule de neige », estime-t-il.

Aujourd'hui, les analystes estiment qu'une attaque de ransomware **visant des entreprises** se produit toutes les 14 secondes**, ce qui représente un coût global de plusieurs milliards de dollars pour les organisations.**

C'est la raison pour laquelle il est important de garder à l'esprit les cinq points suivants :

1. **Face aux attaques de ransomware, les sauvegardes relèvent de la responsabilité des entreprises.**
2. **L'extension de la surface d'attaque expose les sauvegardes aux ransomware.**
3. **Une surveillance intermittente facilite les attaques ciblant les sauvegardes.**
4. **Il existe des points d'entrée dans les clouds publics pour les cybercriminels.**
5. **Des temps de sauvegarde et de restauration trop longs ajoutent de la pénibilité à la demande de rançon.**

« Ce n'est pas qu'il y aura plus de ransomware en 2020, mais les attaques seront de plus grande envergure », affirme en outre David Masson, directeur national de l'entreprise de cyberdéfense Darktrace au Canada.

Le chercheur de Kaspersky souligne le fort potentiel de l'apprentissage automatique pour certaines tâches telles que l'identification des cibles à attaquer. L'année 2020 sera donc très propice à la cybercriminalité.

Entre les évènements sportifs (J.O. de Tokyo en 2021, championnats européens de football, d'athlétisme et de handball, Champions League, Vendée Globe, Championnats du monde de biathlon, Tournoi des Six Nations) et les élections locales et nationales (élections américaines de 2020), les hacktivistes auront l'embarras du choix pour cibler des évènements dont les organisateurs, insuffisamment préparés et armés, n'auront pas d'autre choix que de payer rapidement une rançon pour sauver leur image de marque.

Cinq catégories d'attaque malveillante (ou de virus informatique) nécessitent une attention particulière :

- **ransomware ou virus bloquant l'accès au système ou aux données et réclamant le paiement d'une rançon ;**
- **attaque interne provenant de collaborateurs malintentionnés ;**
- **logiciel malveillant de type RAT (Remote Administration Trojan) permettant un contrôle complet de la machine infectée (ou Remote Administration Tool lorsqu'il s'agit uniquement d'un outil d'administration) ;**
- **logiciel malveillant de minage de cryptomonnaie (cryptojacking) ;**
- **botnets de distribution de menaces (diffusion ou installation d'autres virus) ou ciblant les systèmes bancaires et de paiement (ils visent l'utilisation de la banque en ligne, mais aussi les terminaux de points de vente ou encore les distributeurs de billets de banque).**

Nous nous intéressons ici aux trois premières catégories. Chez Veeam, nous nous efforçons de proposer des infrastructures permettant de protéger ce qui est souvent considéré comme le dernier rempart avant le paiement d'une rançon ou la perte irrémédiable des données : la SAUVEGARDE**.**

Protéger votre infrastructure Veeam consiste à comprendre les vecteurs d'attaque actuels. En effet, savoir contre quoi et contre qui vous vous protégez facilite la prise de contre-mesures efficaces, l'une de celles-ci consistant en un durcissement réduisant fortement votre surface d'attaque.

L'observation de l'architecture Veeam Backup & Replication conduit à assurer la protection des composants suivants :
- serveur de sauvegarde Veeam,
- cible de sauvegarde.

Le serveur Veeam Backup & Replication doit être considéré comme la cible numéro un dans votre infrastructure et son accès doit être très restreint. En général, il est l'objectif principal qu'un pirate va cibler sur votre réseau. Les cibles de sauvegarde qui contiennent les fichiers de sauvegarde constituent également un objectif privilégié.

Pour plus d'informations sur la protection du serveur de sauvegarde Veeam, consultez notre guide des meilleures pratiques (en anglais) : https://www.veeambp.com/infrastructure_hardening

La suite de ce document est consacrée au stockage de vos sauvegardes, donc aux différents types de cible disponibles avec Veeam Backup & Replication v10. Pour chacune d'elles, nous étudierons le ou les types d'attaque contre lesquels prévoir une protection.

Serveur Microsoft Windows

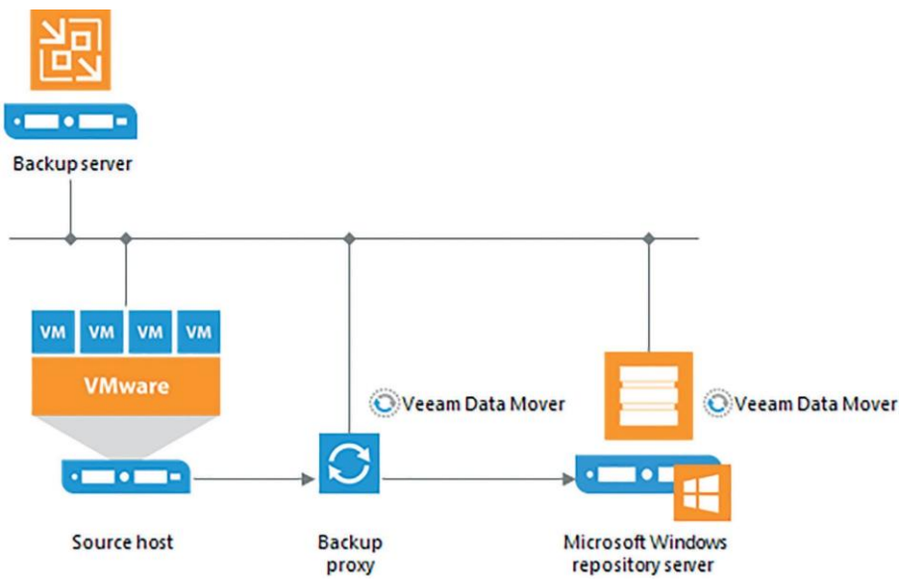
Le premier type de cible disponible dans Veeam Backup &Replication est le serveur Windows disposant localement d'un espace de stockage suffisant pour héberger les sauvegardes.

La première précaution à prendre consiste à dissocier les rôles de serveur et de cible de sauvegarde Veeam.

En effet, si une attaque survient par le biais du serveur de sauvegarde Veeam, il est impératif de la stopper avant qu'elle atteigne les archives de sauvegarde.

Seconde précaution à prendre avec une cible de type Windows : ne pas utiliser un compte de domaine pour la joindre au serveur de sauvegarde Veeam.

En mettant en œuvre ces deux premiers conseils, la communication entre le proxy et la cible se fait par l'intermédiaire des Veeam Data Mover Services (VDMS). Les données étant invisibles sur le réseau, il est donc plus difficile pour un CryptoLocker de se propager.



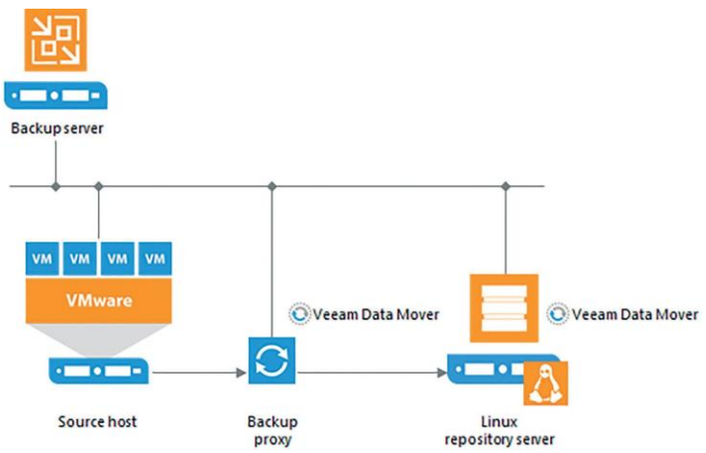
Il est également possible, afin de limiter la surface d'attaque, de déployer le rôle cible sur un Windows Server Core.

Serveur Linux

Utiliser une cible de type Linux est un avantage, car la plupart des CryptoLockers sont développés pour un système d'exploitation bien précis.

Recourir à un système d'exploitation différent de celui du serveur de sauvegarde Veeam protège donc contre la propagation d'une attaque via CryptoLocker.

De plus, comme pour le serveur Windows, la communication entre le proxy et la cible se fait par l'intermédiaire des Veeam Data Mover Services (VDMS).

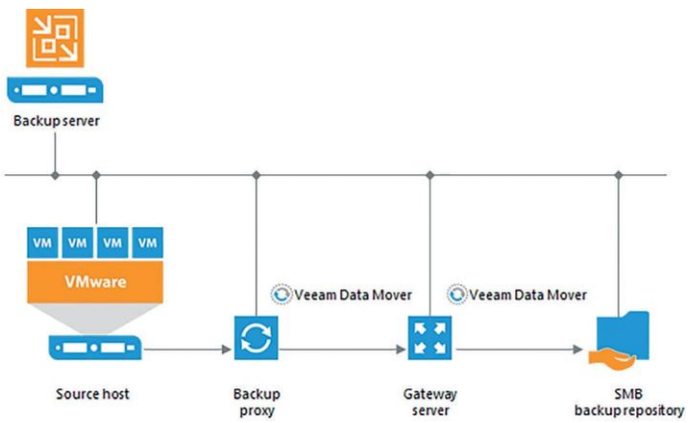


Enfin, il est également plus difficile, mais pas impossible, pour un cyberattaquant utilisant un RAT de s'y connecter depuis un autre serveur pour en supprimer toutes les archives de sauvegarde.

Partage CIFS

La cible de type CIFS est certainement la moins robuste face aux différentes cybermenaces extérieures.

En effet, le protocole CIFS expose les données directement sur le LAN. Il peut certes être protégé par mot de passe, mais cela s'avère largement insuffisant face à la technicité croissante des cyberattaques.



La meilleure manière de protéger ce type de cible consiste à mettre en place des snapshots sur la baie où réside le partage CIFS. Cela permet de revenir en arrière en cas d'altération, avec néanmoins un risque face aux CryptoLockers récents qui permettent la suppression des snapshots.

Partage NFS

Outre ses meilleures performances (notamment sur les NAS d'entrée de gamme), un partage NFS présente par défaut l'avantage d'être moins visible qu'un partage CIFS qui apparaît directement dans le voisinage réseau.

Le partage NFS rend plus difficiles, mais pas impossibles, les cyberattaques de type CryptoLocker ou la prise en main à distance via un RAT.

Appliance de déduplication intégrée

Les intégrations spécifiques des appliances de déduplication dans Veeam Backup & Replication sont disponible sur :

- **HPE StoreOnce (protocole StoreOnce Catalyst)**
- **Exagrid (VDMS embarqué)**
- **Quantum DXi (VDMS embarqué)**
- **Dell EMC DataDomain (DDBoost)**

Ces intégrations permettent la mise en place de sauvegardes dites « air gap » (isolation physique), non visibles sur le LAN, protégeant ainsi contre la propagation des CryptoLockers et autres virus informatiques.

Ces sauvegardes étant invisibles sur le réseau, la suppression des données sauvegardées n'est possible que depuis la console de Veeam Backup & Replication.

Stockage objet

Les cibles de type stockage objet font partie du tier de capacité qui vise à étendre la capacité d'une cible de sauvegarde évolutive (ou SOBR, Scale-Out Backup Repository) et à simplifier l'archivage ou la réplication des données de sauvegarde existantes, directement vers un stockage objet dans le cloud (comme Amazon S3, Microsoft Azure Blob Storage et IBM Cloud Object Storage), ou en utilisant toutes les solutions locales compatibles S3 prises en charge.

Comme ce type de stockage utilise un connecteur spécifique, un CryptoLocker ne peut pas s'y propager depuis l'infrastructure de sauvegarde.

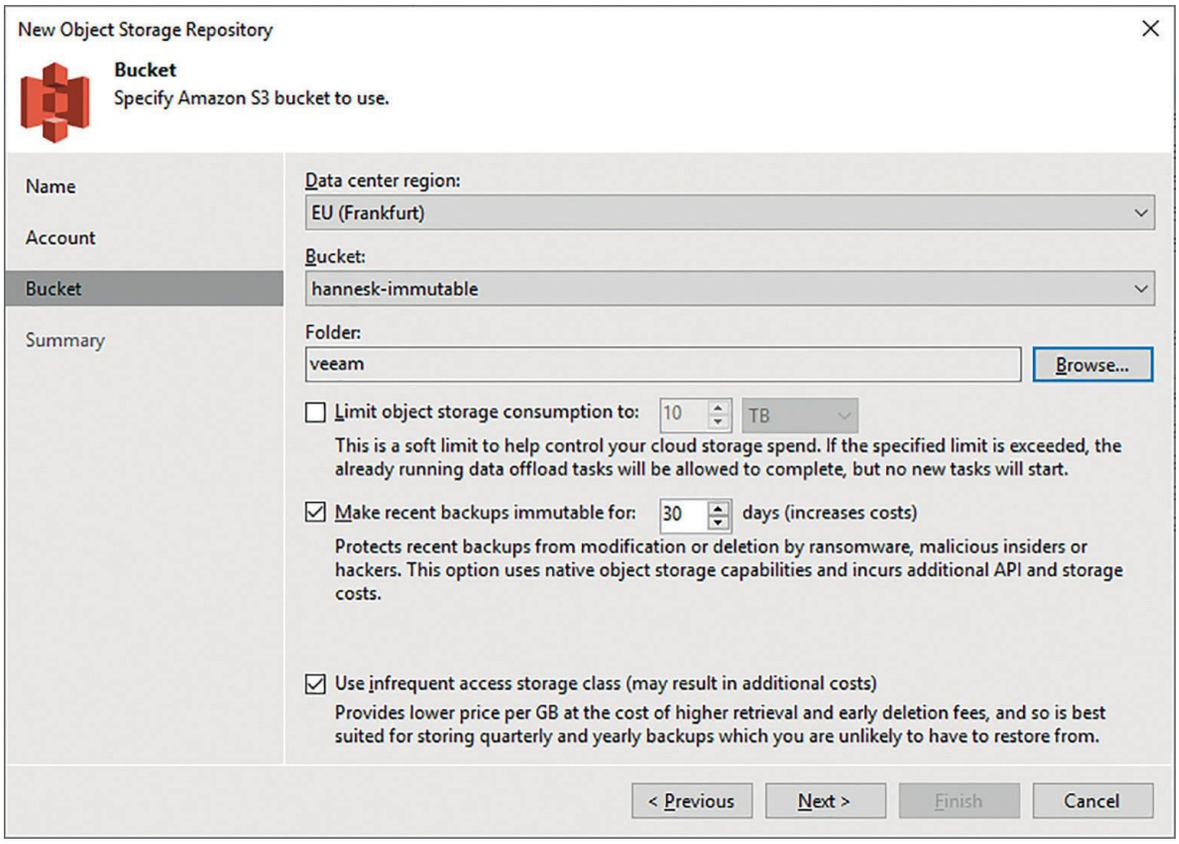
Cependant, l'utilisation d'un RAT donne la possibilité au cyberattaquant de supprimer manuellement les archives de sauvegarde. Cette dernière attaque potentielle peut être contrée grâce aux trois approches suivantes.

Stockage objet S3 immuable

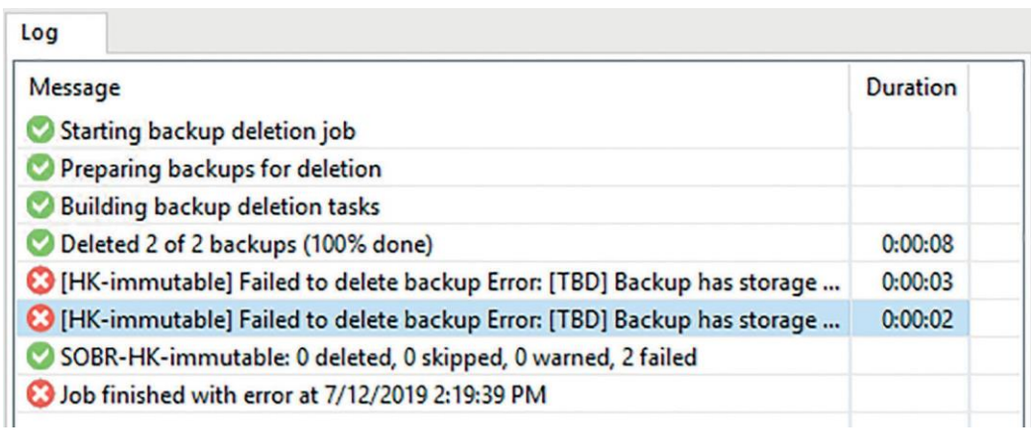
Afin de remédier aux problèmes de suppression manuelle d'une archive hébergée sur un stockage objet, Veeam Backup & Replication permet d'utiliser un stockage Amazon S3 ou compatible S3 disposant de l'API de verrouillage des objets.

Cette API permet de protéger contre la modification et la suppression tout objet stocké pendant une période prédéfinie par l'administrateur.

D'un simple clic dans Veeam Backup & Replication, cette API est utilisée lors de l'enregistrement d'une nouvelle cible de type stockage objet.

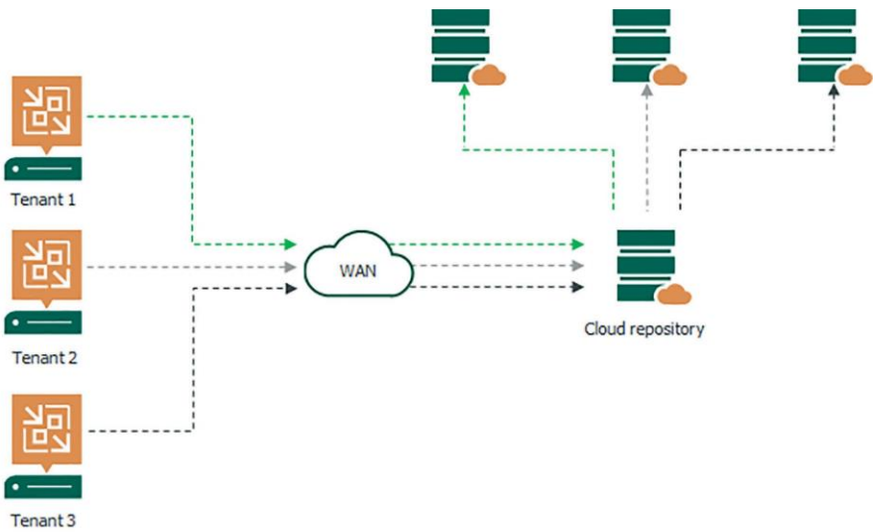


Lorsque l'option « *Make recent backups immutable for XX days* **» (Rendre les sauvegardes récentes inaltérables pendant XX jours) est activée, il est impossible de procéder à une attaque malveillante, et donc d'altérer ou de supprimer les archives de sauvegarde.**



Cible Veeam Cloud Connect

Veeam Cloud Connect est une solution basée sur Veeam Backup & Replication, permettant aux partenaires Veeam Cloud & Service Provider (VCSP) de proposer une solution mutualisée d'externalisation de la sauvegarde.



Les clients utilisant Veeam Backup & Replication peuvent s'appuyer sur Veeam Cloud Connect pour externaliser leurs sauvegardes dans un datacenter avec Veeam Cloud Connect for the Enterprise ou chez un hébergeur VCSP.

Dans certaines situations, le fait de conserver des sauvegardes principales ou supplémentaires dans une cible cloud ne suffit pas toujours à garantir la sécurité des données. En effet, les données sauvegardées peuvent devenir indisponibles en raison d'une attaque interne. Par exemple, un pirate informatique peut accéder à la console de Veeam Backup & Replication du client et supprimer toutes les sauvegardes, y compris celles hors site stockées dans la cible cloud.

Veeam Backup & Replication offre la fonctionnalité « Insider Protection **» (protection contre les menaces internes) pour les types de sauvegarde suivants :**

- **sauvegardes de VM et de Veeam Agents créées par les tâches de sauvegarde configurées dans Veeam Backup & Replication ;**
- **sauvegardes de machines physiques ou virtuelles créées directement par Veeam Agent for Microsoft Windows ou for Linux ;**
- **copies des sauvegardes de VM ou des sauvegardes de Veeam Agents créées par les tâches de copie de sauvegarde configurées dans Veeam Backup & Replication.**

Le fournisseur de services peut activer l'option « Insider Protection **» individuellement pour un client spécifique. Pour ce faire, il doit cocher la case «** *Keep deleted backup files for <N> days* **» (Conserver les fichiers de sauvegarde supprimés pendant <N> jours) dans les propriétés du compte du client. Ainsi, lorsqu'une sauvegarde ou un point de restauration spécifique dans la chaîne de sauvegarde est supprimé sur la cible**

dans le cloud, Veeam Backup & Replication ne supprime pas immédiatement les fichiers de sauvegarde réels. Au lieu de cela, il les place dans la « corbeille ».

Techniquement, une corbeille est un dossier sur la cible de sauvegarde, dans l'infrastructure de sauvegarde du fournisseur de services, dont les ressources de stockage sont exposées aux clients en tant que cible cloud. Veeam Backup & Replication crée automatiquement ce dossier au moment où un fichier de sauvegarde du client est placé dans la corbeille pour la première fois.

Les fichiers de sauvegarde placés dans la corbeille ne consomment pas le quota des clients. Cependant, ils consomment de l'espace disque sur le stockage du fournisseur de services où la cible est configurée.

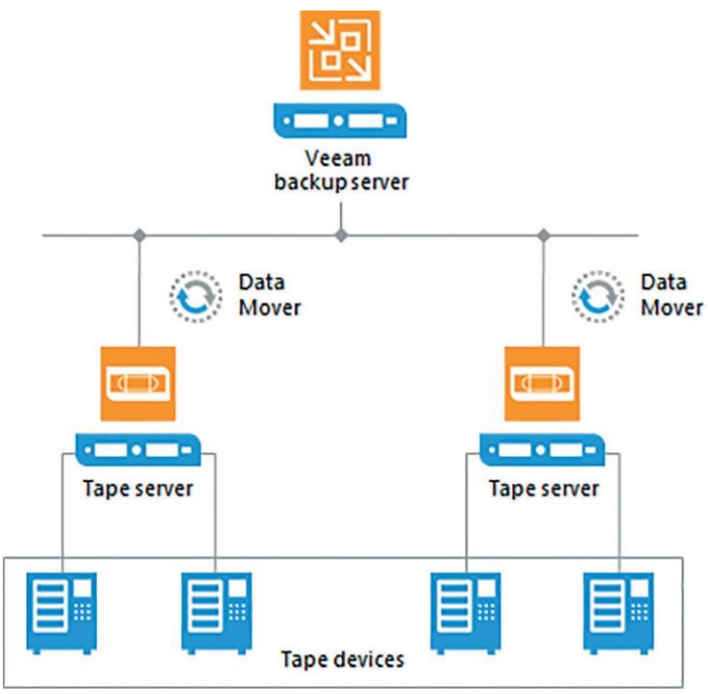
Bande magnétique

Longtemps considérée comme un support arrivé à bout de soufte, la bande magnétique revient sur les devants de la scène de la sauvegarde.

La plupart des clients qui utilisaient historiquement ce support le faisaient pour archiver les données à long terme.

Or, avec la montée en puissance des actes malveillants, la bande est de plus en plus réutilisée non plus pour l'archivage des sauvegardes, mais pour protéger les données les plus récentes (les deux ou trois dernières sauvegardes, par exemple).

Cette utilisation de la bande permet de créer une sauvegarde externalisée hors ligne**, très facilement et à moindre coût.**

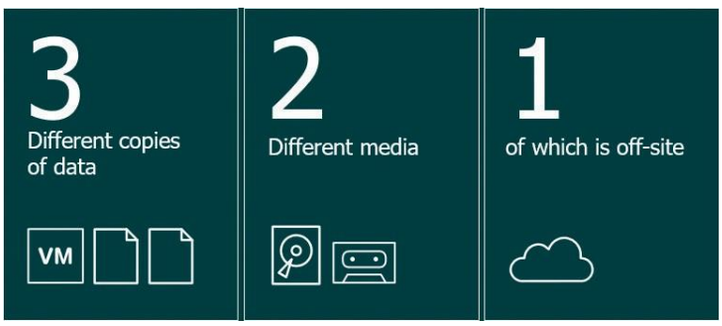


Couplée à des bandes de type WORM (Write Once Read Many), l'externalisation sur bande procure une protection native contre le chiffrement malveillant et la suppression des données.

Règle du 3-2-1-1-0

Les experts de la sauvegarde préconisent la mise en place de la règle du 3-2-1 afin d'assurer la disponibilité des données en cas de sinistre.

Cette règle préconise les précautions suivantes :



- **3 copies des données doivent être conservées (une pour les données de production et deux copies supplémentaires) ;**
- **2 supports différents doivent être utilisés (les snapshots ne sont pas des sauvegardes, ni les réplications de baie à baie) ;**
- **1 copie des données doit résider hors site.**

Avec ces différentes architectures possibles, le support de technologies de stockage des données variées et ses fonctionnalités avancées de gestion des données (Data Management), Veeam va encore plus loin en proposant de suivre la règle du 3-2-1-1-0.

Qu'apporte de plus cette nouvelle version de la règle ?

- **1 copie des données doit se trouver hors ligne ;**
- **des tests de restauration automatisés (SureBackup) permettent de s'assurer de la capacité de restauration des données pour éviter les mauvaises surprises en cas de besoin de restauration urgent.**

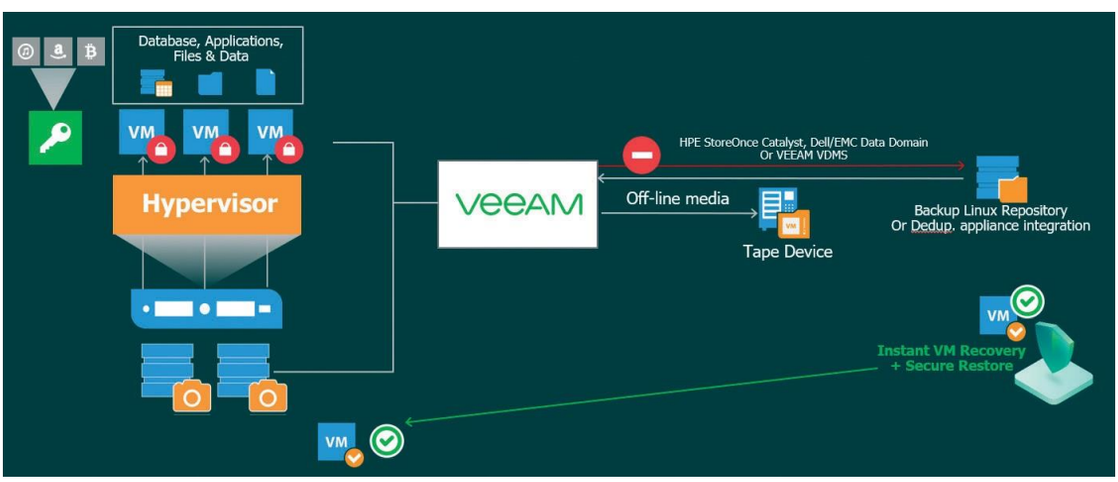
Si cette règle est appliquée, il est impossible à une attaque extérieure d'altérer les archives de sauvegarde Veeam Backup & Replication.

Protection contre les ransomware

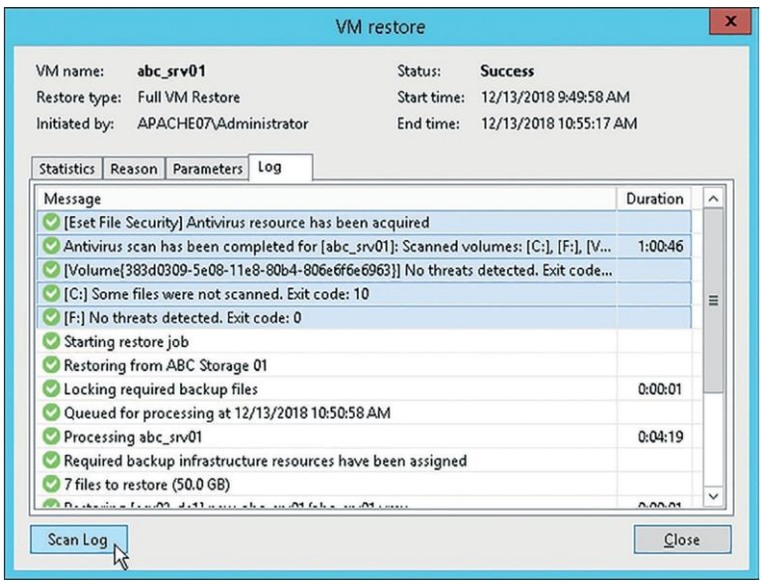
Suite à l'analyse des différentes cibles disponibles avec Veeam version 10, il existe plusieurs types de cible de sauvegarde pour protéger vos sauvegardes des attaques de ransomware.

Toute sauvegarde portant sur l'utilisation d'une des cibles suivantes offre cette protection :

- **serveur Windows dissocié du rôle de serveur de sauvegarde Veeam,**
- **serveur Linux,**
- **baie de déduplication (HPE StoreOnce, Quantum DXi, Exagrid, Dell EMC DataDomain),**
- **cible Veeam Cloud Connect,**
- **bande magnétique.**



Couplé à la fonctionnalité Secure Restore **de Veeam, qui permet une analyse antivirale et antimalware des données sur la machine à restaurer, un logiciel antivirus assure la restauration d'une machine « saine », sans faille et de type jour zéro, dans l'environnement de production.**



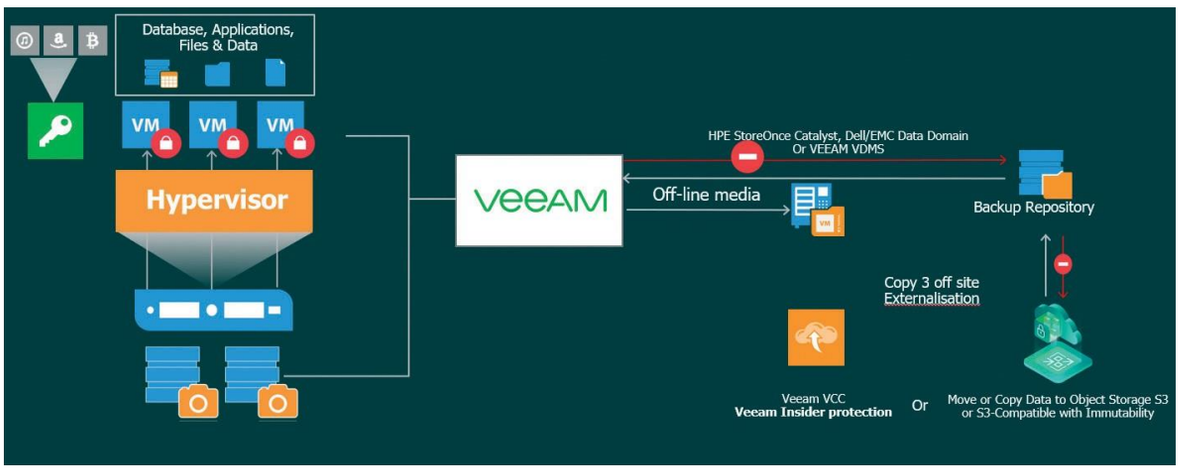
Cette analyse antivirus peut être utilisée dans les opérations suivantes :

- **Instant VM Recovery**
- **Entire VM Restore**
- **Virtual Disks Restore**
- **Restore to Microsoft Azure**
- **Restore to Amazon EC2**
- **EC2 Instance Disks Export**

Protection anti-ransomware et effacement

Si, en plus d'une protection contre les attaques de type ransomware, une protection contre l'effacement des données (accidentel ou non) est nécessaire, il faut opter plutôt pour un support de stockage de type :

- **stockage S3 immuable,**
- **cible Veeam Cloud Connect avec « Insider Protection ».**



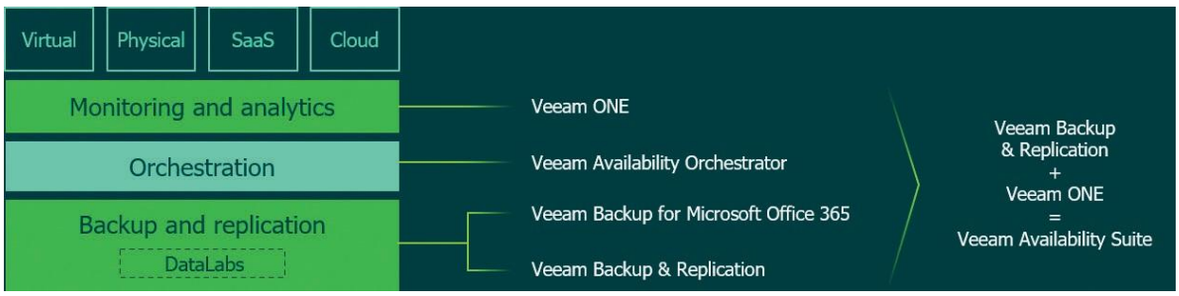
À noter : une bande magnétique de type WORM ou tout simplement exportée de la robotique constitue également un excellent moyen de protection.

Conclusion

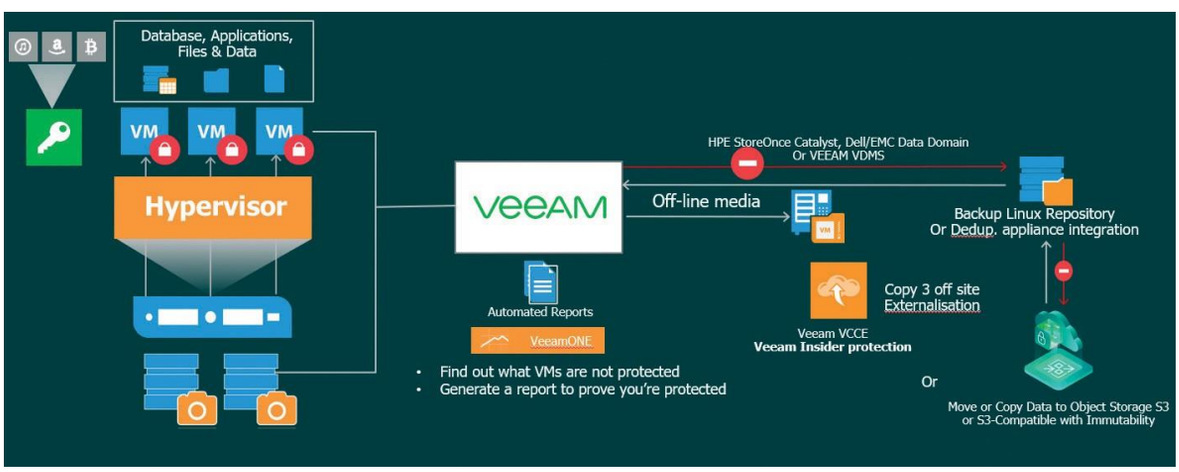
L'importance de la protection des données est encore trop souvent sous-estimée **dans les entreprises. Pourtant, elle constitue généralement le dernier rempart face à une cyberattaque.**

Il est donc très important pour leur survie qu'une politique de cyber-résilience des données soit mise en place dans toutes les entreprises, quels que soient leur secteur d'activité et leur taille.

Depuis des années, Veeam développe des outils qui vont dans ce sens. C'est pourquoi Veeam Availability Suite intègre Veeam ONE, qui fournit des outils de supervision et d'analyse.



Dans sa partie supervision, Veeam ONE intègre des alertes permettant la détection de comportements suspects sur les infrastructures qu'il gère.



Ces alertes portent sur :

- **une activité de ransomware possible (Possible ransomware activity),**
- **une taille de sauvegarde incrémentielle suspecte (Suspicious increment backup size).**

La première se déclenche lorsque :

• la consommation de CPU des serveurs dépasse 70 %

et que

• les I/O d'écriture atteignent 40 Mo/s

ou que

- **les I/O réseau atteignent 40 Mo/s.**

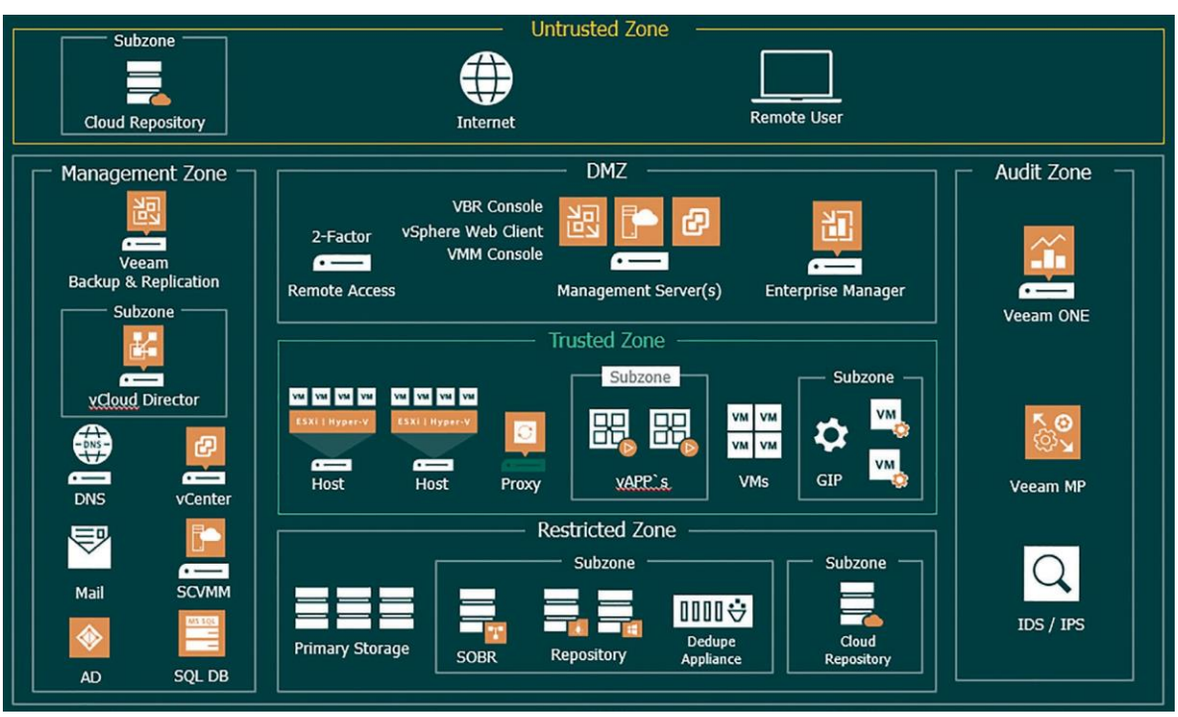
La seconde se déclenche lorsque la taille de l'une des trois dernières sauvegardes incrémentielles est supérieure de 150 %.

Lors du déclenchement d'une de ces alertes, il est possible d'exécuter automatiquement un script pour créer, par exemple, un snapshot au niveau du stockage hébergeant les VM.

Pour conclure, nous avons traité dans ce document la protection de vos archives de sauvegarde contre les attaques extérieures.

Cependant, cela ne suffit pas toujours et à mesure que les virus et autres ransomware se perfectionnent techniquement, il est important, outre la cyber-résilience des données, de mettre en place un durcissement global de l'infrastructure (ou « hardening »), afin de satisfaire les règles de base de la cybersécurité.

Voici un exemple de ce qu'il est possible de mettre en place avec Veeam Backup & Replication.



À propos de l'auteur

Franck GUÉNÉ est ingénieur avant-vente senior depuis plus 10 ans chez Veeam.

Auparavant, il a occupé différents postes dans l'IT : formateur VMware, responsable d'offres de virtualisation chez différents intégrateurs, administrateur de solutions Microsoft.

À propos de Veeam Software

Veeam® est le leader des solutions de sauvegarde pour la gestion des données dans le cloud (Cloud Data Management™). Veeam offre une plateforme unique afin de moderniser la sauvegarde, d'accélérer le cloud hybride et de sécuriser les données. Avec plus de 375 000 clients dans le monde entier, dont 82% des entreprises du Fortune 500 et 67% des Forbes Global 2 000, les scores de satisfaction client de Veeam sont 3,5 fois supérieures à la moyenne de l'industrie —les plus élevés de l'industrie. Son écosystème de distribution 100% indirect compte des partenaires internationaux, ainsi que HPE, NetApp, Cisco et Lenovo comme revendeurs exclusifs. Avec son siège social à Baar, en Suisse, Veeam a des bureaux dans plus de 30 pays. Pour en savoir plus, visitez le site www.veeam.com ou suivez Veeam sur Twitter @veeam.

À propos d'IPgarde

IPgarde est expert Hébergement, Cloud et Virtualisation du Système d'Information de l'entreprise depuis plus de 15 ans. Chez IPgarde, nous pensons que les produits Veeam® offrent une qualité de sauvegarde et une restauration sans égales.

Notre mission est de vous accompagner vers les meilleurs outils disponibles, de vous donner accès à une plateforme moderne capable de répondre aux impératifs de sauvegarde d'aujourd'hui, mais aussi de s'élargir et s'adapter à tout ce dont vous pourriez avoir besoin à l'avenir.

IPgarde est certifié partenaire Veeam® de Niveau GOLD.

Vous souhaitez en savoir plus? Vous avez besoin de conseils ? Vous souhaitez bénéficier d'une version d'évaluation GRATUITE limitée à 30 jours ?
Nos experts IPgarde sont à votre disposition.
Contactez-les : 01 77 49 24 50 / contact@ipgarde.com

VEEAM

Cloud Data

Backup for what's next

5 Stages of Cloud Data Management — start your journey today!

Learn more: veeam.com

ipgarde